2016

Kronecker's Theory of Binary Bilinear Forms with Applications to Representations of Integers as Sums of Three Squares

Jonathan A. Constable
University of Kentucky, jonathan.constable@uky.edu
Digital Object Identifier: http://dx.doi.org/10.13023/ETD.2016.168

STUDENT AGREEMENT:

I represent that my thesis or dissertation and abstract are my original work. Proper attribution has been given to all outside sources. I understand that I am solely responsible for obtaining any needed copyright permissions. I have obtained needed written permission statement(s) from the owner(s) of each third-party copyrighted matter to be included in my work, allowing electronic distribution (if such use is not permitted by the fair use doctrine) which will be submitted to UKnowledge as Additional File.

I hereby grant to The University of Kentucky and its agents the irrevocable, non-exclusive, and royalty-free license to archive and make accessible my work in whole or in part in all forms of media, now or hereafter known. I agree that the document mentioned above may be made available immediately for worldwide access unless an embargo applies.

I retain all other ownership rights to the copyright of my work. I also retain the right to use in future works (such as articles or books) all or part of my work. I understand that I am free to register the copyright to my work.

REVIEW, APPROVAL AND ACCEPTANCE

The document mentioned above has been reviewed and accepted by the student's advisor, on behalf of the advisory committee, and by the Director of Graduate Studies (DGS), on behalf of the program; we verify that this is the final, approved version of the student's thesis including all changes required by the advisory committee. The undersigned agree to abide by the statements above.

Jonathan A. Constable, Student

Dr. David Leep, Major Professor

Dr. Peter Perry, Director of Graduate Studies

Kronecker's Theory of Binary Bilinear Forms with Applications to Representations of Integers as Sums of Three Squares

DISSERTATION

A dissertation submitted in partial
fulfillment of the requirements for
the degree of Doctor of Philosophy
in the College of Arts and Sciences
at the University of Kentucky

By
Jonathan A. Constable
Lexington, Kentucky

Director: Dr. David Leep, Professor of Mathematics
Lexington, Kentucky 2016

ABSTRACT OF DISSERTATION

Kronecker's Theory of Binary Bilinear Forms with Applications to Representations of Integers as Sums of Three Squares

In 1883 Leopold Kronecker published a paper containing a few explanatory remarks to an earlier paper of his from 1866. His work loosely connected the theory of integral binary bilinear forms to the theory of integral binary quadratic forms. In this dissertation we discover the statements within Kronecker's paper and offer detailed arithmetic proofs. We begin by developing the theory of binary bilinear forms and their automorphs, providing a classification of integral binary bilinear forms up to equivalence, proper equivalence and complete equivalence.

In the second chapter we introduce the class number, proper class number and complete class number as well as two refinements, which facilitate the development of a connection with binary quadratic forms.

Our third chapter is devoted to deriving several class number formulas in terms of divisors of the determinant. This chapter also contains lower bounds on the class number for bilinear forms and classifies when these bounds are attained.

Lastly, we use the class number formulas to rigorously develop Kronecker's connection between binary bilinear forms and binary quadratic forms. We supply purely arithmetic proofs of five results stated but not proven in the original paper. We conclude by giving an application of this material to the number of representations of an integer as a sum of three squares and show the resulting formula is equivalent to the well-known result due to Gauss.

KEYWORDS: complete equivalence, binary bilinear forms, binary quadratic forms, class number relations, L. Kronecker, Gauss

Author's signature: Jonathan A. Constable

Date: May 5, 2016

Kronecker's Theory of Binary Bilinear Forms with Applications to Representations of Integers as Sums of Three Squares

By
Jonathan A. Constable

Director of Dissertation: Dr. David Leep

Director of Graduate Studies: Dr. Peter Perry

Date: May 5, 2016

Dedicated to my wife, Tatiana, and our families on both sides of the Atlantic.

ACKNOWLEDGMENTS

This dissertation has benefitted from the insight and encouragement of many people. In particular I wish to thank my advisor Dr. David Leep for his continual optimism and deep mathematical insight which he kindly shared with me. I also wish to thank the members of my committee, Dr. Uwe Nagel, Dr. Avinash Sathaye, Dr. Cidambi Srinivasan, and Dr. Alfred Shapere for their help throughout my time at the University of Kentucky.

In addition I would like to thank my wife, Tatiana McArthur-Constable, and both of our families for their understanding, patience and untiring support that made this work possible.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

Chapter 1 Introduction

> "A pessimist sees the difficulty in every opportunity; an optimist sees the opportunity in every difficulty."
> - Sir Winston Churchill

The theory of binary quadratic forms is a source of classical problems in number theory and has been studied extensively. A lesser known paper by Leopold Kronecker in 1883 [Kr1897] contains a novel manner for connecting the classical class number theory of binary quadratic forms to the class number for binary bilinear forms. Although correct, Kronecker's paper requires prior knowledge of several key results in order to construct his ultimate result; a purely arithmetic proof of the number of representations of a positive integer as a sum of three squares. This weakness was pointed out in a much later paper by André Weil in 1974 [We1974, 3., p. 219].

Kronecker's formula for the number of representations of a positive integer as a sum of three integer squares differs materially from the traditional formulation due to Carl FriedrichGauss, see Theorem 5.4.1 or Grosswald, [Gr1985, p. 51]. The main aim of this dissertation is to provide a detailed arithmetic proof of Kronecker's paper [Kr1897], that does not require any prior analytic results, and to demonstrate that Kronecker's formulation is indeed equivalent to the traditional Gauss formula.

Chapter2 is devoted to providing the reader with the necessary technical background that is required to understand bilinear form theory in the current sense. The culmination of this chapter is Section 2.5, where we develop the theory of automorphs for binary bilinear forms. Our treatment follows in the manner of the classical treatment for automorphs of binary quadratic forms as given by Flath in [Fl1989, p. 125].

Next, Chapter 3 commences our journey towards understanding Kronecker's paper [Kr1897]. We begin with Kronecker's definition of a reduced bilinear form and develop materials to aid our understanding of Kronecker reduced bilinear forms. Notable results include showing there are finitely many Kronecker reduced forms for a given determinant (Theorem 3.1.15), and proving a fundamental claim of Kronecker's - that we may use Kronecker reduced forms to count the complete class number for bilinear forms, $\mathrm{Cl}_c(D)$ (Theorem 3.1.29). We also introduce in Section 3.3 the refinement $\overline{\mathrm{Cl}}_c(D)$ of the class number. The remainder of this chapter begins the exploration of how we count $\mathrm{Cl}_c(D)$ and $\overline{\mathrm{Cl}}_c(D)$ via Kronecker reduced bilinear forms.

In Chapter 4 we derive expressions for the complete class number, $\mathrm{Cl}_c(D)$ (see Theorem 4.4.3), and its refinement $\overline{\mathrm{Cl}}_c(D)$ in terms of sums of divisors of the determinant D. The latter result may be found in Section 4.7. Also of interest in this chapter is Section 4.5. Here we take a break from examining Kronecker's paper in order to derive some lower bounds for the proper bilinear class number, $\mathrm{Cl}_+(D)$. Corollary

4.5.5 shows $2D \leqslant \mathrm{Cl}_+(D)$, and Theorem 4.5.6 shows equality is obtained if and only if D is a prime congruent to 11 mod 12. We go on to obtain various improvements to our lower bound and provide an interesting observation which links the proper bilinear class number to the problem of factoring a product of two distinct primes. Observation 4.5.29 shows if one knows a positive integer D is a product of two distinct primes p and q, then calculating $\mathrm{Cl}_+(D)$ allows for the recovery of the integers p and q.

Our final chapter, Chapter 5, is where we rigorously prove Kronecker's connection between binary quadratic forms and binary bilinear forms. We supply proofs of key results stated by Kronecker but not proven. These are found in Lemma 5.1.7, Lemma 5.1.8, Theorem 5.2.2 and Theorem 5.2.21. Section 5.3 is then where we utilize all of our previous work to derive Kronecker's formula for the number of representations of a positive integer as a sum of three integer squares. Lastly, in Section 5.4 we give a detailed proof of Gauss' Theorem 5.4.1 by using Kronecker's relationships. Thus we show when primitivity is taken into account, Kronecker's formulation concurs with the traditional statement due to Gauss.

We also include several appendices. These initially consist of complementing the reader's knowledge of representations of sums of squares, before providing a detailed walk-through of Weil's 1974 paper, [We1974]. Weil's paper is of particular interest because it offers an elegant way to calculate the number of representations of a positive integer m as a sum of three squares when $m \equiv 3 \bmod 8$. The proof is much shorter than that of Kronecker and it avoids the use of infinite sets. Weil claims to have read Kronecker's paper for inspiration before deriving his method. Weil also states the other cases can be done similarly but with additional complications. It is my hope to continue studying the connections between the papers of Weil and Kronecker in order to understand what Weil had in mind to complete the other cases.

Chapter 2 Preliminaries

"Success is not final, failure is not fatal: it is the courage to continue that counts."
- Sir Winston Churchill

We begin by developing some preliminary ideas and examples for the theory of bilinear forms.

2.1 Introduction to Bilinear Forms

Definition 2.1.1.
Let R be a commutative ring and V be an R-module of rank n. Then $\mathcal{B} : V \times V \to R$ is a **bilinear form** if the following conditions hold:

- $\mathcal{B}(\mathbf{u} + \mathbf{v}, \mathbf{w}) = \mathcal{B}(\mathbf{u}, \mathbf{w}) + \mathcal{B}(\mathbf{v}, \mathbf{w})$
- $\mathcal{B}(\mathbf{u}, \mathbf{v} + \mathbf{w}) = \mathcal{B}(\mathbf{u}, \mathbf{v}) + \mathcal{B}(\mathbf{u}, \mathbf{w})$
- $\mathcal{B}(\lambda\mathbf{u}, \mathbf{v}) = \lambda\mathcal{B}(\mathbf{u}, \mathbf{v})$ and $\mathcal{B}(\mathbf{u}, \lambda\mathbf{v}) = \lambda\mathcal{B}(\mathbf{u}, \mathbf{v})$ for $\lambda \in R$.

We may use a matrix to represent $\mathcal{B}$ in the following manner. Assume V is a free R-module and let $\{\mathbf{e_1}, \cdots, \mathbf{e_n}\}$ be a basis for V. Define the $n \times n$ matrix $[\mathcal{B}]_{\mathbf{e}}$ by $a_{ij} = \mathcal{B}(\mathbf{e_i}, \mathbf{e_j})$. Then for any $\mathbf{v}, \mathbf{w} \in V$, let $\mathbf{x}, \mathbf{y}$ be the $n \times 1$ vectors that represent $\mathbf{v}$ and $\mathbf{w}$ respectively with respect to this basis.

$$\mathcal{B}(\mathbf{v}, \mathbf{w}) = x^t[\mathcal{B}]_{\mathbf{e}}y = \sum_{i,j=1}^{n} a_{ij}x_iy_j$$

Lemma 2.1.2.
Let $\mathbf{x} = x_1\mathbf{e_1} + \cdots + x_n\mathbf{e_n}$ *and* $\mathbf{y} = y_1\mathbf{e_1} + \cdots + y_n\mathbf{e_n}$ *with respect to some* R*-basis.*
Then $\mathcal{B}(\mathbf{x}, \mathbf{y}) = \begin{pmatrix} x_1 & \cdots & x_n \end{pmatrix} [\mathcal{B}]_{\mathbf{e}} \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$.

Proof.
By repeatedly applying the properties of a bilinear form (see Definition 2.1.1) we have:

$$\begin{aligned} \mathcal{B}(\mathbf{x}, \mathbf{y}) &= \mathcal{B}(x_1\mathbf{e_1} + \cdots + x_n\mathbf{e_n}, y_1\mathbf{e_1} + \cdots + y_n\mathbf{e_n}) \\ &= \sum_{i=1}^{n}\sum_{j=1}^{n} \mathcal{B}(\mathbf{e_i}, \mathbf{e_j})\, x_iy_j \\ &= \begin{pmatrix} x_1 & \cdots & x_n \end{pmatrix} [\mathcal{B}]_{\mathbf{e}} \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}. \end{aligned}$$

□

Definition 2.1.3.
Let $\{\mathbf{f_1}, \cdots, \mathbf{f_n}\}$ be another basis for V such that $\{\mathbf{f_1}, \cdots, \mathbf{f_n}\} = \{\mathbf{e_1}, \cdots, \mathbf{e_n}\}M$, where $M \in GL_n(\mathbb{F})$. Then M is called a change of basis matrix.

The new matrix representation for the bilinear form under this new basis is given by M^tAM, where $A = [a_{ij}]$ is the matrix representation for the bilinear form under the original basis.

Notation 2.1.4.

Let $\mathbf{u} = p_1\mathbf{e_1} + \cdots + p_n\mathbf{e_n} \in V$ then we write $[\mathbf{u}]_{\mathbf{e}} = \begin{pmatrix} p_1 \\ \vdots \\ p_n \end{pmatrix}$.

Suppose $\mathbf{f} = \{\mathbf{f_1}, \cdots, \mathbf{f_n}\}$ is another R-basis of V. Then $\mathbf{f_1} = q_{1,1}\mathbf{e_1} + \cdots + q_{n,1}\mathbf{e_n}$, ..., and $\mathbf{f_n} = q_{1,n}\mathbf{e_1} + \cdots + q_{n,n}\mathbf{e_n}$.

We denote the change of basis matrix by $M = \begin{pmatrix} q_{1,1} & \cdots & q_{1,n} \\ \vdots & \ddots & \vdots \\ q_{n,1} & \cdots & q_{n,n} \end{pmatrix} \in GL_n(V)$.

Lemma 2.1.5.
For $\mathbf{u} \in V$, we have $[\mathbf{u}]_{\mathbf{e}} = M[\mathbf{u}]_{\mathbf{f}}$.

Proof.

Let $[\mathbf{u}]_{\mathbf{f}} = \begin{pmatrix} p_1 \\ \vdots \\ p_n \end{pmatrix}$. Then

$$\begin{aligned} \mathbf{u} &= p_1\mathbf{f_1} + \cdots + p_n\mathbf{f_n} \\ &= p_1(q_{1,1}\mathbf{e_1} + \cdots + q_n\mathbf{e_n}) + \cdots + p_n(q_{1,n}\mathbf{e_1} + \cdots + q_{n,n}\mathbf{e_n}) \\ &= (p_1q_{1,1} + \cdots + p_nq_{1,n})\mathbf{e_1} + \cdots + (p_1q_{n,1} + \cdots + p_nq_{n,n})\mathbf{e_n}. \end{aligned}$$

Thus $[\mathbf{u}]_{\mathbf{e}} = \begin{pmatrix} p_1q_{1,1} + \cdots + p_nq_{1,n} \\ \vdots \\ p_1q_{n,1} + \cdots + p_nq_{n,n} \end{pmatrix} = M[\mathbf{u}]_{\mathbf{f}}$. □

Lemma 2.1.6.
Let $\mathcal{B}$ be a bilinear form, then $[\mathcal{B}]_{\mathbf{f}} = M^t[\mathcal{B}]_{\mathbf{e}}M$.

Proof.
By Lemmas 2.1.2 and 2.1.5 we have for each $\mathbf{u}, \mathbf{v} \in V$ that

$$\begin{aligned} [\mathbf{u}]_{\mathbf{f}}^t[\mathcal{B}]_{\mathbf{f}}[\mathbf{v}]_{\mathbf{f}} &= \mathcal{B}(\mathbf{u}, \mathbf{v}) \\ &= [\mathbf{u}]_{\mathbf{e}}^t[\mathcal{B}]_{\mathbf{e}}[\mathbf{v}]_{\mathbf{e}} \\ &= [\mathbf{u}]_{\mathbf{f}}^tM^t[\mathcal{B}]_{\mathbf{e}}M[\mathbf{v}]_{\mathbf{f}}. \end{aligned}$$

Hence $[\mathcal{B}]_{\mathbf{f}} = M^t[\mathcal{B}]_{\mathbf{e}}M$. □

Definition 2.1.7.
A bilinear form $\mathcal{B}$ is said to **represent** $r \in R\backslash\{0\}$ if there exists $\mathbf{v} \in V$, $\mathbf{v} \neq \mathbf{0}$ such that $\mathcal{B}(\mathbf{v}, \mathbf{v}) = r$.
If we let $R = \mathbb{Z}$ then the integer r is said to be **properly represented** by $\mathcal{B}$ if $\mathbf{v} = (v_1, \cdots, v_n)^t$ satisfies $\gcd(v_1, \cdots, v_n) = 1$.

We now define a subset of bilinear forms, the skew-symmetric bilinear forms, and demonstrate why it will be necessary to consider this subset separately.

Definition 2.1.8.
The bilinear form $\mathcal{B}$ is said to be

1. **symmetric** if $\mathcal{B}(\mathbf{v}, \mathbf{w}) = \mathcal{B}(\mathbf{w}, \mathbf{v})$ for all $\mathbf{v}, \mathbf{w} \in V$.
2. **skew-symmetric** if $\mathcal{B}(\mathbf{v}, \mathbf{w}) = -\mathcal{B}(\mathbf{w}, \mathbf{v})$ for all $\mathbf{v}, \mathbf{w} \in V$.
3. **alternating** if $\mathcal{B}(\mathbf{v}, \mathbf{v}) = 0$ for all $\mathbf{v} \in V$

Theorem 2.1.9.
Let $\mathcal{B}$ be a bilinear form. Then for $charR \neq 2$, $\mathcal{B}$ is alternating if and only if $\mathcal{B}$ is skew-symmetric.
When $charR = 2$ then $\mathcal{B}$ is skew-symmetric if and only if it is symmetric.

Proof.
We first prove that regardless of the characteristic of R, if $\mathcal{B}$ is alternating then $\mathcal{B}$ is skew-symmetric. Let $\mathbf{v}, \mathbf{w} \in V$ then

$$\begin{aligned} 0 &= \mathcal{B}(\mathbf{v} + \mathbf{w}, \mathbf{v} + \mathbf{w}) && (2.1)\\ &= \mathcal{B}(\mathbf{v}, \mathbf{v}) + \mathcal{B}(\mathbf{v}, \mathbf{w}) + \mathcal{B}(\mathbf{w}, \mathbf{v}) + \mathcal{B}(\mathbf{w}, \mathbf{w}) && (2.2)\\ &= \mathcal{B}(\mathbf{v}, \mathbf{w}) + \mathcal{B}(\mathbf{w}, \mathbf{v}). && (2.3) \end{aligned}$$

Therefore $\mathcal{B}(\mathbf{v}, \mathbf{w}) = -\mathcal{B}(\mathbf{w}, \mathbf{v})$ for all $\mathbf{v}, \mathbf{w} \in V$.
Now assume $charR \neq 2$ and $\mathcal{B}$ is skew-symmetric. This implies $2\mathcal{B}(\mathbf{v}, \mathbf{v}) = 0$ and hence $\mathcal{B}$ is alternating. Lastly assume $charR = 2$ and $\mathcal{B}$ is skew-symmetric, then $\mathcal{B}(\mathbf{v}, \mathbf{w}) = -\mathcal{B}(\mathbf{w}, \mathbf{v})$ and characteristic 2 implies $\mathcal{B}(\mathbf{v}, \mathbf{w}) = \mathcal{B}(\mathbf{w}, \mathbf{v})$ so $\mathcal{B}$ is symmetric. The converse follows immediately due to $1 = -1$ when $charR = 2$. □

Corollary 2.1.10.
Let $\mathcal{B}$ be a bilinear form. If $\mathcal{B}$ is skew-symmetric then its matrix representation, A, satisfies $A = -A^t$ irrespective of our choice of basis.

Proof.
By Theorem 2.1.9 if $charR \neq 2$ then $\mathcal{B}$ is alternating. From Definition 2.1.1 it is then clear that the matrix representation $[\mathcal{B}]_{\mathbf{e}}$ with respect to any basis $\mathbf{e}$ satisfies $a_{ii} = 0$ and $a_{ij} = -a_{ji}$ for all $i, j \in \{1, \cdots, n\}$. Therefore $A = -A^t$.
If $charR = 2$ then $\mathcal{B}$ is symmetric and thus $a_{ij} = a_{ji}$ in the matrix representation $[\mathcal{B}]_{\mathbf{e}}$ with respect to any basis $\mathbf{e}$. Since $1 = -1$ when the characteristic is two, $A = A^t = -A^t$ follows immediately. □

Lemma 2.1.11.
The subset of elements of R represented by a non-skew-symmetric bilinear form $\mathcal{A}$ is independent of our choice of basis. Further, the set of properly represented elements of R is also independent of our choice of basis.

Proof.
Let $\mathbf{e}$ and $\mathbf{f}$ be the bases defined at the beginning of this section. Let r be a non-zero ring element represented by $\mathcal{A}$. Then there exists $\mathbf{v} \neq \mathbf{0}$ with respect to the basis $\mathbf{e}$ so that $\mathcal{A}(\mathbf{v}, \mathbf{v}) = r$. Let M denote the change of basis matrix from $\mathbf{e}$ to $\mathbf{f}$. We see $M^{-1}\mathbf{v} \neq \mathbf{0}$ as M is invertible and $\mathbf{v} \neq \mathbf{0}$. Then

$$\mathcal{A}\left(M^{-1}\mathbf{v}, M^{-1}\mathbf{v}\right) = \mathbf{v}^t \left(M^{-1}\right)^t \left(M^t A M\right) M^{-1}\mathbf{v} = \mathbf{v}^t A \mathbf{v} = r.$$

Hence every integer represented by $\mathcal{A}$ with respect to the basis $\mathbf{e}$ is represented by $\mathcal{A}$ with respect to the basis $\mathbf{f}$.
By applying the same reasoning but starting with the basis $\mathbf{f}$ and using the change of basis matrix M^{-1} to reach the basis $\mathbf{e}$, we see the converse statement holds true.

Now suppose $r \in R\backslash\{0\}$ is properly represented by $\mathbf{v} \in V\backslash\{\mathbf{0}\}$ with respect to the basis $\mathbf{e}$. In particular this means $\gcd(v_1, \cdots, v_n) = 1$. Since properly represented implies represented this means r is represented by $M\mathbf{v}$ with respect to the basis $\mathbf{f}$. Suppose $M\mathbf{v} = s\mathbf{w}$ where $\mathbf{w}$ satisfies $\gcd(w_1, \cdots, w_n) = 1$, then applying M^{-1} yields $\mathbf{v} = M^{-1}s\mathbf{w} = sM^{-1}\mathbf{w}$. Therefore $s = \pm 1$ because $\gcd(v_1, \cdots, v_n) = 1$. Hence r is properly represented by $\mathbf{w} = M\mathbf{v}$ with respect to the basis $\mathbf{f}$. □

In our next subsection we introduce the concept of equivalence between bilinear forms.

2.2 Equivalence of Bilinear Forms

In this subsection we introduce the various notions of equivalence.
Let V be a free R-module. Recall we may write any bilinear form as a matrix in $GL_n(V)$ with respect to some basis. We consider the group $\mathrm{Aut}(GL_n(V))$ acting on $GL_n(V)$ by conjugation. This gives rise to the following definition of G-Equivalence.

Definition 2.2.1.
Let G be a subgroup of $\mathrm{Aut}(GL_n(V))$ and $\mathcal{A}$, $\mathcal{B}$ be bilinear forms with matrix representations A and B. We say $\mathcal{A}$ and $\mathcal{B}$ are **G-equivalent** if there exists $\gamma \in G$ such that $\gamma(A) = B$.

Lemma 2.2.2.
G-equivalence is an equivalence relation on the set of bilinear forms.

Proof.
Let $\mathcal{A}$, $\mathcal{B}$ and $\mathcal{C}$ be bilinear forms. We observe the identity element, $I_n \in G$ transforms $\mathcal{A}$ into itself. Next, if $M \in G$ transforms $\mathcal{A}$ into $\mathcal{B}$, then since M is invertible, M^{-1} transforms $\mathcal{B}$ into $\mathcal{A}$. Lastly, let $M, N \in G$ transform $\mathcal{A}$ to $\mathcal{B}$ and $\mathcal{B}$ to $\mathcal{C}$ respectively. Since G is a group, $MN \in G$ and transforms $\mathcal{A}$ into $\mathcal{C}$. □

We observe that Definition 2.2.1 does not depend on our choice of basis for the matrix representations of the bilinear forms.
In our work G will be either $\mathrm{GL}_n(\mathbb{Z})$, $\mathrm{SL}_n(\mathbb{Z})$, or the kernel of the homomorphism given in Lemma 2.3.2.

Definition 2.2.3.
Let R be a commutative ring and let $\mathcal{A}$ and $\mathcal{B}$ be bilinear forms with matrix representations A and B. We say

- $\mathcal{A}$ and $\mathcal{B}$ are **equivalent** if there exists $M \in GL_n(R)$ such that $M^tAM = B$.
- $\mathcal{A}$ and $\mathcal{B}$ are **properly equivalent** if there exists $M \in SL_n(R)$ such that $M^tAM = B$. They are **improperly equivalent** if they are equivalent but not properly equivalent.

Notation 2.2.4.
We will utilize the following notation, let

1. $\mathcal{A} \sim \mathcal{B}$ denote when $\mathcal{A}$ and $\mathcal{B}$ are **equivalent**,
2. $\mathcal{A} \sim_+ \mathcal{B}$ denote when $\mathcal{A}$ and $\mathcal{B}$ are **properly equivalent**, and

Observation 2.2.5.
The characterisations of the types of equivalence between bilinear forms amounts to choosing the right basis. In Lemma 2.1.11 we showed that there is a one-to-one correspondence between the (properly) represented non-zero elements in R of a bilinear form under any two bases. Thus we see that with our definition of equivalence, there is a one-to-one correspondence between the non-zero (properly) represented elements in R of any two equivalent bilinear forms.

Lastly, we introduce the notion of the determinant of a bilinear form.

Definition 2.2.6.
Let $\mathcal{A}$ be a bilinear form. We define the determinant of $\mathcal{A}$ to be the determinant of its matrix representation A.

Lemma 2.2.7.
The determinant of a bilinear form $\mathcal{A}$ is well-defined up to squares of units in R.

Proof.
Let $\mathcal{A}$ and $\mathcal{B}$ be equivalent bilinear forms. Then there exists $M \in \mathrm{GL}_n(R)$ such that $M^tAM = B$. Since $\det(M^t) = \det(M) = u$ for some unit $u \in R$, by the multiplicative property of the determinant that equivalent bilinear forms have the same determinant up to multiplication by a square of a unit in R. □

Notes on Section 2.2

Kronecker introduced the concept of complete equivalence on page 434 of [Kr1897]. He observed this is an extension of the idea of proper equivalence as introduced by Gauss.

2.3 $R = \mathbb{Z}$

From this section onwards we let $R = \mathbb{Z}$ and for the moment we will continue to work in the n-dimensional case.

We first prove a lemma regarding the determinant of a bilinear form.

Lemma 2.3.1.
The determinant of a bilinear form is invariant under conjugation via $M \in \mathrm{GL}_n(\mathbb{Z})$.

Proof.
Let $\mathcal{A}$ and $\mathcal{B}$ be bilinear forms and $M \in \mathrm{GL}_n(\mathbb{Z})$ be such that $M^t A M = B$. Since $\det(M^t) = \det(M) = \pm 1$ it follows that $\det(A) = \det(B)$. □

Next, we introduce a homomorphism that will play a pivotal role in Kronecker's investigation.

Lemma 2.3.2.
The map

$$\begin{aligned} \sigma : \mathrm{GL}_n(\mathbb{Z}) &\longrightarrow \{\pm 1\} \times \mathrm{GL}_n\left(\mathbb{Z}/2\mathbb{Z}\right) \\ A &\longmapsto (\det(A), A \bmod 2), \end{aligned}$$

is a surjective homomorphism with $|\mathrm{GL}_n(\mathbb{Z}) : \ker\sigma| = 2\prod_{k=0}^{n-1}\left(2^n - 2^k\right)$.
Note $\{\pm 1\}$ is treated as the multiplicative group of order 2.

Proof.
First note the homomorphism property follows immediately from the multiplicative property of determinants. Next observe changing the sign in a single column will multiply the determinant by -1 yet the representation $\bmod 2$ will remain the same - Thus σ is surjective. Lastly, we count the number of invertible $n \times n$ matrices over $\mathbb{Z}/(2\mathbb{Z})$. Consider such an $n \times n$ matrix then we have $2^n - 1$ choices for the first column. Next, there are $(2^n - 1) - 1 = 2^n - 2$ choices for the second column by a linear independence argument. We continue in this manner to the n^{th} column where we have $2^n - 2^{n-1}$ choices. Taking the product gives the number of invertible $n \times n$ matrices over $\mathbb{Z}/(2\mathbb{Z})$. Finally, multiplying by 2 takes into account the sign of the determinant and yields the result. □

Using this homomorphism we may extend the idea of equivalence between bilinear forms (see Definition 2.2.3) as follows:

Definition 2.3.3.
Let $\mathcal{A}$ and $\mathcal{B}$ be bilinear forms. We say:

- $\mathcal{A}$ and $\mathcal{B}$ are **completely equivalent** if there exists $M \in \ker\sigma$ such that $M^t A M = B$. They are **incompletely equivalent** if they are equivalent but not completely equivalent.

Notation 2.3.4.
We extend the notation found in Notation 2.2.4 as follows:
Let $\mathcal{A} \sim_c \mathcal{B}$ denote when $\mathcal{A}$ and $\mathcal{B}$ are **completely equivalent**.

We now define three types of class number for positive definite binary bilinear forms.

Definition 2.3.5.
Let n be a positive (non-zero) integer. Then

1. $\mathrm{Cl}(k)$ is the number of equivalence classes of bilinear forms with determinant k under $\mathrm{GL}_n(\mathbb{Z})$-equivalence.

2. $\mathrm{Cl}_+(k)$ is the number of proper equivalence classes of bilinear forms with determinant k under $\mathrm{SL}_n(\mathbb{Z})$-equivalence.

3. $\mathrm{Cl}_c(k)$ is the number of complete equivalence classes of bilinear forms with determinant k under complete equivalence.

The quantities $\mathrm{Cl}(k)$, $\mathrm{Cl}_+(k)$ and $\mathrm{Cl}_c(k)$ are called class numbers. We will be particularly interested in the complete class number. Thus if not said explicitly, we will assume we mean $\mathrm{Cl}_c(k)$.

We now use the concept of G-equivalence to determine when bilinear forms properly represent certain integers.

Lemma 2.3.6.
A bilinear form $\mathcal{A}$ properly represents a non-zero integer m if and only if $\mathcal{A}$ is properly equivalent to a bilinear form $\mathcal{B}$ with matrix representation B satisfying $B_{1,1} = m$.

Proof.
($\Leftarrow$) Let m be a non-zero integer. Assume $\mathcal{A}$ be a bilinear form that is properly equivalent to the bilinear form $\mathcal{B}$ with matrix representation B satisfying $B_{1,1} = m$. From Lemma 2.1.11 we know properly represented integers are independent of our choice of basis. So we may use the standard basis $\mathbf{e_1}, \cdots, \mathbf{e_n}$. Then $\mathcal{B}(\mathbf{e_1}, \mathbf{e_1}) = m$ as $B_{1,1} = m$. Hence $\mathcal{B}$ properly represents m and since $\mathcal{A}$ is properly equivalent to $\mathcal{B}$, Observation 2.2.5 shows $\mathcal{A}$ properly represents m.
($\Rightarrow$) Assume $\mathcal{A}$ properly represents the non-zero integer m. Then there exists $\mathbf{v} = (v_1, \cdots, v_n) \in V$ such that $\mathcal{A}(\mathbf{v}, \mathbf{v}) = m$ and $\gcd(v_1, \cdots, v_n) = 1$. By the unimodular column lemma (see Lemma 5.20 [Ro2002, p. 260]) we may extend $\mathbf{v}$ to an $n \times n$ matrix M over $\mathbb{Z}$ with determinant 1. Thus $\mathcal{A}$ is properly equivalent to the bilinear form $\mathcal{B}$, where the matrix representation of $\mathcal{B}$ with respect to the standard basis is $M^t A M$. We observe $\mathcal{B}(\mathbf{e_1}, \mathbf{e_1}) = \mathcal{A}(M\mathbf{e_1}, M\mathbf{e_1}) = \mathcal{A}(\mathbf{v}, \mathbf{v}) = m$ and therefore the matrix representation of $\mathcal{B}$ satisfies $B_{1,1} = m$. □

Lemma 2.3.7.
The minimal non-zero integer in absolute value that is represented by a non-skew-symmetric bilinear form $\mathcal{B}$ is in fact properly represented.

Proof.
Let m be the minimal non-zero integer in absolute value that is represented by $\mathcal{B}$. This exists because we cannot have an infinite decreasing sequence of positive integers. Let $m = \mathcal{B}(\mathbf{v}, \mathbf{v})$ for some $\mathbf{v} = (v_1, \cdots, v_n) \in V$ where $\gcd(v_1, \cdots, v_n) = d$. Let $\mathbf{w} = \frac{1}{d}(v_1, \cdots, v_n)$ and therefore $\gcd(w_1, \cdots w_n) = 1$. Now observe $\mathcal{B}(\mathbf{v}, \mathbf{v}) = \sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}v_iv_j = d^2\sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}w_iw_j$. Thus $m = d^2\mathcal{B}(\mathbf{w}, \mathbf{w})$. However, m is the minimal non-zero integer in absolute value that is properly represented by $\mathcal{B}$. So $d \mid m$ implies $d = 1$ and therefore $\gcd(v_1, \cdots, v_n) = 1$. Hence $\mathcal{B}$ properly represents m. □

Lemma 2.3.8.
Assume $\mathcal{B}$ is a bilinear form obtained from $\mathcal{A}$ via a change of basis then the number of solutions to $\mathcal{A} = r$ and $\mathcal{B} = r$ are equal for any $r \in \mathbb{Z}\backslash\{0\}$.

Proof.
From Lemma 2.1.11 we know a bilinear form represents the same elements regardless of our choice of basis. Let $M \in \mathrm{GL}_n(\mathbb{Z})$ be the change of basis matrix. Since M and M^{-1} are unique, it follows that there is a one-to-one correspondence between representations of a non-zero $r \in \mathbb{Z}$ under the basis $\mathbf{e}$ and the representations of r under the basis $\mathbf{f}$. □

We now introduce the concept of definite and indefinite bilinear forms.

Definition 2.3.9.
Let $\mathcal{B}$ be a bilinear form and $\mathbf{v} \in V\backslash\{\mathbf{0}\}$. We say

1. $\mathcal{B}$ is **positive definite** if $\mathcal{B}(\mathbf{v}, \mathbf{v}) > 0$, and is **positive semi-definite** if $\mathcal{B}(\mathbf{v}, \mathbf{v}) \geqslant 0$ for all such $\mathbf{v}$.
2. $\mathcal{B}$ is **negative definite** if $\mathcal{B}(\mathbf{v}, \mathbf{v}) < 0$, and is **negative semi-definite** if $\mathcal{B}(\mathbf{v}, \mathbf{v}) \leqslant 0$ for all such $\mathbf{v}$.
3. $\mathcal{B}$ is **indefinite** if $\mathcal{B}$ represents both positive and negative integers.

2.4 $R = \mathbb{Z}$, $n = 2$

In this section we restrict ourselves to working over the integers and to having dimension two. It is important to note we will diverge from Kronecker's exposition slightly. This is explained in detail in the notes at the end of this section.

We begin by giving a full description of the map σ found in Definition 2.3.2 for the two dimensional case.

Lemma 2.4.1.
Let $n = 2$ and consider the map σ from Definition 2.3.2.
We have $\ker\sigma = \langle M, N, -I_2\rangle = \left\langle \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\rangle$.

Proof.
($\supseteq$) This inclusion is straightforward to verify.
($\subseteq$) Observe $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}^k = \begin{pmatrix} 1 & 2k \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}^k = \begin{pmatrix} 1 & 0 \\ 2k & 1 \end{pmatrix}$ for any $k \in \mathbb{Z}$.
Let $M = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$, $N = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$ and $A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \ker \sigma$.
Case 1: $\gamma = 0$.
In this case we have $\det(A) = 1$ implies $1 = \alpha\delta$ and thus $\alpha = \delta = \pm 1$. Further, $\beta \equiv 0 \bmod 2$ implies $\beta = 2k$ for some $k \in \mathbb{Z}$ and thus we have $A = \begin{pmatrix} 1 & 2k \\ 0 & 1 \end{pmatrix}$ or $A = \begin{pmatrix} -1 & 2k \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix}^k$. Both of these are clearly formed from our generating set.
Case 2: $|\gamma| > 0$.
In this case we have $M^k A = \begin{pmatrix} 1 & 2k \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} \alpha + 2k\gamma & \beta + 2k\delta \\ \gamma & \delta \end{pmatrix}$, therefore we may find a value of k such that $0 < |\alpha + 2k\gamma| < |\gamma|$. Note both inequalities are strict because $\gamma \equiv 0 \bmod 2$ and $\alpha \equiv 1 \bmod 2$. Thus we may assume A satisfies $|\alpha| < |\gamma|$.
Next, $N^q A = \begin{pmatrix} 1 & 0 \\ 2q & 1 \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ \gamma + 2q\alpha & \delta + 2q\beta \end{pmatrix}$ and so we may choose $q \in \mathbb{Z}$ so that $0 < |\gamma + 2q\alpha| < |\alpha|$. Again, note both inequalities are strict.
Therefore by repeatedly left multiplying by M^k and N^q we get a strictly decreasing sequence of integers $|\gamma|$. This sequence must terminate with $|\gamma| = 0$. Therefore we are now back in the first case and thus $\ker \sigma \subseteq \langle M, N, -I_2 \rangle$. □

Notation 2.4.2. For notational convenience we may write the matrix representation of the bilinear form $\mathcal{A}$ in one line notation as $\mathcal{A} = (A_{11}, A_{12}, A_{21}, A_{22})$.

Lemma 2.4.3.
The determinant of an $n = 2$ skew-symmetric bilinear form is always a square.

Proof.
Any such skew-symmetric bilinear form $\mathcal{A}$ has matrix representation $\begin{pmatrix} 0 & A_{12} \\ -A_{12} & 0 \end{pmatrix}$ for $A_{12} \in \mathbb{Z} \backslash \{0\}$. Therefore $\det(A) = A_{12}^2$. □

We are now able to give a full description of the equivalence class structure for skew-symmetric bilinear forms. Recall the definition of a skew-symmetric bilinear form from Definition 2.1.8.

Lemma 2.4.4.
The equivalence classes of skew-symmetric bilinear forms of determinant k^2 are determined by k, and each equivalence class contains exactly two forms.
The proper equivalence classes of skew-symmetric bilinear forms are singletons determined by k. Further complete equivalence is the same as proper equivalence for skew-symmetric bilinear forms.

Proof.
From Lemma 2.4.3 we know skew-symmetric bilinear forms exist only when the determinant is a square. Further, this implies $A_{12} = k$ where $\det(A) = k^2$.
Let $\mathcal{A}$ be a skew-symmetric bilinear form with matrix representation $A = \begin{pmatrix} 0 & A_{12} \\ -A_{12} & 0 \end{pmatrix}$. Recall from Observation 2.1.10 a skew-symmetric bilinear form is always transformed to another skew-symmetric bilinear form. Suppose $\mathcal{A} \sim \mathcal{B}$ via $M \in \mathrm{GL}_2(\mathbb{Z})$, where $\mathcal{B}$ has matrix representation $\begin{pmatrix} 0 & B_{12} \\ -B_{12} & 0 \end{pmatrix}$.
Let $M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$. Note that $\det(M) = \pm 1$.
Then

$$\begin{aligned} M^t A M &= \begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix} \begin{pmatrix} 0 & A_{12} \\ -A_{12} & 0 \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \\ &= \begin{pmatrix} 0 & (\alpha\delta - \beta\gamma) A_{12} \\ -(\alpha\delta - \beta\gamma) A_{12} & 0 \end{pmatrix} \\ &= \begin{pmatrix} 0 & \det(M) A_{12} \\ -\det(M) A_{12} & 0 \end{pmatrix}. \end{aligned}$$

Thus if $M \in \mathrm{GL}_2(\mathbb{Z})$ we see that $\mathcal{A}$ is equivalent to only $\mathcal{B} = \pm\mathcal{A}$. Hence the equivalence class of $\mathcal{A}$ contains precisely two bilinear forms. Further, the equivalence classes are determined by $|A_{12}| > 0$.
If $M \in \mathrm{SL}_2(\mathbb{Z})$ we see that $\mathcal{A}$ is only properly equivalent to itself. Thus each proper equivalence class contains a single bilinear form and the proper equivalence classes are uniquely determined by A_{12}.
Since $\ker \sigma \leqslant \mathrm{SL}_2(\mathbb{Z})$ it follows that proper and complete equivalence are in fact the same. □

We now return to discussing relations between bilinear forms. The following observation shall be useful for condensing some calculations in future proofs.

Observation 2.4.5.
Let $\mathcal{A}$ be a bilinear form with matrix representation $A = \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix}$ and let $M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathcal{M}^{2\times 2}$. Then

$$\begin{aligned} B &= M^t A M \\ &= \begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix} \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \\ &= \begin{pmatrix} \alpha^2 A_{11} + \alpha\gamma(A_{12} + A_{21}) + \gamma^2 A_{22} & \alpha\beta A_{11} + \gamma\beta A_{21} + \alpha\delta A_{12} + \gamma\delta A_{22} \\ \beta\alpha A_{11} + \alpha\delta A_{21} + \beta\gamma A_{12} + \delta\gamma A_{22} & \beta^2 A_{11} + \beta\delta(A_{12} + A_{21}) + \delta^2 A_{22} \end{pmatrix}. \quad \text{(I)} \end{aligned}$$

We highlight

$$B_{12} + B_{21} = 2\alpha\beta A_{11} + (\alpha\delta + \beta\gamma)(A_{12} + A_{21}) + 2\gamma\delta A_{22} \text{ and}$$

$$B_{12} - B_{21} = \det(M)(A_{12} - A_{21}).$$

Further if $M \in SL_2(\mathbb{Z})$, $\mathcal{B}$ has matrix representation $\begin{pmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{pmatrix}$, and $\mathcal{A} \sim_+ \mathcal{B}$ we have $M^t \mathcal{A} = \mathcal{B} M^{-1}$, that is

$$\begin{aligned} \begin{pmatrix} \alpha A_{11} + \gamma A_{21} & \alpha A_{12} + \gamma A_{22} \\ \beta A_{11} + \delta A_{21} & \beta A_{12} + \delta A_{22} \end{pmatrix} &= \begin{pmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{pmatrix} \begin{pmatrix} \delta & -\beta \\ -\gamma & \alpha \end{pmatrix} \\ &= \begin{pmatrix} \delta B_{11} - \gamma B_{12} & \alpha B_{12} - \beta B_{11} \\ \delta B_{21} - \gamma B_{22} & \alpha B_{22} - \beta B_{21} \end{pmatrix}. \end{aligned} \tag{II}$$

Lemma 2.4.6.
Assume $\mathcal{A}$ and $\mathcal{B}$ are equivalent bilinear forms via the matrix $M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$. Let $A = \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix}$ and $B = \begin{pmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{pmatrix}$ be their respective representation matrices.
Then $A_{12} - A_{21} \equiv B_{12} - B_{21} \bmod 2$. Further, if $\mathcal{A}$ and $\mathcal{B}$ are in fact properly equivalent then we have $A_{12} - A_{21} = B_{12} - B_{21}$. That is, the difference between the off-diagonal elements of their matrix representations is invariant under a transformation matrix $M \in \mathrm{SL}_2(\mathbb{Z})$.

Proof.
Let $\mathcal{A}$ and $\mathcal{B}$ be equivalent bilinear forms. We use Observation 2.4.5 to calculate $M^t A M$, this yields

$$\begin{aligned} B_{12} - B_{21} &= \beta\gamma(A_{21} - A_{12}) + \alpha\delta(A_{12} - A_{21}) \\ &= \underbrace{(\alpha\delta - \beta\gamma)}_{\det(M) = \pm 1}(A_{12} - A_{21}). \end{aligned}$$

Hence we see $A_{12} - A_{21} \equiv B_{12} - B_{21} \bmod 2$, and if $M \in \mathrm{SL}_2(\mathbb{Z})$ then $A_{12} - A_{21} = B_{12} - B_{21}$. □

Lemma 2.4.7.
Let $\mathcal{A}$ and $\mathcal{B}$ be completely equivalent bilinear forms, then $A_{ij} \equiv B_{ij} \bmod 2$, $i, j \in \{1, 2\}$.

Proof.
Let $M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \ker \sigma$ and use Observation 2.4.5. It is helpful to recall $\alpha \equiv \delta \equiv 1 \bmod 2$ and $\beta \equiv \gamma \equiv 0 \bmod 2$. Then we have:

$$\begin{aligned} B_{11} &= \underbrace{\alpha^2}_{\equiv 1 \bmod 2} A_{11} + \underbrace{\alpha\gamma}_{\equiv 0 \bmod 2} (A_{12} + A_{21}) + \underbrace{\gamma^2}_{\equiv 0 \bmod 2} A_{22} \\ &\equiv A_{11} \bmod 2 \\ B_{12} &= \underbrace{\alpha\beta}_{\equiv 0 \bmod 2} A_{11} + \underbrace{\alpha\delta}_{\equiv 1 \bmod 2} A_{12} + \underbrace{\gamma\beta}_{\equiv 0 \bmod 2} A_{21} + \underbrace{\gamma\delta}_{\equiv 0 \bmod 2} A_{22} \end{aligned}$$

$$
\begin{aligned}
&\equiv A_{12} \bmod 2 \\
B_{21} = &\underbrace{\alpha\beta}_{\equiv 0 \bmod 2} A_{11} + \underbrace{\beta\gamma}_{\equiv 0 \bmod 2} A_{12} + \underbrace{\alpha\delta}_{\equiv 1 \bmod 2} A_{21} + \underbrace{\delta\gamma}_{\equiv 0 \bmod 2} A_{22} \\
&\equiv A_{21} \bmod 2 \\
B_{22} = &\underbrace{\beta^2}_{\equiv 0 \bmod 2} A_{11} + \underbrace{\beta\delta}_{\equiv 0 \bmod 2} (A_{12} + A_{21}) + \underbrace{\delta^2}_{\equiv 1 \bmod 2} A_{22} \\
&\equiv A_{22} \bmod 2.
\end{aligned}
$$

□

We now relate a binary quadratic form to a given bilinear form as follows.

Definition 2.4.8.
Let $\mathcal{B}$ be a bilinear form with matrix representation $\begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix}$. We define the **associated binary quadratic form to $\mathcal{B}$** to be

$$A_{\mathcal{B}} = A_{11}x^2 + (A_{12} + A_{21})\,xy + A_{22}y^2.$$

Lemma 2.4.9.
The binary quadratic forms $ax^2 + 2bxy + cy^2$, $a, b, c \in \mathbb{Z}$ are a subset of the bilinear forms with integer coefficients.

Proof.
Let $ax^2+2bxy+cy^2$ where $a, b, c \in \mathbb{Z}$ be a binary quadratic form. Consider the matrix representation of a bilinear form given by $A_{11} = a$, $A_{12} = A_{21} = b$ and $A_{22} = c$. Then letting $\mathbf{x} = \mathbf{y} = \begin{pmatrix} x \\ y \end{pmatrix}$ yields our binary quadratic form. □

Since our work will involve binary quadratic forms from time to time we present a parallel definition of definiteness for binary quadratic forms (see Definition 2.3.9).

Definition 2.4.10.
Let $f(x, y) = ax^2 + rxy + cy^2$ be a binary quadratic form. We say

- f is **positive definite** if $f(x, y) > 0$ for all $(x, y) \neq (0, 0)$. This can be relaxed to **positive semi-definite** if $f(x, y) \geqslant 0$ for all $(x, y) \neq (0, 0)$.
- f is **negative definite** if $f(x, y) < 0$ for all $(x, y) \neq (0, 0)$. This relaxes to **negative semi-definite** if $f(x, y) \leqslant 0$ for all $(x, y) \neq (0, 0)$.
- f is **indefinite** if f represents both positive and negative integers.

Lemma 2.4.11.
Let $f = ax^2 + rxy + cy^2$ be a binary quadratic form. Then

1. *f is positive definite if and only if $a > 0$ and $4\det(f) > 0$*
2. *f is negative definite if and only if $a < 0$ and $4\det(f) > 0$*

3. f is indefinite if and only if $4\det(f) < 0$.

Proof.
We have

$$\begin{aligned} 4af &= 4a^2x^2 + 4arxy + 4acy^2 \\ &= (2ax + ry)^2 + \left(4ac - r^2\right) y^2 \\ &= 4a^2 (2ax + ry)^2 + \left(4ac - r^2\right) y^2. \end{aligned}$$

Therefore we may write

$$f = a\left(x + \frac{r}{2a}y\right)^2 + \left(\frac{4ac - r^2}{4a}\right) y^2. \tag{2.4}$$

1. ($\Rightarrow$) Assume f is positive definite. Then Equation 2.4 implies we must have $a > 0$ and $\frac{4ac-r^2}{4a} > 0$. From this is follows that $4ac - r^2 = 4\det(f) > 0$.
   ($\Leftarrow$) Suppose $a > 0$ and $4\det(f) = 4ac - r^2 > 0$. Then Equation 2.4 implies $f(x, y) > 0$ for all $(x, y) \in (\mathbb{Z} \times \mathbb{Z})\backslash(0, 0)$.

2. ($\Rightarrow$) Assume f is negative definite. Then Equation 2.4 implies we must have $a < 0$ as otherwise whenever $y = 0$ and $x \neq 0$ f would return a positive number. However, we must also have $\frac{4ac-r^2}{4a} < 0$ to cope with when $x = 0$ and $y \neq 0$. This gives the other condition, $4\det(f) = 4ac - r^2 > 0$ as $a < 0$.
   ($\Leftarrow$) Suppose $a < 0$ and $4\det(f) = 4ac - r^2 > 0$. Then Equation 2.4 implies $f(x, y) < 0$ for all $(x, y) \in (\mathbb{Z} \times \mathbb{Z})\backslash(0, 0)$.

3. ($\Rightarrow$) Assume f is indefinite. Firstly, if $a \neq 0$ then we must have $4\det(f) = 4ac - r^2 < 0$ as $4\det(f) = 4ac - r^2 = 0$ yields f producing all positive or all negative (and possibly zero) integers and (1.) and (2.) above exclude $4\det(f) > 0$. If $a = 0$ then $4\det(f) = 4ac - r^2 = -r^2 < 0$.
   ($\Leftarrow$) Suppose $4\det(f) = 4ac - r^2 < 0$. If $a = 0$ then our binary quadratic form simplifies to $f = rxy + by^2$ from which it is straightforward to see it represents both positive and negative integers for $(x, y) \neq (0, 0)$. Thus suppose $a \neq 0$. Then Equation 2.4 implies with careful choice of (x, y) it is possible for f to produce both positive and negative integers. Hence f is an indefinite binary quadratic form.

□

Lemma 2.4.12.
Let $\mathcal{A}$ and $\mathcal{B}$ be (properly) equivalent bilinear forms. Then their associated binary quadratic forms, $A_{\mathcal{A}}$ and $A_{\mathcal{B}}$, are also (properly) equivalent.

Proof.
Let $A = \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix}$ and $B = \begin{pmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{pmatrix}$ be the matrix representations of the bilinear forms $\mathcal{A}$ and $\mathcal{B}$ respectively. Let $M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z})$ (resp. $\mathrm{SL}_2(\mathbb{Z})$)

be such that $M^tAM = B$. Using Observation 2.4.5 (I) we see that the associated binary quadratic form $A_{\mathcal{B}} = A_{\mathcal{M}^t\mathcal{A}\mathcal{M}}$ is given by

$$\begin{aligned} A_{\mathcal{M}^t\mathcal{A}\mathcal{M}} &= \left(\alpha^2 A_{11} + \alpha\gamma(A_{12}+A_{21}) + \gamma^2 A_{22}\right) x^2 + \\ &= \quad (2\alpha\beta A_{11} + (\alpha\delta+\beta\gamma)(A_{12}+A_{21}) + 2\beta\delta A_{22})\, xy + \\ &\quad \left(\beta^2 A_{11} + \beta\delta(A_{12}+A_{21}) + \delta^2 A_{22}\right) y^2. \end{aligned}$$

Now we calculate $M^tA_{\mathcal{A}}M$ directly via Observation 2.4.5 (I)

$$\begin{aligned} M^tA_{\mathcal{A}}M &= \begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix} \begin{pmatrix} A_{11} & \frac{A_{12}+A_{21}}{2} \\ \frac{A_{12}+A_{21}}{2} & A_{22} \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \\ &= \begin{pmatrix} \alpha^2 A_{11} + \alpha\gamma(A_{12}+A_{21}) + \gamma^2 A_{22} & \alpha\beta A_{11} + \frac{\alpha\delta+\beta\gamma}{2}(A_{12}+A_{21}) + \gamma\delta A_{22} \\ \alpha\beta A_{11} + \frac{\alpha\delta+\beta\gamma}{2}(A_{12}+A_{21}) + \gamma\delta A_{22} & \beta^2 A_{11} + \beta\delta(A_{12}+A_{21}) + \delta^2 A_{22} \end{pmatrix} \\ &= A_{\mathcal{M}^t\mathcal{A}\mathcal{M}} \\ &= A_{\mathcal{B}}. \end{aligned}$$

Hence we see $A_{\mathcal{A}} \sim A_{\mathcal{B}}$ ($A_{\mathcal{A}} \sim_+ A_{\mathcal{B}}$) via M. □

Corollary 2.4.13.
Assume $\mathcal{A}$ and $\mathcal{B}$ are equivalent bilinear forms. Then $\det(A_{\mathcal{A}}) = \det(A_{\mathcal{B}})$.

Proof.
Since the bilinear forms $\mathcal{A}$ and $\mathcal{B}$ are equivalent there exists $M \in \mathrm{GL}_2(\mathbb{Z})$ such that $M^tAM = B$. From Lemma 2.3.1 we know $M^tA_{\mathcal{A}}M = A_{\mathcal{B}}$, using $\det(M) = \pm 1$ and $\det(M^t) = \det(M)$ it follows immediately that $\det(A_{\mathcal{A}}) = \det(A_{\mathcal{B}})$. □

We now present a second proof of Corollary 2.4.13.

Proof of Corollary 2.4.13:
Assume $\mathcal{A}$ and $\mathcal{B}$ are equivalent bilinear forms. Then there exists $M \in \mathrm{GL}_2(\mathbb{Z})$ such that $M^tAM = B$. From Lemmas 2.3.1 and 2.4.6 we know $\det(A) = \det(B)$ and $A_{12} - A_{21} = B_{12} - B_{21}$. Thus we consider the determinant of $A_{\mathcal{A}}$ as follows:

$$\begin{aligned} \det(A_{\mathcal{A}}) &= A_{11}A_{22} - \left(\frac{A_{12}+A_{21}}{2}\right)^2 \text{ which implies} \\ 4\det(A_{\mathcal{A}}) &= 4A_{11}A_{22} - (A_{12}+A_{21})^2 \\ &= 4\left(A_{11}A_{22} - A_{12}A_{21}\right) - (A_{12}-A_{21})^2. \end{aligned}$$

$$\text{Thus } A_{11}A_{22} - \left(\frac{A_{12}+A_{21}}{2}\right)^2 = \det(A) - \left(\frac{A_{12}-A_{21}}{2}\right)^2.$$

Thus we see the determinant of $A_{\mathcal{A}}$ is invariant under M and hence $\det(A_{\mathcal{A}}) = \det(A_{\mathcal{B}})$.

□

We now introduce the concept of a reduced bilinear form.

Definition 2.4.14.
Let $\mathcal{A}$ be a bilinear form with matrix representation $A = \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix}$ with respect to some basis. We say that $\mathcal{A}$ is **reduced** if one of the following conditions holds:

1. $-|A_{11}| < A_{12} + A_{21} \leqslant |A_{11}| < |A_{22}|$, or
2. $0 \leqslant A_{12} + A_{21} \leqslant |A_{11}| = |A_{22}|$.

This definition is an extension of the definition of a reduced binary quadratic form. The definition for binary quadratic forms may be found in [NZM1991, p 159].
The following definition defines two types of transformation matrices that are useful when reducing bilinear forms.

Definition 2.4.15.
Let $\beta, \gamma \in \mathbb{Z}$. We define the following transformation matrices:

$$U(\beta) = \begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix} \text{ and } L(\gamma) = \begin{pmatrix} 1 & 0 \\ \gamma & 1 \end{pmatrix}.$$

Lemma 2.4.16.
Assume $\mathcal{A}$ is a definite reduced bilinear form with matrix representation A, then $\det(A) > 0$.

Proof.
Since $\mathcal{A}$ is a definite form we have $A_{11}A_{22} > 0$. This is because A_{11} and A_{22} are represented by $\mathcal{A}$ and so are non-zero and have the same sign. For the same reason we see $\mathcal{A}$ is not the zero bilinear form. Using this we have

$$\begin{aligned} \det(A) = A_{11}A_{22} - A_{12}A_{21} &\geqslant (A_{12} + A_{21})^2 - A_{12}A_{21} \text{ as } \mathcal{A} \text{ is reduced} \\ &= A_{12}^2 + A_{12}A_{21} + A_{21}^2 \\ &= \frac{1}{4}\left[(2A_{12} + A_{21})^2 + 3A_{21}^2\right] \geqslant 0. \end{aligned}$$

In the first line of the above equation we have equality if and only if $(A_{12} + A_{21})^2 = A_{11}A_{22}$. However $\mathcal{A}$ is reduced so we have $(A_{12} + A_{21})^2 \leqslant |A_{11}|^2 = A_{11}^2$, and $|A_{11}| \leqslant |A_{22}|$.
Thus in order to have $\det(A) = 0$ we must have $A_{12} + A_{21} = |A_{11}|$ and $A_{11} = A_{22}$ as $\mathcal{A}$ is a definite form. We note that $A_{12} + A_{21} \neq -|A_{11}|$ because $\mathcal{A}$ is reduced.

Then by the last line of the above equation we see that in order to obtain 0 we require both $2A_{12} + A_{21} = 0$ and $A_{21} = 0$. It follows that $A_{12} = A_{21} = 0$ for this to occur.
To conclude, we have a strict inequality on the first line above unless $A_{12}+A_{21} = |A_{11}|$ and $A_{11} = A_{22}$, and we have a strict inequality on the third line unless $A_{12} = A_{21} = 0$. Hence $\det(A) = 0$ if and only if $\mathcal{A}$ is the zero bilinear form. But $\mathcal{A}$ is not the zero bilinear form and thus $\det(A) > 0$. □

The following lemma is provided as an aide-memoir.

Lemma 2.4.17.
Let a and b be real numbers, then $|a+b| \geqslant ||a|-|b||$.

Proof.
We see $|b| = |a+b+(-a)| \leqslant |a+b| + |-a| = |a+b| + |a|$. Rearranging yields $|a+b| \geqslant |b| - |a|$. By symmetry we may interchange a and b to get $|a+b| \geqslant |a| - |b|$ and hence $|a+b| \geqslant ||a| - |b||$. □

Lemma 2.4.18.
Let $\mathcal{B}$ be a positive definite reduced bilinear form. Let $\mathbf{v} = \begin{pmatrix} x \\ y \end{pmatrix}$. If $\gcd(x,y) = 1$ for some integers $x, y \in \mathbb{Z}$ and $\mathcal{B}(\mathbf{v},\mathbf{v}) \leqslant A_{22}$, then $\mathcal{B}(\mathbf{v},\mathbf{v}) = A_{11}$ or A_{22}, and (x,y) is one of the six points $\pm(0,1)$, $\pm(1,0)$, or $\pm(-1,1)$.
Further, the number of proper representations of A_{11} by $\mathcal{B}$ is:

$$\begin{cases} 6 & \text{if } A_{11} = A_{22} \text{ and } A_{12} + A_{21} = A_{11}, \\ 4 & \text{if } A_{11} = A_{22} \text{ and } A_{12} + A_{21} \neq A_{11}, \\ 2 & \text{otherwise.} \end{cases}$$

Proof.
Recall $\mathcal{B}$ positive definite implies $\mathcal{B}(\mathbf{v},\mathbf{v}) > 0$ for all $\mathbf{v} \neq \mathbf{0}$. In particular, $A_{11} > 0$. Let $\mathbf{v} = \begin{pmatrix} x \\ y \end{pmatrix}$ where $\gcd(x,y) = 1$. Then multiplying by $4A_{11}$, we obtain the following:

$$\begin{aligned} 4A_{11}\mathcal{B}(\mathbf{v},\mathbf{v}) &= 4A_{11}^2x^2 + 4A_{11}(A_{12}+A_{21})xy + 4A_{11}A_{22}y^2 \\ &= (2A_{11}x + (A_{12}+A_{21})y)^2 + \left(4A_{11}A_{22} - (A_{12}+A_{21})^2\right)y^2. \end{aligned} \tag{2.5}$$

If $y = 0$ then $x = \pm 1$ and Equation 2.5 yields $4A_{11}^2$.
Thus $\mathcal{B}\left(\begin{pmatrix} \pm 1 \\ 0 \end{pmatrix}, \begin{pmatrix} \pm 1 \\ 0 \end{pmatrix}\right) = A_{11}$.
Now let $y = \pm 1$ and suppose $|x| \geqslant 2$. Then using the Lemma 2.4.17 we have

$$\begin{aligned} |2A_{11}x + (A_{12}+A_{21})y| &\geqslant 2A_{11}|x| - |A_{12}+A_{21}||y| \\ &= 2A_{11}|x| - |A_{12}+A_{21}| \\ &\geqslant 4A_{11} - |A_{12}+A_{21}| \\ &> |A_{12}+A_{21}|. \end{aligned}$$

Using this Equation 2.5 becomes:

$$\begin{aligned} 4A_{11}\mathcal{B}(\mathbf{v},\mathbf{v}) &= (2A_{11}x + (A_{12}+A_{21})y)^2 + \left(4A_{11}A_{22} - (A_{12}+A_{21})^2\right)y^2 \\ &> (A_{12}+A_{21})^2 + 4A_{11}A_{22} - (A_{12}+A_{21})^2 \\ &= 4A_{11}A_{22}. \end{aligned}$$

Hence $\mathcal{B}(\mathbf{v},\mathbf{v}) > A_{22}$ when $|y| = 1$ and $|x| \geqslant 2$.
Now suppose $|y| \geqslant 2$. Then Equation 2.5 becomes:

$$4A_{11}\mathcal{B}(\mathbf{v},\mathbf{v}) = (2A_{11}x + (A_{12}+A_{21})y)^2 + \left(4A_{11}A_{22} - (A_{12}+A_{21})^2\right)y^2$$

$$
\begin{aligned}
&\geqslant \left(2A_{11}x + \left(A_{12}+A_{21}\right)y\right)^2 + 4\left(4A_{11}A_{22} - \left(A_{12}+A_{21}\right)^2\right) \\
&\geqslant 4\left(4A_{11}A_{22} - \left(A_{12}+A_{21}\right)^2\right) \\
&\geqslant 4\left(4A_{11}A_{22} - A_{11}A_{22}\right) \text{ as } 0 \leqslant \left(A_{12}+A_{21}\right)^2 \leqslant A_{11}^2 \leqslant A_{11}A_{22} \\
&= 12A_{11}A_{22}.
\end{aligned}
$$

Thus $\mathcal{B}(\mathbf{v},\mathbf{v}) \geqslant 3A_{22} > A_{22} > 0$.

So we are left to consider $(x,y) = \pm(0,1), \pm(1,1)$, and $\pm(-1,1)$.
By direct calculation, $\mathcal{B}\left(\begin{pmatrix} 0 \\ \pm 1 \end{pmatrix}, \begin{pmatrix} 0 \\ \pm 1 \end{pmatrix}\right) = A_{22} \geqslant A_{11}$ as $\mathcal{B}$ is reduced. We note that equality holds if and only if $A_{22} = A_{11}$.
Similarly, $\mathcal{B}\left(\begin{pmatrix} \pm 1 \\ \pm 1 \end{pmatrix}, \begin{pmatrix} \pm 1 \\ \pm 1 \end{pmatrix}\right) = A_{11} + (A_{12}+A_{21}) + A_{22} > A_{22}$.
This is because $-A_{11} < A_{12} + A_{21} \leqslant A_{11}$ thus $A_{11} + (A_{12}+A_{21}) > 0$.
Lastly, $\mathcal{B}\left(\pm\begin{pmatrix} -1 \\ 1 \end{pmatrix}, \pm\begin{pmatrix} -1 \\ 1 \end{pmatrix}\right) = A_{11} - (A_{12}+A_{21}) + A_{22} \geqslant A_{22} \geqslant A_{11}$.
This is due to $-A_{11} < A_{12} + A_{21} \leqslant A_{11}$ yielding $A_{11} - (A_{12}+A_{21}) \geqslant 0$. We note that we have equality if and only if $A_{11} = A_{22}$ and $A_{12} + A_{21} = A_{11}$.

Hence A_{11} is properly represented by $\mathcal{B}$ in the following ways:

$$
\begin{cases}
6 \text{ times} & \text{if } A_{22} = A_{11} \text{ and } A_{12} + A_{21} = A_{11} \\
4 \text{ times} & \text{if } A_{22} = A_{11} \text{ and } A_{12} + A_{21} \neq A_{11} \\
2 \text{ times} & \text{otherwise.}
\end{cases}
$$

□

Corollary 2.4.19.
A bilinear form $\mathcal{B}$ is positive definite if and only if $A_{11} > 0$ and $4A_{11}A_{22} - \left(A_{12}+A_{21}\right)^2 > 0$.

Proof.
Let $\mathcal{B}$ be a bilinear form with matrix representation $\begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix}$.
($\Rightarrow$) Assume $\mathcal{B}$ is positive definite, so $\mathcal{B}(\mathbf{v},\mathbf{v}) > 0$ for all $\mathbf{v} \neq \mathbf{0}$. Since $\mathbf{v} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ yields $\mathcal{B}(\mathbf{v},\mathbf{v}) = A_{11}$, we must have $A_{11} > 0$.
We now use the result found in Equation 2.5:

$$
4A_{11}\mathcal{B}(\mathbf{v},\mathbf{v}) = \left(2A_{11}x + \left(A_{12}+A_{21}\right)y\right)^2 + \left(4A_{11}A_{22} - \left(A_{12}+A_{21}\right)^2\right)y^2.
$$

Since $\mathcal{B}$ is positive definite and $A_{11} > 0$ it follows that $4A_{11}\mathcal{B}(\mathbf{v},\mathbf{v}) > 0$ for all $\mathbf{v} \neq \mathbf{0}$.
Since $A_{11} > 0$, taking $\mathbf{v} = \begin{pmatrix} A_{12}+A_{21} \\ -2A_{11} \end{pmatrix} \neq \mathbf{0}$ yields

$$4A_{11}\mathcal{B}(\mathbf{v},\mathbf{v}) = \underbrace{\left(2A_{11}(A_{12}+A_{21})+(A_{12}+A_{21})(-2A_{11})\right)^2}_{=0} + \left(4A_{11}A_{22}-(A_{12}+A_{21})^2\right)(-2A_{11})^2.$$

This implies $\mathcal{B}(\mathbf{v},\mathbf{v}) = \left(4A_{11}A_{22}-(A_{12}+A_{21})^2\right)A_{11}$. Since $A_{11}>0$, it follows that $4A_{11}A_{22}-(A_{12}+A_{21})^2>0$ for $\mathcal{B}$ to be positive definite.
Hence if $\mathcal{B}$ is positive definite then $A_{11}>0$ and $4A_{11}A_{22}-(A_{12}+A_{21})^2>0$.

($\Leftarrow$) Assume $A_{11}>0$ and $4A_{11}A_{22}-(A_{12}+A_{21})^2>0$.
Then for $\mathbf{v}\neq\mathbf{0}$, Equation 2.5 yields

$$4A_{11}\mathcal{B}(\mathbf{v},\mathbf{v}) = \underbrace{\left(2A_{11}x+(A_{12}+A_{21})y\right)^2}_{\geqslant 0} + \left(\underbrace{4A_{11}A_{22}-(A_{12}+A_{21})^2}_{>0}\right)\underbrace{y^2}_{\geqslant 0}.$$

Since $4A_{11}>0$, we will only have $\mathcal{B}(\mathbf{v},\mathbf{v})=0$ if both $y=0$ and
$2A_{11}x+(A_{12}+A_{21})y=0$. However, this implies $2A_{11}x=0$ and so $A_{11}>0$ means $x=0$. Thus $\mathbf{v}=\mathbf{0}$.
So $4A_{11}\mathcal{B}(\mathbf{v},\mathbf{v})>0$ for all $\mathbf{v}\neq\mathbf{0}$ and hence $\mathcal{B}(\mathbf{v},\mathbf{v})>0$ for all $\mathbf{v}\neq\mathbf{0}$.
Hence $\mathcal{B}$ is a positive definite bilinear form. □

Corollary 2.4.20.
A reduced bilinear form $\mathcal{B}$ is positive definite if and only if $0<A_{11}A_{22}$ and $0<A_{11}$.

Proof.
Let $\mathcal{B}$ be a reduced bilinear form.
($\Rightarrow$) Assume $\mathcal{B}$ is positive definite. Then $\mathbf{v}=(1,0)$ yields $\mathcal{B}(\mathbf{v},\mathbf{v})=A_{11}>0$, and $\mathbf{w}=(0,1)$ yields $\mathcal{B}(\mathbf{w},\mathbf{w})=A_{22}>0$. Hence we have $0<A_{11}A_{22}$ and $0<A_{11}$.

($\Leftarrow$) Assume $\mathcal{B}$ satisfies $0<A_{11}A_{22}$ and $0<A_{11}$. Observe the first condition implies $0<A_{11}A_{22}<4A_{11}A_{22}$. Since $\mathcal{B}$ is reduced, we have $-A_{11}<A_{12}+A_{21}\leqslant A_{11}<A_{22}$ or $0\leqslant A_{12}+A_{21}\leqslant A_{11}=A_{22}$ and this gives $4A_{11}A_{22}>(A_{12}+A_{21})^2$.
Hence we have $0<4A_{11}A_{22}-(A_{12}+A_{21})^2$ and Corollary 2.4.19 implies $\mathcal{B}$ is positive definite. □

Corollary 2.4.21.
Let $M\in \mathrm{GL}_2(\mathbb{Z})$ and $\mathcal{A}$ be a positive definite bilinear form. Then M^tAM is a positive definite bilinear form.

Proof.
By Corollary 2.4.19 we need to show $B=M^tAM$ satisfies $B_{11}>0$ and $4B_{11}B_{22}-(B_{12}+B_{21})^2>0$. We note $\mathcal{A}$ satisfies $0<4A_{11}A_{22}-(A_{12}+A_{21})^2$ and

$$\begin{aligned}4A_{11}A_{22}-(A_{12}+A_{21})^2 &= 4(A_{11}A_{22}-A_{12}A_{21})-A_{12}^2-A_{21}^2+2A_{12}A_{21}\\ &= 4\det(A)-(A_{12}-A_{21})^2.\end{aligned}$$

Since $\det(B) = \det(M^tAM) = \det(A)$ and by the proof of Lemma 2.4.6 we have $(B_{12}-B_{21})^2 = (A_{12}-A_{21})^2$, it follows that $4B_{11}B_{22}-(B_{12}+B_{21})^2 = 4A_{11}A_{22}-(A_{12}+A_{21})^2 > 0$. Lastly, using Observation 2.4.5 yields $B_{11} = \alpha^2A_{11}+\alpha\gamma(A_{12}+A_{21})+\gamma^2A_{22}$. Since $\det(M) \neq 0$ we cannot have $\alpha = \gamma = 0$ and thus $\begin{pmatrix} \alpha \\ \gamma \end{pmatrix} \neq \mathbf{0}$. Then we have

$$\begin{pmatrix} \alpha & \gamma \end{pmatrix} \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix} \begin{pmatrix} \alpha \\ \gamma \end{pmatrix} = \alpha^2A_{11} + \alpha\gamma(A_{12} + A_{21}) + \gamma^2A_{22}.$$

Since $\mathcal{A}$ is positive definite, it follows that $\alpha^2A_{11} + \alpha\gamma(A_{12} + A_{21}) + \gamma^2A_{22} > 0$. Therefore we see $B_{11} > 0$, completing the requirements of Corollary 2.4.19 for M^tAM to be a positive definite bilinear form. □

Observation 2.4.22.
Lemma 2.4.18 implies that the minimal non-zero integer properly represented by a positive definite reduced bilinear form is A_{11}.

Theorem 2.4.23.
Every bilinear form $\mathcal{B}$ that is not skew-symmetric is properly equivalent to a reduced bilinear form.

Proof.
Let $\mathcal{B}$ be a non-skew-symmetric bilinear form, then $\mathcal{B}$ represents non-zero integers. Choose $m \in \mathbb{Z}\setminus\{0\}$ properly represented by $\mathcal{B}$ and such that $|m|$ is minimal. By Lemma 2.3.6 $\mathcal{B}$ is properly equivalent to the bilinear form with matrix representation $\begin{pmatrix} m & b \\ c & d \end{pmatrix}$. Thus without loss of generality we may assume that $\mathcal{B} = \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix}$, where $A_{11} \neq 0$ is the integer properly represented by $\mathcal{B}$ such that $|A_{11}|$ is minimal. Observe that $A_{22} = \mathcal{B}\left(\begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}\right)$. Thus since $|A_{11}|$ is properly represented by $\mathcal{B}$ and is minimal, we see that $0 < |A_{11}| \leqslant |A_{22}|$ as A_{22} is properly represented by $\mathcal{B}$. Thus if $\mathcal{B}$ is not reduced then we have $A_{12} + A_{21} \notin (-|A_{11}|, |A_{11}|]$.
By the division algorithm there exists a unique $q \in \mathbb{Z}\setminus\{0\}$ such that $A_{12} + A_{21} = 2qA_{11} + r$ where $-|A_{11}| < r \leqslant |A_{11}|$. Applying the $SL_2(\mathbb{Z})$ change of basis $U(-q)$ (see Definition 2.4.15) yields

$$U(-q)^t AU(-q) = \begin{pmatrix} A_{11} & A_{12} - qA_{11} \\ A_{21} - qA_{11} & A_{22} - q(A_{12} + A_{21}) + q^2A_{11} \end{pmatrix}.$$

Observe the "A_{11}" entry is still properly represented by $\mathcal{B}$ and |"A_{11}"| is minimal. Also observe the new "$A_{12} + A_{21}$" entry is $(A_{12} + A_{21}) - [(A_{12} + A_{21} - r)] = r$. Thus we have $-|A_{11}| <$ "$A_{12} + A_{21}$" $\leqslant |A_{11}|$. It remains to show that |"A_{22}"| $\geqslant |A_{11}|$. This follows immediately because $\mathcal{B}\left(\begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}\right) =$ "A_{22}" and since $|A_{11}|$ is the minimal non-zero integer represented by $\mathcal{B}$ we have $0 < |A_{11}| \leqslant$ |"A_{22}"|.
Thus the only problem that may remain is if $|A_{11}| =$ |"A_{22}"| and $r =$ "$A_{12} +$

A_{21}" < 0. If this is the case then applying $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in SL_2(\mathbb{Z})$ yields the form $\begin{pmatrix} \text{“}A_{22}\text{”} & -\text{“}A_{21}\text{”} \\ -\text{“}A_{12}\text{”} & A_{11} \end{pmatrix}$. Since “$A_{22}$” $= A_{11}$ and $0 \leqslant -r \leqslant |A_{11}|$ we see that this new form is reduced.
Hence every non-skew-symmetric bilinear form is properly equivalent to a reduced bilinear form. □

Theorem 2.4.24.
Let $\mathcal{A}$ be a positive definite bilinear form. Then $\mathcal{A}$ is properly equivalent to a unique reduced bilinear form.

Proof.
Let $\mathcal{A}$ be a positive definite bilinear form. Note this implies $\mathcal{A}(\mathbf{v}, \mathbf{v}) > 0$ for all $\mathbf{v} \neq \mathbf{0}$ and therefore $\mathcal{A}$ is not skew-symmetric. We assume $\mathcal{A}$ is properly equivalent to the reduced bilinear forms $\mathcal{B}$ and $\mathcal{C}$. Let the matrix representations of the reduced forms be $B = \begin{pmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{pmatrix}$ and $C = \begin{pmatrix} C_{11} & C_{12} \\ C_{21} & C_{22} \end{pmatrix}$ respectively.

By Observation 2.4.22, B_{11} is the smallest non-zero integer properly represented by $\mathcal{B}$, and for $\mathcal{C}$ it is C_{11}. By Lemma 2.1.11 and Observation 2.2.5, properly equivalent bilinear forms represent the same set of properly represented integers. Thus $B_{11} = C_{11}$.
Now suppose $B_{22} = B_{11}$. Then Lemma 2.4.18 implies $\mathcal{B}$ properly represents B_{11} at least 4 times. Lemma 2.1.11 and Observation 2.2.5 then forces $C_{22} = C_{11} = B_{11}$ as otherwise $\mathcal{C}$ would only represent B_{11} twice.
Recall from Corollary 2.4.13 that the negative discriminant of the associated binary quadratic form is an invariant. Thus we have

$$B_{11}B_{22} - \left(\frac{B_{12} + B_{21}}{2}\right)^2 = \det(A_{\mathcal{B}}) = \det(A_{\mathcal{C}}) = B_{11}B_{22} - \left(\frac{C_{12} + C_{21}}{2}\right)^2.$$

Hence $(B_{12} + B_{21})^2 = (C_{12} + C_{21})^2$. Then since $\mathcal{B}$ and $\mathcal{C}$ are reduced and $B_{22} = B_{11}$, we have $0 \leqslant B_{12} + B_{21}$ and $0 \leqslant C_{12} + C_{21}$, and so we see $B_{12} + B_{21} = C_{12} + C_{21}$. Using Lemma 2.4.6 we have $B_{12} - B_{21} = C_{12} - C_{21}$; this yields a pair of simultaneous equations with sole solution $B_{12} = C_{12}$ and $B_{21} = C_{21}$.
Hence if $B_{22} = B_{11}$ then we have a unique reduced form.

Next suppose $B_{11} < B_{22}$. Lemma 2.4.18 implies that there are exactly two representations of B_{11}, consequently Lemma 2.1.11 and Observation 2.2.5 imply $\mathcal{C}$ represents B_{11} exactly twice as well. Thus we have $B_{11} < C_{22}$. By Lemma 2.4.18 we see that B_{22} is the second smallest integer properly represented by $\mathcal{B}$, while for $\mathcal{C}$ it is C_{22}. Then Lemma 2.1.11 and Observation 2.2.5 imply $C_{22} = B_{22}$. Again using Corollary 2.4.13 we see that $(C_{12} + C_{21})^2 = (B_{12} + B_{21})^2$ and thus $(C_{12} + C_{21}) = \pm(B_{12} + B_{21})$.
Now let $M = \begin{pmatrix} r & s \\ t & u \end{pmatrix} \in SL_2(\mathbb{Z})$ be such that $M^t B M = C$. Then $\det(M) = ru - ts = 1$ implies $\gcd(r, t) = 1$ and $\gcd(s, u) = 1$. We see that

$B_{11} = \mathcal{C}\left(\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix}\right) = \mathcal{B}\left(\begin{pmatrix} r \\ t \end{pmatrix}, \begin{pmatrix} r \\ t \end{pmatrix}\right)$ and $\gcd(r,t) = 1$ implies this is a proper representation of B_{11}. Thus Lemma 2.4.18 implies $\begin{pmatrix} r \\ t \end{pmatrix} = \pm \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ as we only have two proper representations of A_{11}.
Similarly, $B_{22} = \mathcal{C}\left(\begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}\right) = \mathcal{B}\left(\begin{pmatrix} s \\ u \end{pmatrix}, \begin{pmatrix} s \\ u \end{pmatrix}\right)$ and $\gcd(s,u) = 1$ implies this is a proper representation of B_{22}. Thus Lemma 2.4.18 implies either $\begin{pmatrix} s \\ u \end{pmatrix} = \pm \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ or $\begin{pmatrix} -1 \\ 1 \end{pmatrix}$. Hence the only possibilities for M are $\pm \mathrm{I}_2$ or $\pm \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$.
Applying $M = \pm \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$ yields $\begin{pmatrix} B_{11} & B_{12} - B_{11} \\ B_{21} - B_{11} & B_{11} - (B_{12} + B_{21}) + B_{22} \end{pmatrix}$.
Thus $C_{12} + C_{21} = B_{12} + B_{21} - 2B_{11}$. However, $\mathcal{B}$ is reduced and so satisfies $-B_{11} < B_{12} + B_{21} \leqslant B_{11}$. This implies $-3B_{11} < B_{12} + B_{21} - 2B_{11} \leqslant B_{11}$, contradicting $\mathcal{C}$ being reduced.
Hence $M = \pm \mathrm{I}_2$ and thus we must have $C_{12} + C_{21} = B_{12} + B_{21}$. Then Lemma 2.4.6 yields $C_{12} - C_{21} = B_{12} - B_{21}$ and solving these equations simultaneously gives $C_{12} = B_{12}$ and $C_{21} = B_{21}$.
Hence $\mathcal{B} = \mathcal{C}$ and thus $\mathcal{A}$ is properly equivalent to a unique reduced bilinear form when $B_{11} < B_{22}$.
Hence every positive definite bilinear form is properly equivalent to a unique reduced bilinear form. □

We now use our theory of reduced bilinear forms to show a parallel result for binary quadratic forms.

Lemma 2.4.25.
Let $\mathcal{B}$ be a reduced bilinear form. Then its associated binary quadratic form $A_{\mathcal{B}}$ is reduced. Further, if $\mathcal{B}$ is positive (negative) definite then $A_{\mathcal{B}}$ is positive (negative) definite.

Proof.
Let $\mathcal{B}$ be a reduced bilinear form with matrix representation $\begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix}$. Then we have $-|A_{11}| < A_{12} + A_{21} \leqslant |A_{11}| < |A_{22}|$ or $0 \leqslant A_{12} + A_{21} \leqslant |A_{11}| = |A_{22}|$.
The associated binary quadratic form is $A_{\mathcal{B}} = A_{11}x^2 + 2\left(\frac{A_{12}+A_{21}}{2}\right)xy + A_{22}y^2$. From Definition 2.4.14 we require either $-|A_{11}| < A_{12} + A_{21} \leqslant |A_{11}| < |A_{22}|$ or $0 \leqslant A_{12} + A_{21} \leqslant |A_{11}| = |A_{22}|$. But these are the exact conditions that define $\mathcal{B}$ as a reduced bilinear form. Hence $A_{\mathcal{B}}$ is reduced.
Now assume $\mathcal{B}$ is positive (negative) definite and thus $A_{11}A_{22} > 0$ and $A_{11} > 0$ ($A_{11} < 0$). From Lemma 2.4.11 it remains to show in either case that $\det(A_{\mathcal{B}}) > 0$. We have $\det(A_{\mathcal{B}}) = \left(A_{11}A_{22} - \frac{A_{12}+A_{21}}{2}\right)^2$ and since $\mathcal{B}$ is reduced, we have $0 \leqslant (A_{12} + A_{21})^2 \leqslant A_{11}A_{22}$. Hence $\det(A_{\mathcal{B}}) \geqslant 0$ with equality if and only if $\frac{A_{12}+A_{21}}{2} = A_{12} + A_{21} = A_{11} =$

$A_{22} = 0$. That is $\mathcal{B}$ would have to be a skew-symmetric bilinear form, contradicting $\mathcal{B}$ being a definite form. □

Corollary 2.4.26.
Every positive definite binary quadratic form $f = ax^2 + 2bxy + cy^2$ is properly equivalent to a unique reduced binary quadratic form.

Proof.
By Lemma 2.4.9 we know these binary quadratic forms are a subset of the bilinear forms. From Lemma 2.4.24 we know f is properly equivalent to a unique positive definite bilinear form. We now show this bilinear form is in fact a binary quadratic form. In Theorem 2.4.23 we demonstrated one can reduce a bilinear form via a sequence of the transformations $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ and $U(q)$'s for some $q \in 2\mathbb{Z}$. Using Observation 2.4.5 we see the first transformation yields a bilinear form with "A_{12}" $= -A_{21}$ and "A_{21}" $= -A_{12}$. Since we started with a binary quadratic form we had $A_{12} = A_{21}$ and thus we see the first transformation preserves binary quadratic forms. Again by Observation 2.4.5 transformations of the type $U(q)$ yield a bilinear form with "A_{12}" $= A_{12} + qA_{11}$ and "A_{21}" $= A_{21} + qA_{11}$. Since we started with a binary quadratic form we have $A_{12} = A_{21}$ and thus "A_{12}" $=$ "A_{21}" so these transformations preserve binary quadratic forms.
Hence since these transformations are sufficient to transform any bilinear form to a reduced bilinear form which, by Theorem 2.4.24, is unique, we have shown every positive definite binary quadratic form is properly equivalent to a unique reduced binary quadratic form. □

For the remainder of this section we will assume $\mathcal{A}$ is a positive definite reduced bilinear form with determinant D. We now develop bounds for the coefficients of such a bilinear form and use this to show there are finitely many such bilinear forms. It will be useful to recall $xy \leqslant (\frac{x+y}{2})^2$ for all real numbers x and y.

Lemma 2.4.27.
The bilinear form $\mathcal{A}$ satisfies $0 < A_{11} \leqslant \sqrt{\frac{4D}{3}}$.

Proof.
We have $4A_{11}A_{22} - 4D = 4A_{12}A_{21} \leqslant (A_{12} + A_{21})^2 \leqslant A_{11}^2$. Consequently, we get $3A_{11}^2 = 4A_{11}^2 - A_{11}^2 \leqslant 4A_{11}A_{22} - A_{11}^2 \leqslant 4D$. Since $0 < A_{11}$ this yields $0 < A_{11}^2 \sqrt{\frac{4D}{3}}$. □

Lemma 2.4.28.
The bilinear form $\mathcal{A}$ satisfies $-D < A_{12}A_{21} \leqslant \frac{D}{3}$.

Proof.
From Lemma 2.4.27 we have $4A_{12}A_{21} \leqslant (A_{12} + A_{21})^2 \leqslant A_{11}^2 \leqslant \frac{4D}{3}$ and thus $A_{12}A_{21} \leqslant \frac{D}{3}$. We also have $-A_{12}A_{21} = D - A_{11}A_{22} < D$ as $A_{11}A_{22} > 0$ by the definiteness of our bilinear forms. Hence we have $-D < A_{12}A_{21} \leqslant \frac{D}{3}$. □

Lemma 2.4.29.
The bilinear form $\mathcal{A}$ satisfies $A_{11}^2 \leqslant A_{11}A_{22} \leqslant \sqrt{\frac{4D}{3}}$.

Proof.
From Lemmas 2.4.27 and 2.4.28 we have $A_{11}A_{22} - D = A_{12}A_{21} \leqslant \frac{D}{3}$. By the reduced criteria it then follows that $A_{11}^2 \leqslant A_{11}A_{22} \leqslant \frac{4D}{3}$. □

Lemma 2.4.30.
The bilinear form $\mathcal{A}$ satisfies $A_{22} \leqslant \frac{A_{11}}{4} + \frac{D}{A_{11}}$ and $A_{22} \leqslant D$.

Proof.
From the proof of Lemma 2.4.28 we have $A_{11}A_{22} = A_{12}A_{21} + D \leqslant \frac{A_{11}^2}{4} + D$. Since $A_{11} > 0$, dividing yields $A_{22} \leqslant \frac{A_{11}}{4} + \frac{D}{A_{11}}$. By Lemma 2.4.27 we know $1 \leqslant A_{11} \leqslant \sqrt{\frac{4D}{3}}$. Since the function $f(x) = \frac{x}{4} + \frac{D}{x}$ is decreasing on the interval $1 \leqslant x \leqslant \sqrt{\frac{4D}{3}}$, it follows that $A_{22} \leqslant \frac{A_{11}}{4} + \frac{D}{A_{11}} \leqslant \frac{1}{4} + D$. Since A_{22}, D are integers it follows that $A_{22} \leqslant D$. □

Lemma 2.4.31.
The bilinear form $\mathcal{A}$ satisfies $|A_{12} - A_{21}| \leqslant 2\sqrt{D}$.

Proof.
Applying Proposition 2.4.28 we have

$$\begin{aligned}(A_{12} - A_{21})^2 &= (A_{12} + A_{21})^2 - 4A_{12}A_{21} \\ &\leqslant A_{11}A_{22} - 4A_{12}A_{21} \\ &= D - 3A_{12}A_{21} \\ &\leqslant D + 3D \\ &= 4D.\end{aligned}$$

Therefore $|A_{12} - A_{21}| \leqslant 2\sqrt{D}$. □

Lemma 2.4.32.
The bilinear form $\mathcal{A}$ satisfies $|A_{12}|$, $|A_{21}| \leqslant \sqrt{\frac{4D}{3}}$.

Proof.
By Lemma 2.4.31 we may write $A_{12} = r\sqrt{D}$ and $A_{21} = s\sqrt{D}$ where r, s are real numbers. Then using the reduced criteria we have
$A_{22} \geqslant A_{11} \geqslant A_{12} + A_{21} = (r+s)\sqrt{D}$. Consider the bilinear form

$$B = \begin{pmatrix} (r+s)\sqrt{D} & r\sqrt{D} \\ s\sqrt{D} & (r+s)\sqrt{D} \end{pmatrix}.$$

Then $\det(B) = ((r+s)^2 - rs)\, D \leqslant A_{11}A_{22} - A_{12}A_{21} = D$. From this it follows that $r^2+rs+s^2 \leqslant 1$. To maximise $|A_{12}|$ requires finding the maximal real number $|r|$ where this inequality holds. We have $s^2+rs+(r^2-1) \leqslant 0$ if and only $(2s+r)^2+(3r^2-4) \leqslant 0$. Therefore $3r^2 - 4 \leqslant 0$ and hence $r^2 \leqslant \frac{4}{3}$. Thus $|A_{12}| = |r|\sqrt{D} \leqslant \sqrt{\frac{4D}{3}}$. Rewriting the initial inequality as $r^2 + rs + (s^2 - 1) \leqslant 0$ and proceeding in an identical manner then yields $|A_{21}| \leqslant \sqrt{\frac{4D}{3}}$. □

Corollary 2.4.33.
There are finitely many positive definite reduced bilinear forms with determinant D.

Proof.
In Lemma 2.4.27 we have shown $0 < A_{11} \leqslant \sqrt{\frac{4D}{3}}$ and in Lemma 2.4.30 we showed $0 < A_{22} \leqslant D$. Lastly, in Lemma 2.4.32 we showed $|A_{12}|$, $|A_{21}| \leqslant \sqrt{\frac{4D}{3}}$. Therefore there are finitely many choices for each of A_{11}, A_{12}, A_{21} and A_{22} for a fixed determinant D. Hence there are only finitely many reduced bilinear forms. □

We now provide several examples which show these bounds are optimal.

Example 2.4.34.
Let $D = 3n^2$ for some integer n. Then the bilinear form $B = \begin{pmatrix} \sqrt{\frac{4D}{3}} & \sqrt{\frac{D}{3}} \\ \sqrt{\frac{D}{3}} & \sqrt{\frac{4D}{3}} \end{pmatrix}$ is reduced with determinant D. This example shows that Lemma 2.4.27, the second inequality of Lemma 2.4.28, Lemma 2.4.29 and the first inequality in Lemma 2.4.30 are optimal.

Example 2.4.35.
Assume r is a rational number such that rD and $(1-r)D$ are both squares of integers. For example, let $r = \frac{a^2}{a^2+b^2}$ and $D = (a^2+b^2)n^2$ where a, b, $n \in \mathbb{Z}$. Then the bilinear form $B = \begin{pmatrix} \sqrt{(1-r)D} & \sqrt{rD} \\ -\sqrt{rD} & \sqrt{(1-r)D} \end{pmatrix}$ is a reduced bilinear form with determinant D. We have $A_{12} - A_{21} = 2\sqrt{rD}$ and $A_{12}A_{21} = -rD$. We can make r arbitrarily close to 1 by choosing a sufficiently large and letting $b = 1$. This shows Lemma 2.4.31 and the first inequality in Lemma 2.4.28 are optimal.

Example 2.4.36.
Consider the bilinear form $B = \begin{pmatrix} 1 & 1 \\ 0 & D \end{pmatrix}$. This is a reduced bilinear form with determinant D and that the second inequality in Lemma 2.4.30 is optimal.

Example 2.4.37.
Assume $D = 3n^2$ for some integer n. Then the bilinear form $B = \begin{pmatrix} \sqrt{\frac{D}{3}} & \sqrt{\frac{4D}{3}} \\ -\sqrt{\frac{D}{3}} & \sqrt{\frac{D}{3}} \end{pmatrix}$ is a reduced bilinear form with determinant D. This example shows Lemma 2.4.32 is optimal.

We now demonstrate in detail how to calculate the proper class number for bilinear forms with determinants $D = 1$, $D = 2$, $D = 3$, $D = 4$ and $D = 6$ respectively. These results will be used later in Section 4.5.

Example 2.4.38.
We wish to determine all positive definite reduced bilinear forms with determinant

$D = 1$. From above we see $0 < A_{11} \leqslant \sqrt{\frac{4\cdot 1}{3}} < 2$, $0 < A_{22} \leqslant 1$ and $|A_{12}|$, $|A_{21}| \leqslant \sqrt{\frac{4}{3}}$. Therefore $A_{11} = A_{22} = 1$. Hence $A_{12}A_{21} = 0$ and therefore we get precisely three reduced bilinear forms:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

Example 2.4.39.
Our goal is to find all positive definite reduced bilinear forms of determinant $D = 2$. From above we see $0 < A_{11} \leqslant \sqrt{\frac{4\cdot 2}{3}} < 3$, $0 < A_{22} \leqslant 2$ and $|A_{12}|$, $|A_{21}| \leqslant \sqrt{\frac{8}{3}}$. Thus $A_{11} = 1$ or 2.
Case 1: $A_{11} = 1$
Then $2 = D = A_{22} - A_{12}A_{21}$, if $A_{22} = 1$, then $A_{12}A_{21} = -1$ and thus $A_{12} = \pm 1$, $A_{21} \mp 1$. It is then straightforward to check that $\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$ are the only reduced bilinear forms.
Now if $A_{22} = 2$ then $A_{12}A_{21} = 0$ and using the conditions for being reduced we see that $\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$, $\begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ 1 & 2 \end{pmatrix}$ are the only reduced bilinear forms.
Case 2: $A_{22} = 2$
Then $2 = D = 4 - A_{12}A_{21}$ and thus $A_{12}A_{21} = 2$. Therefore either $A_{12} = 2$, $A_{21} = 1$ or $A_{12} = 1$ and $A_{21} = 2$. However, both of these options yield $A_{12} + A_{21} > A_{11}$. Therefore this case does not contribute any reduced bilinear forms.
By Theorem 2.4.24 every bilinear form is properly equivalent to a unique reduced bilinear form. Since we have five distinct reduced bilinear forms it follows that none of these are properly equivalent to another. Therefore since every proper equivalence class contains a unique reduced bilinear form, it follows that $\mathrm{Cl}_+(2) = 5$.

Example 2.4.40.
Our goal is to find all positive definite reduced bilinear forms of determinant $D = 3$. From above we see $0 < A_{11} \leqslant \sqrt{\frac{4\cdot 3}{3}} = 2$, $0 < A_{22} \leqslant 3$ and $|A_{12}|$, $|A_{21}| \leqslant 2$. Thus $A_{11} = 1$ or 2.
Case 1: $A_{11} = 1$
Then A_{22} is either 1, 2 or 3. If $A_{22} = 1$ then we must have $A_{12}A_{21} = -2$ and then the reduced criterion implies $A_{12} = 2$ and $A_{21} = -1$. Since we may interchange the roles of A_{12} and A_{21} this gives rise to two reduced forms. Next, if $A_{22} = 2$ then $A_{12}A_{21} = -1$ and therefore $A_{12} = 1$ and $A_{21} = -1$ or vice versa. This yields another two reduced forms. Lastly, if $A_{22} = 3$ then $A_{12}A_{21} = 0$ and we get three reduced forms which correspond to $(A_{12}, A_{21}) = (0,0)$, $(1,0)$ and $(0,1)$.
Case 2: $A_{11} = 2$
Then $A_{22} = 2$ or 3. If $A_{22} = 2$ then we have $A_{12}A_{21} = 1$ and then the reduced criterion yields a single reduced form with $A_{12} = 1 = A_{21}$. While if $A_{22} = 3$ then $A_{12}A_{21} = 2$ and there are no integers with this property that also satisfy $A_{12} + A_{21} \leqslant A_{11}$.
Hence the set of positive definite reduced bilinear forms with determinant $D = 3$ is

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & -1 \\ 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ -1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ -1 & 2 \end{pmatrix}, \right.$$

$$\left(\begin{array}{cc} 1 & -1 \\ 1 & 2 \end{array} \right), \left(\begin{array}{cc} 2 & 1 \\ 1 & 2 \end{array} \right) \Big\}.$$

Therefore $\mathrm{Cl}_+(3) = 8 = 2 \cdot 3 + 2$.

Example 2.4.41.
We want to find all positive definite reduced bilinear forms of determinant $D = 4$. From above we see $0 < A_{11} \leqslant \sqrt{\frac{4 \cdot 4}{3}} < 3$, $0 < A_{22} \leqslant \min\{4, \frac{A_{11}}{4} + \frac{D}{A_{11}}$, and $|A_{12}|$, $|A_{21}| \leqslant \sqrt{\frac{4 \cdot 4}{3}} < 3$. Thus $A_{11} = 1$ or $A_{11} = 2$.
Case 1: $A_{11} = 1$.
Then $A_{22} \in \mathbb{Z} \cap [1, 4]$ and for each value of A_{22} we examine $A_{12}A_{21} = 1 \cdot A_{22} - D$. Using the bounds for $|A_{12}|$ and $|A_{21}|$ we get the following reduced bilinear forms

$$\left(\begin{array}{cc} 1 & 0 \\ 0 & 4 \end{array} \right), \left(\begin{array}{cc} 1 & 1 \\ -1 & 3 \end{array} \right), \left(\begin{array}{cc} 1 & -1 \\ 1 & 3 \end{array} \right), \left(\begin{array}{cc} 1 & 2 \\ -1 & 2 \end{array} \right), \left(\begin{array}{cc} 1 & -1 \\ 2 & 2 \end{array} \right), \left(\begin{array}{cc} 1 & 0 \\ 1 & 4 \end{array} \right), \left(\begin{array}{cc} 1 & 1 \\ 0 & 4 \end{array} \right).$$

Case 2: $A_{11} = 2$
Then it follows $A_{22} = 2$ and we have the following reduced bilinear forms:

$$\left(\begin{array}{cc} 2 & 0 \\ 0 & 2 \end{array} \right), \left(\begin{array}{cc} 2 & 0 \\ 1 & 2 \end{array} \right), \left(\begin{array}{cc} 2 & 1 \\ 0 & 2 \end{array} \right), \left(\begin{array}{cc} 2 & 2 \\ 0 & 2 \end{array} \right), \left(\begin{array}{cc} 2 & 0 \\ 2 & 2 \end{array} \right).$$

Now we have considered all possible values for A_{11} and A_{22} with their associated values for A_{12} and A_{21} and therefore we have found all positive definite reduced bilinear forms with determinant $D = 4$. Since every proper equivalence class contains a unique reduced bilinear form and every bilinear form is properly equivalent to a unique reduced bilinear form, we deduce $\mathrm{Cl}_+(4) = 12 = 2D + 4$.

Example 2.4.42.
We want to find all positive definite reduced bilinear forms of determinant $D = 6$. From above we see $0 < A_{11} \leqslant \sqrt{\frac{4 \cdot 6}{3}} = \sqrt{8} < 3$, $0 < A_{22} \leqslant \min\{6, \frac{A_{11}}{4} + \frac{D}{A_{11}}\}$ and $|A_{12}|$,$|A_{21}| \leqslant \sqrt{\frac{4 \cdot 6}{3}} < 3$. Thus $A_{11} = 1$ or $A_{11} = 2$.
Case 1: $A_{11} = 1$.
Then $A_{22} \in \mathbb{Z} \cap [1, 6]$ and for each value of A_{22} we examine $A_{12}A_{21} = 1 \cdot A_{22} - D$. Using the bounds for $|A_{12}|$ and $|A_{21}|$ we get the following reduced bilinear forms for $A_{22} \in \{2, 4, 5\}$

$$\left(\begin{array}{cc} 1 & 2 \\ -2 & 2 \end{array} \right), \left(\begin{array}{cc} 1 & -2 \\ 2 & 2 \end{array} \right), \left(\begin{array}{cc} 1 & 2 \\ -1 & 4 \end{array} \right), \left(\begin{array}{cc} 1 & -1 \\ 2 & 4 \end{array} \right), \left(\begin{array}{cc} 1 & 1 \\ -1 & 5 \end{array} \right), \left(\begin{array}{cc} 1 & -1 \\ 1 & 5 \end{array} \right).$$

Lastly when $A_{22} = 6$ we require at least one of A_{12}, A_{21} to equal zero. Thus we get the following three reduced bilinear forms

$$\left(\begin{array}{cc} 1 & 0 \\ 0 & 6 \end{array} \right), \left(\begin{array}{cc} 1 & 0 \\ 1 & 6 \end{array} \right), \left(\begin{array}{cc} 1 & 1 \\ 0 & 6 \end{array} \right).$$

Case 2: $A_{11} = 2$
Then it follows A_{22} is either 2 or 3. When $A_{22} = 2$ we get the following reduced bilinear forms

$$\begin{pmatrix} 2 & 2 \\ -1 & 2 \end{pmatrix}, \begin{pmatrix} 2 & -1 \\ 2 & 2 \end{pmatrix}.$$

While when $A_{22} = 3$ we require at least one of A_{12}, A_{21} to be zero and therefore we get

$$\begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 1 & 3 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ -1 & 3 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 2 & 3 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 0 & 3 \end{pmatrix}, \begin{pmatrix} 2 & -1 \\ 0 & 3 \end{pmatrix}, \begin{pmatrix} 2 & 2 \\ 0 & 3 \end{pmatrix}.$$

Now we have considered all possible values for A_{11} and A_{22} with their associated values for A_{12} and A_{21} and therefore we have found all positive definite reduced bilinear forms with determinant $D = 6$. Since every proper equivalence class contains a unique reduced bilinear form and every bilinear form is properly equivalent to a unique reduced bilinear form, we deduce $\mathrm{Cl}_+(6) = 18 = 2D + 6$.

Notes on Section 2.4

In chapter 9 of his paper ([Kr1897, p. 452]), Kronecker introduces bilinear forms by stating them in general as $Ax_1y_1 + Bx_1y_2 - Cx_2y_1 + Dx_2y_2$. For ease of exposition, we will avoid this, instead choosing to write $A_{11}x_1y_1 + A_{12}x_1y_2 + A_{21}x_2y_1 + A_{22}x_2y_2$ or even $(A_{11}, A_{12}, A_{21}, A_{22})$ in shorthand.

2.5 Automorphs of Bilinear Forms

In this subsection we turn our considerations to understanding when a proper equivalence class of a bilinear form contains exactly six complete equivalence classes. In order to do this we will develop the theory of bilinear automorphs by following the approach found in [NZM1991, p. 173] and [Fl1989, p. 125] for binary quadratic forms.

We will first investigate the existence of proper and improper automorphs of positive definite reduced bilinear forms. By reduced we will mean the definition given in Definition 2.4.14.
Let $\mathcal{B}$ be a reduced bilinear form with matrix representation $A = \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix}$. Let $M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$.

Definition 2.5.1.
Let $\mathcal{A}$ be a bilinear form. A matrix $M \in \mathrm{GL}_2(\mathbb{Z})$ is called an **automorph** of $\mathcal{A}$ if $M^tAM = A$ where A is the matrix representation of $\mathcal{A}$. We refine the notion to that of an **improper automorph** if $M \in \mathrm{GL}_2(\mathbb{Z})\backslash\mathrm{SL}_2(\mathbb{Z})$, a **proper automorph** if $M \in \mathrm{SL}_2(\mathbb{Z})$ and a **complete automorph** if $M \in \ker\sigma$.

Notation 2.5.2.
Let $\mathcal{A}$ be a bilinear form. We shall write $\mathrm{Aut}(\mathcal{A})$ to denote the set of all automorphs of $\mathcal{A}$, $\mathrm{Aut}^+(\mathcal{A})$ to denote the set of all proper automorphs of $\mathcal{A}$, and $\mathrm{Aut}_c^+(\mathcal{A})$ to denote the set of all complete automorphs of $\mathcal{A}$. We let $|\mathrm{Aut}(\mathcal{A})|$, $|\mathrm{Aut}^+(\mathcal{A})|$ and $|\mathrm{Aut}_c^+(\mathcal{A})|$ denote their respective cardinalities.

The following lemma will be useful when investigating the automorphism groups.

Lemma 2.5.3.
Let G_1, G_2 be groups, $H_1 \leqslant G_1$ and $\tau : G_1 \to G_2$ be a group homomorphism. Then $H_1 \cap \ker\tau \trianglelefteq H_1$.

Proof.
Consider the homomorphism $\tau\Big|_{H_1} : H_1 \to G_2$. Then $\ker\tau\Big|_{H_1} = H_1 \cap \ker\tau$. □

Lemma 2.5.4.
Let $\mathcal{A}$ be a bilinear form. Then $\mathrm{Aut}(\mathcal{A})$ is a subgroup of $\mathrm{GL}_2(\mathbb{Z})$ and $\mathrm{Aut}^+(\mathcal{A})$ is a normal subgroup of $\mathrm{Aut}(\mathcal{A})$. Lastly, $\mathrm{Aut}_c^+(\mathcal{A})$ is a normal subgroup of $\mathrm{Aut}(\mathcal{A})$.

Proof.
Observe that $\pm I \in \mathrm{Aut}_c^+(\mathcal{A}) \subseteq \mathrm{Aut}^+(\mathcal{A}) \subseteq \mathrm{Aut}(\mathcal{A})$. Now suppose that $B, C \in \mathrm{Aut}(\mathcal{A})$, then $B^{-1} \in \mathrm{Aut}(\mathcal{A})$ since $B^tAB = A$ implies that $A = (B^{-1})^tAB^{-1}$. It follows that $BC^{-1} \in \mathrm{Aut}(\mathcal{A})$ since

$$\begin{aligned}(BC^{-1})^tA(BC^{-1}) &= (C^{-1})^tB^tABC^{-1}\\ &= (C^{-1})^tAC^{-1}\\ &= A.\end{aligned}$$

Hence $\mathrm{Aut}(\mathcal{A})$ is a subgroup of $\mathrm{GL}_2(\mathbb{Z})$.

Now observe that $\mathrm{Aut}^+(\mathcal{A}) = \mathrm{Aut}(\mathcal{A}) \cap \mathrm{SL}_2(\mathbb{Z})$ and $\mathrm{Aut}_c^+(\mathcal{A}) = \mathrm{Aut}(\mathcal{A}) \cap \ker\sigma$. Since the intersection of two subgroups is again a subgroup, we have $\mathrm{Aut}^+(\mathcal{A})$ is a subgroup of $\mathrm{Aut}(\mathcal{A})$ and $\mathrm{Aut}_c^+(\mathcal{A})$ is a subgroup of $\mathrm{Aut}(\mathcal{A})$.

Next, consider the homomorphisms det and σ (from Lemma 2.3.2 with $n = 2$). Then the restrictions:
$\det\Big|_{\mathrm{Aut}(\mathcal{A})} : \mathrm{Aut}(\mathcal{A}) \longrightarrow \{\pm 1\}$ given by $M \mapsto \det(M)$, and
$\sigma\Big|_{\mathrm{Aut}(\mathcal{A})} : \mathrm{Aut}(\mathcal{A}) \longrightarrow (\{\pm 1\}, \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}))$,
along with Lemma 2.5.3 yield the result. □

We observed in the proof of Lemma 2.5.4 that $|\mathrm{Aut}_c^+(\mathcal{A})| \geqslant 2$ for all $\mathcal{A}$. This is because $\pm I \in \mathrm{Aut}_c^+(\mathcal{A})$.

Lemma 2.5.5.
Let $\mathcal{A}$ and $\mathcal{B}$ be equivalent bilinear forms. The automorphs of $\mathcal{A}$ are in one-to-one correspondence with the matrices that transform $\mathcal{A}$ to $\mathcal{B}$.

Proof.
Let $\mathcal{T}(\mathcal{A},\mathcal{B}) = \{M \in \mathrm{GL}_2(\mathbb{Z}) | M^tAM = B\}$. Since $\mathcal{A}$ and $\mathcal{B}$ are equivalent bilinear forms it follows $\mathcal{T}(\mathcal{A},\mathcal{B})$ is non-empty. We now fix an $M \in \mathcal{T}(\mathcal{A},\mathcal{B})$ and consider the map $\lambda : \mathrm{Aut}(\mathcal{A}) \to \mathcal{T}(\mathcal{A},\mathcal{B})$ given by $\lambda(K) = KM$.
We show λ is a bijection and hence there is a one-to-one correspondence between the automorphs of $\mathcal{A}$ and matrices that transform A into B.
(1) $KM \in \mathcal{T}(\mathcal{A},\mathcal{B})$ since $(KM)^tA(KM) = M^t(K^tAK)M = M^tAM = B$.
(2) Surjectivity: Choose $M' \in \mathcal{T}(\mathcal{A},\mathcal{B})$ then $M'M^{-1}$ is an automorph of $\mathcal{A}$ since $(M'M^{-1})^tA(M'M^{-1}) = (M^{-1})^tBM^{-1} = A$ and $M^{-1} \in \mathcal{T}(\mathcal{B},\mathcal{A})$.
Then $\lambda(M'M^{-1}) = M'$ and so the map is surjective.
(3) Injectivity: Suppose that $KM = K'M$ for some $K, K' \in \mathrm{Aut}(\mathcal{A})$. Since M is invertible, we must have $K = K'$, i.e. λ is injective.
Further, if $\mathcal{A}$ and $\mathcal{B}$ are properly equivalent, then we replace $\mathcal{T}(\mathcal{A},\mathcal{B})$ with $\mathcal{T}^+(\mathcal{A},\mathcal{B}) = \{M \in \mathrm{SL}_2(\mathbb{Z}) | M^tAM = B\}$ and replace $\mathrm{Aut}(\mathcal{A})$ with $\mathrm{Aut}^+(\mathcal{A})$. The same proof then yields a bijection between $\mathrm{Aut}^+(\mathcal{A})$ and $\mathcal{T}^+(\mathcal{A},\mathcal{B})$.
Similarly, if $\mathcal{A}$ and $\mathcal{B}$ are completely equivalent, one can replace $\mathcal{T}(\mathcal{A},\mathcal{B})$ with $\mathcal{T}_c^+(\mathcal{A},\mathcal{B}) = \{M \in \ker\sigma | M^tAM = B\}$ and replace $\mathrm{Aut}(\mathcal{A})$ with $\mathrm{Aut}_c^+(\mathcal{A})$. The same proof then yields a bijection between $\mathrm{Aut}_c^+(\mathcal{A})$ and $\mathcal{T}_c^+(\mathcal{A},\mathcal{B})$. □

It remains to show $|\mathrm{Aut}(\mathcal{A})|$ is a finite group for any bilinear form $\mathcal{A}$. The next three lemmas provide a stepping stone in this direction.

Lemma 2.5.6.
Let $\mathcal{A}$ and $\mathcal{B}$ be equivalent bilinear forms, then $\mathrm{Aut}(\mathcal{A}) \cong \mathrm{Aut}(\mathcal{B})$.

Proof.
Let $M \in \mathrm{GL}_2(\mathbb{Z})$ be such that $M^tAM = B$. Define $\tau : \mathrm{Aut}(\mathcal{A}) \to \mathrm{Aut}(\mathcal{B})$ by $\tau(K) = M^{-1}KM$. We show that τ is a group isomorphism.
Firstly, observe that $\tau(K) \in \mathrm{Aut}(\mathcal{B})$ since $(M^{-1}KM)^tB(M^{-1}KM) = M^tK^tAKM = B$. To show surjectivity, let $M' \in \mathrm{Aut}(\mathcal{B})$ and so $(M')^tBM' = B$. Also, observe that M is invertible and $MM'M^{-1} \in \mathrm{Aut}(\mathcal{A})$ since $(MM'M^{-1})^tA(MM'M^{-1}) = (M^{-1})^tM'^tBM'M^{-1} = (M^{-1})^tBM^{-1} = A$.
Then $\tau(MM'M^{-1}) = M^{-1}(MM'M^{-1})M = M'$ and so τ is surjective.
For injectivity suppose $K, L \in \mathrm{Aut}(\mathcal{A})$ and $M^{-1}KM = M^{-1}LM$. Since M and M^{-1} are invertible, it follows that $K = L$ and so τ is injective.
Lastly, τ is a homomorphism since for $K, L \in \mathrm{Aut}(\mathcal{A})$ we have $\tau(KL) = M^{-1}KLM = (M^{-1}KM)(M^{-1}LM) = \tau(K)\tau(L)$. Hence τ is an isomorphism of groups and so $\mathrm{Aut}(\mathcal{A})$ is isomorphic to $\mathrm{Aut}(\mathcal{B})$. □

Lemma 2.5.7.
Let $\mathcal{A}$ and $\mathcal{B}$ be properly equivalent bilinear forms.
Define $\tau^+ : \mathrm{Aut}^+(\mathcal{A}) \to \mathrm{Aut}^+(\mathcal{B})$ by $\tau^+(K) = M^{-1}KM$ where $M \in \mathrm{SL}_2(\mathbb{Z})$ is such that $M^tAM = B$. That is, τ^+ is the restriction of the domain of τ to $\mathrm{Aut}^+(\mathcal{A})$. We show τ^+ is a group isomorphism.

Proof.
From above, restricting the domain of τ to $\mathrm{Aut}^+(\mathcal{A})$ still maps into $\mathrm{Aut}(\mathcal{B})$. Since

$M \in \mathrm{SL}_2(\mathbb{Z})$ and $\mathrm{Aut}^+(\mathcal{B}) = \mathrm{Aut}(\mathcal{B}) \cap \mathrm{SL}_2(\mathbb{Z})$ it follows that the map is actually into $\mathrm{Aut}^+(\mathcal{B})$. The result then follows as in the proof of Lemma 2.5.6. Hence τ^+ is a group isomorphism and so $\mathrm{Aut}^+(\mathcal{A})$ is isomorphic to $\mathrm{Aut}^+(\mathcal{B})$. □

Corollary 2.5.8.
Let $\mathcal{A}$ and $\mathcal{B}$ be completely equivalent bilinear forms. Then the map $\tau_c^+ : \mathrm{Aut}_c^+(\mathcal{A}) \to \mathrm{Aut}_c^+(\mathcal{B})$ given by $\tau_c^+(K) = M^{-1}KM$, where $M \in \ker\sigma$ satisfies $M^tAM = B$, is an isomorphism.

Proof.
We restrict the domain of τ to $\mathrm{Aut}_c^+(\mathcal{A})$. This still maps into $\mathrm{Aut}(\mathcal{B})$ and we observe $\mathrm{Aut}_c^+(\mathcal{B}) = \mathrm{Aut}(\mathcal{B}) \cap \ker\sigma$. Since $M \in \ker\sigma$ it follows that τ_c^+ maps into $\mathrm{Aut}_c^+(\mathcal{B})$. The result then follows as in the proof of Lemma 2.5.6. Hence τ_c^+ is a group isomorphism and so $\mathrm{Aut}_c^+(\mathcal{A})$ is isomorphic to $\mathrm{Aut}_c^+(\mathcal{B})$. □

We now show the three automorphism groups are finite by directly calculating the improper and proper automorphs of a reduced bilinear form. Lemmas 2.5.6 and 2.5.7 then show the automorphism groups are finite for any bilinear form.

We first investigate whether any improper automorphs exist.
Improper Automorphs:
Assume $\det(M) = -1$ and that $M^tAM = A$. Using Observation 2.4.5 (I), we get the following system of equations

$$(\alpha+\delta)A_{11} - \gamma(A_{12} - A_{21}) = 0 \tag{2.6}$$
$$\beta A_{11} - 2\alpha A_{12} - \gamma A_{22} = 0 \tag{2.7}$$
$$\beta A_{11} + 2\delta A_{21} - \gamma A_{22} = 0 \tag{2.8}$$
$$(\alpha+\delta)A_{22} + \beta(A_{12} - A_{21}) = 0 \tag{2.9}$$
$$\alpha\delta - \beta\gamma = -1. \tag{2.10}$$

Case I: $\alpha + \delta = 0$
We first suppose $\alpha + \delta = 0$, then $\delta = -\alpha$. This implies $-1 = -\alpha^2 - \beta\gamma$, i.e. $\alpha^2 + \beta\gamma = 1$. Then Equations 2.6 and 2.9 imply either $A_{12} - A_{21} = 0$ or $\beta = \gamma = 0$.

Case I.a: $\beta = \gamma = 0$
If $\beta = \gamma = 0$ then we have $\alpha = \pm 1$ and $\delta = \mp 1$. Further, Equations 2.7 and 2.8 imply $A_{12} = A_{21} = 0$. Thus we have $M = \pm \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ is an improper automorph for $\mathcal{B} = \begin{pmatrix} A_{11} & 0 \\ 0 & A_{22} \end{pmatrix}$.

Case I.b: $A_{12} - A_{21} = 0$, $\beta = 0$ and $\gamma \neq 0$
Now assume $A_{12} - A_{21} = 0$ so $A_{12} = A_{21}$. Observe that Equation 2.7 is now the same as Equation 2.8 since $\delta = -\alpha$. Suppose $\beta = 0$ and $\gamma \neq 0$, else we are in the above case. Then $\alpha = \pm 1$ and $\delta = \mp 1$, and γ is not yet determined.
Equation 2.7 implies $2\alpha A_{12} = -\gamma A_{22}$ and so $2|\alpha||A_{12}| = |\gamma| A_{22}$. But $A_{12} = A_{21}$ and

$|\alpha| = 1$ implies $2\,|\alpha|\,|A_{12}| = |A_{12} + A_{21}|$. Further since $\gamma \neq 0$ and $A_{22} > 0$, we see that $A_{12} \neq 0$. So we have $|A_{12} + A_{21}| = |\gamma|\,A_{22}$ and since $\mathcal{B}$ is reduced, $|A_{12} + A_{21}| \leqslant A_{22}$, which yields $|\gamma| = 1$.
We see that if $\gamma = -\alpha$ then $A_{12} + A_{21} = A_{22}$, so Definition 2.4.14 implies $A_{12} + A_{21} = A_{11} = A_{22}$. Thus $M = \pm \begin{pmatrix} 1 & 0 \\ -1 & -1 \end{pmatrix}$ is an improper automorph to $\mathcal{B} = \begin{pmatrix} 2A_{12} & A_{12} \\ A_{12} & 2A_{12} \end{pmatrix}$.
Now let $\gamma = \alpha$, this implies $A_{12} + A_{21} = -A_{22}$ and since $\mathcal{B}$ is reduced this is clearly impossible.

Case I.c: $A_{12} - A_{21} = 0$, $\beta = 0$ and $\gamma = 0$
Next we suppose $A_{12} - A_{21} = 0$ with $\beta \neq 0$ and $\gamma = 0$. Then $-1 = -\alpha^2$, so $\alpha = \pm 1$ and $\delta = \mp 1$. Again Equations 2.7 and 2.8 are identical and yield $2\alpha A_{12} = \beta A_{11}$. Thus $|A_{12} + A_{21}| = |\beta|\,A_{11}$. Since $\mathcal{B}$ is reduced we have $|\beta| = 1$, and if $\beta = -\alpha$ we have $A_{12} + A_{21} = -A_{11}$, a contradiction. Hence $\beta = \alpha$.
Thus $M = \pm \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}$ is an improper automorph to $\mathcal{B} = \begin{pmatrix} 2A_{12} & A_{12} \\ A_{12} & A_{22} \end{pmatrix}$.

Case I.d: $A_{12} - A_{21} = 0$, $\beta \neq 0$ and $\gamma \neq 0$
To finish the case where $\alpha + \delta = 0$ we suppose $A_{12} - A_{21} = 0$, $\beta \neq 0$, and $\gamma \neq 0$.
Observe $-1 = -\alpha^2 - \beta\gamma$ implies $1 - \alpha^2 = \beta\gamma$. Hence $\alpha \neq \pm 1$ as $\beta\gamma \neq 0$.
If $\alpha = \delta = 0$ then Equation 2.7 implies $A_{11} = A_{22}$ and $M = \pm \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ is an improper automorph to $\mathcal{B} = \begin{pmatrix} A_{11} & A_{12} \\ A_{12} & A_{11} \end{pmatrix}$. Since $\mathcal{B}$ is reduced we require $0 \leqslant 2A_{12} \leqslant A_{11}$.
So suppose $|\alpha| > 1$. This implies $\beta\gamma < 0$ and since β and γ are integers it follows $|\beta - \gamma| \geqslant 2$. Since $A_{11} > 0$ we have

$$0 < 4A_{11}^2 \leqslant (\beta - \gamma)^2 A_{11}^2 \leqslant \beta^2 A_{11}^2 - 2\beta\gamma A_{11}A_{22} + \gamma^2 A_{22}^2 = (\beta A_{11} - \gamma A_{22})^2 . \quad (2.11)$$

Now Equation 2.7 becomes $\beta A_{11} - \gamma A_{22} = 2\alpha A_{12}$ and so

$$\begin{aligned} (\beta A_{11} - \gamma A_{22})^2 &= 4\alpha^2 A_{12}^2 \\ &= 4\,(1 - \beta\gamma)\,A_{12}^2 \text{ via } \det(M) \\ &\leqslant (1 - \beta\gamma)\,A_{11}^2 \text{ as } A_{12} + A_{21} = 2A_{12} \text{ and } |A_{12} + A_{21}| \leqslant A_{11}. \end{aligned}$$

We note that we have a strict inequality if $A_{12} = 0$.
Hence by Equation 2.11 we have $(1 - \beta\gamma)\,A_{11}^2 \geqslant (\beta - \gamma)^2 A_{11}^2$. Dividing by $A_{11}^2 \neq 0$ yields $(\beta - \gamma)^2 \leqslant 1 - \beta\gamma$.
Expanding this gives $\beta^2 - \beta\gamma + \gamma^2 \leqslant 1$. Yet $\beta\gamma < 0$ implies the left hand side is at least 3, a contradiction. Hence $|\alpha| > 1$ cannot occur and the case when $\alpha + \delta = 0$ is complete.

Case II: $\alpha + \delta \neq 0$
Now suppose $\alpha + \delta \neq 0$. If $\beta = 0$ then Equation 2.9 implies $(\alpha + \delta)\,A_{22} = 0$, a

contradiction. If $\gamma = 0$ then Equation 2.6 implies $(\alpha + \delta) A_{11} = 0$, a contradiction. Thus $\beta\gamma \neq 0$.
Similarly observe that Equations 2.6 and 2.9 give the same contradictions if $A_{12} - A_{21} = 0$. Hence $A_{12} - A_{21} \neq 0$.
Using this, Equations 2.6 and 2.9 respectively imply $\gamma = \dfrac{(\alpha + \delta) A_{11}}{A_{12} - A_{21}} \neq 0$ and $\beta = \dfrac{-(\alpha + \delta) A_{22}}{A_{12} - A_{21}} \neq 0$. As a consequence of this and $0 < A_{11}A_{22}$ it follows that $\beta\gamma < 0$. Using the determinant equation, it follows also that $\alpha\delta = -1 + \beta\gamma < 0$.
Next, Equation 2.7 implies $\beta A_{11} - \gamma A_{22} = 2\alpha A_{12}$ and Equation 2.8 implies $\beta A_{11} - \gamma A_{22} = -2\delta A_{21}$. These yield the following:

$$\begin{aligned}(\beta A_{11} - \gamma A_{22})^2 &= -4\alpha\delta A_{12}A_{21} \\ &= 4(1 - \beta\gamma) A_{12}A_{21} \text{ via } \det(M) \\ &= 2(1 - \beta\gamma)(2A_{12}A_{21}) \\ &< 2(1 - \beta\gamma) A_{11}^2.\end{aligned}$$

This strict inequality is justified by the following reasoning.
Consider $0 \leqslant (\beta A_{11} - \gamma A_{22})^2 = -4\alpha\delta A_{12}A_{21}$, note $\alpha\delta < 0$ implies $A_{12}A_{21} \geqslant 0$. Then $A_{12} - A_{21} \neq 0$ implies at least one of A_{12}, A_{21} is not zero.
Hence $0 \leqslant 2A_{12}A_{21} < A_{12}^2 + 2A_{12}A_{21} + A_{21}^2 = (A_{12} + A_{21})^2 \leqslant A_{11}^2$ as $\mathcal{B}$ is reduced.
Next recall that β and γ are integers, and so $\beta\gamma < 0$ implies $|\beta - \gamma| \geqslant 2$. So we have the following inequality:

$$\begin{aligned}0 < 4A_{11}^2 &\leqslant (\beta - \gamma)^2 A_{11}^2 \\ &\leqslant \beta^2 A_{11}^2 - 2\beta\gamma A_{11}A_{22} + \gamma^2 A_{22}^2 \text{ since } \beta\gamma < 0 \text{ and } A_{11}^2 \leqslant A_{11}A_{22} \leqslant A_{22}^2 \\ &= (\beta A_{11} - \gamma A_{22})^2.\end{aligned}$$

Thus we have $(\beta - \gamma)^2 A_{11}^2 < 2(1 - \beta\gamma) A_{11}^2$. Since $A_{11}^2 > 0$, we may divide by it to get $\beta^2 - 2\beta\gamma + \gamma^2 < 2 - 2\beta\gamma$, which implies $\beta^2 + \gamma^2 < 2$. Therefore at least one of β, γ must equal zero, a contradiction. So there are no improper automorphs when $\alpha + \delta \neq 0$.

Now we investigate the proper automorphs.
Proper Automorphs:
Assume $\det(M) = 1$ and that $M^t A M = A$. Using Observation 2.4.5 (I) we get the following system of equations:

$$(\alpha - \delta) A_{11} + \gamma(A_{12} + A_{21}) = 0 \tag{2.12}$$
$$\beta A_{11} + \gamma A_{22} = 0 \tag{2.13}$$
$$(\alpha - \delta) A_{22} - \beta(A_{12} + A_{21}) = 0 \tag{2.14}$$
$$\alpha\delta - \beta\gamma = 1. \tag{2.15}$$

Case I.a: $\alpha - \delta = 0$ and $\gamma = 0$
We first suppose $\alpha - \delta = 0$, i.e. $\alpha = \delta$. Then Equation 2.12 implies $\gamma(A_{12} + A_{21}) = 0$,

so either $\gamma = 0$ or $A_{12}+A_{21} = 0$. Assume $\gamma = 0$, then Equation 2.13 implies $\beta A_{11} = 0$, $A_{11} > 0$ then says $\beta = 0$. Using the determinant equation we see $\alpha = \pm 1$. This gives $M = \pm I_2$.

Case I.b: $\alpha - \delta = 0$, $\gamma \neq 0$ and $A_{12} + A_{21} = 0$
Assume $\gamma \neq 0$, then $A_{12} + A_{21} = 0$. This leaves Equation 2.13 where clearly $\beta \neq 0$ else $\gamma A_{22} = 0$, a contradiction. Therefore we have $A_{11} = -\frac{\gamma}{\beta} A_{22}$ and since we started with a reduced form we have $0 < -\frac{\gamma}{\beta} \leqslant 1$ as $A_{11}A_{22} > 0$. In particular observe β and γ have opposing signs, so $\beta \neq \gamma$. Using Equation 2.15 we have $\beta\gamma = \alpha^2 - 1$.
If $\alpha = 0$ then $\beta\gamma = -1$, which implies $\beta = \pm 1$ and $\gamma = \mp 1$. Further, Equation 2.13 then requires $A_{11} = A_{22}$. Therefore $M = \pm \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ is a proper automorph to $\mathcal{B} = \begin{pmatrix} A_{11} & A_{12} \\ -A_{12} & A_{11} \end{pmatrix}$.
Note that $\alpha \neq \pm 1$ else at least one of β, γ is zero, which is a contradiction. So now assume $|\alpha| > 1$, it follows that $\alpha^2 - 1 = \beta\gamma \geqslant 3$, so β and γ must have the same sign. This contradicts our earlier result that they have opposite signs as neither β or γ are zero.
This completes the case when $\alpha - \delta = 0$.

Case II: $\alpha - \delta \neq 0$
Next suppose $\alpha - \delta \neq 0$. Observe that Equation 2.13 continues to imply if $\beta = 0$ then $\gamma = 0$ and vice versa. This yields $M = \pm I_2$ again. So assume $\beta \neq 0$ and $\gamma \neq 0$. Equation 2.13 again implies $A_{11} = -\frac{\gamma}{\beta} A_{22}$, with γ and β having opposite signs because $0 < A_{11}A_{22}$. Note that by the reduced criteria we have $0 < -\frac{\gamma}{\beta} \leqslant 1$. Also observe that $A_{12} + A_{21} \neq 0$ else Equation 2.12 implies $\alpha - \delta = 0$, a contradiction.
Case II.a: $\alpha - \delta \neq 0$ and $\alpha = 0$
First suppose $\alpha = 0$, then $1 = -\beta\gamma$ implies $\beta = \pm 1$ and $\gamma = \mp 1$. Then Equation 2.13 yields $A_{11} = A_{22}$. Now $\gamma (A_{12} + A_{21}) \neq 0$ and $\beta (A_{12} + A_{21}) \neq 0$ imply $\delta A_{11} = \gamma (A_{12} + A_{21}) \neq 0$ and $\delta A_{22} = -\beta (A_{12} + A_{21}) \neq 0$. Hence $\delta \neq 0$.
Equation 2.12 implies $\delta^2 A_{11}^2 = (A_{12} + A_{21})^2$, and $\mathcal{B}$ reduced implies $(A_{12} + A_{21})^2 \leqslant A_{11}^2$, so we have $(A_{12} + A_{21})^2 \leqslant A_{11}^2 \leqslant \delta^2 A_{11}^2 = (A_{12} + A_{21})^2$. Hence $\delta = \pm 1$.
If $\delta = -\gamma$ then we have $-\gamma A_{11} = \gamma (A_{12} + A_{21})$ and so $-A_{11} = A_{12} + A_{21}$, which contradicts $\mathcal{B}$ being reduced. Hence $\delta = \gamma = \pm 1 = -\beta$ and $A_{12} + A_{21} = A_{11} = A_{22}$. Thus $M = \pm \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$ is a proper automorph to $\mathcal{B} = \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{11} \end{pmatrix}$, where $A_{21} \neq -A_{12}$ and $A_{12} + A_{21} = A_{11} = A_{22}$.

Case II.b: $\alpha - \delta \neq 0$, $\alpha \neq 0$ and $\delta = 0$
Now suppose $\alpha \neq 0$ and $\delta = 0$. Then again we have $1 = -\beta\gamma$, which implies $\beta = \pm 1$ and $\gamma = \mp 1$. Equation 2.13 then yields $A_{11} = A_{22}$. Further, Equation 2.12 implies $\alpha^2 A_{11}^2 = \gamma^2 (A_{12} + A_{21})^2 = (A_{12} + A_{21})^2$. Now $\mathcal{B}$ being reduced implies $(A_{12} + A_{21})^2 \leqslant A_{11}^2$, so again we have $(A_{12} + A_{21})^2 \leqslant A_{11}^2 \leqslant \alpha^2 A_{11}^2 = (A_{12} + A_{21})^2$. Thus $\alpha = \pm 1$. Suppose $\alpha = \gamma$, then Equation 2.12 implies $\gamma A_{11} = -\gamma (A_{12} + A_{21})$, i.e. $-A_{11} = A_{12} + A_{21}$, contradicting $\mathcal{B}$ being reduced.

So $\alpha = -\gamma$ and $A_{12}+A_{21} = A_{11} = A_{22}$. Then we have $M = \pm \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}$ is a proper automorph to $\mathcal{B} = \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{11} \end{pmatrix}$, where $A_{21} \neq -A_{12}$, $A_{12} + A_{21} = A_{11} = A_{22}$.

Case II.c: $\alpha - \delta \neq 0$, $\alpha \neq 0$ and $\delta \neq 0$
Lastly suppose $\alpha \neq 0$ and $\delta \neq 0$. By the determinant we have $\alpha\delta = 1 + \beta\gamma$ and $\beta\gamma < 0$ imply $\alpha\delta < 0$. Thus since α and δ are integers it follows that $|\alpha - \delta| \geqslant 2$.
Next, Equations 2.12 and 2.14 imply $(\alpha - \delta) = -\gamma\,(A_{12} + A_{21})$ and
$(\alpha - \delta) = \beta\,(A_{12} + A_{21})$. Multiplying these together yields the following:

$$\begin{aligned}(\alpha+\delta)^2 &= -\beta\gamma\,(A_{12}+A_{21})^2 \\ &= (1-\alpha\delta)\,(A_{12}+A_{21}) \text{ by the determinant} \\ &\leqslant (1-\alpha\delta)\,A_{11}A_{22} \text{ by reducedness.}\end{aligned}$$

We also have $0 < A_{11}A_{22}$ and $|\alpha - \delta| \geqslant 2$, which imply $0 < 4A_{11}A_{22} \leqslant (\alpha-\delta)^2 A_{11}A_{22}$. Hence using the above result we have $0 < (\alpha-\delta)^2 \leqslant 1-\alpha\delta$. This yields $\alpha^2 - \alpha\delta + \delta^2 \leqslant 1$ and we recall that $\alpha\delta < 0$, thus the left hand side is at least 3 as $\alpha \neq 0$, $\delta \neq 0$. This is a contradiction, so no proper automorph exists in this case.

Summary 2.5.9.
We summarize the automorphs of bilinear forms in the following tables:

Improper Automorphs:

Name	Automorph	Corresponding bilinear forms	Case(s)	Order
N_1	$\pm \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$	$\begin{pmatrix} A_{11} & 0 \\ 0 & A_{22} \end{pmatrix}$	I.a	2 (2)
N_2	$\pm \begin{pmatrix} 1 & 0 \\ -1 & -1 \end{pmatrix}$	$\begin{pmatrix} 2A_{12} & A_{12} \\ A_{12} & 2A_{12} \end{pmatrix}$, $A_{12} \neq 0$	I.b	2 (2)
N_3	$\pm \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}$	$\begin{pmatrix} 2A_{12} & A_{12} \\ A_{12} & A_{22} \end{pmatrix}$, $0 < 2A_{12} \leqslant A_{22}$	I.c	2 (2)
N_4	$\pm \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} A_{11} & A_{12} \\ A_{12} & A_{11} \end{pmatrix}$, $0 \leqslant 2A_{12} \leqslant A_{11}$	I.d	2 (2)

Table 2.1: Improper Automorphs of a Positive Definite Reduced Bilinear Form

Proper Automorphs:

Name	Automorph	Corresponding bilinear forms	Case(s)	Order
M_1	$\pm\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	Any bilinear form	I.a	1 (2)
M_2	$\pm\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$	$\begin{pmatrix} A_{11} & A_{12} \\ -A_{12} & A_{11} \end{pmatrix}$	I.b	4 (4)
M_3	$\pm\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$	$\begin{pmatrix} A_{12}+A_{21} & A_{12} \\ A_{21} & A_{12}+A_{21} \end{pmatrix}$,	II.a	6 (3)
M_4	$\pm\begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}$	$A_{21} \neq -A_{12}$	II.b	6 (3)

Table 2.2: Proper Automorphs of a Positive Definite Reduced Bilinear Form

Notes:

- It is useful to recall that in Case II. of the improper automorphs and in Case II.c. of the proper automorphs no such automorphs exist.
- The name given to an automorph refers to the positive version. We will preface the name with -, i.e. $-M_2$, when referring to the negative of an automorph.
- In the Order column a number in () refers to the order of the negative of the given automorph.

Observation 2.5.10.
We note that if $\mathcal{A}$ is a symmetric bilinear form and we consider $\mathcal{A}(\mathbf{v}, \mathbf{v})$ then we have a binary quadratic form and the above results become precisely the well-known results from the automorph theory of binary quadratic forms.

Corollary 2.5.11.
Let $\mathcal{A}$ be a positive definite bilinear form then $\mathrm{Aut}_c^+(\mathcal{A}) = \{\pm I_2\} \cong \mathbb{Z}_2$.

Proof.
From Lemma 2.4.24 we know $\mathcal{A}$ is properly equivalent to a unique reduced bilinear form $\mathcal{B}$. By Lemma 2.5.7 properly equivalent bilinear forms have isomorphic proper automorph groups, thus $\mathcal{A} \cong \mathcal{B}$. By Summary 2.5.9 we know $\mathcal{B}$ has exactly two complete automorphs, $\pm I_2$ and thus $\mathrm{Aut}_c^+(\mathcal{B}) = \{\pm I_2\}$. Since $\mathrm{Aut}_c^+(\mathcal{B})$ is a subgroup of $\mathrm{Aut}^+(\mathcal{B})$ and group isomorphisms preserve subgroup structure, it follows that $\mathrm{Aut}_c^+(\mathcal{A}) = \{\pm I_2\} \cong \mathbb{Z}_2$. □

Notation 2.5.12.
We shall refer to the automorphs $\pm I$ as the **trivial automorphs**.

Observation 2.5.13.
It is straightforward to verify each of the improper automorphs satisfies $N^2 = I$.

Lemma 2.5.14.
Let $\mathcal{A}$ be a reduced bilinear form. If none of the following conditions are satisfied then $\mathrm{Aut}(\mathcal{A}) = \mathrm{Aut}^+(\mathcal{A}) = \mathrm{Aut}_c^+(\mathcal{A}) = \{\pm I\} \cong \mathbb{Z}_2$*:*

- $A_{11} \leqslant A_{22}$ *and* $A_{12} = A_{21} = 0$
- $A_{11} = 2A_{12} = 2A_{21}$ *and* $0 < A_{11} \leqslant A_{22}$
- $A_{11} = A_{22}$, $A_{12} = A_{21}$ *and* $0 < 2A_{12} < A_{11}$
- $A_{11} = A_{22}$ *and* $A_{21} = -A_{12}$
- $A_{11} = A_{22} = A_{12} + A_{21}$ *and* $A_{21} \neq -A_{12}$.

Proof.
This follows immediately from Summary 2.5.9. □

We now describe the group structure of the automorphism groups when a positive definite reduced bilinear form has an non-trivial automorphism. The following notation is provided for clarity.

Notation 2.5.15.
Let D_n denote the dihedral group that acts on the set of n vertices of a regular n-gon. Recall the dihedral group has $2n$ elements and representation
$D_n = \langle a, b \mid a^n = e, b^2 = e, bab^{-1} = a^{-1} \rangle$.

Lemma 2.5.16.
Let $\mathcal{A}$ be a positive definite reduced bilinear form satisfying one of the five conditions stated in Lemma 2.5.14. Then $\mathcal{A}$ lies in one of the following seven cases:

1. $A = \begin{pmatrix} A_{11} & 0 \\ 0 & A_{22} \end{pmatrix}$, $0 < A_{11} < A_{22}$, $\mathrm{Aut}(\mathcal{A}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ *and* $\mathrm{Aut}^+(\mathcal{A}) \cong \mathbb{Z}_2$.
2. $A = \begin{pmatrix} A_{11} & 0 \\ 0 & A_{11} \end{pmatrix}$, $0 < A_{11}$, $\mathrm{Aut}(\mathcal{A}) \cong D_4$ *and* $\mathrm{Aut}^+(\mathcal{A}) \cong \mathbb{Z}_4$.
3. $A = \begin{pmatrix} 2A_{12} & A_{12} \\ A_{12} & 2A_{12} \end{pmatrix}$, $0 < A_{12}$, $\mathrm{Aut}(\mathcal{A}) \cong D_6$ *and* $\mathrm{Aut}^+(\mathcal{A}) \cong \mathbb{Z}_6$.
4. $A = \begin{pmatrix} 2A_{12} & A_{12} \\ A_{12} & A_{22} \end{pmatrix}$, $0 < 2A_{12} < A_{22}$, $\mathrm{Aut}(\mathcal{A}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ *and* $\mathrm{Aut}^+(\mathcal{A}) \cong \mathbb{Z}_2$.
5. $A = \begin{pmatrix} A_{11} & A_{12} \\ A_{12} & A_{11} \end{pmatrix}$, $A_{11} \neq 2A_{12}$, $A_{12} \neq 0$, $\mathrm{Aut}(\mathcal{A}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ *and* $\mathrm{Aut}^+(\mathcal{A}) \cong \mathbb{Z}_2$.
6. $A = \begin{pmatrix} A_{11} & A_{12} \\ -A_{12} & A_{11} \end{pmatrix}$, $A_{12} \neq 0$, $\mathrm{Aut}(\mathcal{A}) \cong \mathrm{Aut}^+(\mathcal{A}) \cong \mathbb{Z}_4$.
7. $A = \begin{pmatrix} A_{12} + A_{21} & A_{12} \\ A_{21} & A_{12} + A_{21} \end{pmatrix}$, $A_{21} \neq |A_{12}|$, $\mathrm{Aut}(\mathcal{A}) \cong \mathrm{Aut}^+(\mathcal{A}) \cong \mathbb{Z}_6$.

Proof.
We consider each of the above cases in turn.

1. From Summary 2.5.9 the automorphs of $\mathcal{A}$ are $\pm I_2$ and $\pm N_1$. Thus $|\operatorname{Aut}(\mathcal{A})| = 4$. With the exception of I_2 these all have order 2 and hence $\operatorname{Aut}(\mathcal{A}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. Since there are no non-trivial proper automorphs of $\mathcal{A}$ it follows that $\operatorname{Aut}^+(\mathcal{A}) = \operatorname{Aut}_c^+(\mathcal{A}) \cong \mathbb{Z}_2$.

2. From Summary 2.5.9 the automorphs of $\mathcal{A}$ are $\pm I_2$, $\pm N_1$, $\pm N_4$ and $\pm M_2$. Thus $|\operatorname{Aut}(\mathcal{A})| = 8$. We observe $|M_2| = 4$, $|N_1| = 2$ and $N_1 M_2 N_1^{-1} = M_2^{-1}$. Hence we have a group of order 8 satisfying the relations for D_4. Therefore $\operatorname{Aut}(\mathcal{A}) \cong D_4$. Similarly, we observe the proper automorphs of $\mathcal{A}$ are $\pm I_2$ and $\pm M_2$. Since $|M_2| = 4$ it follows immediately that $\operatorname{Aut}^+(\mathcal{A}) \cong \mathbb{Z}_4$.

3. From Summary 2.5.9 the automorphs of $\mathcal{A}$ are $\pm I_2$, $\pm N_2$, $\pm N_3$, $\pm N_4$, $\pm M_3$ and $\pm M_4$. Thus $|\operatorname{Aut}(\mathcal{A})| = 12$. Next, observe $|M_3| = 6$, $|N_4| = 2$ and $N_4 M_3 N_4^{-1} = M_3^{-1}$. Hence we have a group of order 12 satisfying the relations for D_6. Therefore $\operatorname{Aut}(\mathcal{A}) \cong D_6$.
   Similarly, we observe the proper automorphs of $\mathcal{A}$ are $\pm I_2$, $\pm M_3$ and $\pm M_4$. Since $|M_3| = |M_4| = 6$ it follows that $\operatorname{Aut}^+(\mathcal{A}) \cong \mathbb{Z}_6$.

4. From Summary 2.5.9 the automorphs of $\mathcal{A}$ are $\pm I_2$ and $\pm N_3$. Thus $|\operatorname{Aut}(\mathcal{A})| = 4$. With the exception of I_2 these all have order 2 and hence $\operatorname{Aut}(\mathcal{A}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. Since there are no non-trivial proper automorphs of $\mathcal{A}$ it follows that $\operatorname{Aut}^+(\mathcal{A}) = \operatorname{Aut}_c^+(\mathcal{A}) \cong \mathbb{Z}_2$.

5. From Summary 2.5.9 the automorphs of $\mathcal{A}$ are $\pm I_2$ and $\pm N_4$. Thus $|\operatorname{Aut}(\mathcal{A})| = 4$. With the exception of I_2 these all have order 2 and hence $\operatorname{Aut}(\mathcal{A}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. Since there are no non-trivial proper automorphs of $\mathcal{A}$ it follows that $\operatorname{Aut}^+(\mathcal{A}) = \operatorname{Aut}_c^+(\mathcal{A}) \cong \mathbb{Z}_2$.

6. From Summary 2.5.9 the automorphs of $\mathcal{A}$ are $\pm I - 2$ and $\pm M_2$.
   Thus $|\operatorname{Aut}(\mathcal{A})| = 4$. Since $|M_2| = 4$ and $\mathcal{A}$ has no improper automorphs it follows that $\operatorname{Aut}(\mathcal{A}) = \operatorname{Aut}^+(\mathcal{A}) \cong \mathbb{Z}_4$.

7. From Summary 2.5.9 the automorphs of $\mathcal{A}$ are $\pm I_2$, $\pm M_3$ and $\pm M_4$. Thus $|\operatorname{Aut}(\mathcal{A})| = 6$. Since $|M_3| = |M_4| = 6$ and $\mathcal{A}$ has no improper automorphs, we see $\operatorname{Aut}(\mathcal{A}) \cong \operatorname{Aut}^+(\mathcal{A}) \cong \mathbb{Z}_6$.

□

Observation 2.5.17.
Assume $\mathcal{A}$ and $\mathcal{B}$ are positive definite bilinear forms with $\det(\mathcal{A}) = \det(\mathcal{B})$. By Lemma 2.4.24 $\mathcal{A}$ and $\mathcal{B}$ are properly equivalent to unique reduced bilinear forms $\mathcal{P}$ and $\mathcal{Q}$ respectively. Hence if $\mathcal{P} \neq \mathcal{Q}$ then $\mathcal{A}$ cannot be properly equivalent to $\mathcal{B}$.

Lemma 2.5.18.
Let $\mathcal{A}$ and $\mathcal{B}$ be properly equivalent positive definite bilinear forms. Let P and Q

respectively transform $\mathcal{A}$ and $\mathcal{B}$ to the unique reduced bilinear form $\mathcal{C}$. Then $\mathcal{A}$ and $\mathcal{B}$ are completely equivalent if and only if $\sigma(PVQ^{-1}) = (1, I_2)$ for some $V \in \mathrm{Aut}(\mathcal{C})$.

Proof.
($\Rightarrow$) Assume $\mathcal{A} \sim_c \mathcal{B}$ then there exists a matrix $M \in \ker\sigma$ such that $M^tAM = B$. Let $V = P^{-1}MQ$, then:

$$\begin{aligned} V^tCV &= \left(P^{-1}MQ\right)^t CP^{-1}MQ \\ &= Q^tM^t(P^{-1})^tCP^{-1}MQ \\ &= Q^tM^tAMQ \text{ as } P^tAP = C \\ &= Q^tBQ \text{ as } M^tAM = B \\ &= C. \end{aligned}$$

Hence $V \in \mathrm{Aut}(\mathcal{C})$ and $(1, I_2) = \sigma(M) = \sigma(PVQ^{-1})$.
($\Leftarrow$) Assume $(1, I_2) = \sigma(PVQ^{-1})$ for some $V \in \mathrm{Aut}(\mathcal{C})$. Let $M = PVQ^{-1}$, it follows that $\sigma(M) = \sigma(PVQ^{-1}) = (1, I_2)$, thus $M \in \ker\sigma$. Then,

$$\begin{aligned} M^tAM &= \left(PVQ^{-1}\right)^t A \left(PVQ^{-1}\right) \\ &= \left(Q^{-1}\right)^t V^tP^tAPV \left(Q^{-1}\right) \\ &= \left(Q^{-1}\right)^t V^tCV \left(Q^{-1}\right) \\ &= \left(Q^{-1}\right)^t C \left(Q^{-1}\right) \\ &= B. \end{aligned}$$

Hence $\mathcal{A}$ and $\mathcal{B}$ are completely equivalent. □

Corollary 2.5.19.
Using the notation found in Lemma 2.5.18 if $\mathcal{C}$ has no non-trivial automorphs then $\sigma(P) = \sigma(Q)$.

Proof.
Assume $\mathcal{C}$ has no non-trivial automorphs, that is, by Corollary 2.5.11 $\mathrm{Aut}(\mathcal{C}) = \mathrm{Aut}_c^+(\mathcal{C}) = \pm I_2$. This implies $V = \pm I_2$. Consequently if $\mathcal{A}$ and $\mathcal{B}$ are properly equivalent then the reverse direction of Lemma 2.5.18 implies $(1, I_2) = \sigma(PQ^{-1})$. Lemma 2.3.2 reminds us the map σ is a group homomorphism and hence $\sigma(P) = \sigma(Q)$. □

Theorem 2.5.20.
Let $\mathcal{A}$ be a reduced bilinear form. Then the equivalence class of $\mathcal{A}$ has exactly one proper equivalence class if and only if there exists an improper automorph of $\mathcal{A}$.

Proof.
Since our transformation matrices lie in $\mathrm{GL}_2(\mathbb{Z})$ it follows that the equivalence class of $\mathcal{A}$ contains at most two distinct proper equivalence classes as the determinant of the transformation is 1 or -1.
($\Rightarrow$) Consider the bilinear form $\mathcal{B}$ with matrix representation K^tAK where $K \in$

$\mathrm{GL}_2(\mathbb{Z})\backslash\mathrm{SL}_2(\mathbb{Z})$, that is, $\det(K) = -1$. Assume $\mathcal{A}$ is properly equivalent to $\mathcal{B}$, then there exists $L \in \mathrm{SL}_2(\mathbb{Z})$ such that $L^t\,(K^tAK)\,L = A$. Thus $KL \in \mathrm{Aut}(\mathcal{A})$ and $\det(KL) = \det(K)\det(L) = -1$. Hence KL is an improper automorph of $\mathcal{A}$.
($\Leftarrow$) Conversely, assume L is an improper automorph of $\mathcal{A}$. Let $K \in \mathrm{GL}_2(\mathbb{Z})\backslash\mathrm{SL}_2(\mathbb{Z})$, so $\det(K) = -1$. Then $(LK)^tA(LK) = K^tAK$. Further, $\det(LK) = \det(L)\det(K) = (-1)(-1) = 1$ and so $\mathcal{A}$ is properly equivalent to the bilinear form $\mathcal{B}$ with matrix representation K^tAK. Hence the equivalence class of $\mathcal{A}$ contains exactly one proper equivalence class. □

Having determined which reduced bilinear forms have non-trivial automorphs, our goal now is to calculate the number of complete equivalence classes within a proper equivalence class for a given reduced bilinear form. It is useful to recall that an equivalence class can contain at most two proper equivalence classes as the determinant of the transformation matrix is either 1 or -1. Further, recall that each proper equivalence class may contain at most six distinct complete equivalence classes. This is a consequence of the map σ. The following observation shall prove useful.

Observation 2.5.21.
We observe that the matrices $\begin{pmatrix} 2a & a+b \\ a-b & a \end{pmatrix}$ and $\begin{pmatrix} 2a & b-a \\ -(a+b) & a \end{pmatrix}$ are completely equivalent via $P = \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix} \in \ker\sigma$.
Further, the matrices $\begin{pmatrix} a & b-a \\ -(a+b) & 2a \end{pmatrix}$ and $\begin{pmatrix} a & a+b \\ a-b & 2a \end{pmatrix}$ are completely equivalent via $Q = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \in \ker\sigma$.

Lemma 2.5.22.
Let $\mathcal{A} = (A_{11}, A_{12}, A_{21}, A_{22})$ be a reduced bilinear form that does not satisfy any of the conditions for a proper or improper automorphism to exist (see Summary 2.5.9). Then the equivalence class of $\mathcal{B}$ contains two proper equivalence classes, each of which contains six complete equivalence classes.

Proof.
Since $\mathcal{A}$ does not have any improper automorphs, Theorem 2.5.20 implies there are exactly two proper equivalence classes within the equivalence class of $\mathcal{A}$. Then Lemma 2.5.18 and Corollary 2.5.19 imply any pair of bilinear forms, chosen with distinct transformation matrices under the map σ, cannot be completely equivalent. Hence each of the proper equivalence classes contains six complete equivalence classes. □

We now examine what happens when a reduced bilinear form has non-trivial automorphs. From Summary 2.5.9 there are six cases to consider. We first develop a couple of small results to smooth our path.

Definition 2.5.23.
From Lemma 2.3.2 we know $|\mathrm{GL}_2(\mathbb{Z}) : \ker\sigma| = 12$ and thus we may choose a set of

representatives for the transformation matrices used to generate the complete equivalence classes for a given bilinear form. We will follow Kronecker's lead and let

$$S = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \right\}. \tag{2.16}$$

Similarly we may generate a further 6 representatives for the transformation matrices via $T = S \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

Observe there are 12 distinct matrices in $S \cup T$ and each maps to a distinct element under σ. Further, all matrices in the set S lie in $\mathrm{SL}_2(\mathbb{Z})$ whilst those in the set T lie in $\mathrm{GL}_2(\mathbb{Z}) \backslash \mathrm{SL}_2(\mathbb{Z})$.

Lemma 2.5.24.
Let $A \in \mathrm{GL}_2(\mathbb{Z})$, then there exists a unique $B \in S \cup T$ such that $A = KB$ where $K \in \ker \sigma$.

Proof.
Since σ is a surjective homomorphism there exists $B \in S \cup T$ such that $\sigma(B) = \sigma(A)$. Now we express A as $A = KB$ where $K = AB^{-1}$. Recalling the map σ is a homomorphism then yields

$$\begin{aligned} \sigma(A) &= \sigma(KB) \\ &= \sigma(K)\sigma(B) \\ &= \sigma(K)\sigma(A) \end{aligned}$$

and therefore $\sigma(K)$ is the identity element. Hence $K \in \ker \sigma$.
Since the determinant of A is either 1 or -1 it follows that B is either in S or in T respectively. Further, within the set S or within the set T the elements are distinct mod 2. Thus B is in fact unique. □

Observation 2.5.25.
Lemma 2.5.24 provides a way to quickly determine whether bilinear forms from two seemingly distinct complete equivalence classes actually belong to the same complete equivalence class. By Theorem 2.4.24, if we start with an arbitrary bilinear form we may reduce it to a reduced bilinear form via the matrix transformation $A = KB$, for some $K \in \ker \sigma$ and $B \in \mathrm{SL}_2(\mathbb{Z})$. Therefore we may start with a reduced bilinear form and generate 6 seemingly distinct complete equivalence classes within its proper equivalence class by using the matrix transformations found in S. Let A be the matrix representation of the reduced bilinear form and let $S_i, S_j \in S$, $i \neq j$. If the complete equivalence class represented by the bilinear form $S_i^t A S_i$ is completely equivalent to the complete equivalence class represented by the bilinear form $S_j^t A S_j$ then there exists a matrix $K \in \ker \sigma$ such that $S_j^t A S_j = K^t S_i^t A S_i K$. Rearranging this yields $A = (S_i K S_j^{-1})^t A (S_i K S_j^{-1})$ and thus $S_i K S_j^{-1}$ is an automorph of the reduced bilinear form. In fact, since $S_i, S_j \in S$ and $K \in \ker \sigma$, $S_i K S_j^{-1}$ is a proper

automorph.
Now applying the map σ yields $\sigma\left(S_iKS_j^{-1}\right) = \sigma(S_i)\sigma(S_j^{-1})$ as $K \in \ker\sigma$. This must then be the same as applying σ to the proper automorph. Consequently, since complete equivalence is an equivalence relation, we see that we may generate the seemingly distinct complete equivalence classes via the matrices in S and compare $\sigma(S_i)\sigma(S_j^{-1})$ to σ applied to each proper automorph of the reduced bilinear form. If these do not agree then the two complete equivalence classes are indeed distinct.
It is particularly important to note that complete equivalence being an equivalence relation is vital here. For certain reduced bilinear forms it is possible for $S_i^tAS_i$ to generate the same representative as say $S_k^tAS_k$ $(i \neq k)$. Clearly those two complete equivalence classes are the same one. Complete equivalence being an equivalence relation permits us not to worry about whether we chose the correct S_i when comparing under σ with a seemingly distinct bilinear form computed via S_j. The transitivity property of an equivalence relation prevents us from having $S_k^tAS_k$ being completely equivalent to $S_j^tAS_j$ while $S_i^tAS_i$ is not completely equivalent to $S_j^tAS_j$. This greatly reduces the computations required to determine the number of complete equivalence classes within the proper equivalence class of a reduced bilinear form that has a proper automorph.
Furthermore, note that we avoided $i = j$ and so $S_iKS_j^{-1}$ is a non-trivial proper automorph.

Lemma 2.5.26.
If a reduced bilinear form has no improper automorphs then the two proper equivalence classes within its equivalence class each contain the same number of complete equivalence classes.

Proof.
By Theorem 2.5.20 and Lemma 2.5.22 it is sufficient for us to consider only those families of reduced bilinear forms which have non-trivial proper automorphs but no improper automorphs. From Summary 2.5.9 this leaves two families for us to investigate.
Let $M = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z})\backslash\mathrm{SL}_2(\mathbb{Z})$.
Case I: $\begin{pmatrix} A_{11} & A_{12} \\ -A_{12} & A_{11} \end{pmatrix}$
Applying the matrix transformation M yields the bilinear form $\begin{pmatrix} A_{11} & -A_{12} \\ A_{12} & A_{11} \end{pmatrix}$.
Since our initial bilinear form was reduced it is easy to verify that this transformed bilinear form is also reduced. Further, this new bilinear form is of the same family as the initial bilinear form and therefore has no improper automorphs. Since every proper equivalence class contains a unique reduced bilinear form, we deduce that in Case I the two proper equivalence classes have the same cardinalities with respect to the number of complete equivalence classes they contain.
Case II: $\begin{pmatrix} A_{12}+A_{21} & A_{12} \\ A_{21} & A_{12}+A_{21} \end{pmatrix}$, $A_{21} \neq -A_{12}$
Applying the matrix transformation M yields the bilinear form

$\begin{pmatrix} A_{12}+A_{21} & A_{21} \\ A_{12} & A_{12}+A_{21} \end{pmatrix}$. Since our initial bilinear form was reduced it is straightforward to check this transformed bilinear form is also reduced. Further, it is clear that it is in the same family of reduced bilinear forms as our original reduced bilinear form. Hence since our original and transformed bilinear forms are improperly equivalent, it follows that both of the proper equivalence classes within the equivalence class contain the same number of complete equivalence classes. □

We are now ready to determine the number of complete equivalence classes within the proper equivalence class for each of the reduced bilinear forms in our six special cases.

Case 1:

Consider the reduced bilinear form $\begin{pmatrix} A_{11} & A_{12} \\ -A_{12} & A_{11} \end{pmatrix}$, $A_{11} > 0$. The only non-trivial automorph of this bilinear form is $L = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$.

Using the matrix transformation representatives found in the set S we compute a set of possibly distinct representatives for the complete equivalence classes as follows:

$$\left\{ \begin{pmatrix} A_{11} & A_{12} \\ -A_{12} & A_{11} \end{pmatrix}, \begin{pmatrix} 2A_{11} & A_{11}+A_{12} \\ A_{11}-A_{12} & A_{11} \end{pmatrix}, \begin{pmatrix} A_{11} & A_{12}+A_{11} \\ A_{11}-A_{12} & 2A_{11} \end{pmatrix} \right\}.$$

Using Observation 2.5.25 we see the cardinality of this set is 3 since $S_2S_3^{-1} \equiv \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \bmod 2 \neq L \bmod 2$, $S_2S_5^{-1} \equiv \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \bmod 2 \neq L \bmod 2$ and $S_3S_5^{-1} \equiv \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \bmod 2 \neq L \bmod 2$.

Hence the proper equivalence class contains three complete equivalence classes.

Case 2:

Consider the reduced bilinear form $\begin{pmatrix} A_{12}+A_{21} & A_{12} \\ A_{21} & A_{12}+A_{21} \end{pmatrix}$, where $A_{12} \neq A_{21}$ and $A_{12}+A_{21} \neq 0$.

Using the matrix transformation representatives found in the set S we get a set of possibly distinct representatives for the complete equivalence classes as follows:

$$\left\{ \begin{pmatrix} A_{12}+A_{21} & A_{12} \\ A_{21} & A_{12}+A_{21} \end{pmatrix}, \begin{pmatrix} A_{12}+A_{21} & -A_{21} \\ -A_{12} & A_{12}+A_{21} \end{pmatrix} \right\}.$$

Using Observation 2.5.25 we see the cardinality of this set is 2 since $S_2S_3^{-1} \equiv \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \bmod 2 \not\equiv \underbrace{\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}}_{\pm M_3 \bmod 2}$ or $\underbrace{\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}}_{\pm M_4 \bmod 2}$. Hence the proper equivalence class contains two complete equivalence classes.

Case 3:

Consider the reduced bilinear form $\begin{pmatrix} 2A_{12} & A_{12} \\ A_{12} & 2A_{12} \end{pmatrix}$, where $A_{12} > 0$.

Using the matrix transformation representatives from the set S we get the following set of possibly distinct representatives for the complete equivalence classes:

$$\left\{ \begin{pmatrix} 2A_{12} & A_{12} \\ A_{12} & 2A_{12} \end{pmatrix}, \begin{pmatrix} 2A_{12} & -A_{12} \\ -A_{12} & 2A_{12} \end{pmatrix} \right\}.$$

Applying Observation 2.5.25 we see the cardinality of this set is 2 since $S_2 S_3^{-1} \equiv \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \bmod 2 \not\equiv \underbrace{\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}}_{\pm N_2 \bmod 2}$. Thus the proper equivalence class contains two complete equivalence classes.

Case 4:
Consider the reduced bilinear form $\begin{pmatrix} A_{11} & 0 \\ 0 & A_{22} \end{pmatrix}$, where $0 < A_{11} < A_{22}$.
We note that this type of reduced bilinear form has no non-trivial proper automorphs. Consequently the proper equivalence class must contain exactly six distinct complete equivalence classes.

Case 5:
Consider the reduced bilinear form $\begin{pmatrix} A_{11} & A_{12} \\ A_{12} & A_{11} \end{pmatrix}$, where $0 < A_{11}$, $A_{12} \neq 0$ and $A_{11} \neq 2A_{12}$.
We note that this type of reduced bilinear form has no non-trivial proper automorphs. Consequently the proper equivalence class must contain exactly six distinct complete equivalence classes.

Case 6:
Consider the reduced bilinear form $\begin{pmatrix} 2A_{12} & A_{12} \\ A_{12} & A_{22} \end{pmatrix}$, where $0 < 2A_{12} < A_{22}$.
We note that this type of reduced bilinear form has no non-trivial proper automorphs. Consequently the proper equivalence class must contain exactly six distinct complete equivalence classes.

Summary 2.5.27.
See Table 2.3 at the end of this section.

From this work we get the following corollary.

Corollary 2.5.28.
The complete class number for bilinear forms with determinant D is odd if and only if D is a square.

Proof.
Let $D \in \mathbb{Z}_{>0}$.
($\Rightarrow$) Assume $\mathrm{Cl}_c(D)$ is odd. By Summary 2.5.27 we know that either proper equivalence classes come in pairs with each containing the same number of complete equivalence classes, or if there is only one proper equivalence class within an equivalence

class then that proper equivalence class contains an even number of complete equivalence classes unless we have the reduced bilinear form found in the second row of the table. Thus we must have an odd number of reduced forms of the type $\begin{pmatrix} A_{11} & 0 \\ 0 & A_{11} \end{pmatrix}$. Further, since we are dealing with positive definite reduced bilinear forms there can only be one such reduced form in this family as this type of reduced form must satisfy $A_{11}^2 = D$. Consequently D is a square.
($\Leftarrow$) Assume D is a square. Then since we are dealing with positive definite reduced bilinear forms there is one and only one reduced form of the type found in the second row of Summary 2.5.27. Since all other proper equivalence classes occur in pairs or contain an even number of complete equivalence classes, it follows that $\mathrm{Cl}_c(D)$ is odd. □

Type of Reduced Form	Number of proper equivalence classes within an equivalence class	Number of complete equivalence classes within a proper equivalence class
$\begin{pmatrix} A_{11} & A_{12} \\ -A_{12} & A_{11} \end{pmatrix}$ $A_{11} > 0,\ A_{12} \neq 0$	2	3
$\begin{pmatrix} A_{11} & 0 \\ 0 & A_{11} \end{pmatrix}$ $A_{11} > 0$	1	3
$\begin{pmatrix} A_{12} + A_{21} & A_{12} \\ A_{21} & A_{12} + A_{21} \end{pmatrix}$ $A_{12} + A_{21} \neq 0,\ A_{12} \neq A_{21}$	2	2
$\begin{pmatrix} 2A_{12} & A_{12} \\ A_{12} & 2A_{12} \end{pmatrix}$ $A_{12} > 0$	1	2
$\begin{pmatrix} A_{11} & 0 \\ 0 & A_{22} \end{pmatrix}$ $0 < A_{11} < A_{22}$	1	6
$\begin{pmatrix} A_{11} & A_{12} \\ A_{12} & A_{11} \end{pmatrix}$ $0 < A_{11}, A_{12},\ A_{11} \neq 2A_{12}$	1	6
$\begin{pmatrix} 2A_{12} & A_{12} \\ A_{12} & A_{22} \end{pmatrix}$ $0 < 2A_{12} < A_{22}$	1	6
Otherwise	2	6

Table 2.3: Relationships between the cardinalities of equivalence, proper equivalence and complete equivalence classes for reduced bilinear forms.

Notes on Section 2.5

In his paper, Kronecker does not explicitly calculate the number of complete equivalence classes contained within a proper equivalence class for bilinear forms. He gives an argument in his fifth chapter for binary quadratic forms.

Chapter 3 Kronecker Reduced Bilinear Forms

"Never, never, never give up."
- Sir Winston Churchill

In this chapter we develop the idea of a Kronecker reduced bilinear form and explore its connection to the complete class number.

3.1 Kronecker's concept of a reduced bilinear form

In this subsection we introduce the idea of a Kronecker reduced bilinear form. We prove some elementary results relating to this concept before proving a key theorem - that the complete class number may be enumerated via Kronecker reduced bilinear forms.

Definition 3.1.1.
Let $\mathcal{A} = \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix}$ be a bilinear form. We will call $\mathcal{A}$ **Kronecker reduced** if it satisfies the following conditions:

- $|\frac{A_{12}+A_{21}}{2}| \leqslant |A_{11}|$ and $|\frac{A_{12}+A_{21}}{2}| \leqslant |A_{22}|$, but where equality cannot hold simultaneously, and
- $A_{11}A_{22} > 0$.

Observation 3.1.2.
The requirement that we cannot have simultaneous equality in the conditions for a Kronecker reduced bilinear form ensures we are only considering definite bilinear forms. If we had simultaneous equality then we get $4A_{11}A_{22} - (A_{12} + A_{21})^2 = 0$, which contradicts Corollary 2.4.19.

Lemma 3.1.3.
If $\mathcal{A}$ is a definite reduced bilinear form then $\mathcal{A}$ is Kronecker reduced.

Proof.
Let $\begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix}$ be the matrix representation of the definite reduced bilinear form $\mathcal{A}$. Since $\mathcal{A}$ is definite it follows that $0 < A_{11}A_{22}$ and thus $\mathcal{A}$ is not skew-symmetric and satisfies the second condition found in Definition 3.1.1.
By Lemma 2.4.18 we know $|A_{11}|$ is the minimal non-zero integer represented by $\mathcal{A}$. Thus we have $\left|\frac{A_{12}+A_{21}}{2}\right| \leqslant |A_{12} + A_{21}| \leqslant |A_{11}| \leqslant |A_{22}|$.
However, the definition of a Kronecker reduced bilinear form requires $\left|\frac{A_{12}+A_{21}}{2}\right| \leqslant |A_{11}|$ and $\left|\frac{A_{12}+A_{21}}{2}\right| \leqslant |A_{22}|$ where equality cannot hold simultaneously. If $|A_{11}| = |A_{22}|$ then by Definition 2.4.14 we have $0 \leqslant A_{12} + A_{21} \leqslant |A_{11}|$. So we can have simultaneous equality if and only if $A_{12} + A_{21} = 0$, in which case $A_{11} = A_{22} = 0$ also,

contradicting $0 < A_{11}A_{22}$.
Hence every definite reduced bilinear form is Kronecker reduced. □

Theorem 3.1.4.
Every Kronecker reduced bilinear form satisfying $0 < A_{11}$ is positive definite.

Proof.
Assume that $\mathcal{A}$ is a Kronecker reduced bilinear form satisfying $0 < A_{11}$. Since $0 < A_{11}A_{22}$, it follows that $0 < A_{22}$ also. Kronecker reduced also implies $|A_{12} + A_{21}| \leqslant 2A_{11}$ and $|A_{12} + A_{21}| \leqslant 2A_{22}$, and we cannot have equality simultaneously. Thus we see $(A_{12} + A_{21})^2 < 4A_{11}A_{22}$. Corollary 2.4.19 then implies $\mathcal{A}$ is positive definite. □

Corollary 3.1.5.
Every Kronecker reduced bilinear form satisfying $0 < A_{11}$ is properly equivalent to a unique reduced bilinear form.

Proof.
By Theorem 3.1.4, a Kronecker reduced bilinear form satisfying $0 < A_{11}$ is positive definite. By Theorem 2.4.24 every such form is properly equivalent to a unique reduced bilinear form. □

Lemma 3.1.6.
Every positive definite Kronecker reduced bilinear form, $\mathcal{A}$, satisfies $\det(\mathcal{A}) > 0$.

Proof.
By Corollary 3.1.5 $\mathcal{A}$ is properly equivalent to a unique reduced bilinear form, $\mathcal{B}$. By Lemma 2.4.16 we have $\det(\mathcal{B}) > 0$. Finally, by Lemma 2.3.1 we know the determinant is an invariant under equivalence and hence $\det(\mathcal{A}) > 0$. □

Lemma 3.1.7.
Let $D \in \mathbb{Z}_{>0}$ and define $\mathcal{K}_{D,<}$ to be the set of Kronecker reduced bilinear forms which, satisfy $A_{11} < 0$ and have determinant D. Similarly, define $\mathcal{K}_{D,>}$ be the set of Kronecker reduced bilinear forms which, satisfy $A_{11} > 0$ and have determinant D. Define the map $\tau : \mathcal{K}_{D,<} \longrightarrow \mathcal{K}_{D,>}$ by $\tau(A_{11}, A_{12}, A_{21}, A_{22}) = (-A_{11}, A_{12}, A_{21}, -A_{22})$. Then τ is a bijection.

Proof.
The second condition in Definition 3.1.1, $0 < A_{11}A_{22}$, implies the outer coefficients have the same sign and are non-zero. Thus any Kronecker reduced form satisfies either $A_{11} < 0$ or $A_{11} > 0$.
The map τ is well-defined since for any $\mathcal{A} = (A_{11}, A_{12}, A_{21}, A_{22}) \in \mathcal{K}_{D,<}$ we have $A_{11}, A_{22} < 0$, thus $-A_{11}, -A_{22} > 0$. Also $\det \tau(\mathcal{A}) = (-A_{11}) \cdot (-A_{22}) - A_{12}A_{21} = A_{11}A_{22} - A_{12}A_{21} = D$.
Lastly, we have $\frac{1}{2}|A_{12} + A_{21}| \leqslant A_{11} = |-A_{11}|$ and $\frac{1}{2}|A_{12} + A_{21}| \leqslant A_{22} = |-A_{22}|$, and equality cannot hold simultaneously as $\mathcal{A}$ is Kronecker reduced.
Injectivity is straightforward to show by equating coefficients.
Lastly, the map τ is surjective. Let $\mathcal{B} = (B_{11}, B_{12}, B_{21}, B_{22}) \in \mathcal{K}_{D,>}$ and consider $\mathcal{A} = (-B_{11}, B_{12}, B_{21}, -B_{22})$. Since $B_{11}, B_{22} > 0$, it follows that $-B_{11}, -B_{22} < 0$. A

quick calculation checks $\det \mathcal{A} = \det \mathcal{B}$ and again we see $\frac{1}{2}|B_{12}+B_{21}| \leqslant |-B_{11}| = B_{11}$ and $\frac{1}{2}|B_{12}+B_{21}| \leqslant |-B_{22}| = B_{22}$. Finally, we observe $\tau(\mathcal{A}) = (B_{11}, B_{12}, B_{21}, B_{22})$. Thus the map τ is surjective and hence a bijection. □

Hence from this point onwards we will restrict ourselves to only considering positive definite (Kronecker reduced) bilinear forms with integer coefficients.

We now prove the set $\mathcal{K}_{D,>}$ is finite for any $D \in \mathbb{Z}_{>0}$. We will do this via a series of lemmas showing there are finitely many choices for each of A_{11}, $|A_{12}|$, $|A_{21}|$ and A_{22}.

Lemma 3.1.8.
Let $\mathcal{A}$ be a Kronecker reduced bilinear form with $0 < A_{11}$ and without loss of generality assume $A_{11} \leqslant A_{22}$. Then $|A_{12}+A_{21}| < 2A_{22}$.

Proof.
If not then $|A_{12}+A_{21}| = 2A_{22}$. Thus we have $|A_{12}+A_{21}| \leqslant 2A_{11} \leqslant 2A_{22} = |A_{12}+A_{21}|$ and so equality holds throughout. This contradicts equality holding at most once in Definition 3.1.1. □

Lemma 3.1.9.
$A_{11} \leqslant D$ and $|A_{12}+A_{21}| \leqslant 2D$.

Proof.
Recall $xy \leqslant \left(\frac{x+y}{2}\right)^2$ for all real numbers x, y. By assumption there exists $n \in \mathbb{Z}_{\geqslant 0}$ such that $A_{11}+n = A_{22}$. If $n \geqslant 1$ then we have

$$\begin{aligned} D &= A_{11}A_{22} - A_{12}A_{21} \\ &\geqslant A_{11}(A_{11}+n) - \left(\frac{A_{12}+A_{21}}{2}\right)^2 \\ &= A_{11}^2 + nA_{11} - \left(\frac{A_{12}+A_{21}}{2}\right)^2 \\ &\geqslant nA_{11} \\ &\geqslant A_{11}. \end{aligned}$$

Then since $|A_{12}+A_{21}| \leqslant 2A_{11}$ it follows that $|A_{12}+A_{21}| \leqslant 2D$. □

Lemma 3.1.10.
$|A_{12}-A_{21}| < 2\sqrt{D}$.

Proof.
Lemma 3.1.8 implies
$(A_{12}-A_{21})^2 = (A_{12}+A_{21})^2 - 4A_{12}A_{21} < (2A_{11})(2A_{22}) - 4A_{12}A_{21} = 4D$. □

We observe Lemma 3.1.10 gives an easier proof that positive definite Kronecker reduced bilinear forms satisfy $D > 0$.

Lemma 3.1.11.
$A_{12}A_{21} \leqslant A_{11}^2 \leqslant D^2$.

Proof.
Recall $xy \leqslant \left(\frac{x+y}{2}\right)^2$ for all real numbers x and y. Then we have

$$\begin{aligned} 4A_{12}A_{21} &\leqslant (A_{12}+A_{21})^2 \\ &\leqslant 4A_{11}^2 \\ &\leqslant 4D^2 \text{ (by Lemma 3.1.9).} \end{aligned}$$

□

Lemma 3.1.12.
$A_{22} \leqslant A_{11} + \frac{D}{A_{11}} \leqslant D+1$.

Proof.
We have

$$\begin{aligned} A_{11}A_{22} &= A_{12}A_{21} + D \\ &\leqslant A_{11}^2 + D \text{ (by Lemma 3.1.11).} \end{aligned}$$

Hence $A_{22} \leqslant A_{11} + \frac{D}{A_{11}}$. Further, by Lemma 3.1.9 we have $0 < A_{11} \leqslant D$, which implies $1 < \frac{D}{A_{11}}$. Therefore $A_{22} \leqslant A_{11} + \frac{D}{A_{11}} \leqslant D+1$. □

Our next lemma is provided as an aide-memoir.

Lemma 3.1.13.
Let $a, b \in \mathbb{R}$ be such that $ab > 0$, then $|a+b| = |a| + |b|$.

Proof.
We have

$$\begin{aligned} (|a+b|)^2 &= (a+b)^2 \\ &= a^2 + 2ab + b^2 \\ &= |a|^2 + 2|a||b| + |b|^2 \\ &= (|a|+|b|)^2. \end{aligned}$$

Hence $||a+b|| = ||a|+|b||$ and thus $|a+b| = |a|+|b|$. □

Lemma 3.1.14.
$|A_{12}| \leqslant D$ and $|A_{21}| \leqslant D$.

Proof.
First assume $A_{12}A_{21} < 0$ and thus neither of A_{12}, A_{21} are zero. This gives

$$\begin{aligned} D &= A_{11}A_{22} - A_{12}A_{21} \\ &= A_{11}A_{22} + |A_{12}A_{21}| \\ &\geqslant |A_{12}A_{21}| \\ &\geqslant \begin{cases} |A_{12}| \\ |A_{21}|. \end{cases} \end{aligned}$$

Now assume $A_{12}A_{21} \geqslant 0$, we will show $|A_{12}| \leqslant D$. Assume $|A_{12}| = D + a$ for some integer $a > 0$. From Lemma 3.1.11 we know $0 \leqslant A_{12}A_{21} = |A_{12}||A_{21}| \leqslant D^2$ and thus $0 \leqslant (D+a)|A_{21}| \leqslant D^2$. This implies $0 \leqslant |A_{21}| \leqslant \frac{D^2}{D+a} < \frac{D^2}{D} = D$. Hence $|A_{21}| = D-b$ for some integer b such that $0 < b \leqslant D$. Next, since $0 \leqslant A_{12}A_{21} = |A_{12}||A_{21}|$, Lemma 3.1.13 implies $|A_{12} + A_{21}| = |A_{12}| + |A_{21}|$. Then using Lemma 3.1.9 we have $2D + (a - b) = |A_{12}| + |A_{21}| = |A_{12} + A_{21}| \leqslant 2D$ and hence $a - b \leqslant 0$. This yields $0 < a \leqslant b \leqslant D$.
Applying Lemma 3.1.8 then gives $2D + (a - b) = |A_{12}| + |A_{21}| = |A_{12} + A_{21}| < 2A_{22}$. Therefore we have two cases to consider.
Case 1: $a \equiv b \bmod 2$
Then $2D + a - b + 2 \leqslant 2A_{22}$ and being Kronecker reduced implies $2D + a - b = |A_{12} + A_{21}| \leqslant 2A_{11}$.
Thus $4A_{11}A_{22} \geqslant (2D + (a - b))\,(2D + (a - b) + 2)$.
Case 2: $a \not\equiv b \bmod 2$
Then $2D + a - b + 1 \leqslant 2A_{22}$. Further, $2D + a - b < 2A_{11}$ as $2D + a - b \equiv 1 \bmod 2$ so we have $2D + a - b + 1 \leqslant 2A_{11}$. This then gives $4A_{11}A_{22} \geqslant (2D + a - b + 1)^2$.
Using the property that $(x + 1)^2 > (x + 2)x$ for all real numbers x, we see in either case we have

$$4A_{11}A_{22} \geqslant (2D + (a - b) + 2)(2D + (a - b)).$$

Finally, we have

$$\begin{aligned}
4D &= 4A_{11}A_{22} - 4A_{12}A_{21} \\
&\geqslant (2D + (a - b) + 2)(2D + (a - b)) - 4(D + a)(D - b) \\
&= (2D + (a - b))^2 + 2(2D + (a - b)) + 4(D^2 + (a - b)D - ab) \\
&= (a - b)^2 + 4D + 2(a - b) + 4ab \\
&= 4D + (a - b + 1)^2 + 4ab - 1 \\
&> 4D \text{ as } a, b \text{ are positive non-zero integers.}
\end{aligned}$$

This contradicts $|A_{12}| > D$ and hence $|A_{12}| \leqslant D$. It remains to show $|A_{21}| \leqslant D$ simultaneously.
Write $|A_{12}| = D-d$ where $0 \leqslant d \leqslant D$ and in a similar manner we assume $|A_{21}| = D+c$ for some integer $c > 0$. Since $0 \leqslant A_{12}A_{21}$ it follows that $2D + c - d = |A_{12}| + |A_{21}| = |A_{12} + A_{21}| \leqslant 2D$ and hence $c - d \leqslant 0$. Therefore we have $0 < c \leqslant d \leqslant D$.
Applying Lemma 3.1.8 gives $2D + c - d = |A_{12} + A_{21}| < 2A_{22}$ and so we have two cases to consider.
Case 1: $c \equiv d \bmod 2$
Then $2D + c - d + 2 \leqslant 2A_{22}$ and being Kronecker reduced yields $2D + c - d \leqslant 2A_{11}$. Therefore we have $4A_{11}A_{22} \geqslant (2D + c - d + 2)(2D + c - d)$.
Case 2: $c \not\equiv d \bmod 2$
Then $2D + c - d + 1 \leqslant 2A_{22}$ and $2D + c - d < 2D + c - d + 1 \leqslant 2A_{11}$. Thus $4A_{11}A_{22} \geqslant (2D + c - d + 1)^2$.
Consequently, in either case we have

$$4A_{11}A_{22} > (2D + c - d + 2)(2D + c - d).$$

Repeating the above argument for the determinant D then yields a contradiction. Therefore we must simultaneously have $|A_{12}| \leqslant D$ and $|A_{21}| \leqslant D$. □

Theorem 3.1.15.
The set $\mathcal{K}_{D,>}$ is finite.

Proof.
Fix $D \in \mathbb{Z}_{>0}$ and assume $0 < A_{11} \leqslant A_{22}$. Then Lemma 3.1.9 shows $A_{11} \leqslant D$ while Lemma 3.1.12 shows $A_{22} \leqslant D + 1$. Lastly, Lemma 3.1.14 has shown under these conditions that $|A_{12}| \leqslant D$ and $|A_{21}| \leqslant D$. Therefore there are only finitely many choices for the entries of the matrix representation of a positive definite Kronecker reduced bilinear form. Hence there are only finitely many positive definite Kronecker reduced bilinear forms satisfying $A_{11} \leqslant A_{22}$. By the symmetry of the initial condition for being a positive definite Kronecker reduced bilinear form it follows that there are only finitely many such forms satisfying $A_{22} < A_{11}$. Hence the set $\mathcal{K}_{D,>}$ is finite. □

Theorem 3.1.16.
Let $\mathcal{A}$ be a positive definite bilinear form, then the complete equivalence class of $\mathcal{A}$ contains at least one Kronecker reduced bilinear form.

Proof. Let $A = \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix}$ be the matrix representation of $\mathcal{A}$. If $\mathcal{A}$ is Kronecker reduced then we are done, so suppose this is not the case.
It follows either $|A_{12} + A_{21}| > 2A_{11}$ or $|A_{12} + A_{21}| > 2A_{22}$ or both. Consider the transformation matrix $U(\beta)$ from Definition 2.4.15 and suppose $A_{11} > A_{22}$. Applying this transformation yields

$$M^t A M = \begin{pmatrix} A_{11} & \beta A_{11} + A_{12} \\ \beta A_{11} + A_{21} & \beta^2 A_{11} + \beta(A_{12} + A_{21}) + A_{22} \end{pmatrix} = \begin{pmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{pmatrix}.$$

Then we have

$$\begin{aligned} B_{22} &= \beta^2 A_{11} + \beta(A_{12} + A_{21}) + A_{22} \\ &\geqslant \beta^2 A_{11} + \beta(A_{12} + A_{21}) + \frac{A_{12} + A_{21}}{2} \text{ as } |A_{12} + A_{21}| \leqslant 2A_{22} \\ &= \beta^2 A_{11} + \frac{A_{12} + A_{21}}{2}(2\beta + 1). \end{aligned}$$

Now we observe if $A_{12} + A_{21} \geqslant 0$ then letting $\beta = 2$ yields $B_{22} \geqslant 4A_{11} > A_{11} = B_{11}$. Similarly, if $A_{12} + A_{21} < 0$ then letting $\beta = -2$ yields $B_{22} \geqslant 4A_{11} + \frac{3}{2}|A_{12} + A_{21}| > A_{11} = B_{11}$. In each case we have $U(\beta) \in \ker \sigma$ and thus we may assume without loss of generality that our initial positive definite bilinear form satisfies $A_{11} \leqslant A_{22}$.
If $|A_{12} + A_{21}| > 2A_{11}$ then let Q be the unique non-zero integer such that $-2A_{11} < A_{12} + A_{21} + 4QA_{11} \leqslant 2A_{11}$. Then applying $U(2Q)$ yields a positive definite bilinear form $\mathcal{B}$ that satisfies $|B_{12} + B_{21}| = |A_{12} + A_{21} + 4QA_{11}| \leqslant 2A_{11} = 2B_{11} < |A_{12} + A_{21}|$. If this is Kronecker reduced then we are done.
If it is not then we must have $|B_{12} + B_{21}| > 2B_{22}$ because $\mathrm{GL}_2(\mathbb{Z})$ transformations

preserve positive definite forms (Corollary 2.4.21) and Observation 3.1.2 shows if we have simultaneous equality then $4B_{11}B_{22} - (B_{12} + B_{21})^2 = 0$, contradicting $\mathcal{B}$ being positive definite.
We now apply $L(2K)$ where K is the unique non-zero integer such that $-2B_{22} < B_{12} + B_{21} + 4KB_{22} \leqslant 2B_{22}$. This yields a positive definite bilinear form $\mathcal{C}$ where $|C_{12} + C_{21}| \leqslant B_{22} = C_{22} < |B_{12} + B_{21}|$. If this is not Kronecker reduced then we continue this process, alternating between $U(2Q)$ and $L(2K)$ transformations.
This yields a strictly decreasing sequence, $|A_{12}+A_{21}| > |B_{12}+B_{21}| > |C_{12}+C_{21}| > \ldots$ and hence this process either terminates at a Kronecker reduced form or we end up with $b_{12} + b_{21} = 0$. Since $b_{11} > 0$ and $b_{22} > 0$ it follows that this form is Kronecker reduced. Hence we must terminate with a Kronecker reduced bilinear form.
Now observe each of our transformation matrices lie in $\ker \sigma$ and therefore we have shown the complete equivalence class of a positive definite bilinear form $\mathcal{A}$ contains at least one Kronecker reduced bilinear form. □

We now investigate when the complete equivalence class of a positive definite bilinear form $\mathcal{A}$ contains exactly one Kronecker reduced bilinear form.
We first prove a lemma that will help us eliminate certain cases that arise.

Lemma 3.1.17.
Let $\alpha\delta - \beta\gamma = 1$, $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$ and assume $\alpha > 0$, $\beta \neq 0$ and $\gamma \neq 0$. If $\gamma > 0$ then $\beta\delta > 0$ and if $\gamma < 0$ then $\beta\delta < 0$.

Proof.
First let $\gamma > 0$ then if $\delta > 0$ we have $\alpha\delta > 0$ and then $\alpha\delta - \beta\gamma = 1$ implies $0 < \beta\gamma < \alpha\delta$. Since $\gamma > 0$, $\beta > 0$ follows and hence $\beta\delta > 0$. Similarly, if $\delta < 0$ then $\alpha\delta < 0$ and $\beta\gamma = \alpha\delta - 1 < 0$. Since $\gamma > 0$ it follows that $\beta < 0$ and so $\beta\delta > 0$. Hence when $\gamma > 0$ we have $\beta\delta > 0$.
Now assume $\gamma < 0$ then if $\delta > 0$ we have $\alpha\delta > 0$ and $\alpha\delta - \beta\gamma = 1$ implies $\beta\gamma > 0$ else $\alpha\delta - \beta\gamma \geqslant 2$. Therefore $\beta < 0$ as $\gamma < 0$ and thus $\beta < 0$, $\delta > 0$ implies $\beta\delta < 0$. So now suppose $\delta < 0$, then we have $\alpha\delta < 0$ and $\beta\gamma = \alpha\delta - 1 < 0$. Then $\gamma < 0$ implies $\beta > 0$, combined with $\delta < 0$ we get $\beta\delta < 0$.
Consequently when $\gamma < 0$ we have $\beta\delta < 0$. □

Now let $\mathcal{A}$ be a positive definite Kronecker reduced bilinear form with matrix representation $\begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix}$. Then one of the following three cases hold:

i. $|A_{12} + A_{21}| < 2A_{11} = 2A_{22}$

ii. $|A_{12} + A_{21}| \leqslant 2A_{11} < 2A_{22}$

iii. $|A_{12} + A_{21}| \leqslant 2A_{22} < 2A_{11}$.

Let $M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \ker \sigma$ and assume the resulting form, M^tAM, under this transformation is also Kronecker reduced.

$$M^tAM = \begin{pmatrix} \alpha^2A_{11} + \alpha\gamma(A_{12} + A_{21}) + \gamma^2A_{22} & \alpha\beta A_{11} + \alpha\delta A_{12} + \beta\gamma A_{21} + \delta\gamma A_{22} \\ \alpha\beta A_{11} + \alpha\delta A_{21} + \beta\gamma A_{12} + \delta\gamma A_{22} & \beta^2A_{11} + \beta\delta(A_{12} + A_{21}) + \delta^2A_{22} \end{pmatrix}.$$

Since M^tAM is Kronecker reduced, it also satisfies one of the three cases above. So we have

$$|2\alpha\beta A_{11} + (\alpha\delta + \beta\gamma)(A_{12} + A_{21}) + 2\delta\gamma A_{22}| \leqslant 2\left(\alpha^2 A_{11} + \alpha\gamma(A_{12} + A_{21}) + \gamma^2 A_{22}\right)$$
$$|2\alpha\beta A_{11} + (\alpha\delta + \beta\gamma)(A_{12} + A_{21}) + 2\delta\gamma A_{22}| \leqslant 2\left(\beta^2 A_{11} + \beta\delta(A_{12} + A_{21}) + \delta^2 A_{22}\right).$$

This gives rise to the following four inequalities:

$$\begin{aligned}
2\alpha\beta A_{11} + (\alpha\delta + \beta\gamma)(A_{12} + A_{21}) + 2\delta\gamma A_{22} &\leqslant 2\alpha^2 A_{11} + 2\alpha\gamma(A_{12} + A_{21}) + 2\gamma^2 A_{22} \\
-2\alpha^2 A_{11} - 2\alpha\gamma(A_{12} + A_{21}) - 2\gamma^2 A_{22} &\leqslant 2\alpha\beta A_{11} + (\alpha\delta + \beta\gamma)(A_{12} + A_{21}) + 2\delta\gamma A_{22} \\
2\alpha\beta A_{11} + (\alpha\delta + \beta\gamma)(A_{12} + A_{21}) + 2\delta\gamma A_{22} &\leqslant 2\beta^2 A_{11} + 2\beta\delta(A_{12} + A_{21}) + 2\delta^2 A_{22} \\
-2\beta^2 A_{11} - 2\beta\delta(A_{12} + A_{21}) - 2\delta^2 A_{22} &\leqslant 2\alpha\beta A_{11} + (\alpha\delta + \beta\gamma)(A_{12} + A_{21}) + 2\delta\gamma A_{22}.
\end{aligned}$$

Recall being a positive definite Kronecker reduced bilinear form means equality may occur precisely once in the above four inequalities.

Rearranging these inequalities we get:

$$\begin{aligned}
2\alpha(\alpha - \beta)A_{11} + (A_{12} + A_{21})(2\alpha\gamma - \alpha\delta - \beta\gamma) + 2\gamma(\gamma - \delta) &\geqslant 0 \\
2\alpha(\alpha + \beta)A_{11} + (A_{12} + A_{21})(\alpha\delta + \beta\gamma + 2\alpha\gamma) + 2\gamma(\gamma + \delta) &\geqslant 0 \\
2\beta(\beta - \alpha)A_{11} + (A_{12} + A_{21})(2\beta\delta - \alpha\delta - \beta\gamma) + 2\delta(\delta - \gamma) &\geqslant 0 \\
2\beta(\beta + \alpha)A_{11} + (A_{12} + A_{21})(2\beta\delta + \alpha\delta + \beta\gamma) + 2\delta(\gamma + \delta) &\geqslant 0.
\end{aligned}$$

Now observe $2\alpha\gamma - \alpha\delta - \beta\gamma = \alpha(\gamma - \delta) + \gamma(\alpha - \beta)$. Using this and three other similar identities permits us to rewrite the above inequalities as:

$$2\alpha(\alpha - \beta)A_{11} + \alpha(\gamma - \delta)(A_{12} + A_{21}) + \gamma(\alpha - \beta)(A_{12} + A_{21}) + 2\gamma(\gamma - \delta)A_{22} \geqslant 0 \tag{3.1}$$
$$2\alpha(\alpha + \beta)A_{11} + \alpha(\gamma + \delta)(A_{12} + A_{21}) + \gamma(\alpha + \beta)(A_{12} + A_{21}) + 2\gamma(\gamma + \delta)A_{22} \geqslant 0 \tag{3.2}$$
$$2\beta(\beta - \alpha)A_{11} + \beta(\delta - \gamma)(A_{12} + A_{21}) + \delta(\beta - \alpha)(A_{12} + A_{21}) + 2\delta(\delta - \gamma)A_{22} \geqslant 0 \tag{3.3}$$
$$2\beta(\beta + \alpha)A_{11} + \beta(\delta + \gamma)(A_{12} + A_{21}) + \delta(\beta + \alpha)(A_{12} + A_{21}) + 2\delta(\delta + \gamma)A_{22} \geqslant 0. \tag{3.4}$$

Recall applying the transformation $-I_2 \in \ker\sigma$ results in initial bilinear form remaining the same. However, it changes M from $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ to $\begin{pmatrix} -\alpha & -\beta \\ -\gamma & -\delta \end{pmatrix}$. Therefore without loss of generality we may assume M satisfies $\alpha > 0$. Note that this does not change $\alpha \equiv \delta \equiv 1 \bmod 2$ and $\beta \equiv \gamma \equiv 0 \bmod 2$.

We first deal with two special cases:

Special Case 1: $\gamma = 0$
Here $\alpha\delta - \beta\gamma = 1$ becomes $\alpha\delta = 1$ and we have $\alpha > 0$ yields $\alpha = \delta = 1$. Then our four inequalities become

$$\begin{aligned} 2(1-\beta)A_{11} - (A_{12} + A_{21}) &\geqslant 0 \\ 2(1+\beta)A_{11} + (A_{12} + A_{21}) &\geqslant 0 \\ 2\beta(\beta-1)A_{11} + \beta(A_{12} + A_{21}) + (\beta-1)(A_{12} + A_{21}) + 2A_{22} &\geqslant 0 \\ 2\beta(\beta+1) + \beta(A_{12} + A_{21}) + (\beta+1)(A_{12} + A_{21}) + 2A_{22} &\geqslant 0. \end{aligned}$$

Using the conditions for being Kronecker reduced the first inequality yields:

$$\begin{aligned} 2(1-\beta)A_{11} &\geqslant A_{12} + A_{21} \geqslant -2A_{11} \\ \Rightarrow 2 - 2\beta &\geqslant -2 \\ \Rightarrow 4 &\geqslant 2\beta \\ \Rightarrow \beta &\leqslant 2. \end{aligned}$$

Similarly the second inequality yields:

$$\begin{aligned} 2(1+\beta)A_{11} &\geqslant -(A_{12} + A_{21}) \geqslant -2A_{11} \\ \Rightarrow 2 + 2\beta &\geqslant -2 \\ \Rightarrow 2\beta &\geqslant -4 \\ \Rightarrow \beta &\geqslant -2. \end{aligned}$$

Hence $\beta \in [-2, 2] \cap \mathbb{Z}$ and $\beta \equiv 0 \bmod 2$ then implies $\beta \in \{-2, 0, 2\}$. Further, note $\beta = 0$ corresponds to $M = I_2$. Thus we first suppose $\beta = -2$. Then the first and second inequalities yield $-2(1+\beta)A_{11} \leqslant A_{12} + A_{21} \leqslant 2(1-\beta)$. That is, $2A_{11} \leqslant A_{12} + A_{21} \leqslant 6A_{11}$. However, since our form is Kronecker reduced this can only happen if $A_{12} + A_{21} = 2A_{11}$.
Substituting $\beta = -2$ and $A_{12} + A_{21} = 2A_{11}$ into the remaining inequalities gives:

$$\begin{aligned} 12A_{11} - 2(A_{12} + A_{21}) - 3(A_{12} + A_{21}) + 2A_{22} &\geqslant 0 \\ \Rightarrow 6(A_{12} + A_{21}) - 5(A_{12} + A_{21}) + 2A_{22} &\geqslant 0 \\ \Rightarrow 2A_{22} &\geqslant -(A_{12} + A_{21}) \text{ and} \\ 4A_{11} - 2(A_{12} + A_{21}) - (A_{12} + A_{21}) + 2A_{22} &\geqslant 0 \\ \Rightarrow 2(A_{12} + A_{21}) - 3(A_{12} + A_{21}) + 2A_{22} &\geqslant 0 \\ \Rightarrow (A_{12} + A_{21}) &\leqslant 2A_{22}. \end{aligned}$$

Thus $|A_{12} + A_{21}| \leqslant 2A_{22}$ and so the form is Kronecker reduced.
Now suppose $\beta = 2$. Then the first and second inequalities yield $-6A_{11} \leqslant A_{12} + A_{21} \leqslant -2A_{11}$. However, since our form is Kronecker reduced this can only occur if we have $A_{12} + A_{21} = -2A_{11}$. Substituting $\beta = 2$ and $A_{12} + A_{21} = -2A_{11}$ into the remaining inequalities gives:

$$4A_{11} + 2(A_{12} + A_{21}) + (A_{12} + A_{21}) + 2A_{22} \geqslant 0$$

$$\begin{aligned}
&\Rightarrow -2(A_{12}+A_{21}+3(A_{12}+A_{21})+2A_{22} \geqslant 0\\
&\qquad\qquad\qquad\qquad\qquad\qquad \Rightarrow -2A_{22} \leqslant (A_{12}+A_{21}) \text{ and}\\
&12A_{11}+2(A_{12}+A_{21})+3(A_{12}+A_{21})+2A_{22} \geqslant 0\\
&\Rightarrow -6(A_{12}+A_{21})+5(A_{12}+A_{21})+2A_{22} \geqslant 0\\
&\qquad\qquad\qquad\qquad\qquad\qquad \Rightarrow (A_{12}+A_{21}) \leqslant 2A_{22}.
\end{aligned}$$

Thus $|A_{12}+A_{21}| \leqslant 2A_{22}$ and we have a Kronecker reduced form.
Hence we see if $A_{12}+A_{21}=2A_{11}>0$ then the Kronecker reduced bilinear form $\begin{pmatrix} \frac{A_{12}+A_{21}}{2} & A_{12} \\ A_{21} & A_{22} \end{pmatrix}$ is completely equivalent to the Kronecker reduced bilinear form $\begin{pmatrix} \frac{A_{12}+A_{21}}{2} & -A_{21} \\ -A_{12} & A_{22} \end{pmatrix}$ via $M=\begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix} \in \ker\sigma$.
Similarly if $A_{12}+A_{21}=-2A_{11}<0$ then the Kronecker reduced bilinear form $\begin{pmatrix} -\frac{(A_{12}+A_{21})}{2} & A_{12} \\ A_{21} & A_{22} \end{pmatrix}$ is completely equivalent to the Kronecker reduced bilinear form $\begin{pmatrix} -\frac{(A_{12}+A_{21})}{2} & -A_{21} \\ -A_{12} & A_{22} \end{pmatrix}$ via $M=\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \in \ker\sigma$.
This completes our first special case.

Special Case 2: $\beta=0$
Here $\alpha\delta-\beta\gamma=1$ becomes $\alpha\delta=1$ and $\alpha>0$ implies $\alpha=\delta=1$. Then our four inequalities become:

$$\begin{aligned}
2A_{11}+(\gamma-1)(A_{12}+A_{21})+\gamma(A_{12}+A_{21})+2\gamma(\gamma-1)A_{22} &\geqslant 0\\
2A_{11}+(\gamma+1)(A_{12}+A_{21})+\gamma(A_{12}+A_{21})+2\gamma(\gamma+1)A_{22} &\geqslant 0\\
-(A_{12}+A_{21})+2(1-\gamma)A_{22} &\geqslant 0\\
(A_{12}+A_{21})+2(1+\gamma)A_{22} &\geqslant 0.
\end{aligned}$$

Using the conditions for being Kronecker reduced the third inequality yields:

$$\begin{aligned}
&2(1-\gamma)A_{22} \geqslant A_{12}+A_{21} \geqslant -2A_{22}\\
&\Rightarrow 2-2\gamma \geqslant -2\\
&\qquad \Rightarrow 4 \geqslant 2\gamma\\
&\Rightarrow 2 \geqslant \gamma.
\end{aligned}$$

Similarly the fourth inequality yields:

$$\begin{aligned}
&2(1+\gamma)A_{22} \geqslant -(A_{12}+A_{21}) \geqslant -2A_{22}\\
&\Rightarrow 2+2\gamma \geqslant -2\\
&\qquad \Rightarrow 2\gamma \geqslant -4\\
&\qquad \Rightarrow \gamma \geqslant -2.
\end{aligned}$$

Hence we have $\gamma \in [-2,2] \cap \mathbb{Z}$ and $\gamma \equiv 0 \bmod 2$ implies $\gamma \in \{-2,0,2\}$. Note when $\gamma=0$ then $M=I_2$, a trivial automorph.

Thus we first suppose $\gamma = -2$. Then the third and fourth inequalities yield $2A_{22} \leqslant A_{12} + A_{21} \leqslant 6A_{22}$, which can only occur if $2A_{22} = A_{12} + A_{21}$. Substituting $2A_{22} = A_{12} + A_{21}$ and $\gamma = -2$ into the first and second inequalities then gives:

$$\begin{aligned} 2A_{11} - 3(A_{12} + A_{21}) - 2(A_{12} + A_{21}) + 12A_{22} &\geqslant 0 \\ \Rightarrow 2A_{11} - 5(A_{12} + A_{21}) + 6(A_{12} + A_{21}) &\geqslant 0 \\ \Rightarrow 2A_{11} &\geqslant -(A_{12} + A_{21}) \text{ and} \\ 2A_{11} - (A_{12} + A_{21}) - 2(A_{12} + A_{21}) + 4A_{22} &\geqslant 0 \\ \Rightarrow 2A_{11} - 3(A_{12} + A_{21}) + 2(A_{12} + A_{21}) &\geqslant 0 \\ \Rightarrow 2A_{11} &\geqslant A_{12} + A_{21}. \end{aligned}$$

Hence we have $|A_{12} + A_{21}| \leqslant 2A_{11}$ and so the form is Kronecker reduced.
Now suppose $\gamma = 2$. Then the third and fourth inequalities yield $-6A_{22} \leqslant A_{12}+A_{21} \leqslant -2A_{22}$, which can only happen if $A_{12} + A_{21} = -2A_{22}$. Substituting this and $\gamma = 2$ into the first and second inequalities yields:

$$\begin{aligned} 2A_{11} + (A_{12} + A_{21}) + 2(A_{12} + A_{21}) + 4A_{22} &\geqslant 0 \\ \Rightarrow 2A_{11} + 3(A_{12} + A_{21}) - 2(A_{12} + A_{21}) &\geqslant 0 \\ \Rightarrow 2A_{11} &\geqslant -(A_{12} + A_{21}) \text{ and} \\ 2A_{11} + 3(A_{12} + A_{21}) + 2(A_{12} + A_{21}) + 12A_{22} &\geqslant 0 \\ \Rightarrow 2A_{11} + 5(A_{12} + A_{21}) - 6(A_{12} + A_{21}) &\geqslant 0 \\ \Rightarrow 2A_{11} &\geqslant A_{12} + A_{21}. \end{aligned}$$

Hence we have $|A_{12} + A_{21}| \leqslant 2A_{11}$ and thus the form is Kronecker reduced.
Therefore we see if $A_{12} + A_{21} = 2A_{22} > 0$ then the Kronecker reduced form $\begin{pmatrix} A_{11} & A_{12} \\ A_{21} & \frac{A_{12}+A_{21}}{2} \end{pmatrix}$ is completely equivalent to the Kronecker reduced form $\begin{pmatrix} A_{11} & -A_{21} \\ -A_{12} & \frac{A_{12}+A_{21}}{2} \end{pmatrix}$ via $M = \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix} \in \ker \sigma$.
Similarly if $A_{12}+A_{21} = -2A_{22} < 0$ then the Kronecker reduced form $\begin{pmatrix} A_{11} & A_{12} \\ A_{21} & \frac{A_{12}+A_{21}}{2} \end{pmatrix}$ is completely equivalent to the Kronecker reduced form $\begin{pmatrix} A_{11} & -A_{21} \\ -A_{12} & -\frac{(A_{12}+A_{21})}{2} \end{pmatrix}$ via $M = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \in \ker \sigma$.
This completes our second special case.

We now assume $\alpha\delta - \beta\gamma = 1$, $\alpha > 0$, $\beta \neq 0$, $\gamma \neq 0$, $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$, $\alpha \equiv \delta \equiv 1 \bmod 2$ and $\beta \equiv \gamma \equiv 0 \bmod 2$. These conditions will be referred to as our base assumptions. We will produce a contradiction to the four inequalities given in 3.1 - 3.4. This will show in these circumstances there is no non-trivial mapping in $\ker \sigma$ of a Kronecker reduced bilinear form to another Kronecker reduced bilinear form.

To do this we will examine all of the possibilities for β, γ and δ.

1. $\beta > 0$, $\gamma > 0$ and $\delta > 0$
2. $\beta > 0$, $\gamma > 0$ and $\delta < 0$
3. $\beta > 0$, $\gamma < 0$ and $\delta > 0$
4. $\beta > 0$, $\gamma < 0$ and $\delta < 0$
5. $\beta < 0$, $\gamma > 0$ and $\delta > 0$
6. $\beta < 0$, $\gamma > 0$ and $\delta < 0$
7. $\beta < 0$, $\gamma < 0$ and $\delta > 0$
8. $\beta < 0$, $\gamma < 0$ and $\delta < 0$.

Using Lemma 3.1.17 we can immediately see cases 2 and 5 cannot occur as $\gamma > 0$ yet $\beta\delta < 0$. Similarly cases 3 and 8 cannot occur as $\gamma < 0$ yet $\beta\delta > 0$. This leaves four cases to consider. We first prove two lemmas that will aid our investigation.
It is important to remember our base assumptions imply the following: $\alpha - \beta \neq 0$, $\alpha - \gamma \neq 0$, $\gamma - \delta \neq 0$ and $\beta - \delta \neq 0$.

Lemma 3.1.18.
Under our base assumptions and assuming $\gamma > 0$ it follows that $(\alpha - \beta)(\gamma - \delta) > 0$.

Proof.
Note $\delta \equiv 1 \bmod 2$ implies $\beta \neq 0$ and $\delta \neq 0$. From Lemma 3.1.17 we have $\beta\delta > 0$ so we have two cases to consider. First suppose $\beta < 0$ and $\delta < 0$ then we have $\beta < 0 < \alpha$ and $\delta < 0 < \gamma$. These imply $\alpha - \beta > 0$ and $\gamma - \delta > 0$ and our result follows immediately.
Thus suppose $\beta > 0$ and $\delta > 0$. Observe if $0 < \beta < \alpha$ and $0 < \delta < \gamma$ then our result follows. Similarly if $0 < \alpha < \beta$ and $0 < \gamma < \delta$ then our result follows. Next, note that if $0 < \alpha < \beta$ and $0 < \delta < \gamma$ then we have $\alpha\delta < \beta\gamma$ which, contradicts $\alpha\delta - \beta\gamma = 1$. Lastly we consider $0 < \beta < \alpha$ and $0 < \gamma < \delta$, then we have $\alpha - \beta > 0$ and $\beta > 0$ implies $\beta \geqslant 2$ and thus $\alpha > 1$, giving $0 < \beta \leqslant \alpha - 1$. Likewise this case gives $\gamma \geqslant 2$ and so $\delta > 1$, thus $0 < \gamma \leqslant \delta - 1$. Then we have:

$$\begin{aligned} 1 = \alpha\delta - \beta\gamma &\geqslant \alpha\delta - (\alpha - 1)(\delta - 1) \\ &= \alpha\delta - \alpha\delta + \alpha + \delta - 1 \\ &= \alpha + \delta - 1 \\ &\geqslant 5 \text{ as } \alpha \geqslant 3, \delta \geqslant 3. \end{aligned}$$

Hence this last case cannot occur and so under our base assumptions and $\gamma > 0$ we have $(\alpha - \beta)(\gamma - \delta) > 0$. □

Lemma 3.1.19.
Under our base assumptions and assuming $\gamma < 0$ it follows that $(\beta - \alpha)(\gamma - \delta) > 0$.

Proof.
By Lemma 3.1.17 we know $\beta\delta < 0$ thus again we have two cases to consider. First suppose $\beta < 0$ and $\delta > 0$. Then we have:

$$\begin{aligned}(\beta-\alpha)(\gamma-\delta) &= \beta\gamma - \alpha\gamma - \beta\delta + \alpha\delta \\ &= |\beta\gamma| + |\alpha\gamma| + |\beta\delta| + \alpha\delta \\ &\geqslant 4 > 0.\end{aligned}$$

Now suppose $\beta > 0$ and $\delta < 0$. Observe if $0 < \alpha < \beta$ and $\delta < \gamma < 0$ then $(\beta-\alpha)(\gamma-\delta) > 0$. Similarly, if $0 < \beta < \alpha$ and $\gamma < \delta < 0$ then $(\beta-\alpha)(\gamma-\delta) > 0$. Next, if $0 < \beta < \alpha$ and $\delta < \gamma < 0$ then we have $\alpha\delta < \beta\gamma < 0$, contradicting $\alpha\delta - \beta\gamma = 1$. Lastly,if $0 < \alpha < \beta$ and $\gamma < \delta < 0$ then we have $\gamma + 1 \leqslant \delta < 0$ as $\gamma \leqslant -2$. Likewise we have $0 < \alpha \leqslant \beta - 1$ as $\beta \geqslant 2$. Thus $(\beta-1)(\gamma+1) \leqslant \alpha\delta < 0$. This gives:

$$\begin{aligned}1 = \alpha\delta - \beta\gamma &\geqslant (\beta-1)(\gamma+1) - \beta\gamma \\ &= \beta\gamma - \gamma + \beta - 1 - \beta\gamma \\ &= \beta - \gamma - 1 \\ &\geqslant 3 \text{ as } \gamma \leqslant -2, \beta \geqslant 2.\end{aligned}$$

Hence this last case cannot occur and so under our base assumptions and assuming $\gamma < 0$ it follows that $(\beta-\alpha)(\gamma-\delta) > 0$. □

We now examine each of the four remaining cases found under our base assumptions.

Case 1: We have $\alpha > 0$, $\beta > 0$, $\gamma > 0$ and $\delta > 0$. We split into two subcases, $\alpha - \beta > 0$ and $\alpha - \beta < 0$.
Case 1a: $0 < \beta < \alpha$
Then Lemma 3.1.18 implies $0 < \delta < \gamma$. We first prove a lemma that will help substantially.

Lemma 3.1.20.
Under the assumptions of Case 1a we have $(\beta-\delta)(\beta-\alpha+\gamma-\delta) \leqslant 0$.

Proof.
Recall $\beta \not\equiv \delta \bmod 2$ and $\alpha \not\equiv \gamma \bmod 2$. We split into two cases.
First suppose $\beta - \delta > 0$, then $\beta\delta$ and this implies $\delta \leqslant \beta - 1$. Assume $\beta - \alpha + \gamma - \delta > 0$, then $\beta - \delta > \alpha - \gamma$. Next, assume $\alpha - \gamma < 0$, then $\alpha < \gamma$ and thus $\alpha \leqslant \gamma - 1$. This yields:

$$\begin{aligned}1 = \alpha\delta - \beta\gamma &\leqslant (\gamma-1)(\beta-1) - \beta\gamma \\ &= \beta\gamma - \beta - \gamma + 1 - \beta\gamma \\ &= 1 - \beta - \gamma \\ &\leqslant -3 \text{ as } \beta \geqslant 2, \gamma \geqslant 2.\end{aligned}$$

This is a contradiction and thus we have $0 < \alpha - \gamma < \beta - \delta$. Further, note that $\delta(\alpha-\gamma) > 0$ and $\gamma(\beta-\delta) > 0$. Now observe $1 = \alpha\delta-\beta\gamma = \delta(\alpha-\gamma)-\gamma(\beta-\delta)$ and thus $1+\gamma(\beta-\delta) = \delta(\alpha-\gamma)$. Therefore we have $1+\gamma(\beta-\delta) = \delta(\alpha-\gamma) < \delta(\beta-\delta) < \gamma(\beta-\delta)$. This is a contradiction, thus we must have $\beta - \alpha + \gamma - \delta \leqslant 0$. Recalling $\beta - \delta > 0$ then yields the result in this case.
Now suppose $\beta - \delta < 0$. This gives $\delta \geqslant \beta + 1$. Assume $\beta - \alpha + \gamma - \delta < 0$, which implies $\beta - \delta < \alpha - \gamma$. Next, assume $\alpha - \gamma > 0$, then $\alpha > \gamma$ which implies $\alpha \geqslant \gamma + 1$. This yields:

$$\begin{aligned} 1 = \alpha\delta - \beta\gamma &\geqslant (\gamma+1)(\beta+1) - \beta\gamma \\ &= \beta\gamma + \beta + \gamma + 1 - \beta\gamma \\ &= \beta + \gamma + 1 \\ &\geqslant 5. \end{aligned}$$

This is a contradiction so $\beta - \delta < \alpha - \gamma < 0$. Thus $|\alpha - \gamma| < |\beta - \delta|$ and we also have $1 = \delta(\alpha - \gamma) - \gamma(\beta - \delta)$, which implies $1 + \gamma(\beta - \delta) = \delta(\alpha - \gamma)$. Therefore we have $|\delta(\alpha - \gamma)| = |1 + \gamma(\beta - \delta)|$ and so $|\delta(\alpha - \gamma)| = |\gamma(\beta - \delta)| - 1$. Thus

$$\begin{aligned} |\gamma(\beta - \delta)| - 1 &= |\delta(\alpha - \gamma)| \\ &< |\gamma(\alpha - \gamma)| \\ &< |\gamma(\beta - \delta)|. \end{aligned}$$

This is a contradiction because it implies two consecutive integers are separated by at least two. Therefore $\beta - \alpha + \gamma - \delta \geqslant 0$. Recalling $\beta - \delta < 0$ then yields the result. Hence in both subcases we have $(\beta - \delta)(\beta - \alpha + \gamma - \delta) \leqslant 0$. □

Now under the assumptions of Case 1a we have $\beta - \alpha < 0$ and $\delta - \gamma < 0$. Therefore $\beta(\beta - \alpha) < 0$ and $\delta(\delta - \gamma) < 0$ as $\delta > 0$ and $\beta > 0$. Let $A_{ii} = \min\{A_{11}, A_{22}\} > 0$. Note at $\beta(\delta - \gamma) < 0$ and $\delta(\beta - \alpha) < 0$. Consequently 3.3 we have

$$\begin{aligned} 0 &\leqslant 2\underbrace{\beta(\beta-\alpha)}_{<0}A_{11} + \beta(\delta-\gamma)(A_{12}+A_{21}) + \delta(\beta-\alpha)(A_{12}+A_{21}) + 2\underbrace{\delta(\delta-\gamma)}_{<0}A_{22} \\ &\leqslant 2\left(\underbrace{\beta(\beta-\alpha)+\delta(\delta-\gamma)}_{<0}\right)A_{ii} + (A_{12}+A_{21})\left(\underbrace{\beta(\delta-\gamma)+\delta(\beta-\alpha)}_{<0}\right). \end{aligned}$$

We see if $A_{12} + A_{21} \geqslant 0$ then the right hand side is negative as each summand is negative. This is a contradiction.
So we assume $A_{12} + A_{21} < 0$. Then inequality 3.3 becomes

$$\begin{aligned} 0 &\leqslant 2\left(\beta(\beta-\alpha)+\delta(\delta-\gamma)\right)A_{ii} + |A_{12}+A_{21}|\left(\beta(\gamma-\delta)+\delta(\alpha-\beta)\right) \\ &\leqslant 2\left(\beta(\beta-\alpha)+\delta(\delta-\gamma)\right)A_{ii} + 2A_{ii}\left(\beta(\gamma-\delta)+\delta(\alpha-\beta)\right) \text{ as } |A_{12}+A_{21}| \leqslant 2A_{ii} \\ &= 2A_{ii}\left(\beta(\beta-\alpha)+\delta(\delta-\gamma)+\beta(\gamma-\delta)+\delta(\alpha-\beta)\right) \\ &= 2A_{ii}\left(\beta-\delta\right)\left(\beta-\alpha+\gamma-\delta\right). \end{aligned}$$

Due to our form being Kronecker reduced, we note that equality cannot hold throughout. Therefore we have $0 < 2A_{ii}(\beta-\delta)(\beta-\alpha+\gamma-\delta)$. Yet, by Lemma 3.1.20 we have $(\beta-\delta)(\beta-\alpha+\gamma-\delta) \leqslant 0$, a contradiction.
This completes Case 1a.

Case 1b: $0 < \alpha < \beta$
Then Lemma 3.1.19 implies $0 < \gamma < \delta$. We first prove a lemma to help us out.

Lemma 3.1.21.
Under the assumptions of Case 1b we have $(\alpha-\gamma)(\beta-\alpha+\gamma-\delta) \geqslant 0$.

Proof.
We split into two cases. First suppose $0 < \alpha < \gamma$ and notice that we must have $0 < \beta < \delta$ in order to avoid contradicting $1 = \alpha\delta - \beta\gamma$. Suppose $\beta-\alpha+\gamma-\delta > 0$ which, implies $0 < \delta-\beta < \gamma-\alpha$. Also, note that $1 = \alpha\delta-\beta\gamma = \alpha(\delta-\beta)-\beta(\gamma-\alpha)$ and therefore $\alpha(\delta-\beta) = 1+\beta(\gamma-\alpha)$. Observe $\alpha(\delta-\beta) > 0$ and $\beta(\gamma-\alpha) > 0$. This then yields

$$\begin{aligned} 0 < 1+\beta(\gamma-\alpha) &= \alpha(\delta-\beta) \\ &< \beta(\delta-\beta) \\ &< \beta(\gamma-\alpha), \end{aligned}$$

which is a contradiction. Therefore we must have $\beta-\alpha+\gamma-\delta \leqslant 0$. Recalling $\alpha-\gamma < 0$ yields the result in this case.
Now suppose $0 < \gamma < \alpha$ and so $\alpha-\gamma > 0$. Note that $\alpha \geqslant \gamma+1$ and $\gamma \geqslant 2$. Assume $0 < \beta < \delta$, then we have $\delta \geqslant \beta+1$ and $\beta \geqslant 2$. This gives

$$\begin{aligned} 1 = \alpha\delta-\beta\gamma &> (\gamma+1)(\beta+1)-\beta\gamma \\ &= \beta\gamma+\gamma+\beta+1-\beta\gamma \\ &= \beta+\gamma+1 \\ &\geqslant 5, \end{aligned}$$

which is a contradiction. Thus we have $0 < \delta < \beta$. Now assume $\beta-\alpha+\gamma-\delta < 0$, this rearranges to $\beta-\alpha < \delta-\gamma$. Note that $1 = \alpha\delta-\beta\gamma = \beta(\delta-\gamma)-\delta(\beta-\alpha)$ and using this gives

$$0 < \delta(\beta-\alpha) < \beta(\beta-\alpha) < \beta(\delta-\gamma) = 1+\delta(\beta-\alpha).$$

This is a contradiction because it implies two consecutive integers are separated by a difference of at least two. Therefore we have $\beta-\alpha+\gamma-\delta \geqslant 0$ and recalling $\alpha-\gamma > 0$ then yields $(\alpha-\gamma)(\beta-\alpha+\gamma-\delta) \geqslant 0$.
Hence we always have $(\alpha-\gamma)(\beta-\alpha+\gamma-\delta) \geqslant 0$. □

Now under the assumptions of Case 1b we have $\alpha-\beta < 0$ and $\gamma-\delta < 0$. It follows that $\alpha(\alpha-\beta < 0$, $\gamma(\gamma-\delta) < 0$, $\alpha(\gamma-\delta)$ and $\gamma(\alpha-\beta) < 0$. As before, let $A_{ii} = \min\{A_{11}, A_{22}\} > 0$. Then inequality 3.1 yields

$$0 \leqslant \underbrace{2\alpha(\alpha-\beta)}_{<0}A_{11} + \underbrace{\alpha(\gamma-\delta)}_{<0}(A_{12}+A_{21}) + \underbrace{\gamma(\alpha-\beta)}_{<0}(A_{12}+A_{21}) + \underbrace{2\gamma(\gamma-\delta)}_{<0}A_{22}.$$

We immediately see we have a contradiction if $A_{12}+A_{21} \geqslant 0$. So assume $A_{12}+A_{21} < 0$. Then the inequality becomes

$$\begin{aligned} 0 &\leqslant 2\alpha(\alpha-\beta)A_{11} + |A_{12}+A_{21}||\alpha(\gamma-\delta)+\gamma(\alpha-\beta)| + 2\gamma(\gamma-\delta)A_{22} \\ &\leqslant 2A_{ii}\left(\alpha(\alpha-\beta)+\gamma(\gamma-\delta)\right) + |A_{12}+A_{21}||\alpha(\gamma-\delta)+\gamma(\alpha-\beta)| \\ &\leqslant 2A_{ii}\left(\alpha(\alpha-\beta)+\gamma(\gamma-\delta)\right) + 2A_{ii}|\alpha(\gamma-\delta)+\gamma(\alpha-\beta)|. \end{aligned}$$

Since our form is Kronecker reduced we note equality cannot hold throughout the above inequality. Thus we have

$$0 < 2A_{ii}\left(\alpha(\alpha-\beta)+\gamma(\gamma-\delta)+|\alpha(\gamma-\delta)+\gamma(\alpha-\beta)|\right). \tag{3.5}$$

Since $\alpha+\gamma > 0$, $\beta-\alpha > 0$ and $\delta-\gamma > 0$ due to our setup in Case 1b, we have $(\alpha+\gamma)(\beta-\alpha+\delta-\gamma) > 0$. This gives

$$\begin{aligned} 0 &< (\alpha+\gamma)(\beta-\alpha+\delta-\gamma) \\ &= (\delta-\gamma)(\gamma+\alpha) + (\beta-\alpha)(\gamma+\alpha) \\ &= \left(\alpha(\delta-\gamma)+\gamma(\beta-\alpha)\right) + \left(\alpha(\beta-\alpha)+\gamma(\delta-\gamma)\right). \end{aligned}$$

From this we get

$$\alpha(\gamma-\delta)+\gamma(\alpha-\beta) < \alpha(\beta-\alpha)+\gamma(\delta-\gamma). \tag{3.6}$$

By Lemma 3.1.21 we have $(\alpha-\gamma)(\beta-\alpha+\gamma-\delta) \geqslant 0$. This yields $0 \leqslant (\beta-\alpha)(\alpha-\gamma)+(\gamma-\alpha)(\delta-\gamma)$ and therefore we get

$$\alpha(\delta-\gamma)+\gamma(\beta-\alpha) \leqslant \alpha(\beta-\alpha)+\gamma(\delta-\gamma). \tag{3.7}$$

Using $\alpha(\delta-\gamma)+\gamma(\beta-\alpha) = -\left(\alpha(\gamma-\delta)+\gamma(\alpha-\beta)\right)$ we see that inequalities 3.6 and 3.7 combine to give

$$|\alpha(\gamma-\delta)+\gamma(\alpha-\beta)| \leqslant \alpha(\beta-\alpha)+\gamma(\delta-\gamma).$$

Hence we have $\alpha(\alpha-\beta)+\gamma(\gamma-\delta)+|\alpha(\gamma-\delta)+\gamma(\alpha-\beta)| \leqslant 0$. This contradicts inequality 3.5 and therefore this case cannot occur.

This completes Case 1 and we have shown this case cannot arise.

Case 4: We have $\alpha > 0$, $\beta > 0$, $\gamma < 0$ and $\delta < 0$. We split into two subcases, $\alpha-\beta > 0$ and $\alpha-\beta < 0$.
Case 4a: $0 < \beta < \alpha$
In this subcase, Lemma 3.1.19 implies $\delta < \gamma < 0$. We now prove a lemma to assist us with this subcase.

Lemma 3.1.22.
Under the assumptions of Case 4a we have $(\beta+\delta)(\beta-\alpha+\delta-\gamma) \leqslant 0$.

Proof.
We split into two cases. First suppose $\beta+\delta>0$ and recall $\beta \not\equiv \delta \bmod 2$ as well as $\alpha \not\equiv \gamma \bmod 2$. Since $\alpha>0$ we have $\alpha(\beta+\delta)>0$ and thus $1=\alpha\delta-\beta\gamma=\alpha(\beta+\delta)-\beta(\alpha+\gamma)$, which yields $0<\alpha(\beta+\delta)=1+\beta(\alpha+\gamma)$. Since $\beta \geqslant 2$ and $\alpha+\gamma \neq 0$ $\alpha+\gamma>0$ follows immediately.
Assume $\beta-\alpha+\delta-\gamma>0$, then we have $\beta+\delta>\alpha+\gamma>0$. Therefore we have

$$0<\beta(\alpha+\gamma)<\alpha(\alpha+\gamma)<\alpha(\beta+\delta)=1+\beta(\alpha+\gamma),$$

which is a contradiction. Thus we have $\beta-\alpha+\delta-\gamma \leqslant 0$. Recalling $\beta+\delta>0$ yields the result in this subcase.
Now suppose $\beta+\delta<0$, then $\alpha(\beta+\delta)<0$. We assume $\beta-\alpha+\delta-\gamma<0$. Next, we have $1=\alpha(\beta+\delta)-\beta(\alpha+\gamma)$ implies $1+\beta(\alpha+\gamma)=\alpha(\beta+\delta)<0$ and therefore $\beta(\alpha+\gamma)<0$. Since $\beta>0$ it follows that $\alpha+\gamma<0$. Thus from the conditions of Case 4a ($\gamma<\delta<0<\beta<\alpha$) we get $\beta+\delta<\alpha+\gamma<0$ and hence $|\alpha+\gamma|<|\beta+\delta|$. Then we have $|1+\beta(\alpha+\gamma)|=|\alpha(\beta+\delta)|$ and so $|\alpha(\beta+\delta)|=|\beta(\alpha+\gamma)|-1$. Therefore we get

$$|\beta(\alpha+\gamma)|<\alpha|\alpha+\gamma|<\alpha|\beta+\delta|=|\alpha(\beta+\delta)|=|\beta(\alpha+\gamma)|-1,$$

which is a contradiction. Thus we must have $\beta-\alpha+\delta-\gamma \geqslant 0$. Recalling $\beta+\delta<0$ yields the result in this case. Hence we always have $(\beta+\delta)(\beta-\alpha+\delta-\gamma) \leqslant 0$. □

Now under the assumptions of Case 4a we have $\beta-\alpha<0$ and $\delta-\gamma>0$, which imply $\beta(\beta-\alpha)<0$ and $\delta(\delta-\gamma)<0$. Let $A_{ii}=\min\{A_{11},A_{22}\}>0$ and note $\beta(\delta-\gamma)>0$ and $\delta(\beta-\alpha)>0$. Then inequality 3.3 becomes

$$\begin{aligned}
0 &\leqslant \underbrace{2\beta(\beta-\alpha)}_{<0}A_{11}+\underbrace{\beta(\delta-\gamma)}_{>0}(A_{12}+A_{21})+\underbrace{\delta(\beta-\alpha)}_{>0}(A_{12}+A_{21})+2\underbrace{\delta(\delta-\gamma)}_{<0}A_{22}\\
&\leqslant 2\beta(\beta-\alpha)A_{ii}+(A_{12}+A_{21})(\beta(\delta-\gamma)+\delta(\beta-\alpha))+2\delta(\delta-\gamma)A_{ii}\\
&\leqslant 2\beta(\beta-\alpha)A_{ii}+2A_{ii}(\beta(\delta-\gamma)+\delta(\beta-\alpha))+2\delta(\delta-\gamma)A_{ii} \text{ as } |A_{12}+A_{21}| \leqslant 2A_{ii}\\
&= 2A_{ii}\left(\beta(\beta-\alpha)+\beta(\delta-\gamma)+\delta(\beta-\alpha)+\delta(\delta-\gamma)\right)\\
&= 2A_{ii}(\beta+\delta)(\beta-\alpha+\delta-\gamma).
\end{aligned}$$

We note the condition for being Kronecker reduced implies we cannot have equality throughout. Therefore we have $0<2A_{ii}(\beta+\delta)(\beta-\alpha+\delta-\gamma)$. However, $A_{ii}>0$ and Lemma 3.1.22 yields $(\beta+\delta)(\beta-\alpha+\delta-\gamma) \leqslant 0$ and thus we have a contradiction. So Case 4a cannot arise.

Case 4b: $0<\alpha<\beta$
Then Lemma 3.1.19 implies $\delta<\gamma<0$. We first prove a lemma to streamline this subcase.

Lemma 3.1.23.
Under the assumptions of Case 4b we have $(\alpha+\gamma)(\alpha-\beta+\gamma-\delta) \leqslant 0$.

Proof.
Observe $1 = \alpha\delta - \beta\gamma = \delta(\alpha+\gamma) - \gamma(\beta+\delta)$. We split into two cases. First suppose $\alpha+\gamma > 0$, then $1 = \alpha\delta + \beta(-\gamma) < \alpha\delta + \alpha\beta = \alpha(\beta+\delta)$. Since $\alpha > 0$ it follows that $\beta+\delta > 0$. Note also that $\delta(\alpha+\gamma) < 0$ and $\gamma(\beta+\delta) < 0$. Assume $\alpha-\beta+\gamma-\delta > 0$, then we have $\alpha+\gamma > \beta+\delta > 0$. Next, $1 = \delta(\alpha+\gamma) - \gamma(\beta+\delta)$ implies $1+\gamma(\beta+\delta) = \delta(\alpha+\gamma) < 0$. Therefore we get:

$$\begin{aligned} 0 < |\delta(\alpha+\gamma)| &= |1+\gamma(\beta+\delta)| \\ &= |\gamma(\beta+\delta)| - 1 \\ &< |\gamma|(\alpha+\gamma) \\ &< |\delta|(\alpha+\gamma), \end{aligned}$$

which is a contradiction. Therefore we have $\alpha-\beta+\gamma-\delta \leqslant 0$ and recalling $\alpha+\gamma > 0$ yields our result in this case.
Now suppose $\alpha+\gamma < 0$. Then $\delta < 0$ implies $\delta(\alpha+\gamma) > 0$. Using $\gamma(\beta+\delta) = \delta(\alpha+\gamma) - 1 \geqslant 0$ and $\gamma < 0$ we see that $\beta+\delta < 0$ as $\beta \not\equiv \delta \bmod 2$. Assume $\alpha-\beta+\gamma-\delta < 0$, then we have $\alpha+\gamma < \beta+\delta < 0$. Using this along with $0 < \gamma(\beta+\delta) = \delta(\alpha+\gamma) - 1$ gives:

$$\begin{aligned} 0 &< |\gamma(\beta+\delta)| \\ &< |\delta||\beta+\delta| \\ &< |\delta||\alpha+\gamma| \\ &= |\gamma||\beta+\delta| + 1 \text{ as } 0 < \gamma(\beta+\delta). \end{aligned}$$

This is a contradiction as it implies consecutive integers are separated by at least two. Therefore we must have $\alpha-\beta+\gamma-\delta \geqslant 0$. Recalling $\alpha+\gamma < 0$ then gives our result.
Hence we always have $(\alpha+\gamma)(\alpha-\beta+\gamma-\delta) \leqslant 0$. □

Now under the assumptions of Case 4b we have $\alpha(\alpha-\beta) < 0$, $\gamma(\gamma-\delta) < 0$, $\alpha(\gamma-\delta) > 0$ and $\gamma(\alpha-\beta) > 0$. Let $A_{ii} = \min\{A_{11}, A_{22}\} > 0$, then inequality 3.1 becomes:

$$\begin{aligned} 0 &\leqslant 2\underbrace{\alpha(\alpha-\beta)}_{<0}A_{11} + \underbrace{\alpha(\gamma-\delta)}_{>0}(A_{12}+A_{21}) + \underbrace{\gamma(\alpha-\beta)}_{>0}(A_{12}+A_{21}) + 2\underbrace{\gamma(\gamma-\delta)}_{<0}A_{22} \\ &\leqslant 2(\alpha(\alpha-\beta)+\gamma(\gamma-\delta))A_{ii} + (\alpha(\gamma-\delta)+\gamma(\alpha-\beta))(A_{12}+A_{21}) \\ &\leqslant 2(\alpha(\alpha-\beta)+\gamma(\gamma-\delta))A_{ii} + 2(\alpha(\gamma-\delta)+\gamma(\alpha-\beta))A_{ii} \text{ as } |A_{12}+A_{21}| \leqslant 2A_{ii} \\ &= 2A_{ii}(\alpha+\gamma)(\alpha-\beta+\gamma-\delta). \end{aligned}$$

Observe the conditions for being Kronecker reduced imply equality cannot hold throughout. Therefore we have $0 < 2A_{ii}(\alpha+\gamma)(\alpha-\beta+\gamma-\delta)$. Using $A_{ii} > 0$ and recalling Lemma 3.1.23 implies $(\alpha+\gamma)(\alpha-\beta+\gamma-\delta) \leqslant 0$ gives a contradiction and thus Case 4b cannot occur.

This completes Case 4, showing that it cannot arise.

Case 6: We have $\alpha > 0$, $\beta < 0$, $\gamma > 0$ and $\delta < 0$. We split into two subcases, $\alpha+\beta > 0$ and $\alpha + \beta < 0$.
Case 6a: $\alpha + \beta > 0$
Observe that if $0 < \gamma < -\delta = |\delta|$ then we have

$$\begin{aligned} 1 = \alpha\delta - \beta\gamma &= |\beta|\gamma - \alpha|\delta| \\ &< \alpha\gamma - \alpha|\delta| \\ &< \alpha\gamma - \alpha\gamma = 0, \end{aligned}$$

which is a contradiction. Therefore we have $0 < -\delta < \gamma$, i.e. $\gamma + \delta > 0$. We now prove a lemma to streamline this case.

Lemma 3.1.24.
Under the assumptions of Case 6a we have $(\beta - \delta)(\alpha + \beta - \delta - \gamma) \leqslant 0$.

Proof.
We split into two subcases: $\beta - \delta > 0$ and $\beta - \delta < 0$ as $\beta \not\equiv \delta \bmod 2$.
First suppose $\beta-\delta > 0$. Next, assume $\alpha+\beta-\delta-\gamma > 0$. It follows that $\beta-\delta > \gamma-\alpha$. We observe if $\gamma - \alpha < 0$ then we get the following contradiction

$$1 = \alpha\delta - \beta\gamma = |\beta|\gamma - \alpha|\delta| < |\beta|\gamma - \alpha|\beta| < |\beta|\alpha - |\beta|\alpha = 0.$$

Therefore we have $0 < \gamma-\alpha < \beta-\delta$. Now observe $1 = \alpha\delta-\beta\gamma = (\alpha-\gamma)\delta-(\beta-\delta)\gamma$. This yields $\delta(\alpha - \gamma) = 1 + (\beta - \delta)\gamma$. Then we see:

$$\begin{aligned} 1 + (\alpha - \gamma)\delta &= 1 + (\gamma - \alpha)|\delta| \\ &< 1 + (\gamma - \alpha)\gamma \text{ as } |\delta| < \gamma \text{ in Case 6a} \\ &< 1 + (\beta - \delta)\gamma \\ &= (\alpha - \gamma)\delta. \end{aligned}$$

This is clearly a contradiction. Therefore we require $\alpha+\beta-\delta-\gamma \leqslant 0$. Hence recalling $\beta + \delta > 0$ yields the result in this case.
Now suppose $\beta - \delta < 0$, since $\beta < 0$, $\delta < 0$ this yields $0 < |\delta| < |\beta|$. Assume $\alpha + \beta - \delta - \gamma < 0$, that is $\beta - \delta < \gamma - \alpha$. If we suppose $0 < \gamma - \alpha$ then we obtain

$$1 = \alpha\delta - \beta\gamma = |\beta|\gamma - \alpha|\delta| < |\delta|\gamma - \alpha|\delta| < |\delta|\alpha - |\delta|\alpha = 0.$$

This again is a contradiction and thus we have $\beta - \delta < \gamma - \alpha < 0$ as $\alpha \not\equiv \gamma \bmod 2$.
Next, we see $1 = (\alpha - \gamma)\delta - (\beta - \delta)\gamma$ gives

$$\begin{aligned} (\alpha - \gamma)\delta = 1 + (\beta - \delta)\gamma & \\ &< 1 + (\gamma - \alpha)\gamma \\ &< 1 + (\gamma - \alpha)|\delta| \text{ as in Case 6a } |\delta| < \gamma \\ &= 1 + (\alpha - \gamma)\delta. \end{aligned}$$

This is a contradiction because it implies two consecutive integers are separated by at least two. Therefore we have $\alpha+\beta-\delta-\gamma \geqslant 0$. Recalling $\beta-\delta<0$ yields the result.
Hence under the assumptions of Case 6a we have $(\beta-\delta)(\alpha+\beta-\delta-\gamma) \leqslant 0$. $\square$

Now under the assumptions of Case 6a we have $\beta(\alpha+\beta)<0$, $\delta(\alpha+\beta)<0$, $\delta(\delta+\gamma)<0$ and $\beta(\delta+\gamma)<0$. Using inequality 3.4 we immediately see if $A_{12}+A_{21} \geqslant 0$ then we have a contradiction. Hence we suppose $A_{12}+A_{21}<0$. Let $A_{ii}=\min\{A_{11},A_{22}\}>0$, then inequality 3.4 becomes:

$$\begin{aligned}0 &\leqslant 2\beta(\alpha+\beta)A_{11}+\underbrace{(\beta(\delta+\gamma)+\delta(\alpha+\beta)}_{<0}\underbrace{(A_{12}+A_{21})}_{<0}+2\delta(\delta+\gamma)A_{22}\\ &\leqslant 2\left(\beta(\alpha+\beta)+\delta(\delta+\gamma)\right)A_{ii}+|\beta(\delta+\gamma)+\delta(\alpha+\beta)|\,|A_{12}+A_{21}|\\ &\leqslant 2A_{ii}\left(\beta(\alpha+\beta)+\delta(\delta+\gamma)+|\beta(\delta+\gamma)+\delta(\alpha+\beta)|\right).\end{aligned}$$

Observe the conditions for being Kronecker reduced imply equality cannot hold throughout. Thus we have $0<2A_{ii}\left(\beta(\alpha+\beta)+\delta(\delta+\gamma)+|\beta(\delta+\gamma)+\delta(\alpha+\beta)|\right)$. This rearranges to give $0<2A_{ii}(\beta-\delta)(\alpha+\beta-\delta-\gamma)$. Lemma 3.1.24 implies $(\beta-\delta)(\alpha+\beta-\delta-\gamma)\leqslant 0$ and since $A_{ii}>0$ we see there is a contradiction. Therefore Case 6a cannot arise.

Case 6b: $\alpha+\beta<0$
Observe that if $0<|\delta|=-\delta<\gamma$ then we have

$$\begin{aligned}1&=\alpha\delta-\beta\gamma\\ &=|\beta|\gamma-\alpha|\delta|\\ &>|\beta|\gamma-\alpha\gamma\\ &=(|\beta|-\alpha)\,\gamma\\ &>0.\end{aligned}$$

This is because $\alpha+\beta<0$ implies $0<\alpha<-\beta=|\beta|$, thus $|\beta|-\alpha$ and γ are both positive non-zero integers. Since no integer exists in $(0,1)$ it follows that $0<\gamma<-\delta=|\delta|$ as $\gamma\not\equiv\delta \bmod 2$. Hence $\delta+\gamma<0$. We now prove a lemma to streamline this case.

Lemma 3.1.25.
Under the assumptions of Case 6b we have $(\alpha-\gamma)(\alpha+\beta-\gamma-\delta)\leqslant 0$.

Proof.
We split into two cases, $\alpha-\gamma>0$ and $\alpha-\gamma<0$ since $\alpha\not\equiv\gamma \bmod 2$.
First suppose $\alpha-\gamma>0$, that is $0<\gamma<\alpha$. Next, assume $\alpha+\beta-\gamma-\delta>0$, then $\alpha-\gamma>\delta-\beta$. We observe if $\delta-\beta>0$, i.e. $0<|\delta|<|\beta|$, then we get the following contradiction:

$$\begin{aligned}1=\alpha\delta-\beta\gamma&=|\beta|\gamma-\alpha|\delta|\\ &>|\beta|\alpha-\alpha|\delta|\end{aligned}$$

$$\begin{aligned} &= \alpha(|\beta| - |\delta|) \\ &> 0. \end{aligned}$$

This is because α and $|\beta| - |\delta|$ are positive integers and there is no integer in the interval $(0, 1)$. Thus we have $\delta - \beta < 0 < \alpha - \gamma$. From this we have $1 = \alpha\delta - \beta\gamma = (\alpha - \gamma)\delta - (\beta - \delta)\gamma$, which implies $\underbrace{(\alpha - \gamma)\delta}_{<0} = 1 + \underbrace{\gamma(\beta - \delta)}_{>0}$. This is a contradiction and thus $\alpha + \beta - \gamma - \delta \leqslant 0$. Recalling $\alpha - \gamma > 0$ then gives the result in this case.
Now suppose $\alpha - \gamma < 0$. Assume $\alpha + \beta - \gamma - \delta < 0$, then we have $\alpha - \gamma < \delta - \beta$. We observe if $\delta - \beta < 0$ then we get the following contradiction:

$$\begin{aligned} 1 = \alpha\delta - \beta\gamma &= |\beta|\gamma - \alpha|\delta| \\ &> |\beta|\gamma - \alpha|\beta| \\ &= |\beta|(\gamma - \alpha) \\ &> 0. \end{aligned}$$

This is because $|\beta|$ and $\gamma - \alpha$ are positive integers and there is no integer in the interval $(0, 1)$. Thus we have $\alpha - \gamma < 0 < \delta - \beta$. Using this we see $1 = \alpha\delta - \beta\gamma = (\alpha - \gamma)\delta - (\beta - \delta)\gamma$ implies $\underbrace{(\alpha - \gamma)\delta}_{>0} = 1 + \underbrace{(\beta - \delta)\gamma}_{<0} < 1$. Since we are dealing with integers this is a contradiction. Therefore we must have $\alpha + \beta - \gamma - \delta \geqslant 0$. Recalling $\alpha - \gamma < 0$ gives the result in this case.
Hence we see that under the assumptions of Case 6b we always have $(\alpha - \gamma)(\alpha + \beta - \gamma - \delta) \leqslant 0$. □

Now under the assumptions of Case 6b we have $\alpha(\alpha+\beta) < 0$, $\alpha(\gamma+\delta) < 0$, $\gamma(\alpha+\beta) < 0$ and $\gamma(\gamma+\delta) < 0$. Using inequality 3.2 we immediately see if $A_{12} + A_{21} \geqslant 0$ then we have a contradiction. Hence we suppose $A_{12} + A_{21} < 0$ and let $A_{ii} = \min\{A_{11}, A_{22}\} > 0$. Then inequality 3.2 becomes:

$$\begin{aligned} 0 &\leqslant 2\alpha(\alpha + \beta)A_{11} - (\alpha(\gamma + \delta) + \gamma(\alpha + \beta))\,|A_{12} + A_{21}| + 2\gamma(\gamma + \delta)A_{22} \\ &\leqslant 2\,(\alpha(\alpha + \beta) + \gamma(\gamma + \delta))\,A_{ii} - (\alpha(\gamma + \delta) + \gamma(\alpha + \beta))\,|A_{12} + A_{21}| \\ &\leqslant 2\,(\alpha(\alpha + \beta) + \gamma(\gamma + \delta))\,A_{ii} - 2A_{ii}\,(\alpha(\gamma + \delta) + \gamma(\alpha + \beta)) \\ &= 2A_{ii}(\alpha - \gamma)(\alpha + \beta - \gamma - \delta). \end{aligned}$$

Since we are dealing with Kronecker reduced bilinear forms, we cannot have equality throughout. Hence we have

$$0 < 2A_{ii}(\alpha - \gamma)(\alpha + \beta - \gamma - \delta).$$

Lemma 3.1.25 implies $(\alpha - \gamma)(\alpha + \beta - \gamma - \delta) \leqslant 0$ and since $A_{ii} > 0$ it follows that we have a contradiction. Therefore Case 6b cannot arise.

Case 7: We have $\alpha > 0$, $\beta < 0$, $\gamma < 0$ and $\delta > 0$. We split into two subcases: $\alpha+\beta > 0$ and $\alpha + \beta < 0$ as $\alpha \not\equiv \beta \bmod 2$.

Case 7a: $\alpha + \beta > 0$
Observe if $\delta + \gamma > 0$ then we have the following contradiction:

$$\begin{aligned} 1 = \alpha\delta - \beta\gamma &= \alpha\delta - |\beta||\gamma| \\ &> |\beta|\delta - |\beta||\gamma| \text{ as } \alpha > -\beta = |\beta| > 0 \\ &= |\beta|(\delta + \gamma) \\ &> 0. \end{aligned}$$

Thus $\alpha + \beta > 0$ implies $\delta + \gamma < 0$. We now prove a lemma to help streamline this case.

Lemma 3.1.26.
Under the assumptions of Case 7a we have $(\beta + \delta)(\alpha + \beta + \gamma + \delta) \leqslant 0$.

Proof.
We split into two cases: $\beta + \delta > 0$ and $\beta + \delta < 0$ as $\beta \not\equiv \delta \bmod 2$.
First suppose $\beta + \delta > 0$, thus $0 < |\beta| = -\beta < \delta$ and so $1 - \beta \leqslant \delta$. Next, assume $\alpha + \beta + \gamma + \delta > 0$, then we have $-(\alpha + \gamma) < \beta + \delta$. If we assume $\alpha + \gamma > 0$ then $\alpha > -\gamma = |\gamma|$ and we get the following contradiction:

$$\begin{aligned} 1 = \alpha\delta - \beta\gamma &\geqslant (1 - \gamma)(1 - \beta) - \beta\gamma \\ &= 1 - \gamma - \beta + \beta\gamma - \beta\gamma \\ &= 1 - \gamma - \beta \\ &\geqslant 5 \text{ as } \gamma \leqslant -2 \text{ and } \beta \leqslant -2. \end{aligned}$$

Therefore we must have $\alpha + \gamma < 0$ and thus $0 < -(\alpha + \gamma) < \beta + \delta$. That is $|\alpha + \gamma| < |\beta + \delta|$. Further we have $1 = \alpha\delta - \beta\gamma = (\alpha + \gamma)\delta - \gamma(\beta + \delta)$ so $1 + \gamma(\delta + \beta) = (\alpha + \gamma)\delta < 0$. Therefore we have $|\gamma(\beta + \delta)| - 1 = |1 + \gamma(\beta + \delta)| = |\delta(\alpha + \gamma)|$. Then recalling $\delta + \gamma < 0$, that is, $0 < \delta < |\gamma|$ yields:

$$|\gamma(\beta + \delta)| - 1 = |\delta(\alpha + \gamma)| < |\gamma||\alpha + \gamma| < |\gamma||\beta + \delta|.$$

This is a contradiction because it implies two consecutive integers are separated by more than two integers. Therefore we must have $\alpha + \beta + \gamma + \delta \leqslant 0$ and recalling $\beta + \delta > 0$ gives the result in this case.
Now suppose $\beta + \delta < 0$ and so $0 < \delta < -\beta = |\beta|$. Therefore $\delta \leqslant -1 - \beta$. Further assume $\alpha + \beta + \gamma + \delta < 0$, which implies $\beta + \delta < -(\alpha + \gamma)$. If we assume $\alpha + \gamma < 0$ then we get the following contradiction:

$$\begin{aligned} 1 = \alpha\delta - \beta\gamma &\leqslant (-1 - \beta)(-1 - \gamma) - \beta\gamma \\ &= (1 + \beta)(1 + \gamma) - \beta\gamma \\ &= 1 + \beta + \gamma \\ &\leqslant -3 \text{ as } \beta \leqslant -2 \text{ and } \gamma \leqslant -2. \end{aligned}$$

Therefore $\alpha+\gamma>0$ and we have $\beta+\delta<-(\alpha+\gamma)<0$. Hence $|\alpha+\gamma|<|\beta+\delta|$. Recall $\delta+\gamma<0$ yields $0<\delta<|\gamma|$ and observe $\gamma(\beta+\delta)>0$ and $\delta(\alpha+\gamma)>0$. Next, $1=\alpha\delta-\beta\gamma=(\alpha+\gamma)\delta-\gamma(\beta+\delta)$ gives $(\alpha+\gamma)\delta=1+\gamma(\beta+\delta)$. Hence we get

$$\begin{aligned}1+\gamma(\beta+\delta)&=(\alpha+\gamma)\delta\\&=|(\alpha+\gamma)\delta|\\&<|\alpha+\gamma||\gamma|\\&<|\beta+\delta||\gamma|\\&=|\gamma(\beta+\delta)|\\&=\gamma(\beta+\delta).\end{aligned}$$

This is a contradiction and therefore we must have $\alpha+\beta+\gamma+\delta\geqslant 0$. Recalling $\beta+\delta<0$ then yields the result in this case.
Hence under the assumptions of Case 7a we always have $(\beta+\delta)(\alpha+\beta+\gamma+\delta)\leqslant 0$. $\square$

Now observe under the assumptions of Case 7a we have $\beta(\alpha+\beta)<0$, $\delta(\delta+\gamma)<0$, $\beta(\delta+\gamma)>0$ and $\delta(\alpha+\beta)>0$. We let $A_{ii}=\min\{A_{11},A_{22}\}$ and consider inequality 3.4. This yields:

$$\begin{aligned}0&\leqslant 2\beta(\alpha+\beta)A_{11}+\beta(\delta+\gamma)(A_{12}+A_{21})+\delta(\alpha+\beta)(A_{12}+A_{21})+2\delta(\delta+\gamma)A_{22}\\&\leqslant 2A_{ii}(\beta(\alpha+\beta)+\delta(\delta+\gamma))+(A_{12}+A_{21})(\beta(\delta+\gamma)+\delta(\alpha+\beta))\text{ as subtracting less}\\&\leqslant 2A_{ii}(\beta(\alpha+\beta)+\delta(\delta+\gamma))+2A_{ii}(\beta(\delta+\gamma)+\delta(\alpha+\beta))\text{ as }|A_{12}+A_{21}\leqslant 2A_{ii}\\&=2A_{ii}(\beta+\delta)(\alpha+\beta+\gamma+\delta).\end{aligned}$$

We observe that since our bilinear forms are Kronecker reduced we cannot have equality holding throughout. Thus

$$0<2A_{ii}(\beta+\delta)(\alpha+\beta+\gamma+\delta).$$

Since $A_{ii}>0$ and Lemma 3.1.26 yields $(\beta+\delta)(\alpha+\beta+\gamma+\delta)\leqslant 0$, we have a contradiction. Hence Case 7a cannot arise.

Case 7b: $\alpha+\beta<0$
Observe that if $\delta+\gamma<0$ then we get the following contradiction:

$$\begin{aligned}1&=\alpha\delta-\beta\gamma\\&=\alpha\delta-|\beta||\gamma|\\&<\alpha|\gamma|-|\beta||\gamma|\\&=|\gamma|(\alpha+\beta)\\&<0.\end{aligned}$$

Hence in Case 7b we have $\delta+\gamma>0$. We now prove a lemma to help streamline our proof.

Lemma 3.1.27.
Under the assumptions of Case 7b we have $(\alpha+\gamma)(\alpha+\beta+\gamma+\delta)\leqslant 0$.

Proof.
We split into two subcases: $\alpha+\gamma>0$ and $\alpha+\gamma<0$ as $\alpha \not\equiv \gamma \bmod 2$. First suppose $\alpha+\gamma>0$ and so $0<|\gamma|=-\gamma<\alpha$, which implies $-1-\gamma \leqslant \alpha$ as $\gamma \leqslant -2$. Next assume $\alpha+\beta+\gamma+\delta>0$, then we have $\alpha+\gamma>-(\beta+\delta)$. If we suppose $\beta+\delta>0$ then we get the following contradiction:

$$\begin{aligned} 1=\alpha\delta-\beta\gamma &\leqslant (-1-\beta)(-1-\gamma)-\beta\gamma \\ &= (1+\beta)(1+\gamma)-\beta\gamma \\ &= 1+\beta+\gamma \\ &\leqslant -3 \text{ as } \beta \leqslant -2 \text{ and } \gamma \leqslant -2. \end{aligned}$$

Therefore we have $\beta+\delta<0$ and so $0<-(\beta+\delta)<\alpha+\gamma$, which yields $|\beta+\delta|<|\alpha+\gamma|$. Now we write $1=\alpha\delta-\beta\gamma=(\alpha+\gamma)\delta-\gamma(\delta+\beta)$, which gives $0<(\alpha+\gamma)\delta=1+\gamma(\delta+\beta)$. Recall $\delta+\gamma>0$ implies $0<|\gamma|<\delta$. Then we have

$$\gamma(\delta+\beta)=|\gamma(\delta+\beta)|<|\delta(\delta+\beta)|<|\delta(\alpha+\gamma)|=1+\gamma(\delta+\beta).$$

This is a contradiction as we have two consecutive integers separated by at least two integers. Therefore in this case we must have $\alpha+\beta+\gamma+\delta \leqslant 0$ and recalling $\alpha+\gamma>0$ yields the result here.
Now suppose $\alpha+\gamma<0$ so $0<\alpha<|\gamma|$. Further assume $\alpha+\beta+\gamma+\delta<0$, which gives $\alpha+\gamma<-(\beta+\delta)$. If we suppose $\beta+\delta<0$ then we get the following contradiction:

$$1=\alpha\delta-\beta\gamma \leqslant (-1-\beta)(-1-\gamma)-\beta\gamma=1+\beta+\gamma \leqslant -3.$$

Therefore we have $\beta+\delta>0$ and thus $\alpha+\gamma<-(\beta+\delta)<0$. This yields $|\beta+\delta|<|\alpha+\gamma|$. Then we have $1=\alpha\delta-\beta\gamma=(\alpha+\gamma)\delta-(\delta+\beta)\gamma$ which rearranges to $1+\gamma(\delta+\beta)=(\alpha+\gamma)\delta<0$. This gives $|(\alpha+\gamma)\delta|=|1+\gamma(\delta+\beta)|=|\gamma(\delta+\beta)|-1$ and thus:

$$|\gamma(\delta+\beta)|<|\delta(\delta+\beta)|<|\delta(\alpha+\gamma)|=|\gamma(\delta+\beta)|-1.$$

This is clearly a contradiction and so we must have $\alpha+\beta+\gamma+\delta \geqslant 0$. Recalling $\alpha+\delta<0$ yields the result in this case.
Hence under the assumptions of Case 7b we always have $(\alpha+\gamma)(\alpha+\beta+\gamma+\delta) \leqslant 0$. □

Now under the assumptions of Case 7b we have $\alpha(\alpha+\beta)<0$, $\gamma(\delta+\gamma)<0$, $\alpha(\delta+\gamma)>0$ and $\gamma(\alpha+\beta)>0$. Again, let $A_{ii}=\min\{A_{11},A_{22}\}$ and consider inequality 3.2. This gives

$$\begin{aligned} 0 &\leqslant 2\alpha(\alpha+\beta)A_{11}+\alpha(\delta+\gamma)(A_{12}+A_{21})+\gamma(\alpha+\beta)(A_{12}+A_{21})+2\gamma(\gamma+\delta)A_{22} \\ &\leqslant 2\left((\alpha+\beta)\alpha+\gamma(\delta+\gamma)\right)A_{ii}+\left(\alpha(\delta+\gamma)+\gamma(\alpha+\beta)\right)(A_{12}+A_{21}) \\ &\leqslant 2\left(\alpha(\alpha+\beta)+\gamma(\delta+\gamma)\right)A_{ii}+2A_{ii}\left(\alpha(\delta+\gamma)+\gamma(\alpha+\beta)\right) \text{ as } |A_{12}+A_{21} \leqslant 2A_{ii} \\ &= 2A_{ii}(\alpha+\gamma)(\alpha+\beta+\gamma+\delta). \end{aligned}$$

Since we are dealing with Kronecker reduced forms we cannot have equality holding throughout. Therefore we have

$$0<2A_{ii}(\alpha+\gamma)(\alpha+\beta+\gamma+\delta).$$

Lemma 3.1.27 implies $(\alpha+\gamma)(\alpha+\beta+\gamma+\delta) \leqslant 0$ and we have $A_{ii} > 0$. This gives a contradiction and hence Case 7b cannot arise.

This completes our investigation of the eight cases and thus we have proved the following theorem.

Theorem 3.1.28.
The complete equivalence class of a bilinear form contains exactly one Kronecker reduced bilinear form unless the Kronecker reduced bilinear form satisfies either $|A_{12}+A_{21}| = 2A_{11}$ *or* $|A_{12}+A_{21}| = 2A_{22}$*, in which case it contains exactly two Kronecker reduced bilinear forms.*

Our goal now is prove a result that Kronecker stated but did not prove in his paper. Kronecker's result is given in the following theorem.

Theorem 3.1.29.
Let $D \in \mathbb{Z}_{>0}$ *then* $\mathrm{Cl}_c(D) = |B^0| + |B^1|$ *where*

$$B^0 = \{(A_{11}, A_{12}, A_{21}, A_{22}) \,|A_{11}A_{22} - A_{12}A_{21} = D, 0 < \frac{1}{2}(A_{12}+A_{21}) \leqslant A_{11}, \\ 0 < \frac{1}{2}(A_{12}+A_{21}) \leqslant A_{22}, \text{ equality holds at most once}\}$$

and

$$B^1 = \{(A_{11}, A_{12}, A_{21}, A_{22}) \,|A_{11}A_{22} - A_{12}A_{21} = D, 0 \leqslant \frac{1}{2}(A_{12}+A_{21}) < A_{11}, \\ 0 \leqslant \frac{1}{2}(A_{12}+A_{21}) < A_{22}\}.$$

Observation 3.1.30.
The following provides a sketch of the proof of Theorem 3.1.29. It is intended to serve as a guide while working through the proof and to indicate how the sets B^0 and B^1 were probably chosen by Kronecker.
From Theorem 3.1.28 we know that with only one exception there is exactly one Kronecker reduced bilinear form within any complete equivalence class of positive definite bilinear forms. This exception is when the Kronecker reduced bilinear form satisfies $|A_{12}+A_{21}| = 2A_{11}$ or $|A_{12}+A_{21}| = 2A_{22}$ in which case there are two Kronecker reduced bilinear forms in the complete equivalence class.
In the conditions for being Kronecker reduced we note that when both inequalities are strict and $A_{12}+A_{21} \neq 0$, the absolute value requirement means there are two Kronecker reduced forms to be counted simply by multiplying each of A_{12} and A_{21} by -1. Thus the intersection of the sets B^0 and B^1 accounts for all of these Kronecker reduced forms exactly once.
Now we consider those Kronecker reduced bilinear forms where equality holds exactly once. We know that the Kronecker reduced bilinear forms $(A_{11}, A_{12}, A_{21}, A_{22})$ and $(A_{11}, -A_{12}, -A_{21}, A_{22})$ are distinct (as $A_{12}+A_{21} \neq 0$) and contained within the same complete equivalence class in this situation. Therefore it is sufficient to count only

those Kronecker forms for which $0 < A_{12} + A_{21}$ ($= 2A_{11}$ or $2A_{22}$. These are counted exactly once by the equality condition found in the set B^0.
Lastly, we consider those Kronecker reduced bilinear forms which satisfy $0 = A_{12} + A_{21}$. In this situation there is exactly one Kronecker reduced bilinear form in the complete equivalence class and so changing the sign of A_{12} and A_{21} results in a new complete equivalence class. Therefore we do not double count when we count these forms by introducing the conditions $0 \leqslant A_{12} + A_{21} < 2A_{11}$ and $0 \leqslant A_{12} + A_{21} < 2A_{22}$ in the set B^1.
Consequently, by using the sets B^0 and B^1 we have consistently counted all of the complete equivalence classes of positive definite binary bilinear forms exactly once.

Before we prove this theorem we need the following lemma.

Lemma 3.1.31.
Let
$V_+ = \{A = (A_{11}, A_{12}, A_{21}, A_{22}) | \det(A) = D, 0 < A_{12} + A_{21} < 2\min\{A_{11}, A_{22}\}\}$ *and*
$V_- = \{A = (A_{11}, A_{12}, A_{21}, A_{22}) | \det(A) = D, -2\min\{A_{11}, A_{22}\} < A_{12} + A_{21} < 0\}$.
Then the map

$$\begin{aligned} \nu : V_- &\longrightarrow V_+ \\ (A_{11}, A_{12}, A_{21}, A_{22}) &\longmapsto (A_{11}, -A_{12}, -A_{21}, A_{22}) = (a_{11}, a_{12}, a_{21}, a_{22}) \end{aligned}$$

is a bijection and thus $|V_-| = |V_+|$.

Proof.
Observe the sets V_+ and V_- are subsets of $\mathcal{K}_{D,>}$, the set of complete equivalence classes of positive definite bilinear forms of determinant $D \in \mathbb{Z}_{>0}$. In Theorem 3.1.15 we proved $\mathcal{K}_{D,>}$ is finite and thus so are V_+ and V_-. We fix $D \in \mathbb{Z}_{>0}$.
Well-defined: Observe

$$\begin{aligned} \det(\nu(A_{11}, A_{12}, A_{21}, A_{22})) &= A_{11}A_{22} - (-A_{12})(-A_{21}) \\ &= \det(A_{11}, A_{12}, A_{21}, A_{22}) \\ &= D. \end{aligned}$$

We also have $a_{12} + a_{21} = -A_{12} - A_{21} = -(A_{12} + A_{21})$ and since $-2\min\{A_{11}, A_{22}\} < A_{12} + A_{21} < 0$ this implies $0 < a_{12} + a_{21} < 2\min\{A_{11}, A_{22}\}$. Hence ν is well-defined.
Injectivity: This is straightforward to verify directly.
Surjectivity: Let $\mathcal{B} = (B_{11}, B_{12}, B_{21}, B_{22}) \in V_+$ and consider
$\mathcal{C} = (B_{11}, -B_{12}, -B_{21}, B_{22})$. This lies in V_- since $\det(C) = B_{11}B_{22} - (-B_{12})(-B_{21}) = D$ and $-2\min\{B_{11}, B_{22}\} < -(B_{12} + B_{21}) < 0$ since $\mathcal{B} \in V_+$.
Noting $\nu(B_{11}, -B_{12}, -B_{21}, B_{22}) = (B_{11}, B_{12}, B_{21}, B_{22})$ yields surjectivity.
Hence the map ν is a bijection between finite sets and we have $|V_-| = |V_+|$. □

We now prove Theorem 3.1.29.

Proof.
Let $D \in \mathbb{Z}_{>0}$ and consider the set of all positive definite Kronecker reduced bilinear

forms of determinant D. From Theorem 3.1.16 we know every complete equivalence class of a positive definite bilinear form of determinant D contains at least one Kronecker reduced bilinear form. Therefore using Theorem 3.1.15 we know $\mathrm{Cl}_c(D) \leqslant |\mathcal{K}_{D,>}| < \infty$. Next, from our work in Section 3.1 we know there is exactly one Kronecker reduced bilinear form in a complete equivalence class if and only if that Kronecker reduced bilinear form does not satisfy either $|A_{12} + A_{21}| = 2A_{11}$ or $|A_{12} + A_{21}| = 2A_{22}$.
We partition the set of complete equivalence classes of positive definite bilinear forms of determinant D into the four (finite) disjoint sets, V_+, V_- (from Lemma 3.1.31), V_0 and $V_=$, where
$V_0 = \{(A_{11}, A_{12}, A_{21}, A_{22}) \mid \det(A) = D, 0 = A_{12} + A_{21}, 0 < A_{11}, 0 < A_{22}\}$ and
$V_= = \{(A_{11}, A_{12}, A_{21}, A_{22}) \mid \det(A) = D, 2A_{11} = |A_{12} + A_{21}| \text{ or } 2A_{22} = |A_{12} + A_{21}|\}$.
Observe that the set B^1 is precisely the union of V_+ and V_0, each of which contain Kronecker reduced forms that have their own unique complete equivalence classes.
Now let $A = (A_{11}, A_{12}, A_{21}, A_{22})$ be a Kronecker reduced bilinear form satisfying exactly one of $2A_{11} = |A_{12} + A_{21}|$ or $2A_{22} = |A_{12} + A_{21}|$, that is $A \in V_=$. In Section 3.1 we demonstrated the complete equivalence class of such a Kronecker reduced form contains exactly one other Kronecker reduced form, namely $A'- = (A_{11}, -A_{12}, -A_{21}, A_{22})$. Therefore we may choose our representative for this complete equivalence class to satisfy $0 < A_{12} + A_{21} = 2A_{11}$ or $0 < A_{12} + A_{21} = 2A_{22}$ respectively. It is straightforward to see that each of these equivalence classes are counted by equality within the conditions of the set B^0. We now examine $B^0 \backslash V_=$. Applying Lemma 3.1.31 we see that $|B^0 \backslash V_=| = |V_-|$.
Hence we have $\mathrm{Cl}_c(D) = |V_+| + |V_-| + |V_0| + |V_=| = |B^0| + |B^1|$. □

Notes on Section 3.1

In his paper [Kr1897] Kronecker does not explicitly demonstrate that there are finitely many Kronecker reduced forms. It could be argued this is implicit under the assumption that the reader at the time is familiar with the finiteness of the set of properly equivalent bilinear forms of a fixed determinant. Kronecker also lacks a proof that the complete class number, $\mathrm{Cl}_c(D)$ is counted by the complete equivalence classes Kronecker reduced forms.

3.2 Investigating the Complete Class Number

We now commence a detailed investigation into the structure of the sets B^0 and B^1.

Observation 3.2.1.
One of the conditions for the set B^0 is that at least of the inequalities must be strict. Therefore we may observe any form in B^0 satisfies

$$\begin{aligned} A_{12} + A_{21} &= \frac{1}{2}(A_{12} + A_{21}) + \frac{1}{2}(A_{12} + A_{21}) \\ &< A_{11} + A_{22}. \end{aligned}$$

This rearranges to give $A_{11} - A_{12} - A_{21} + A_{22} > 0$ and thus we use this inequality to replace the cumbersome expression "*no simultaneous equality*" found in B^0 .
We also note this condition clearly holds for any form in the set B^1.

The following illustration provides a detailed overview of our investigation into the structure of the sets B^0 and B^1.

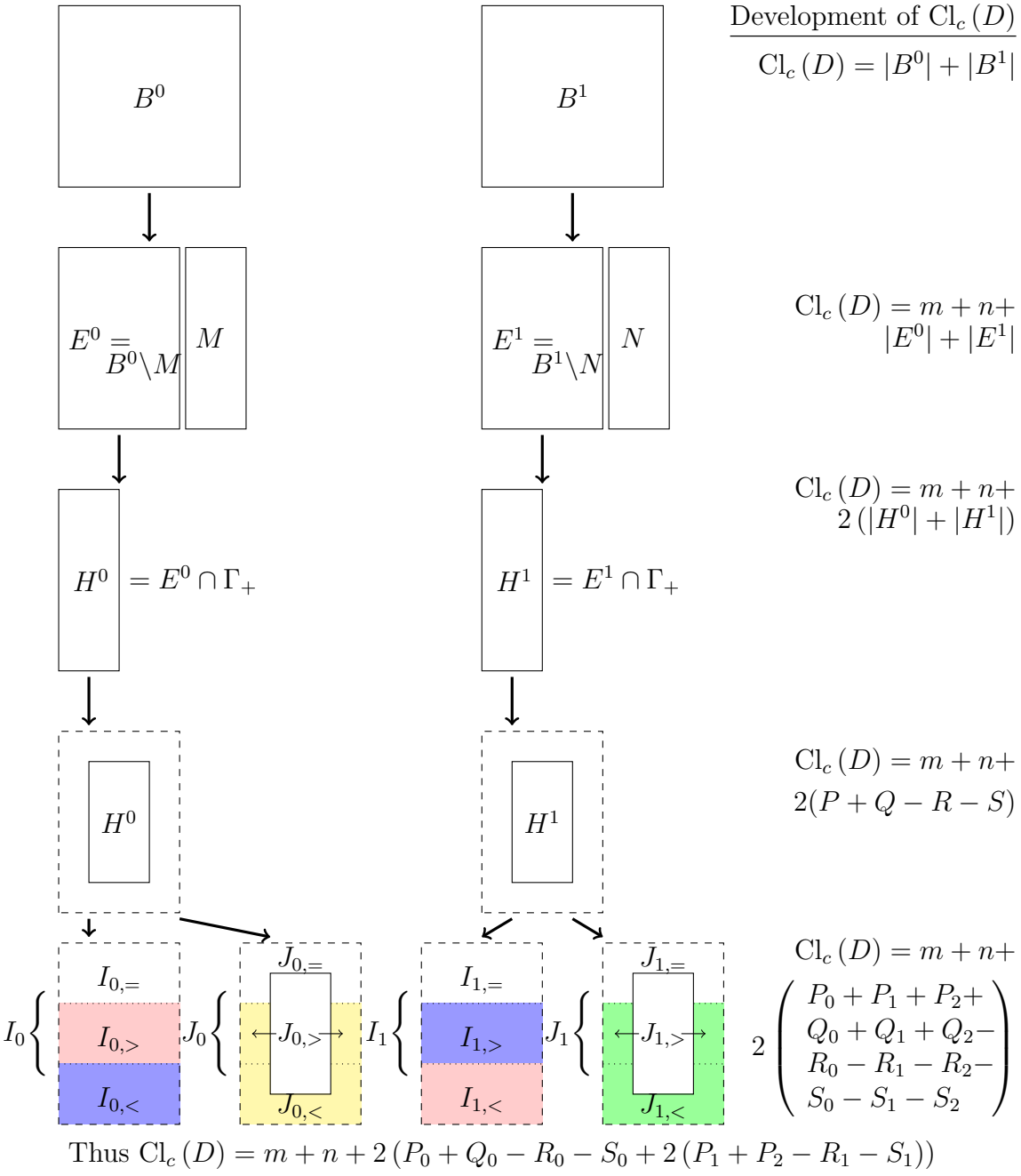
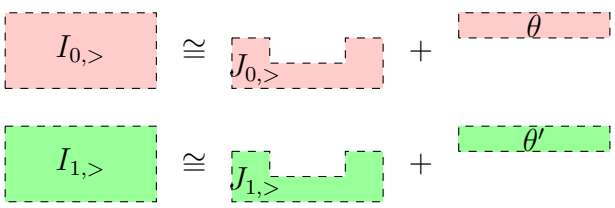


Figure 3.1: Outline of the initial sets used to count $\mathrm{Cl}_c(D)$.



$$\mathrm{Cl}_c(D) = m + n + 2(P_0 + Q_0 - R_0 - S_0) + 4(K + L)$$

Figure 3.2: Continuation of Figure 3.1 showing the relationships $P_1 = R_1 + K$ and $P_2 = S_1 + L$.

We continue to follow in the outline of Kronecker's footsteps by considering subsets of B^0 and B^1 that satisfy $A_{11} = A_{12} - A_{21} + A_{22}$.

Definition 3.2.2.
Let $M \subseteq B^0$ and $N \subseteq B^1$ be defined in the following manner:

$$\begin{aligned} M = \{(A_{11}, A_{12}, A_{21}, A_{22}) \mid \det(A) = D, 0 < \frac{(A_{12} + A_{21})}{2} \leqslant \min\{A_{11}, A_{22}\}, \\ A_{11} - A_{12} - A_{21} + A_{22} > 0, A_{11} = A_{12} - A_{21} + A_{22} \}, \\ N = \{ (A_{11}, A_{12}, A_{21}, A_{22}) \mid \det(A) = D, 0 \leqslant \frac{A_{12} + A_{21}}{2} < \min\{A_{11}, A_{22}\}, \\ A_{11} - A_{12} - A_{21} + A_{22} > 0, A_{11} = A_{12} - A_{21} + A_{22} \}. \end{aligned}$$

We let $m = |M|$ and $n = |N|$.
For convenience we will let $E^0 = B^0 \backslash M$ and $E^1 = B^1 \backslash N$.

It is important to note that $m = 0$ or $n = 0$ may arise for certain determinants.

Using our notation we then have

$$\mathrm{Cl}_c(D) - m - n = \left|E^0\right| + \left|E^1\right|.$$

We now make a more general observation.

Lemma 3.2.3.
Let $\Gamma_+ = \{(A_{11}, A_{12}, A_{21}, A_{22}) \mid \det = D, A_{22} - A_{21} > A_{11} - A_{12}\}$ *and*
$\Gamma_- = \{(A_{11}, A_{12}, A_{21}, A_{22}) \mid \det = D, A_{22} - A_{21} < A_{11} - A_{12}\}$.
Define

$$\begin{aligned} \gamma : \Gamma_+ &\longrightarrow \Gamma_- \\ (A_{11}, A_{12}, A_{21}, A_{22}) &\longmapsto (A_{22}, A_{21}, A_{12}, A_{11}) = (a_{11}, a_{12}, a_{21}, a_{22}). \end{aligned}$$

Then γ *is a bijection.*

Proof.
Firstly, $\det(\gamma(A_{11}, A_{12}, A_{21}, A_{22})) = A_{22} \cdot A_{11} - A_{21} \cdot A_{12} = A_{11}A_{22} - A_{12}A_{21} = D$.
Next, observe $(A_{11}, A_{12}, A_{21}, A_{22})$ satisfies $A_{22} - A_{21} > A_{11} - A_{12}$ and thus $a_{22} - a_{21} = A_{11} - A_{12} < A_{22} - A_{21} = a_{11} - a_{12}$. Hence $\gamma(A_{11}, A_{12}, A_{21}, A_{22}) \in \Gamma_-$.

Injectivity: This is straightforward to verify directly.
Surjectivity: Let $(A_{11}, A_{12}, A_{21}, A_{22}) \in \Gamma_-$ be arbitrary. Let $\mathcal{B} = (A_{22}, A_{21}, A_{12}, A_{11})$. Then $\det \mathcal{B} = A_{11}A_{22} - A_{12}A_{21} = D$ and we have $a_{22} - a_{21} = A_{11} - A_{12} > A_{22} - A_{21} = a_{11} - a_{12}$, thus $\mathcal{B} \in \Gamma_+$.
Lastly, $\gamma(\mathcal{B}) = (A_{11}, A_{12}, A_{21}, A_{22})$, so γ is surjective.
Hence γ is a bijection. □

Applying Lemma 3.2.3 in the restricted context of the subsets E^0 and E^1, we see it is sufficient to consider only those forms in $\Gamma_+ \cap E^0$ and $\Gamma_+ \cap E^1$. This is because the sets M and N took care of when $A_{22} - A_{21} = A_{11} - A_{12}$. Consequently, we have

$$\mathrm{Cl}_c(D) - m - n = 2\left(\left|\Gamma_+ \cap E^0\right| + \left|\Gamma_+ \cap E^1\right|\right).$$

Next, recall from Observation 3.2.1 that bilinear forms in the sets B^0 and B^1 satisfy $A_{22} - A_{21} > A_{12} - A_{11}$. Further, since we have now restricted to subsets of Γ_+, we also have $A_{22} - A_{21} > A_{11} - A_{12}$ and therefore we may replace these two conditions with $|A_{11} - A_{12}| < A_{22} - A_{21}$.
This yields

$$\mathrm{Cl}_c(D) - m - n = 2\left(\left|H^0\right| + \left|H^1\right|\right), \text{ where}$$

$$\begin{aligned} H^0 = \{\, (A_{11}, A_{12}, A_{21}, A_{22}) \,|\, \det(A) = D, 0 < \frac{(A_{12} + A_{21})}{2} \leqslant \min\{A_{11}, A_{22}\}, \\ |A_{11} - A_{12}| < A_{22} - A_{21} \,\}, \\ H^1 = \{\, (A_{11}, A_{12}, A_{21}, A_{22}) \,|\, \det(A) = D, 0 \leqslant \frac{(A_{12} + A_{21})}{2} < \min\{A_{11}, A_{22}\}, \\ |A_{11} - A_{12}| < A_{22} - A_{21} \,\}. \end{aligned}$$

Observe there is a certain symmetry in the sets H^0 and H^1 due to $\min\{A_{11}, A_{22}\}$. We now re-express this symmetry by formulating each as a difference of two new sets.

Let

$$\begin{aligned} I_0 = \{\, (A_{11}, A_{12}, A_{21}, A_{22}) \,|\, \det(A) = D, 0 < \frac{(A_{12} + A_{21})}{2} \leqslant A_{11}, \\ |A_{11} - A_{12}| < A_{22} - A_{21} \,\} \end{aligned} \tag{3.8}$$

$$\begin{aligned} J_0 = \{\, (A_{11}, A_{12}, A_{21}, A_{22}) \,|\, \det(A) = D, 0 < \frac{(A_{12} + A_{21})}{2} \leqslant A_{11}, \\ |A_{11} - A_{12}| < A_{22} - A_{21}, A_{22} < \frac{A_{12} + A_{21}}{2} \,\}. \end{aligned} \tag{3.9}$$

Then $H^0 = I_0 \backslash J_0$.

Let

$$I_1 = \{\, (A_{11}, A_{12}, A_{21}, A_{22}) \,|\, \det(A) = D, 0 \leqslant \frac{(A_{12} + A_{21})}{2} < A_{11},$$

$$|A_{11} - A_{12}| < A_{22} - A_{21} \}\,, \tag{3.10}$$

$$J_1 = \{\ (A_{11}, A_{12}, A_{21}, A_{22}) \,|\, \det(A) = D, 0 \leqslant \frac{(A_{12} + A_{21})}{2} < A_{11},$$
$$A_{22} \leqslant \frac{(A_{12} + A_{21})}{2}, |A_{11} - A_{12}| < A_{22} - A_{21} \}\,. \tag{3.11}$$

Then $H^1 = I_1 \backslash J_1$.

Observation 3.2.4. It is important to note that defining the sets H^0 and H^1 as differences of sets means we are no longer only considering positive definite forms. In particular, $A_{22} < 0$ is now permissible in each of I_0, J_0, I_1 and J_1. It is only through their respective differences that we recover positive definiteness. Further, we no longer know whether these sets are finite.

In order to be consistent with Kronecker's notation we adopt the following convention.

Notation 3.2.5.
Let $|I_0| = P$, $|J_0| = R$, $|I_1| = Q$ and $|J_1| = S$.

This gives rise to

$$\mathrm{Cl}_c\,(D) - m - n = 2\,(P + Q - R - S)\,. \tag{3.12}$$

We now prove a lemma that justifies a small simplification in the conditions found in J_0.

Lemma 3.2.6.
We may simplify the set J_0 as follows:

$$J_0 = \{\ (A_{11}, A_{12}, A_{21}, A_{22}) \,|\, \det(A) = D, 0 < \frac{1}{2}\,(A_{12} + A_{21}) < A_{11},$$
$$A_{22} < \frac{1}{2}\,(A_{12} + A_{21})\,, |A_{11} - A_{12}| < A_{22} - A_{21} \}\,. \tag{3.13}$$

That is, in J_0 we cannot have $A_{11} = \frac{1}{2}\,(A_{12} + A_{21})$.

Proof.
Assume $2A_{11} = A_{12} + A_{21}$, then from the definition of J_0 we have
$2A_{22} < A_{12} + A_{21} = 2A_{11}$, so $A_{22} < A_{11}$ $(\star)$. We have two cases:
Case I: $A_{11} \geqslant A_{12}$
This implies $A_{22} - A_{21} > |A_{11} - A_{12}| = A_{11} - A_{12}$. This gives $A_{22} - A_{11} > A_{21} - A_{12}$ and in conjunction with $(\star)$ we get

$$\begin{aligned} 0 &> A_{22} - A_{11} \\ &> A_{21} - A_{12} \\ &= A_{12} + A_{21} - 2A_{12} \\ &= 2\underbrace{(A_{11} - A_{12})}_{\geqslant 0}. \end{aligned}$$

Clearly, we have a contradiction.
Case II: $A_{11} < A_{12}$
This implies $A_{22} - A_{21} > |A_{11} - A_{12}| = A_{12} - A_{11}$.
This yields $A_{22} + A_{11} > A_{12} + A_{21} = 2A_{11}$ and hence $A_{22} > A_{11}$. This contradicts $(\star)$.
Hence bilinear forms in J_0 cannot satisfy $A_{11} = \frac{1}{2}(A_{12} + A_{21})$ and so we have

$$J_0 = \{ (A_{11}, A_{12}, A_{21}, A_{22}) \,|\, \det(A) = D, 0 < \frac{1}{2}(A_{12} + A_{21}) < A_{11}, \\ A_{22} < \frac{1}{2}(A_{12} + A_{21}), |A_{11} - A_{12}| < A_{22} - A_{21} \}.$$

□

Notes on Section 3.2

A key ambiguity of Kronecker's paper occurs in section 9 [Kr1897, p. 454]. In section 9 Kronecker introduces the class number for bilinear forms. Firstly it is implicit that he is referring to the complete class number as opposed to the proper class number. Secondly he does not make it clear whether his class number refers to definite bilinear forms or positive definite bilinear forms. On page 454, where he says the class number is twice the cardinalities of the sets $\mathfrak{B}$ and $\mathfrak{B}'$, Kronecker is referring to both positive and negative definite bilinear forms. In our work, we focus solely on positive definite bilinear forms and so our results shall differ from Kronecker's by a factor of 2.

One should also note that Kronecker does not provide a proof as to why the sets $\mathfrak{B}^0$ and $\mathfrak{B}'$ provide a method for counting the complete class number. This result is only stated on [Kr1897, p. 455]. For notational clarity we replace Kronecker's fraktur scripts, $\mathfrak{B}^0$ and $\mathfrak{B}'$, with B^0 and B^1 respectively.

We have further deviated from the notation used by Kronecker in the following manner.
To avoid confusion with the determinant D and the sets labelled $\mathfrak{D}^0$ and $\mathfrak{D}^1$ ([Kr1897, p. 456]), we will use E^0 and E^1 respectively.
Similarly, to avoid confusion with his class numbers F and F, and his sets $\mathfrak{E}^0$ and $\mathfrak{E}'$, we will use H^0 and H^1 (see [Kr1897, p. 456]).
Continuing in this vein, on p. 457 Kronecker expresses $\mathfrak{E}^0$ as the set difference of $\mathfrak{E}_1$ and $\mathfrak{E}_3$. We will instead write I_0 for $\mathfrak{E}_1$ and J_0 for $\mathfrak{E}_3$. Thus in our notation we have $H^0 = I_0 \backslash J_0$. Similarly Kronecker expresses $\mathfrak{E}^1$ as the set difference of $\mathfrak{E}_2$ and $\mathfrak{E}_4$. We will instead write I_1 for $\mathfrak{E}_2$ and J_1 for $\mathfrak{E}_4$. Hence in our notation we have $H^1 = I_1 \backslash J_1$.

Note that our result found in Theorem 3.3.14 continues to differ from Kronecker's ([Kr1897, p. 459]) by a factor of 2. This is still due to our focus on positive definite bilinear forms.

3.3 Introducing $\overline{\mathrm{Cl}}_c(D)$.

In this section we introduce a refinement, $\overline{\mathrm{Cl}}_c(D)$, of the class number $\mathrm{Cl}_c(D)$.

Notation 3.3.1.
Let $(A_{11}, A_{12}, A_{21}, A_{22})$ be a bilinear form. For brevity, we may refer to A_{11} and A_{22} as the "outer coefficients", and A_{12} and A_{21} as the "middle coefficients" or "inner coefficients".

We now single out two subsets of the set of complete equivalence classes of bilinear forms.

Definition 3.3.2.
Let $\overline{\mathrm{Cl}}_c(D)$ be the cardinality of the subset of complete equivalence classes of bilinear forms satisfying the following two conditions:

1. At least one of A_{11} and A_{22} is odd, and
2. $A_{12} - A_{21} \equiv 0 \bmod 2$.

Definition 3.3.3.
Let $\mathrm{Cl}'_c(D)$ be the cardinality of the subset of complete equivalence classes of bilinear forms satisfying the following two conditions:

1. Exactly one of A_{11} and A_{22} is odd (that is, $A_{11} + A_{22} \equiv 1 \bmod 2$), and
2. $A_{12} - A_{21} \equiv 0 \bmod 2$.

Observation 3.3.4.
Definitions 3.3.2 and 3.3.3 are well defined on complete equivalence classes because any two completely equivalent bilinear forms must be congruent to each other modulo 2 (see Lemma 2.4.7). Consequently modulo two they must have the same sum of their outer coefficients, and the same sum of their inner coefficients.

Observation 3.3.5.
Observe any bilinear form which is counted in $\mathrm{Cl}'_c(D)$ is also counted in $\overline{\mathrm{Cl}}_c(D)$. However, if a bilinear form has both outer coefficients odd then it is counted in $\overline{\mathrm{Cl}}_c(D)$ but not in $\mathrm{Cl}'_c(D)$.
Hence $\mathrm{Cl}'_c(D) \leqslant \overline{\mathrm{Cl}}_c(D) \leqslant \mathrm{Cl}_c(D)$.

Theorem 3.3.6.
Let $\mathcal{A}$ be a bilinear form with matrix representation A, let $M \in \mathrm{GL}_2(\mathbb{Z})$ and $B = M^t A M$. Then $A_{11} \equiv A_{22} \equiv A_{12} - A_{21} \equiv 0 \bmod 2$ if and only if $B_{11} \equiv B_{22} \equiv B_{12} - B_{21} \equiv 0 \bmod 2$.

Proof.
($\Rightarrow$) Assume $A_{11} \equiv A_{22} \equiv A_{12} - A_{21} \equiv 0 \bmod 2$.
From Lemma 2.4.6 we have $B_{12}+B_{21} \equiv B_{12}-B_{21} \equiv A_{12}-A_{21} \equiv A_{12}+A_{21} \equiv 0 \bmod 2$.
Applying Observation 2.4.5 (I) with $M \in \mathrm{GL}_2(\mathbb{Z})$ yields

$$\begin{aligned} B_{11} &= \alpha^2 A_{11} + \alpha\gamma(A_{12} + A_{21}) + \gamma^2 A_{22} \equiv 0 \bmod 2 \text{ and} \\ B_{22} &= \beta^2 A_{11} + \beta\delta(A_{12} + A_{21}) + \delta^2 A_{22} \ \equiv 0 \bmod 2. \end{aligned}$$

($\Leftarrow$) Since $M \in \mathrm{GL}_2(\mathbb{Z})$ it is invertible. Write $A = (M^{-1})^t B M^{-1}$ and apply ($\Rightarrow$). $\square$

Corollary 3.3.7.
There is no Kronecker reduced form, $\begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix}$ *satisfying* $A_{12} - A_{21} \equiv 0 \bmod 2$ *and at least one of* A_{11}, A_{22} *odd, that is properly equivalent to the reduced form* $\begin{pmatrix} a_{12}+a_{21} & a_{12} \\ a_{21} & a_{12}+a_{21} \end{pmatrix}$, *where* $a_{12}+a_{21} > 0$.

Proof.
Recall Kronecker reduced forms are positive definite and every positive definite form is properly equivalent to a unique reduced form. Let $A = \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix}$ be a Kronecker reduced form with $A_{12} - A_{21} \equiv 0 \bmod 2$ and at least one of its outer coefficients odd. Assume $B = M^t A M = \begin{pmatrix} a_{12}+a_{21} & a_{12} \\ a_{21} & a_{12}+a_{21} \end{pmatrix}$ where $a_{12}+a_{21} > 0$ and $M \in \mathrm{SL}_2(\mathbb{Z})$.
Then Lemma 2.4.6 implies the reduced form satisfies $a_{12}+a_{21} \equiv a_{12}-a_{21} \equiv 0 \bmod 2$ and thus $a_{11} \equiv a_{22} \equiv 0 \bmod 2$. Next, the matrix M^{-1} transforms the reduced form back to the Kronecker reduced form A. However, Theorem 3.3.6 implies $A_{11} \equiv A_{22} \equiv 0 \bmod 2$, contradicting at least one of A_{11}, A_{22} is odd.
Hence there does not exist a Kronecker reduced form with $A_{12} - A_{21} \equiv 0 \bmod 2$ and at least one of its outer coefficients odd which is properly equivalent to the reduced form $\begin{pmatrix} a_{12}+a_{21} & a_{12} \\ a_{21} & a_{12}+a_{21} \end{pmatrix}$, where $a_{12}+a_{21} > 0$. □

Lemma 3.3.8.
Let $M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in GL_2(\mathbb{Z})$. *Then at least one and at most two of* α, β, γ *and* δ *are even. Further, if two of them are even then either* α *and* δ *are both even, or* β *and* γ *are both even.*

Proof.
Since $M \in \mathrm{GL}_2(\mathbb{Z})$, $\det(M) = \pm 1$. Working mod. 2 shows we cannot have zero, three or four zeroes mod2 without making $\det(M) = 0$. Hence at least one and at most two of the entries in M are even integers. Further, $\det(M) = \pm 1$ requires no row or column to consist solely of zeros mod. 2. Therefore if exactly two entries in M are even they are either α and δ, or β and γ. □

Lemma 3.3.9.
Let $\mathcal{A}$ *be a bilinear form satisfying* $A_{12} - A_{21} \equiv 0 \bmod 2$. *Consider the bilinear form* $\mathcal{B}$ *which results from applying an* $SL_2(\mathbb{Z})$ *transformation. Then* $B_{11}+B_{22}$ *is congruent to either* $A_{11}+A_{22}$, A_{11} *or* $A_{22} \bmod 2$.

Proof.
Let $M \in \mathrm{SL}_2(\mathbb{Z})$. By Lemma 3.3.8 we know M has at least one and at most two zeros modulo 2. Further, we cannot have two zeros (modulo 2) in the same row or column. By Observation 2.4.5 (I) we have

$$B_{11}+B_{22} = \left(\alpha^2+\beta^2\right) A_{11} + (\alpha\delta+\beta\gamma)\left(A_{12}+A_{21}\right) + \left(\gamma^2+\delta^2\right) A_{22}$$

$$\equiv \ (\alpha^2+\beta^2)\,A_{11}+(\gamma^2+\delta^2)\,A_{22} \bmod 2.$$

If M has two even entries then it is clear $B_{11}+B_{22}\equiv A_{11}+A_{22} \bmod 2$. While if M has precisely one even entry then either $B_{11}+B_{22}\equiv A_{11}$ or $B_{11}+B_{22}\equiv A_{22}$. □

For a given reduced bilinear form we now consider the structure of the complete equivalence classes in its proper equivalence class with respect to $\overline{\mathrm{Cl}}_c(D)$ and $\mathrm{Cl}'_c(D)$. We will continue to use the representatives found in Equation 2.16 to describe the transformation matrices used to generate the complete equivalence classes.

Lemma 3.3.10.
Let $\mathcal{A}$ be a bilinear form with matrix representation A. Assume the proper equivalence class of $\mathcal{A}$ contains six distinct representatives for the complete equivalence classes of $\mathcal{A}$ and let $\mathcal{A}\sim_+\mathcal{B}$. If B satisfies $B_{11}\equiv B_{22}\equiv B_{12}-B_{21}\equiv 0 \bmod 2$ then all six complete equivalence classes satisfy $a_{11}+a_{22}\equiv 0 \bmod 2$. While if $B_{12}-B_{21}\equiv 0 \bmod 2$ and at least one of B_{11}, B_{22} is odd then only two of the complete equivalence classes have forms satisfying $a_{11}+a_{22}\equiv 0 \bmod 2$.

Proof.
Let B satisfy $B_{12}-B_{21}\equiv 0 \bmod 2$, then any bilinear form properly equivalent to B also has this property. From Lemma 3.3.9 we know any bilinear form that is properly equivalent to B satisfies $a_{11}+a_{22}$ is congruent to either $B_{11}+B_{22}$, B_{11} or $B_{22} \bmod 2$. Now recall completely equivalent bilinear forms have the same entries $\bmod 2$ in their matrix representations. Thus using Observation 2.4.5 (I) along with each of the 6 complete equivalence class representatives found in S, we see exactly two complete equivalence classes yield bilinear forms satisfying $a_{11}+a_{22}\equiv B_{11} \bmod 2$, two more satisfy $a_{11}+a_{22}\equiv B_{22} \bmod 2$, while the remaining two satisfy $a_{11}+a_{22}\equiv B_{11}+B_{22} \bmod 2$.
The only way for all of these to be $0 \bmod 2$ is if $B_{11}\equiv B_{22}\equiv 0 \bmod 2$. We now observe if exactly one of B_{11}, B_{22} is odd then only one of B_{11}, B_{22} and $B_{11}+B_{22}$ is even. Whilst if both B_{11} and B_{22} are odd then only $B_{11}+B_{22}$ is even.
Hence either all six complete equivalence classes of bilinear forms within the proper equivalence class satisfy $a_{11}+a_{22}\equiv 0 \bmod 2$ (when $B_{11}\equiv B_{22}\equiv 0 \bmod 2$); otherwise only two complete equivalence classes within the proper equivalence class have this property. □

Our next lemma and theorem prove a key result due to Kronecker.

Lemma 3.3.11.
Consider the subset of positive definite Kronecker reduced bilinear forms $\mathcal{A}$ satisfying the following two conditions:

1. *At least one of their outer coefficients is odd, and*
2. *$A_{12}-A_{21}\equiv 0 \bmod 2$.*

Then within the proper equivalence class of such a bilinear form, there is a 2:1 ratio of the number of complete equivalence classes with the property $A_{11}+A_{22}\equiv 1 \bmod 2$ to those with the property $A_{11}+A_{22}\equiv 0 \bmod 2$.

Proof.
Consider the set of Kronecker reduced bilinear forms with the properties as given in the statement of the lemma. Recall every Kronecker reduced bilinear form is properly equivalent to a unique reduced bilinear form. Consequently, Lemma 2.4.6 implies this reduced bilinear form also satisfies $a_{12} - a_{21} \equiv 0 \bmod 2$. Further, Theorem 3.3.6 implies the reduced form must have at least one of its outer coefficients odd because the Kronecker reduced form has at least one odd outer coefficient. Further still, Theorem 3.3.6 implies all bilinear forms within the proper equivalence class have this property. If the proper equivalence class of the reduced bilinear form contains 6 distinct representatives for the complete equivalence classes, then Lemma 3.3.10 implies that exactly two of the six complete equivalence classes have forms satisfying $A_{11} + A_{22} \equiv 0 \bmod 2$. This is because our reduced form does not satisfy $A_{11} \equiv A_{22} \equiv 0 \bmod 2$. Consequently in this case we have a 2:1 ratio of complete equivalence classes with the property $A_{11} + A_{22} \equiv 1 \bmod 2$ to those that have $A_{11} + A_{22} \equiv 0 \bmod 2$.
We now deal with the situation when the proper equivalence class of the reduced bilinear form contains less than 6 distinct complete equivalence classes. This means the reduced form has a proper automorph. Therefore we must consider reduced bilinear forms of the types found in the first four rows of Summary 2.5.27.
Observe that the form in the fourth row is a special case of the form in the third row, where $A_{21} = A_{21}$. By Corollary 3.3.7 we know there is no Kronecker reduced form with at least one odd outer coefficient odd, and the sum of its inner coefficients even that reduces to $\begin{pmatrix} a_{12}+a_{21} & a_{12} \\ a_{21} & a_{12}+a_{21} \end{pmatrix}$. Hence the third and fourth types of reduced bilinear form cannot arise when we reduce our Kronecker reduced bilinear form. We investigate rows one and two separately.
Consider the bilinear form $\begin{pmatrix} A_{11} & A_{12} \\ -A_{12} & A_{11} \end{pmatrix}$, where $A_{11} \equiv 1 \bmod 2$. Then the set of complete equivalence classes within its proper equivalence class is given by

$$\left\{ \begin{pmatrix} A_{11} & A_{12} \\ -A_{12} & A_{11} \end{pmatrix}, \begin{pmatrix} 2A_{11} & A_{11}+A_{12} \\ A_{11}-A_{12} & A_{11} \end{pmatrix}, \begin{pmatrix} A_{11} & A_{11}+A_{12} \\ A_{11}-A_{12} & 2A_{11} \end{pmatrix} \right\}.$$

It is easy to visually verify all of these complete equivalence classes contain bilinear forms satisfying $a_{12} - a_{21} \equiv 0 \bmod 2$ and it is straightforward to check that only the first form satisfies $a_{11} + a_{22} \equiv 0 \bmod 2$. Hence we have a 2:1 ratio.
Now consider the bilinear form $\begin{pmatrix} A_{11} & 0 \\ 0 & A_{11} \end{pmatrix}$, where $A_{11} \equiv 1 \bmod 2$. Then the set of complete equivalence classes within its proper equivalence class is given by

$$\left\{ \begin{pmatrix} A_{11} & 0 \\ 0 & A_{11} \end{pmatrix}, \begin{pmatrix} 2A_{11} & A_{11} \\ A_{11} & A_{11} \end{pmatrix}, \begin{pmatrix} A_{11} & A_{11} \\ A_{11} & 2A_{11} \end{pmatrix} \right\}.$$

It is clear all of these complete equivalence classes contain bilinear forms satisfying $a_{12} - a_{21} \equiv 0 \bmod 2$ and straightforward to verify only the first form satisfies $a_{11} + a_{22} \equiv 0 \bmod 2$. Hence we have a 2:1 ratio.
Thus we always have a 2:1 ratio of complete equivalence classes where $a_{11} + a_{22} \equiv 1 \bmod 2$ to those where $a_{11} + a_{22} \equiv 0 \bmod 2$ within the proper equivalence class of

any Kronecker reduced bilinear form that satisfies $A_{12} - A_{21} \equiv 0 \bmod 2$ and has at least one odd outer coefficient. □

Theorem 3.3.12.
Let $D \in \mathbb{Z}_{>0}$ then $3\mathrm{Cl}'_c(D) = 2\overline{\mathrm{Cl}}_c(D)$.

Proof.
Recall that the set of complete equivalence classes of bilinear forms that are counted by $\mathrm{Cl}'_c(D)$ are contained within the set of complete equivalence classes of bilinear forms counted by $\overline{\mathrm{Cl}}_c(D)$. Also recall the bilinear forms in a complete equivalence class that are counted by $\mathrm{Cl}'_c(D)$ all have the property $A_{11} + A_{22} \equiv 1 \bmod 2$. Then Lemma 3.3.11 shows that within a proper equivalence class of a Kronecker reduced form which has at least one odd outer coefficient and the sum of its inner coefficients even, we have a 2:1 ratio of complete equivalence classes that satisfy $A_{11} + A_{22} \equiv 1 \bmod 2$ to those satisfying $A_{11} + A_{22} \equiv 0 \bmod 2$. Hence $\mathrm{Cl}'_c(D) = \frac{2}{3}\overline{\mathrm{Cl}}_c(D)$ and thus $3\mathrm{Cl}'_c(D) = 2\overline{\mathrm{Cl}}_c(D)$. □

We now extend the ideas developed in Section 3.2.

Definition 3.3.13.
Let $\overline{\Theta_i} = \{A \in \Theta_i \mid A_{11} + A_{22} \equiv 1 \bmod 2, A_{12} + A_{21} \equiv 0 \bmod 2\}$ for $\Theta \in \{I, J\}$ and $i \in \{0, 1\}$.
Let $\overline{P} = \left|\overline{I_0}\right|$, $\overline{R} = \left|\overline{J_0}\right|$, $\overline{Q} = \left|\overline{I_1}\right|$ and $\overline{S} = \left|\overline{J_1}\right|$.

Theorem 3.3.14.
Let $D \in \mathbb{Z}$ then $\overline{\mathrm{Cl}}_c(D) = 3\left(\overline{P} + \overline{Q} - \overline{R} - \overline{S}\right)$.

Proof.
We are considering subsets of the sets B^0 and B^1 from Section 3.2. Recall bilinear forms in the subsets M and N satisfy $A_{11} = A_{12} - A_{21} + A_{22}$. Since our bilinear forms satisfy $A_{12} - A_{21} \equiv 0 \bmod 2$ it follows that $A_{11} \equiv A_{22} \bmod 2$ for the subset of our bilinear forms contained in the sets M and N. This yields $A_{11} + A_{22} \equiv 0 \bmod 2$, which cannot be. Hence M and N are the empty set when considering only those bilinear forms whose sum of their inner coefficients is even and sum of their outer coefficients is odd.
Therefore, in the same manner as we constructed $\mathrm{Cl}_c(D)$, we have

$$\mathrm{Cl}'_c(D) = 2\left(\overline{P} + \overline{Q} - \overline{R} - \overline{S}\right).$$

Applying Theorem 3.3.12 then yields

$$\begin{aligned}\overline{\mathrm{Cl}}_c(D) &= \frac{3}{2}\mathrm{Cl}'_c(D) \\ &= 3\left(\overline{P} + \overline{Q} - \overline{R} - \overline{S}\right).\end{aligned}$$

This is because the map γ found in Lemma 3.2.3 preserves $A_{12} - A_{21}$. □

The following diagram (Figure 3.3) provides a good reference point for understanding the $\overline{\mathrm{Cl}}_c(D)$ class number.

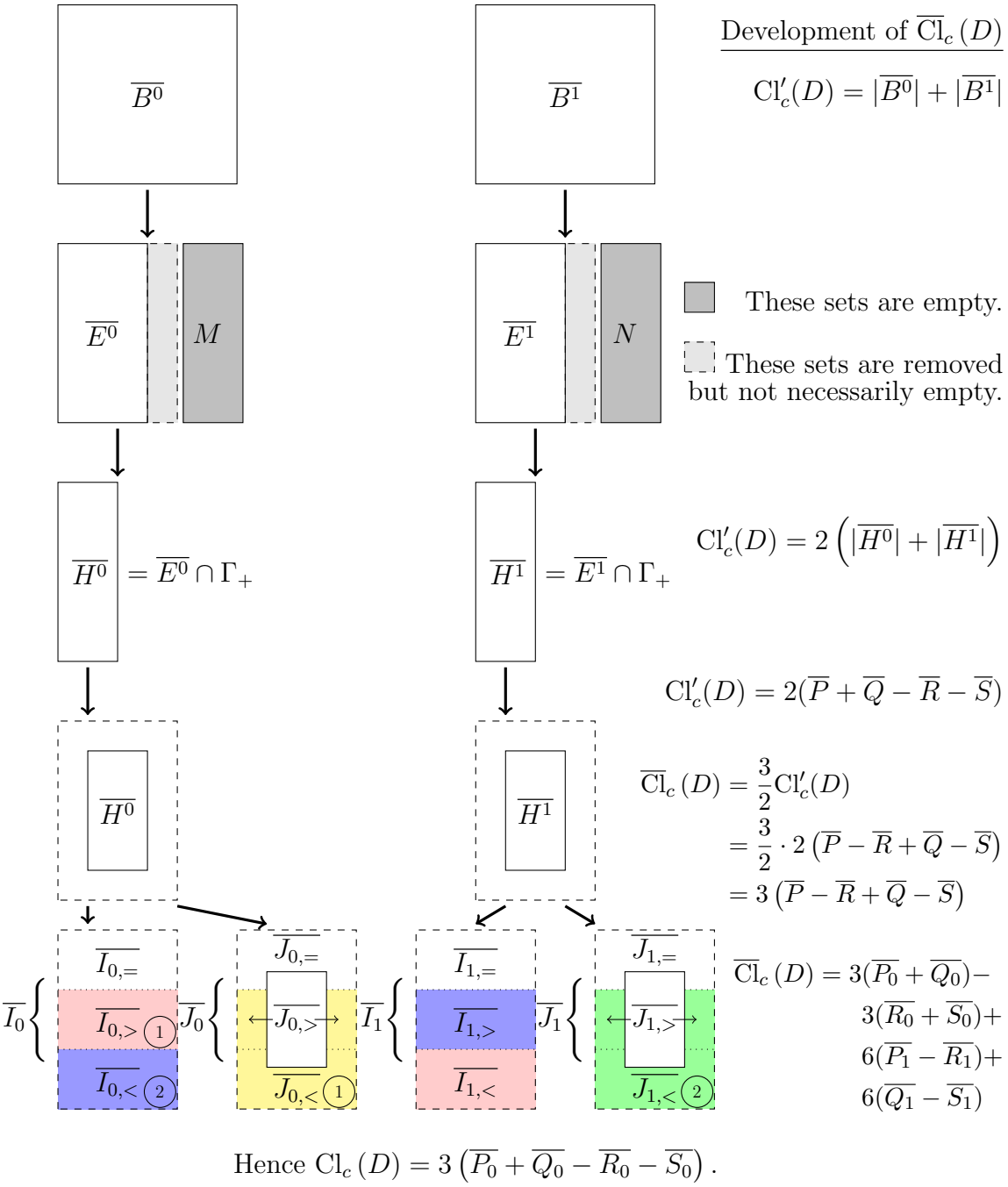


Figure 3.3: Outline of the sets used to count $\overline{\mathrm{Cl}}_c(D)$. Circled numbers and shaded regions indicate the same cardinalities.

Notes on Section 3.3

Since Kronecker chose to write his bilinear forms as $(A, B, -C, D)$, he uses the condition $B + C \equiv 0 \bmod 2$. Whereas, since we denote our bilinear forms by $(A_{11}, A_{12}, A_{21}, A_{22})$, we will write $A_{12} - A_{21} \equiv 0 \bmod 2$ for ease of comparison to Kronecker's original text.

3.4 Towards Establishing the Finiteness of P, Q, R and S.

In this section we begin to establish the finiteness of P, Q, R, S, $\overline{P}$, $\overline{Q}$, $\overline{R}$ and $\overline{S}$. We will used Kronecker's outline but take a more direct approach wherever possible. However, we will provide Kronecker's insight in the notes at the end of each section. We continue to let $D \in \mathbb{Z}_{>0}$ denote the determinant of the bilinear forms under consideration.

We first define some partitions of the sets I_0, J_0, I_1 and J_1 (see Equations 3.8, 3.10, 3.11 and 3.13 for details).

Definition 3.4.1.
We partition the sets I_0 and I_1 as follows:

$$I_0 = I_{0,=} \cup I_{0,>} \cup I_{0,<} \text{ and } I_1 = I_{1,=} \cup I_{1,>} \cup I_{1,<}, \text{ where}$$

$$\begin{aligned}
I_{0,=} &= \left\{\mathcal{A} \in I_0 \middle| A_{11} = A_{12}\right\} \\
&= \left\{\mathcal{A} \middle| \det(A) = D, -A_{11} < A_{21} \leqslant A_{11}, 0 < A_{22} - A_{21}\right\}, \\
I_{0,>} &= \left\{\mathcal{A} \middle| \det(A) = D, 0 < \frac{A_{12}+A_{21}}{2} \leqslant A_{11}, A_{22} - A_{21} > |A_{11} - A_{12}|, A_{11} > A_{12}\right\}, \\
I_{0,<} &= \left\{\mathcal{A} \middle| \det(A) = D, 0 < \frac{A_{12}+A_{21}}{2} \leqslant A_{11}, A_{22} - A_{21} > |A_{11} - A_{12}|, A_{11} < A_{12}\right\}
\end{aligned}$$

and

$$\begin{aligned}
I_{1,=} &= \left\{\mathcal{A} \in I_1 \middle| A_{11} = A_{12}\right\} \\
&= \left\{\mathcal{A} \middle| \det(A) = D, -A_{11} \leqslant A_{21} < A_{11}, 0 < A_{22} - A_{21}\right\}, \\
I_{1,>} &= \left\{\mathcal{A} \middle| \det(A) = D, 0 \leqslant \frac{A_{12}+A_{21}}{2} < A_{11}, A_{22} - A_{21} > |A_{11} - A_{12}|, A_{11} > A_{12}\right\}. \\
I_{1,<} &= \left\{\mathcal{A} \middle| \det(A) = D, 0 \leqslant \frac{A_{12}+A_{21}}{2} < A_{11}, A_{22} - A_{21} > |A_{11} - A_{12}|, A_{11} < A_{12}\right\}.
\end{aligned}$$

Lastly, as per Kronecker, we define $P_0 = |I_{0,=}|$, $P_1 = |I_{0,>}|$, $P_2 = |I_{0,<}|$, $Q_0 = |I_{1,=}|$, $Q_1 = |I_{1,>}|$ and $Q_2 = |I_{1,<}|$.

Definition 3.4.2.
We partition the sets J_0 and J_1 as follows:

$$J_0 = J_{0,=} \cup J_{0,>} \cup J_{0,<} \text{ and } J_1 = J_{1,=} \cup J_{1,>} \cup J_{1,<}, \text{ where}$$

$$\begin{aligned}
J_{0,=} &= \left\{\mathcal{A} \in J_0 \middle| A_{22} = 0\right\} \\
&= \left\{\mathcal{A} \middle| \det(A) = -A_{12}A_{21} = D, 0 < \frac{A_{12}+A_{21}}{2} < A_{11}, A_{21} < -|A_{11} - A_{12}|\right\}, \\
J_{0,>} &= \left\{\mathcal{A} \middle| \det(A) = D, 0 < A_{22} < \frac{A_{12}+A_{21}}{2} \leqslant A_{11}, A_{22} - A_{21} > |A_{11} - A_{12}|\right\},
\end{aligned}$$

$$J_{0,<} = \left\{ \mathcal{A} \middle| \det(A) = D, A_{22} < 0 < \frac{A_{12}+A_{21}}{2} \leqslant A_{11}, A_{22} - A_{21} > |A_{11} - A_{12}| \right\}$$

and

$$\begin{aligned} J_{1,=} &= \left\{ \mathcal{A} \in J_1 \middle| A_{22} = 0 \right\} \\ &= \left\{ \mathcal{A} \middle| \det(A) = -A_{12}A_{21} = D, 0 \leqslant \frac{A_{12}+A_{21}}{2} < A_{11}, A_{21} < -|A_{11} - A_{12}| \right\}, \\ J_{1,>} &= \left\{ \mathcal{A} \middle| \det(A) = D, 0 < A_{22} \leqslant \frac{A_{12}+A_{21}}{2} < A_{11}, A_{22} - A_{21} > |A_{11} - A_{12}| \right\}, \\ J_{1,<} &= \left\{ \mathcal{A} \middle| \det(A) = D, A_{22} < 0 \leqslant \frac{A_{12}+A_{21}}{2} < A_{11}, A_{22} - A_{21} > |A_{11} - A_{12}| \right\}. \end{aligned}$$

Again, as per Kronecker, we define $R_0 = |J_{0,=}|$, $R_1 = |J_{0,>}|$, $R_2 = |J_{0,<}|$, $S_0 = |J_{1,=}|$, $S_1 = |J_{1,>}|$ and $S_2 = |J_{1,<}|$.

Observation 3.4.3.
By construction we have $\Theta_{i,j} \cap \Theta_{i,k} = \emptyset$ for $\Theta \in \{I, J\}$, $i \in \{0, 1\}$ and $j, k \in \{=, >, <\}$, $j \neq k$.
Hence $|I_0| = P = P_0 + P_1 + P_2$, $|I_1| = Q = Q_0 + Q_1 + Q_2$, $|J_0| = R = R_0 + R_1 + R_2$ and $|J_1| = S = S_0 + S_1 + S_2$.

We now make a useful observation about the structure of D in these sets.

Observation 3.4.4.
In $I_{0,=}$ and $I_{1,=}$ we have $A_{11} = A_{12}$, which yields $D = A_{11}(A_{22} - A_{21})$.
In $J_{0,=}$ and $J_{1,=}$ we have $A_{22} = 0$, which yields $D = -A_{12}A_{21}$.
In what follows it is straightforward to verify the identities by expanding the right hand side and collecting terms to arrive at $A_{11}A_{22} - A_{12}A_{21}$.
In $I_{0,>}$ and $I_{1,>}$ we have $A_{11} > A_{12}$, i.e. $A_{11} - A_{12} > 0$ and we may write

$$D = (A_{11} - A_{12})^2 + (A_{12} + A_{21})(A_{11} - A_{12}) + A_{11}(-A_{11} + A_{12} - A_{21} + A_{22}).$$

Also, in $I_{0,<}$ and $I_{1,<}$ we have $A_{11} < A_{12}$, i.e. $A_{12} - A_{11} > 0$ and we may write

$$D = (A_{12} - A_{11})^2 + (2A_{11} - A_{12} - A_{21})(A_{12} - A_{11}) + A_{11}(A_{11} - A_{12} - A_{21} + A_{22}).$$

Similarly in $J_{0,>}$ and $J_{1,>}$ we have $A_{22} > 0$ and we may write

$$D = (A_{22} - A_{21})^2 + (A_{12} + A_{21} - 2A_{22})(A_{22} - A_{21}) + A_{22}(A_{11} - A_{12} - A_{21} + A_{22}).$$

Also, in $J_{0,<}$ and $J_{1,<}$ we have $A_{22} < 0$ and we may write

$$D = (A_{22} - A_{21})^2 + (A_{12} + A_{21})(A_{22} - A_{21}) + (-A_{22})(-A_{11} + A_{12} - A_{21} + A_{22}).$$

The key observation to make is that D is either a product of two integers, or $D = \alpha^2 + \alpha\delta + \beta\gamma$ for some integers α, β, γ, δ, where $\alpha > 0$.

We also observe that these determinant results hold regardless of whether we impose the additional conditions $A_{12} + A_{21} \equiv 0 \bmod 2$ and $A_{11} + A_{22} \equiv 1 \bmod 2$.

Our goal now is to establish that P, Q, R, S, $\overline{P}$, $\overline{Q}$, $\overline{R}$ and $\overline{S}$ are finite.

Lemma 3.4.5.
Let $X_1 = \{(\alpha, \beta, \gamma, \delta) \mid \alpha^2 + \alpha\delta + \beta\gamma = D, \alpha > 0, \gamma > 0, 0 < \delta \leqslant 2\beta\}$ *and define the map*

$$\begin{aligned} \phi : X_1 &\longrightarrow I_{0,>} \\ (\alpha, \beta, \gamma, \delta) &\longmapsto (\beta, \beta - \alpha, \alpha - \beta + \delta, 2\alpha - \beta + \gamma + \delta) = (A_{11}, A_{12}, A_{21}, A_{22}) . \end{aligned}$$

Then ϕ *is a well-defined bijection.*

Proof.
Well-defined: Observe

$$\begin{aligned} \det(A) &= \beta (2\alpha - \beta + \gamma + \delta) - (\beta - \alpha)(\alpha - \beta + \delta) \\ &= 2\alpha\beta - \beta^2 + \beta\gamma + \beta\delta - \left(\alpha\beta - \alpha^2 - \beta^2 + \alpha\beta + \beta\delta - \alpha\delta\right) \\ &= \alpha^2 + \alpha\delta + \beta\gamma \\ &= D. \end{aligned}$$

Now note that $A_{11} = \beta$ and $\frac{A_{12}+A_{21}}{2} = \frac{\delta}{2}$. Since forms in X_1 satisfy $0 < \delta \leqslant 2\beta$, we immediately get $0 < \frac{A_{12}+A_{21}}{2} \leqslant A_{11}$.
Next, $\alpha > 0$, $\beta > 0$ and $A_{12} = \beta - \alpha$, therefore $A_{11} = \beta > \beta - \alpha = A_{12}$.
Next, we have

$$\begin{aligned} A_{22} - A_{21} &= 2\alpha - \beta + \gamma + \delta - (\alpha - \beta + \delta) \\ &= \alpha + \gamma \\ &> \alpha \text{ since in } X_1 \text{ we have } \gamma > 0 \\ &= A_{11} - A_{12} \\ &= |A_{11} - A_{12}| \text{ as } A_{11} > A_{12} \text{ by above.} \end{aligned}$$

Hence ϕ is well-defined and maps into $I_{0,>}$.
Injectivity: Suppose $\phi(\alpha, \beta, \gamma, \delta) = \phi\left(\hat{\alpha}, \hat{\beta}, \hat{\gamma}, \hat{\delta}\right)$. Then

$$(\beta, \beta - \alpha, \alpha - \beta + \delta, 2\alpha - \beta + \gamma + \delta) = \left(\hat{\beta}, \hat{\beta} - \hat{\alpha}, \hat{\alpha} - \hat{\beta} + \hat{\delta}, 2\hat{\alpha} - \hat{\beta} + \hat{\gamma} + \hat{\delta}\right).$$

Equating the entries from left to right yields $\beta = \hat{\beta}$, $\alpha = \hat{\alpha}$, $\delta = \hat{\delta}$ and $\gamma = \hat{\gamma}$. Therefore ϕ is injective.
Surjectivity: Let $(A_{11}, A_{12}, A_{21}, A_{22}) \in I_{0,>}$ be arbitrary.
Consider $f = (A_{11} - A_{12}, A_{11}, -A_{11} + A_{12} - A_{21} + A_{22}, A_{12} + A_{21}) = (\alpha, \beta, \gamma, \delta)$, we will show $f \in X_1$ and $\phi(f) = (A_{11}, A_{12}, A_{21}, A_{22})$.
We have f satisfies

$$\begin{aligned} \alpha^2 + \alpha\delta + \beta\gamma = (A_{11} - A_{12})^2 &+ (A_{11} - A_{12})(A_{12} + A_{21}) \\ &+ A_{11}(-A_{11} + A_{12} - A_{21} + A_{22}) \end{aligned}$$

$$= A_{11}A_{22} - A_{12}A_{21}$$
$$= D.$$

Also, $A_{11} > A_{12}$ implies $A_{11} - A_{12} > 0$, i.e. $\alpha > 0$. It also implies $A_{22} - A_{21} > A_{11} - A_{12}$ which rearranges to $\gamma = -A_{11} + A_{12} - A_{21} + A_{22} > 0$. Lastly, $0 < \frac{A_{12}+A_{21}}{2} \leqslant A_{11}$ implies $\delta = A_{12} + A_{21} > 0$ and $2\beta = 2A_{11} \leqslant A_{12} + A_{21} = \delta$. Hence $0 < \delta \leqslant 2\beta$. Thus $f \in X_1$.
Finally it is straightforward to check that $\phi(f) = (A_{11}, A_{12}, A_{21}, A_{22})$.
Hence ϕ is surjective and thus a bijection. □

Corollary 3.4.6.
The cardinality of X_1 is finite and $|X_1| = |I_{0,>}| = P_1$.

Proof.
In the definition of X_1 in Lemma 3.4.5 we see that α, β, γ and δ are all strictly positive and satisfy $D = \alpha^2 + \alpha\delta + \beta\gamma$. Consequently there can only be finitely many choices for α, β, γ and δ. Thus $|X_1|$ is finite.
Definition 3.4.1 in conjunction with Lemma 3.4.5 yields $|X_1| = |I_{0,>}| = P_1$. □

Lemma 3.4.7.
Let $X_2 = \{(\alpha, \beta, \gamma, \delta) \mid \alpha^2 + \alpha\delta + \beta\gamma = D, 0 < \alpha, 0 < \gamma, 0 \leqslant \delta < 2\beta\}$ and define the map

$$\begin{aligned} \psi : X_2 &\longrightarrow I_{0,<} \\ (\alpha, \beta, \gamma, \delta) &\longmapsto (\beta, \alpha + \beta, \beta - \alpha - \delta, \gamma + \beta - \delta) = (A_{11}, A_{12}, A_{21}, A_{22}) . \end{aligned}$$

Then ψ is a well-defined bijection.

Proof.
Well-defined: Observe

$$\begin{aligned} \det(A) &= \beta(\gamma + \beta - \delta) - (\alpha + \beta)(\beta - \alpha - \delta) \\ &= \alpha^2 + \alpha\delta + \beta\gamma \\ &= D. \end{aligned}$$

Next, notice that $0 \leqslant \delta < 2\beta$ implies $0 < \frac{2\beta-\delta}{2} = \frac{(\alpha+\beta)+(\beta-\alpha-\delta)}{2} = \frac{A_{12}+A_{21}}{2}$. Also since $0 \leqslant \delta$ we have $\frac{A_{12}+A_{21}}{2} = \frac{2\beta-\delta}{2} = \beta - \frac{\delta}{2} \leqslant \beta = A_{11}$. Thus $0 < \frac{A_{12}+A_{21}}{2} \leqslant A_{11}$.
Now observe $A_{11} = \beta < \beta + \alpha$ as $0 < \alpha$, hence $A_{11} - A_{12} < 0$. Using this, it is enough to show that $A_{22} - A_{21} > A_{12} - A_{11}$. We have

$$\begin{aligned} A_{22} - A_{21} &= \gamma + \beta - \delta - (\beta - \alpha - \delta) \\ &= \gamma + \alpha \\ &> \alpha \text{ as } 0 < \gamma \\ &= (\alpha + \beta) - \beta \\ &= A_{12} - A_{11}. \end{aligned}$$

Hence ψ is well-defined and maps into $I_{0,<}$.
Injectivity: Suppose $\psi(\alpha,\beta,\gamma,\delta) = \psi\left(\hat{\alpha},\hat{\beta},\hat{\gamma},\hat{\delta}\right)$, then
$(\beta, \alpha+\beta, \beta-\alpha-\delta, \gamma+\beta-\delta) = \left(\hat{\beta}, \hat{\alpha}+\hat{\beta}, \hat{\beta}-\hat{\alpha}-\hat{\delta}, \hat{\gamma}+\hat{\beta}-\hat{\delta}\right)$. Equating the entries yields $(\alpha,\beta,\gamma,\delta) = \left(\hat{\alpha},\hat{\beta},\hat{\gamma},\hat{\delta}\right)$ and so ψ is injective.
Surjectivity: Let $(A_{11}, A_{12}, A_{21}, A_{22}) \in I_{0,<}$ be arbitrary.
Let $f = (A_{12}-A_{11}, A_{11}, A_{11}-A_{12}-A_{21}+A_{22}, 2A_{11}-A_{12}-A_{21}) = (\alpha,\beta,\gamma,\delta)$, we will show $f \in X_2$ and $\psi(f) = (A_{11}, A_{12}, A_{21}, A_{22})$.
By Observation 3.4.4 f satisfies $\alpha^2+\alpha\delta+\beta\gamma = D$. Next we have $A_{11} < A_{12}$ implies $0 < A_{12}-A_{11} = \alpha$. This also implies $A_{22}-A_{21} > A_{12}-A_{11}$, which rearranges to $\gamma = A_{11}-A_{12}-A_{21}+A_{22} > 0$. Now $0 < \frac{A_{12}+A_{21}}{2} \leqslant A_{11}$ yields $2\beta = 2A_{11} > 2A_{11}-(A_{12}+A_{21}) = \delta \geqslant 0$. Thus $0 \leqslant \delta < 2\beta$ and hence $f \in X_2$. Lastly, it is straightforward to verify that $\psi(f) = (A_{11}, A_{12}, A_{21}, A_{22})$.
Thus ψ is a surjection and hence is a bijection. □

Corollary 3.4.8.
The cardinality of the set $I_{0,<}$ is finite and equal to $|X_2|$.

Proof.
An element in the set X_2 has α, β and γ all strictly positive. Also δ is non-negative. Consequently there are only finitely many values of α, β, γ and δ that satisfy $D = \alpha^2+\alpha\delta+\beta\gamma$ for a fixed positive integer D. Definition 3.4.1 in conjunction with Lemma 3.4.7 shows we have a bijection between X_2 and $I_{0,<}$ and thus $|X_2| = |I_{0,<}| = P_2$. □

Corollary 3.4.9.
The cardinality of the set $I_0 \backslash I_{0,=}$ is finite with $P_1+P_2 = |X_1|+|X_2|$.

Proof.
By construction we have $I_0\backslash I_{0,=} = I_{0,>} \cup I_{0,<}$. Corollaries 3.4.6 and 3.4.8 demonstrate this set is in fact finite with cardinality $|X_1|+|X_2| = |I_0\backslash I_{0,=}| = P_1+P_2$. □

Lemma 3.4.10.
The map

$$\begin{aligned} \pi : I_0\backslash I_{0,=} &\longrightarrow I_1\backslash I_{1,=} \\ (A_{11},A_{12},A_{21},A_{22}) &\longmapsto (A_{11}, 2A_{11}-A_{12}, -A_{21}, A_{22}-2A_{21}) = (a_{11},a_{12},a_{21},a_{22}) \end{aligned}$$

is a well-defined bijection.

Proof.
Well-defined: We have

$$\begin{aligned} \det(a) &= a_{11}a_{22}-a_{12}a_{21} \\ &= A_{11}(A_{22}-2A_{21}) - (2A_{11}-A_{12})(-A_{21}) \\ &= A_{11}A_{22} - 2A_{11}A_{21} - (-2A_{11}A_{21}+A_{12}A_{21}) \\ &= A_{11}A_{22} - A_{12}A_{21} \end{aligned}$$

$$= \det(A).$$

Next we have $\frac{a_{12}+a_{21}}{2} = \frac{2A_{11}-A_{12}-A_{21}}{2} = A_{11} - \frac{A_{12}+A_{21}}{2} \geqslant 0$. Further, $a_{11} - \frac{a_{12}+a_{21}}{2} = A_{11} - \left(A_{11} - \frac{A_{12}+A_{21}}{2}\right) = \frac{A_{12}+A_{21}}{2} > 0$. Thus $0 \leqslant \frac{a_{12}+a_{21}}{2} < a_{11}$.
Continuing in this vein we have

$$\begin{aligned} a_{22} - a_{21} &= A_{22} - 2A_{21} + A_{21} \\ &= A_{22} - A_{21} \\ &> |A_{11} - A_{12}| \\ &= |A_{12} - A_{11}| \\ &= |A_{11} - (2A_{11} - A_{12})| \\ &= |a_{11} - a_{12}|. \end{aligned}$$

Lastly, suppose $a_{11} = a_{12}$ then we have $A_{11} = a_{11} = a_{12} = 2A_{11} - A_{12}$ and this implies $A_{11} = A_{12}$, a contradiction.
Hence the map π is well-defined.
Injectivity: This follows immediately by equating coefficients.
Surjectivity: Let $(a_{11}, a_{12}, a_{21}, a_{22}) \in I_1 \backslash I_{1,=}$ and let $f = (a_{11}, 2a_{11} - a_{12}, -a_{21}, a_{22} - 2a_{21}) = (A_{11}, A_{12}, A_{21}, A_{22})$, we will show this lies in $I_0 \backslash I_{0,=}$ and
$\pi(f) = (a_{11}, a_{12}, a_{21}, a_{22})$. We have

$$\begin{aligned} \det(f) &= (a_{11})(a_{22} - 2a_{21}) - (2a_{11} - a_{12})(-a_{21}) \\ &= a_{11}a_{22} - a_{12}a_{21} \\ &= \det(a). \end{aligned}$$

Next, we have $\frac{A_{12}+A_{21}}{2} = \frac{2a_{11}-a_{12}-a_{21}}{2} = a_{11} - \frac{a_{12}+a_{21}}{2} > 0$ and $A_{11} - \frac{A_{12}+A_{21}}{2} = a_{11} - \left(a_{11} - \frac{a_{12}+a_{21}}{2}\right) = \frac{a_{12}+a_{21}}{2} \geqslant 0$. Thus $0 < \frac{A_{12}+A_{21}}{2} \leqslant A_{11}$. The remaining two properties, $A_{22} - A_{21} > |A_{11} - A_{12}|$ and $A_{11} \neq A_{12}$, are derived in exactly the same manner as in the proof that π is well-defined. Hence π is a surjection and therefore a bijection. □

Corollary 3.4.11.
The set $I_1 \backslash I_{1,=}$ is finite with cardinality $Q_1 + Q_2 = |X_1| + |X_2|$.

Proof.
From Lemma 3.4.10 we have a bijection between the sets $I_0 \backslash I_{0,=}$ and $I_1 \backslash I_{1,=}$. Applying Corollary 3.4.9 then yields $|X_1| + |X_2| = |I_0 \backslash I_{0,=}| = |I_1 \backslash I_{1,=}| = Q_1 + Q_2$. □

Corollary 3.4.12.
In Kronecker's notation we have $P_1 + P_2 = Q_1 + Q_2$.

Proof.
We have $P_1 + P_2 = |X_1| + |X_2| = Q_1 + Q_2$. □

We now perform a similar analysis on the sets J_0 and J_1. The following lemma will help us to be more concise than using the method Kronecker alluded to.

Lemma 3.4.13.
Let S be an arbitrary, non-empty set and let $\rho : S \longrightarrow S$ be such that $\rho^2 = id$. Then ρ is a bijection.

Proof.
Injectivity: Suppose $\rho(s) = \rho(t)$. Then $\rho^2(s) = \rho^2(t)$. However, $\rho^2(s) = \mathrm{id}(s) = s$ and $\rho^2(t) = t$. Thus $s = t$.
Surjectivity: Let $s \in S$ be arbitrary, then $\rho^2(s) = \rho(\rho(s)) = s$. Thus ρ maps $\rho(s)$ onto s. Since $s \in S$ was arbitrary, and $\rho(s) \in S$, the map ρ is surjective.
Hence ρ is a bijection. □

Lemma 3.4.14.
The map

$$\begin{aligned} \rho : J_0 &\longrightarrow J_0 \\ (A_{11}, A_{12}, A_{21}, A_{22}) &\longmapsto (2A_{12} - A_{11}, A_{12}, A_{21} - 2A_{22}, -A_{22}) = (a_{11}, a_{12}, a_{21}, a_{22}) \end{aligned}$$

is a well-defined involution.

Proof.
Recall $J_0 = \{A \mid \det(A) = D, 0 < \frac{A_{12}+A_{21}}{2} \leqslant A_{11}, A_{22} < \frac{A_{12}+A_{21}}{2}, A_{22} - A_{21} > |A_{11} - A_{12}|\}$. We first show ρ is well-defined. Let $(A_{11}, A_{12}, A_{21}, A_{22}) \in J_0$ be arbitrary, then we have

$$\begin{aligned} \det(a) &= a_{11}a_{22} - a_{12}a_{21} \\ &= (2A_{12} - A_{11})(-A_{22}) - (A_{12})(A_{21} - 2A_{22}) \\ &= A_{11}A_{22} - 2A_{12}A_{22} + 2A_{12}A_{22} - A_{12}A_{21} \\ &= \det(A). \end{aligned}$$

Next, $\frac{a_{12}+a_{21}}{2} = \frac{A_{12}+A_{21}-2A_{22}}{2} = \frac{A_{12}+A_{21}}{2} - A_{22} > 0$. Further,

$$\begin{aligned} a_{11} &= 2A_{12} - A_{11} \\ &\geqslant 2A_{12} - (A_{22} - A_{21} + A_{12}) \text{ as } A_{11} > 0 \text{ and } A_{11} - A_{12} < A_{22} - A_{21} \\ &= A_{12} + A_{21} - A_{22} \\ &> \frac{A_{12} + A_{21}}{2} - A_{22} \text{ as } 0 < \frac{A_{12} + A_{21}}{2} \\ &= \frac{a_{12} + a_{21}}{2}. \end{aligned}$$

Thus we have $0 < \frac{a_{12}+a_{21}}{2} < a_{11}$. Next, $0 < \frac{A_{12}+A_{21}}{2}$ also implies $a_{22} = -A_{22} < -A_{22} + \frac{A_{12}+A_{21}}{2} = \frac{a_{12}+a_{21}}{2}$. Lastly we have

$$\begin{aligned} |a_{11} - a_{12}| &= |2A_{12} - A_{11} - A_{12}| \\ &= |A_{12} - A_{11}| \\ &< A_{22} - A_{21} \\ &= -A_{22} - (A_{21} - 2A_{22}) \end{aligned}$$

$$= a_{22} - a_{21}.$$

Hence the map ρ is well-defined.
Finally, we have

$$\begin{aligned}\rho^2(A_{11}, A_{12}, A_{21}, A_{22}) &= \rho(2A_{12} - A_{11}, A_{12}, A_{21} - 2A_{22}, -A_{22}) \\ &= (2A_{12} - [2A_{12} - A_{11}], A_{12}, A_{21} - 2A_{22} - 2(-A_{22}), -(-A_{22})) \\ &= (A_{11}, A_{12}, A_{21}, A_{22}).\end{aligned}$$

Therefore by Lemma 3.4.13 the map ρ is a bijection and hence an involution. □

Corollary 3.4.15.
The cardinalities of the sets $J_{0,>}$ and $J_{0,<}$ are identical. Thus $R_1 = R_2$.

Proof.
We use the involution ρ from Lemma 3.4.14. Recall we may write $J_0 = J_{0,=} \cup J_{0,>} \cup J_{0,<}$ and observe $\rho(J_{0,=}) \subseteq J_{0,=}$ because elements in $J_{0,=}$ satisfy $A_{22} = 0$. We also have $\rho(J_{0,>}) \subseteq J_{0,<}$ and $\rho(J_{0,<}) \subseteq J_{0,>}$ as the map ρ changes the sign of the (non-zero) A_{22} entry.
Hence $R_1 = |J_{0,>}| = |J_{0,<}| = R_2$. □

We now develop a new set to prove the above cardinality is in fact finite. This new set will later be used to explicitly count the elements in $J_{0,>}$ and $J_{0,<}$.

Lemma 3.4.16.
Let $Y_1 = \{(\alpha, \beta, \gamma, \delta) \mid \alpha^2 + \alpha\delta + \beta\gamma = D, 0 < \beta, 0 < \delta, 0 < \gamma < 2\alpha\}$ and define the map

$$\begin{aligned}\iota : Y_1 &\longrightarrow J_{0,>} \\ (\alpha, \beta, \gamma, \delta) &\longmapsto (\gamma + \delta + \beta, \delta + \beta + \alpha, \beta - \alpha, \beta) = (A_{11}, A_{12}, A_{21}, A_{22}).\end{aligned}$$

Then ι is a well-defined bijection.

Proof.
Well-defined: Observe

$$\begin{aligned}\det(A) &= (\gamma + \delta + \beta)(\beta) - (\delta + \beta + \alpha)(\beta - \alpha) \\ &= \alpha^2 + \alpha\delta + \beta\gamma \\ &= D.\end{aligned}$$

We also have $A_{22} = \beta > 0$ and

$$\begin{aligned}\frac{A_{12} + A_{21}}{2} &= \frac{\delta + \beta + \alpha + \beta - \alpha}{2} \\ &= \frac{2\beta + \delta}{2} \\ &= \beta + \frac{\delta}{2}\end{aligned}$$

$$> \beta \text{ as } \delta > 0.$$

Further, we have $A_{11} = \gamma + \delta + \beta > \beta + \frac{\delta}{2}$ as $\gamma, \delta > 0$. Consequently, we have $0 < A_{22} < \frac{A_{12}+A_{21}}{2} < A_{11}$.
Next, observe $2\alpha > \gamma$ implies $\alpha > \gamma - \alpha$. Also, $\gamma > 0$ implies $\alpha > \alpha - \gamma$. Combining these together yields $A_{22} - A_{21} = \beta - (\beta - \alpha) = \alpha > |\gamma - \alpha| = |A_{11} - A_{12}|$.
Hence ι is well defined and maps into $J_{0,>}$.
Injectivity: Suppose $\iota(\alpha, \beta, \gamma, \delta) = \iota\left(\hat{\alpha}, \hat{\beta}, \hat{\gamma}, \hat{\delta}\right)$ and thus

$$(\gamma + \delta + \beta, \delta + \beta + \alpha, \beta - \alpha, \beta) = \left(\hat{\gamma} + \hat{\delta} + \hat{\beta}, \hat{\delta} + \hat{\beta} + \hat{\alpha}, \hat{\beta} - \hat{\alpha}, \hat{\beta}\right).$$

Equating the entries yields injectivity.
Surjectivity: Let $(A_{11}, A_{12}, A_{21}, A_{22}) \in J_{0,>}$ be arbitrary.
Let $f = (A_{22} - A_{21}, A_{22}, A_{11} - A_{12} - A_{21} + A_{22}, A_{12} + A_{21} - 2A_{22}) = (\alpha, \beta, \gamma, \delta)$, we will show this lies in Y_1. First, by Observation 3.4.4 we have $\alpha^2 + \alpha\delta + \beta\gamma = D$. Next, $\beta = A_{22} > 0$ and further $A_{22} < \frac{A_{12}+A_{21}}{2}$ implies $\frac{\delta}{2} = \frac{A_{12}+A_{21}}{2} - A_{22} > 0$; hence $\delta > 0$. We also see $A_{22} - A_{21} > |A_{11} - A_{12}|$ implies $A_{22} - A_{21} > A_{12} - A_{11}$, that is $\gamma = A_{11} - A_{12} - A_{21} + A_{22} > 0$. Lastly,

$$\begin{aligned} 2\alpha &= (A_{22} - A_{21}) + (A_{22} - A_{21}) \\ &> A_{22} - A_{21} + |A_{11} - A_{12}| \\ &\geqslant A_{22} - A_{21} + A_{11} - A_{12} \\ &= \gamma. \end{aligned}$$

Thus we have $0 < \gamma < 2\alpha$.
Hence f lies in Y_1. It is straightforward to show that $\iota(f) = (A_{11}, A_{12}, A_{21}, A_{22})$. Thus ι is surjective and hence a bijection. □

Corollary 3.4.17.
The set Y_1 is finite and $|Y_1| = |J_{0,>}| = R_1$.

Proof.
By the definition of Y_1 in Lemma 3.4.16, all of α, β, γ and δ are strictly positive and must satisfy $D = \alpha^2 + \alpha\delta + \beta\gamma$. Consequently there can be at most finitely many such $(\alpha, \beta, \gamma, \delta)$. By Lemma 3.4.16 we have $|Y_1| = |J_{0,>}| = R_1$. □

We are able to repeat this construction for the set J_1 and do so below. We will use the map ρ from Lemma 3.4.14, re-purposing it to the set J_1.

Lemma 3.4.18.
The map

$$\begin{aligned} \rho : J_1 &\longrightarrow J_1 \\ (A_{11}, A_{12}, A_{21}, A_{22}) &\longmapsto (2A_{12} - A_{11}, A_{12}, A_{21} - 2A_{22}, -A_{22}) = (a_{11}, a_{12}, a_{21}, a_{22}) \end{aligned}$$

is a well-defined involution.

Proof.
First, we show the map is well-defined. Let $(A_{11}, A_{12}, A_{21}, A_{22}) \in J_1$ be arbitrary. We inherit the properties $\det(a) = \det(A)$, $|a_{11} - a_{12}| < a_{22} - a_{21}$ and $\frac{a_{12}+a_{21}}{2} < a_{11}$ from the proof of Lemma 3.4.14. Next, $\frac{A_{12}+A_{21}}{2} < A_{11}$ yields $\frac{a_{12}+a_{21}}{2} = \frac{A_{12}+A_{21}-2A_{22}}{2} = \frac{A_{12}+A_{21}}{2} - A_{22} \geqslant 0$. Lastly, $0 \leqslant \frac{A_{12}+A_{21}}{2}$ implies $a_{22} = -A_{22} \leqslant -A_{22} + \frac{A_{12}+A_{21}}{2} = \frac{a_{12}+a_{21}}{2}$. Hence ρ is well-defined.
Finally, as in the proof of Lemma 3.4.14, we have $\rho^2 = \mathrm{id}$. Therefore by Lemma 3.4.13 the map ρ is a bijection and hence an involution. □

Lemma 3.4.19.
Let $Y_2 = \{(\alpha, \beta, \gamma, \delta) \mid \alpha^2 + \alpha\delta + \beta\gamma = D, 0 < \beta, 0 \leqslant \delta, 0 < \gamma < 2\alpha\}$ *and define the map*

$$\begin{aligned} \Gamma : Y_2 &\longrightarrow J_{1,>} \\ (\alpha, \beta, \gamma, \delta) &\longmapsto (\gamma + \delta + \beta, \beta + \delta + \alpha, \beta - \alpha, \beta) = (A_{11}, A_{12}, A_{21}, A_{22}) . \end{aligned}$$

The Γ *is a well-defined bijection.*

Proof.
Well-defined: Observe

$$\begin{aligned} \det(A) &= (\gamma + \delta + \beta)\,\beta - (\beta + \delta + \alpha)\,(\beta - \alpha) \\ &= \alpha^2 + \alpha\delta + \beta\gamma \\ &= D. \end{aligned}$$

Next we see $A_{22} = \beta > 0$ and $A_{12} + A_{21} = 2\beta + \delta$. Using $0 \leqslant \delta$ with this we see $0 < A_{22} = \beta \leqslant \beta + \frac{\delta}{2} = \frac{A_{12}+A_{21}}{2}$. We also have

$$\begin{aligned} A_{11} &= \gamma + \delta + \beta \\ &> \delta + \beta \text{ as } \gamma > 0 \\ &\geqslant \frac{\delta}{2} + \beta \text{ as } 0 \leqslant \delta \\ &= \frac{A_{12} + A_{21}}{2}. \end{aligned}$$

Therefore $0 < A_{22} \leqslant \frac{A_{12}+A_{21}}{2} < A_{11}$.
Lastly, observe $2\alpha > \gamma$ implies $\alpha > \gamma - \alpha$, and $\gamma > 0$ implies $\alpha - \gamma < \alpha$. Consequently we have $A_{22} - A_{21} = \alpha > |\gamma - \alpha| = |A_{11} - A_{12}|$.
Hence Γ is well-defined and maps into $J_{1,>}$.
Injectivity: Suppose $\Gamma(\alpha, \beta, \gamma, \delta) = \Gamma\left(\hat{\alpha}, \hat{\beta}, \hat{\gamma}, \hat{\delta}\right)$, thus

$$(\gamma + \delta + \beta, \beta + \delta + \alpha, \beta - \alpha, \beta) = \left(\hat{\gamma} + \hat{\delta} + \hat{\beta}, \hat{\beta} + \hat{\delta} + \hat{\alpha}, \hat{\beta} - \hat{\alpha}, \hat{\beta}\right).$$

Equating the entries yields injectivity.
Surjectivity: Let $(A_{11}, A_{12}, A_{21}, A_{22}) \in J_{1,>}$ be arbitrary.

Let $f = (A_{22} - A_{21}, A_{22}, A_{11} - A_{12} - A_{21} + A_{22}, A_{12} + A_{21} - 2A_{22}) = (\alpha, \beta, \gamma, \delta)$, we will show this lies in Y_2.
Observation 3.4.4 shows that f satisfies $\alpha^2 + \alpha\delta + \beta\gamma = D$. Next, $A_{22} - A_{21} > |A_{11} - A_{12}|$ implies $\alpha = A_{22} - A_{21} > 0$. Further, this inequality also implies $\gamma = A_{11} - A_{12} - A_{21} + A_{22} > 0$. Notice $\beta = A_{22} > 0$ and $A_{22} \leqslant \frac{A_{12}+A_{21}}{2}$ implies $A_{12} + A_{21} - 2A_{22} \geqslant 0$, that is $\delta \geqslant 0$. Lastly, by way of $A_{22} - A_{21} > |A_{11} - A_{12}|$, we have $2\alpha = 2A_{22} - 2A_{21} > A_{22} - A_{21} + (A_{11} - A_{12}) = \gamma$ and therefore $0 < \gamma < 2\alpha$. Hence it follows that $f \in Y_2$.
Finally, it is straightforward to see $\Gamma(f) = (A_{11}, A_{12}, A_{21}, A_{22})$.
Consequently Γ is surjective and thus a bijection. □

Corollary 3.4.20.
The set Y_2 is finite and has the same cardinality as the set $J_{1,>}$. Thus $|Y_2| = |J_{1,>}| = S_1$.

Proof.
By the definition of Y_2 in Lemma 3.4.19, α, β, and γ are strictly positive, whilst δ must be non-negative. Further, all must satisfy $D = \alpha^2 + \alpha\delta + \beta\gamma$. Consequently there can be at most finitely many $(\alpha, \beta, \gamma, \delta)$. By Lemma 3.4.19 we have $|Y_2| = |J_{1,>}| = S_1$. □

We now apply the knowledge found in the section to simplify our expression for the complete class number as found in Equation 3.12. We have

$$\begin{aligned}\mathrm{Cl}_c(D) - m - n &= 2(P + Q - R - S)\\ &= 2(P_0 + P_1 + P_2 + Q_0 + Q_1 + Q_2 - R_0 - R_1 - R_2 - S_0 - S_1 - S_2)\\ &= 2(P_0 + Q_0 - R_0 - S_0 + 2(P_1 + P_2 - R_1 - S_1)). \qquad (3.14)\end{aligned}$$

Notes on Section 3.4

In his paper, Kronecker has opted to state his results without proof. However, he does indicate the general structure of the sets X_1, X_2, Y_1 and Y_2 on page [Kr1897, p. 461]. Kronecker's approach is also longer than ours as he indicates he knew $P_1 = Q_2$ and $P_2 = Q_1$. It is straightforward but tedious to show this is true by verifying the following two lemmas:

Lemma 3.4.21.
The map $\hat{\phi}$ given by

$$\begin{aligned}\hat{\phi} : X_2 &\longrightarrow I_{1,>}\\ (\alpha, \beta, \gamma, \delta) &\longmapsto (\beta, \beta - \alpha, \alpha - \beta + \delta, 2\alpha - \beta + \gamma + \delta) = (A_{11}, A_{12}, A_{21}, A_{22})\end{aligned}$$

is a well-defined bijection.

This yields $P_2 = Q_1$.

Lemma 3.4.22.
The map $\hat{\psi}$ given by

$$\hat{\psi} : X_1 \longrightarrow I_{1,<}$$

$$(\alpha, \beta, \gamma, \delta) \longmapsto (\beta, \alpha + \beta, \beta - \alpha - \delta, \gamma + \beta - \delta) = (A_{11}, A_{12}, A_{21}, A_{22})$$

is a well-defined bijection.

This yields $P_1 = Q_2$.

Further, since Kronecker stated his results rather giving a series of proofs, it appears he proved $R_1 = R_2$ and $S_1 = S_2$ by constructing pairs of bijections as opposed to using an involution. For completeness one may verify this by checking the following two lemmas:

Lemma 3.4.23.
The map $\hat{\iota}$ given by

$$\begin{aligned} \hat{\iota} : Y_1 &\longrightarrow J_{0,<} \\ (\alpha, \beta, \gamma, \delta) &\longmapsto (2\alpha + \beta - \gamma + \delta, \delta + \beta + \alpha, -\beta - \alpha, -\beta) = (A_{11}, A_{12}, A_{21}, A_{22}) \end{aligned}$$

is a well-defined bijection.

This yields $R_2 = |Y_1| = R_1$.

Lemma 3.4.24.
The map $\hat{\Gamma}$ given by

$$\begin{aligned} \hat{\Gamma} : Y_2 &\longrightarrow J_{1,<} \\ (\alpha, \beta, \gamma, \delta) &\longmapsto (2\alpha + \beta - \gamma + \delta, \alpha + \beta + \delta, -\beta - \alpha, -\beta) = (A_{11}, A_{12}, A_{21}, A_{22}) \end{aligned}$$

is a well-defined bijection.

This yields $S_2 = |Y_2| = S_1$.

We should also note our proof has yielded $P_1 + P_2 = Q_1 + Q_2$ and therefore we derived Equation 3.14. Whereas in his paper [Kr1897, p. 461], Kronecker states $P + Q - R - S = P_0 + Q_0 - R_0 - S_0 + 2(P_1 + Q_1 - R_1 - S_1)$ instead.

3.5 Towards Establishing the Finiteness of $\overline{P}$, $\overline{Q}$, $\overline{R}$ and $\overline{S}$

We continue in the manner of Section 3.4; this time our goal is working towards showing $\overline{P}$, $\overline{Q}$, $\overline{R}$ and $\overline{S}$ are finite. Recall that adding a bar to our notation means we are including the conditions $A_{11} + A_{22} \equiv 1 \bmod 2$ and $A_{12} - A_{21} \equiv 0 \bmod 2$.

Definition 3.5.1.
Extend Definition 3.3.13 in the same manner as we did for Definitions 3.4.1 and 3.4.2 as follows:
$\overline{\Theta_{i,j}} = \{A \in \Theta_{i,j} \mid A_{11} + A_{22} \equiv 1 \bmod 2, A_{12} - A_{21} \equiv 0 \bmod 2\}$, where $\Theta \in \{I, J\}$, $i \in \{0, 1\}$ and $j \in \{=, <, >\}$.
We extend the notation developed in Definitions 3.4.1 and 3.4.2 by placing a bar over the previous notation. For example, $\overline{P_1} = \left|\overline{I_{0,>}}\right|$.

Observation 3.5.2.
It is important to observe that the sets in Definition 3.5.1 are mutually disjoint. Therefore $|\overline{\Theta_{i,j}}| = |\overline{\Theta_{i,=}}| + |\overline{\Theta_{i,>}}| + |\overline{\Theta_{i,<}}|$, where $\Theta \in \{I, J\}$, $i \in \{0, 1\}$ and $j \in \{=, >, <\}$. Further, since $\overline{\Theta_{i,j}} \subseteq \Theta_{i,j}$, where it is known $\Theta_{i,j}$ is finite then it follows immediately that $\overline{\Theta_{i,j}}$ is also finite.

Lemma 3.5.3.
The restriction of the map π found in Lemma 3.4.10 to the subset $\overline{I_0}\backslash\overline{I_{0,=}}$ gives a well-defined bijection to the set $\overline{I_1}\backslash\overline{I_{1,=}}$. Hence we have $\overline{P_1} + \overline{P_2} = \overline{Q_1} + \overline{Q_2}$.

Proof.
To show the restriction map is well-defined we will prove $a_{11} + a_{22} \equiv 1 \bmod 2$ and $a_{12} - a_{21} \equiv 0 \bmod 2$. We have $a_{11} + a_{22} = A_{11} + A_{22} - 2A_{21} \equiv 1 \bmod 2$ and $a_{12} - a_{21} = 2A_{11} - A_{12} - A_{21} \equiv 0 \bmod 2$. Thus the restriction map is well-defined.
Injectivity is inherited, so it remains to show surjectivity.
For an arbitrary $(a_{11}, a_{12}, a_{21}, a_{22}) \in \overline{I_1}\backslash\overline{I_{1,=}}$ we know from the proof of Lemma 3.4.10 that the element $f = (a_{11}, 2a_{11} - a_{12}, -a_{21}, a_{22} - 2a_{21}) = (A_{11}, A_{12}, A_{21}, A_{22})$ will be sufficient if we can show $A_{11} + A_{22} \equiv 1 \bmod 2$ and $A_{12} - A_{21} \equiv 0 \bmod 2$. We have $A_{11} + A_{22} = a_{11} + a_{22} - 2a_{21} \equiv 1 \bmod 2$ and $A_{12} - A_{21} = 2a_{11} - a_{12} - a_{21} \equiv 0 \bmod 2$. Hence the restriction map is surjective and thus a bijection. It immediately follows that $\overline{P_1} + \overline{P_2} = \overline{Q_1} + \overline{Q_2}$. □

Since our eventual goal is to enumerate these sets, we now give restrictions of the sets X_1 and X_2 and establish bijections to them.

Lemma 3.5.4.
Let $\overline{X_1} = \{(\alpha, \beta, \gamma, \delta) \in X_1 \mid \gamma \equiv 1 \bmod 2, \delta \equiv 0 \bmod 2\}$. Then the restriction of the map ϕ found in Lemma 3.4.5 to the subset $\overline{X_1}$ gives a well-defined bijection to the set $\overline{I_{0,>}}$. Consequently, $|\overline{X_1}| = \overline{P_1}$.

Proof.
Since the map ϕ is a bijection from X_1 to $I_{0,>}$, it is sufficient to show $A_{11} + A_{22} \equiv 1 \bmod 2$ and $A_{12} - A_{21} \equiv 0 \bmod 2$. We have

$$\begin{aligned} A_{11} + A_{22} &= \beta + 2\alpha - \beta + \gamma + \delta \\ &\equiv \gamma + \delta \bmod 2 \\ &\equiv 1 \bmod 2, \text{ and} \\ A_{12} - A_{21} &= \beta - \alpha - \alpha + \beta - \delta \\ &\equiv \delta \bmod 2 \\ &\equiv 0 \bmod 2. \end{aligned}$$

Therefore the restriction map is well-defined. We note that injectivity is inherited and so it remains to prove surjectivity.
It is sufficient to show $f = (A_{11} - A_{12}, A_{11}, -A_{11} + A_{12} - A_{21} + A_{22}, A_{12} + A_{21}) = (\alpha, \beta, \gamma, \delta)$ satisfies $\gamma \equiv 1 \bmod 2$ and $\delta \equiv 0 \bmod 2$. We have

$$\gamma = -A_{11} + A_{12} - A_{21} + A_{22}$$

$$\begin{aligned}
&\equiv (A_{11} + A_{22}) \bmod 2 + (A_{12} - A_{21}) \bmod 2 \\
&\equiv 1 + 0 = 1 \bmod 2, \text{ and we have} \\
\delta &= A_{12} + A_{21} \\
&\equiv A_{12} - A_{21} \bmod 2 \\
&\equiv 0 \bmod 2.
\end{aligned}$$

Hence the restriction map is surjective and thus a bijection. Therefore $|\overline{X_1}| = \overline{P_1}$. □

Lemma 3.5.5.
Let $\overline{X_2} = \{(\alpha, \beta, \gamma, \delta) \in X_2 \mid \gamma \equiv 1 \bmod 2, \delta \equiv 0 \bmod 2\}$. Then the restriction of the map ψ found in Lemma 3.4.7 to the subset $\overline{X_2}$ gives a well-defined bijection to the set $\overline{I_{0,<}}$. Consequently, $|\overline{X_2}| = \overline{P_2}$.

Proof.
Since the map ψ is a bijection from X_2 to $I_{0,<}$, it is sufficient to show $A_{11} + A_{22} \equiv 1 \bmod 2$ and $A_{12} - A_{21} \equiv 0 \bmod 2$. We have

$$\begin{aligned}
A_{11} + A_{22} &= \beta + \gamma + \beta - \delta \\
&\equiv \gamma + \delta \bmod 2 \\
&\equiv 1 \bmod 2 \text{ and} \\
A_{12} - A_{21} &= \alpha + \beta - \beta + \alpha + \delta \\
&\equiv \delta \bmod 2 \\
&\equiv 0 \bmod 2.
\end{aligned}$$

Therefore the restriction map is well-defined. We note again that injectivity is inherited and so it remains to prove surjectivity. It is sufficient to show
$f = (A_{12} - A_{11}, A_{11}, A_{11} - A_{12} - A_{21} + A_{22}, 2A_{11} - A_{12} - A_{21}) = (\alpha, \beta, \gamma, \delta)$ satisfies $\gamma \equiv 1 \bmod 2$ and $\delta \equiv 0 \bmod 2$. We have

$$\begin{aligned}
\gamma &= A_{11} - A_{12} - A_{21} + A_{22} \\
&\equiv (A_{11} + A_{22}) \bmod 2 + (A_{12} - A_{21}) \bmod 2 \\
&\equiv 1 \bmod 2, \text{ and} \\
\delta &= 2A_{11} - A_{12} - A_{21} \\
&\equiv A_{12} - A_{21} \bmod 2 \\
&\equiv 0 \bmod 2.
\end{aligned}$$

Hence the restriction map is surjective and thus is a bijection. Therefore we have $|\overline{X_2}| = \overline{P_2}$. □

We now perform a similar analysis for $\overline{R_1}$, $\overline{R_2}$, $\overline{S_1}$ and $\overline{S_2}$.

Lemma 3.5.6.
The restriction of the map ρ found in Lemma 3.4.14 to the subset $\overline{J_0}$ gives a well-defined involution to the set $\overline{J_0}$. Further, we have $\overline{R_1} = \overline{R_2}$.

Proof.
Since the map ρ in Lemma 3.4.14 is a bijection, it is sufficient to show $a_{11} + a_{22} \equiv 1 \bmod 2$ and $a_{12} - a_{21} \equiv 0 \bmod 2$ in order to show the map is well-defined. We have

$$\begin{aligned} a_{11} + a_{22} &= 2A_{12} - A_{11} - A_{22} \\ &\equiv A_{11} + A_{22} \bmod 2 \\ &\equiv 1 \bmod 2 \text{ and} \\ a_{12} - a_{21} &= A_{12} - A_{21} + 2A_{22} \\ &\equiv A_{12} - A_{21} \bmod 2 \\ &\equiv 0 \bmod 2. \end{aligned}$$

Therefore the restriction map is well-defined. Since we inherit $\rho^2 = \mathrm{id}$ it follows that the restriction map is a involution on the set $\overline{J_0}$.
We now observe that $\rho(\overline{J_{0,=}}) \subseteq \overline{J_{0,=}}$, $\rho(\overline{J_{0,>}}) \subseteq \overline{J_{0,<}}$ and $\rho(\overline{J_{0,<}}) \subseteq \overline{J_{0,>}}$ for the same reasons as given in the proof of Corollary 3.4.15. Therefore we get $\overline{R_1} = |\overline{J_{0,>}}| = |\overline{J_{0,<}}| = \overline{R_2}$. □

Again, since we will be interested in enumerating these sets, we provide a bijection below to a subset of Y_1 that will help us to do so.

Lemma 3.5.7.
Let $\overline{Y_1} = \{(\alpha, \beta, \gamma, \delta) \in Y_1 \mid \gamma \equiv 1 \bmod 2, \delta \equiv 0 \bmod 2\}$. Then the restriction of the map ι, found in Lemma 3.4.16, to the subset $\overline{Y_1}$ gives a well-defined bijection to the set $\overline{J_{0,>}}$. Consequently, $\overline{R_1} = |\overline{J_{0,>}}| = |\overline{Y_1}|$.

Proof.
Since the map ι is a bijection, in order to show the restriction map is well-defined, it is sufficient to show $a_{11} + a_{22} \equiv 1 \bmod 2$ and $a_{12} - a_{21} \equiv 0 \bmod 2$. We have

$$\begin{aligned} a_{11} + a_{22} &= \gamma + \delta + \beta + \beta \\ &\equiv \gamma + \delta \bmod 2 \\ &\equiv 1 \bmod 2, \text{ and} \\ a_{12} + a_{21} &= \delta + \beta + \alpha + \beta - \alpha \\ &\equiv \delta \bmod 2 \\ &\equiv 0 \bmod 2. \end{aligned}$$

Hence the restriction map is well-defined. We inherit injectivity and so it remains to show surjectivity.
It is enough to show $f = (A_{22} - A_{21}, A_{22}, A_{11} - A_{12} - A_{21} + A_{22}, A_{12} + A_{21} - 2A_{22}) = (\alpha, \beta, \gamma, \delta)$ satisfies $\gamma \equiv 1 \bmod 2$ and $\delta \equiv 0 \bmod 2$. We have

$$\begin{aligned} \gamma &= A_{11} - A_{12} - A_{21} + A_{22} \\ &\equiv (A_{11} + A_{22}) \bmod 2 + (A_{12} - A_{21}) \bmod 2 \\ &\equiv 1 \bmod 2, \text{ and} \end{aligned}$$

$$\begin{aligned}\delta &= A_{12} + A_{21} - 2A_{22} \\ &\equiv A_{12} - A_{21} \bmod 2 \\ &\equiv 0 \bmod 2.\end{aligned}$$

Thus the restriction map is a surjective and therefore a bijection. It follows immediately that $\overline{R_1} = |\overline{J_{0,>}}| = |\overline{Y_1}|$. □

In a similar manner we have

Lemma 3.5.8.
The restriction of the map ρ (found in Lemma 3.4.18) to the subset $\overline{J_1}$ gives a well-defined involution on the set $\overline{J_1}$. Further, we have $\overline{S_1} = \overline{S_2}$.

Proof.
Since the map ρ in Lemma 3.4.18 is a bijection, in order to show the restriction map is well-defined it is sufficient to show $a_{11} + a_{22} \equiv 1 \bmod 2$ and $a_{12} - a_{21} \equiv 0 \bmod 2$. We have

$$\begin{aligned}a_{11} + a_{22} &= \gamma + \delta + \beta + \beta \\ &\equiv \gamma + \delta \bmod 2 \\ &\equiv 1 \bmod 2, \text{ and} \\ a_{12} - a_{21} &= \beta + \delta + \alpha - \beta + \alpha \\ &\equiv \delta \bmod 2 \\ &\equiv 0 \bmod 2.\end{aligned}$$

Therefore the restriction map is well-defined. Since we inherit $\rho^2 = \mathrm{id}$ it follows that the restriction map is an involutionon the set $\overline{J_1}$.
We now observe that $\rho(\overline{J_{1,=}}) \subseteq \overline{J_{1,=}}$, $\rho(\overline{J_{1,>}}) \subseteq \overline{J_{1,<}}$ and $\rho(\overline{J_{1,<}}) \subseteq \overline{J_{1,>}}$ for the same reasons as given in the proof of Corollary 3.4.20. Therefore we get $\overline{S_1} = |\overline{J_{1,>}}| = |\overline{J_{1,<}}| = \overline{S_2}$. □

We now provide a bijection to a subset of Y_2 in order to be able to enumerate this set.

Lemma 3.5.9.
Let $Y_2 = \{(\alpha, \beta, \gamma, \delta) \in Y_2 \mid \gamma \equiv 1 \bmod 2, \delta \equiv 0 \bmod 2\}$. Then the restriction of the map Γ (found in Lemma 3.4.19) to the subset $\overline{Y_2}$ gives a well-defined bijection to the set $\overline{J_{1,>}}$. Consequently we have $\overline{S_1} = |\overline{Y_2}|$.

Proof.
Since the map Γ is a bijection, it is sufficient to show $a_{11} + a_{22} \equiv 1 \bmod 2$ and $a_{12} - a_{21} \equiv 0 \bmod 2$ to see the restriction map is well-defined. We have

$$\begin{aligned}a_{11} + a_{22} &= \gamma + \delta + \beta + \beta \\ &\equiv \gamma + \delta \bmod 2 \\ &\equiv 1 \bmod 2, \text{ and}\end{aligned}$$

$$\begin{aligned} a_{12} - a_{21} &= \beta + \delta + \alpha - \beta + \alpha \\ &\equiv \delta \bmod 2 \\ &\equiv 0 \bmod 2. \end{aligned}$$

Therefore the restriction map is well-defined. We inherit injectivity and therefore it remains to show surjectivity.
It is enough to show $f = (A_{22} - A_{21}, A_{22}, A_{11} - A_{12} - A_{21} + A_{22}, A_{12} + A_{21} - 2A_{22}) = (\alpha, \beta, \gamma, \delta)$ satisfies $\gamma \equiv 1 \bmod 2$ and $\delta \equiv 0 \bmod 2$. We have

$$\begin{aligned} \gamma &= A_{11} - A_{12} - A_{21} + A_{22} \\ &\equiv (A_{11} + A_{22}) \bmod 2 + (A_{12} - A_{21}) \bmod 2 \\ &\equiv 1 \bmod 2, \text{ and} \\ \delta &= A_{12} + A_{21} - 2A_{22} \\ &\equiv A_{12} - A_{21} \bmod 2 \\ &\equiv 0 \bmod 2. \end{aligned}$$

Therefore the restriction map is a surjection and thus a bijection. It immediately follows that $\overline{S_1} = |\overline{J_{1,>}}| = |\overline{Y_2}|$. □

We now use the results developed in this section to provide a simplification to the class number as derived in Theorem 3.3.14.

Lemma 3.5.10.
Let $D \in \mathbb{Z}_{>0}$, then $\overline{\mathrm{Cl}}_c(D) = 3\left(\overline{P_0} + \overline{Q_0} - \overline{R_0} - \overline{S_0} + 2\left(\overline{P_1} + \overline{P_2} - \overline{R_1} - \overline{S_1}\right)\right)$.

Proof.
From Theorem 3.3.14 we have $\overline{\mathrm{Cl}}_c(D) = 3(\overline{P} + \overline{Q} - \overline{R} - \overline{S})$. Applying the results found in this section we get

$$\begin{aligned} \overline{\mathrm{Cl}}_c(D) &= 3(\overline{P} + \overline{Q} - \overline{R} - \overline{S}) \\ &= 3\left(\overline{P_0} + \overline{P_1} + \overline{P_2} + \overline{Q_0} + \overline{Q_1} + \overline{Q_2} - \overline{R_0} - \overline{R_1} - \overline{R_2} - \overline{S_0} - \overline{S_1} - \overline{S_2}\right) \\ &= 3\left(\overline{P_0} + \overline{Q_0} - \overline{R_0} - \overline{S_0} + 2\left(\overline{P_1} + \overline{P_2} - \overline{R_1} - \overline{S_1}\right)\right). \end{aligned}$$

□

Notes on Section 3.5

We continue to observe that Kronecker only states his results instead of proving them. From his exposition it is highly likely that he continued to construct the necessary bijections as opposed to using an involution.

When comparing with Kronecker's original text, it is important to note that he stated $\overline{Q_2} = \overline{P_1}$ and $\overline{P_2} = \overline{Q_1}$. These results are straightforward to determine by verifying the following two corollaries:

Corollary 3.5.11.
The restriction of the map $\hat{\phi}$ (see Lemma 3.4.21) to the set $\overline{X_2} \subseteq X_2$, given by

$$\hat{\phi}|_{\overline{X_2}} : \overline{X_2} \longrightarrow \overline{I_{1,>}} \subseteq I_{1,>} \ ,$$

is a well-defined bijection and hence $\overline{Q_2} = \overline{P_1}$.

Corollary 3.5.12.
The restriction of the map $\hat{\psi}$ (see Lemma 3.4.22) to the set $\overline{X_1} \subseteq X_1$, given by

$$\hat{\psi}|_{\overline{X_1}} : \overline{X_1} \longrightarrow \overline{I_{1,<}} \subseteq I_{1,<} \ ,$$

is a well-defined bijection and hence $\overline{P_2} = \overline{Q_1}$.

Therefore, Kronecker's result is the same as our Lemma 3.5.10, but not stated in this form in his paper. Kronecker proceeds to perform several more manipulations of the sets before stating an updated expression for $\overline{\mathrm{Cl}}_c\,(D)$ (see [Kr1897, p. 464]).

For completeness we give but do not prove the following two further corollaries. The proofs follow in the natural manner.

Corollary 3.5.13.
The restriction of the map $\hat{\imath}$ (see Lemma 3.4.23) to the set $\overline{Y_1} \subseteq Y_1$, given by

$$\hat{\imath}|_{\overline{Y_1}} : \overline{Y_1} \longrightarrow \overline{J_{0,<}} \ ,$$

is a well-defined bijection and hence $\overline{R_2} = \left|\overline{Y_1}\right|$.

Corollary 3.5.14.
The restriction of the map $\hat{\Gamma}$ (see Lemma 3.4.24) to the set $\overline{Y_2} \subseteq Y_2$, given by

$$\hat{\Gamma}|_{\overline{Y_2}} : \overline{Y_2} \longrightarrow \overline{J_{1,<}} \ ,$$

is a well-defined bijection and hence $\overline{S_2} = \left|\overline{Y_2}\right|$.

3.6 The Relationships between P_1 and R_1, and also between P_2 and S_1

In this section we explore the connections between P_1 and R_1, as well as between P_2 and S_2. We encourage the reader to consult the notes at the end of the section for the details relating our results to those of Kronecker.

Definition 3.6.1.
Fix $D \in \mathbb{Z}_{>0}$. From Lemma 3.4.5 we have the following definition for the set X_1,

$$X_1 = \left\{(\alpha, \beta, \gamma, \delta) \mid \alpha^2 + \alpha\delta + \beta\gamma = D, 0 < \alpha, 0 < \gamma, 0 < \delta \leqslant 2\beta\right\}.$$

From Lemma 3.4.16 we have the following definition for the set Y_1,

$$Y_1 = \left\{(\alpha, \beta, \gamma, \delta) \mid \alpha^2 + \alpha\delta + \beta\gamma = D, 0 < \beta, 0 < \delta, 0 < \gamma < 2\alpha\right\}.$$

Then

$$X_1 \cap Y_1 = \left\{(\alpha, \beta, \gamma, \delta) \mid \alpha^2 + \alpha\delta + \beta\gamma = D, 0 < \gamma < 2\alpha, 0 < \delta \leqslant 2\beta\right\}.$$

Now define the set Θ by

$$\Theta = \left\{(\alpha, \beta, \gamma, \delta) \mid \alpha^2 + \alpha\delta + \beta\gamma = D, 0 < 2\alpha \leqslant \gamma, 0 < \delta \leqslant 2\beta, \gamma \equiv 0 \bmod 2\alpha\right\}.$$

Let K denote the cardinality of the set Θ.

Observation 3.6.2.
Recall from Corollaries 3.4.6 and 3.4.17 that $P_1 = |X_1|$ and $R_1 = |Y_1|$ are finite. In a similar manner we see that $|\Theta|$ is finite.
Notice that $\Theta \cap (X_1 \cap Y_1) = \emptyset$. This is because forms in Θ must satisfy the extra condition of $\gamma \equiv 0 \bmod 2\alpha$, while forms in $X_1 \cap Y_1$ satisfy $0 < \gamma < 2\alpha$. Since $\Theta \subseteq X_1$ it follows that $\Theta \subseteq X_1 \backslash (X_1 \cap Y_1)$.

We now give a description of the sets $X_1 \backslash (X_1 \cap Y_1)$ and $Y_1 \backslash (X_1 \cap Y_1)$.

$$X_1 \backslash (X_1 \cap Y_1) = \left\{(\alpha, \beta, \gamma, \delta) \mid \alpha^2 + \alpha\delta + \beta\gamma = D, 0 < \delta \leqslant 2\beta, 0 < 2\alpha \leqslant \gamma\right\}, \quad (3.15)$$

$$Y_1 \backslash (X_1 \cap Y_1) = \left\{(\alpha, \beta, \gamma, \delta) \mid \alpha^2 + \alpha\delta + \beta\gamma = D, 0 < \gamma < 2\alpha, 0 < 2\beta < \delta\right\}. \quad (3.16)$$

Observation 3.6.3.
By Observation 3.6.2 we have $\Theta \subseteq X_1 \backslash (X_1 \cap Y_1)$, we now use Θ to partition the set X_1 as follows:

$$X_1 \backslash (X_1 \cap Y_1) = \Theta \cup (X_1 \backslash ((X_1 \cap Y_1) \cup \Theta)).$$

For clarity we have:

$$X_1 \backslash ((X_1 \cap Y_1) \cup \Theta) = \{\ (\alpha, \beta, \gamma, \delta) \mid \alpha^2 + \alpha\delta + \beta\gamma = D, 0 < 2\alpha \leqslant \gamma, 0 < \delta \leqslant 2\beta, \gamma \not\equiv 0 \bmod 2\alpha\ \}.$$

Our goal is to construct a bijection $W : Y_1 \backslash (X_1 \cap Y_1) \longrightarrow X_1 \backslash ((X_1 \cap Y_1) \cup \Theta)$.

Lemma 3.6.4.
Fix $D \in \mathbb{Z}_{>0}$. For any integer m and arbitrary $4-$ tuple $(\alpha, \beta, \gamma, \delta)$ with $D = \alpha^2 + \alpha\delta + \beta\gamma$, the map ω_m given by

$$\begin{aligned}\omega_m(\alpha, \beta, \gamma, \delta) &= (\alpha, \beta, \gamma - 2m\alpha, \delta + 2m\beta) \\ &= (\alpha', \beta', \gamma', \delta')\end{aligned}$$

satisfies $D' = \alpha'^2 + \alpha'\delta' + \beta'\delta' = D$.

Proof.
We have

$$\begin{aligned}D' &= \alpha'^2 + \alpha'\delta' + \beta'\gamma' \\ &= \alpha^2 + \alpha(\delta + 2m\beta) + \beta(\gamma - 2m\alpha) \\ &= \alpha^2 + \alpha\delta + \beta\gamma \\ &= D.\end{aligned}$$

□

Lemma 3.6.5.
Assume $0 < \gamma < 2\alpha$. Then for any integer m, we have

$$\begin{aligned}\omega_m(\alpha,\beta,\gamma,\delta) &= (\alpha,\beta,\gamma-2m\alpha,\delta+2m\beta)\\ &= (\alpha',\beta',\gamma',\delta')\end{aligned}$$

satisfies $\gamma' \not\equiv 0 \bmod 2\alpha'$.

Proof.
We have $\gamma' = \gamma - 2m\alpha$ and $\alpha' = \alpha$. Hence $\gamma' \equiv \gamma \bmod 2\alpha$. But $0 < \gamma < 2\alpha$ implies $\gamma \not\equiv 0 \bmod 2\alpha$. Therefore $\gamma' \not\equiv 0 \bmod 2\alpha'$. □

We now explore the set $Y_1 \backslash (X_1 \cap Y_1)$.

Lemma 3.6.6.
For any form $(\alpha,\beta,\gamma,\delta) \in Y_1 \backslash (X_1 \cap Y_1)$ there is a unique integer m such that

$$\omega_m(\alpha,\beta,\gamma,\delta) = (\alpha,\beta,\gamma-2m\alpha,\delta+2m\beta) = (\alpha',\beta',\gamma',\delta')$$

satisfies $0 < \delta' \leqslant 2\beta'$ and $0 < 2\alpha' \leqslant \gamma'$.

Proof.
Consider $(\alpha',\beta',\gamma',\delta')$ as defined in Lemma 3.6.6. Clearly we have $0 < \alpha = \alpha'$ and $0 < \beta = \beta'$. Now in order to have $0 < \delta' \leqslant 2\beta'$ we require $-\frac{\delta}{2\beta} < m \leqslant 1 - \frac{\delta}{2\beta}$. Similarly, in order to have $2\alpha' \leqslant \gamma'$ we require $m \leqslant \frac{\gamma}{2\alpha} - 1$. Observe that in $Y_1 \backslash (X_1 \cap Y_1)$ we have $\gamma < 2\alpha$ and so $\frac{\gamma}{2\alpha} - 1 < 0$. Furthermore, since $\alpha, \gamma > 0$ it follows that $-1 < \frac{\gamma}{2\alpha} - 1$. We also have $0 < 2\beta < \delta$ in $Y_1 \backslash (X_1 \cap Y_1)$ and so $1 - \frac{\delta}{2\beta} < 0$. Thus we require $-\frac{\delta}{2\beta} < m \leqslant \min\left\{1 - \frac{\delta}{2\beta}, \frac{\gamma}{2\alpha} - 1\right\} < 0$. Clearly, if $1 - \frac{\delta}{2\beta} \leqslant -1$ then there is a unique integer $m \in \left(-\frac{\delta}{2\beta}, 1 - \frac{\delta}{2\beta}\right]$. Now suppose that $-1 < 1 - \frac{\delta}{2\beta} < 0$, this yields $-2 < -\frac{\delta}{2\beta} < -1$ and thus $m = -1$ is the unique integer in the interval $\left(-\frac{\delta}{2\beta}, \min\left\{1 - \frac{\delta}{2\beta}, \frac{\gamma}{2\alpha} - 1\right\}\right]$. □

Corollary 3.6.7.
The set $Y_1 \backslash (X_1 \cap Y_1) = \bigcup_{m \in \mathbb{Z}_{<0}} B_m$ is a finite disjoint union, where

$$B_m = \left\{(\alpha,\beta,\gamma,\delta) \in Y_1 \backslash (X_1 \cap Y_1) \,\middle|\, m \in \left(-\frac{\delta}{2\beta}, 1 - \frac{\delta}{2\beta}\right]\right\}.$$

Proof.
By Lemma 3.6.6 for each $(\alpha,\beta,\gamma,\delta) \in Y_1 \backslash (X_1 \cap Y_1)$ there exists a unique integer $m < 0$ such that $m \in \left(-\frac{\delta}{2\beta}, 1 - \frac{\delta}{2\beta}\right]$. We partition $Y_1 \backslash (X_1 \cap Y_1)$ into a disjoint union of the sets $B_m = \left\{(\alpha,\beta,\gamma,\delta) \in Y_1 \backslash (X_1 \cap Y_1) \mid m \in \left(-\frac{\delta}{2\beta}, 1 - \frac{\delta}{2\beta}\right]\right\}$. Clearly $B_m \cap B_n = \emptyset$ if $n \neq m$. Further, by Corollary 3.4.17 Y_1 is a finite set. Thus

$$Y_1 \backslash (X_1 \cap Y_1) = \bigcup_{m \in \mathbb{Z}_{<0}} B_m$$

is a finite disjoint union. □

We now examine the set $X_1 \setminus (X_1 \cap Y_1)$ in an analogous manner.

Lemma 3.6.8.
Let $(\alpha', \beta', \gamma', \delta')$ be a form in $X_1 \setminus (X_1 \cap Y_1)$ such that $\gamma' \not\equiv 0 \bmod 2\alpha'$. Then there is a unique integer n such that $\tau(\alpha', \beta', \gamma', \delta') = (\alpha', \beta', \gamma' + 2n\alpha', \delta' - 2n\beta') = (\alpha, \beta, \gamma, \delta)$ satisfies $0 < \gamma < 2\alpha$ and $0 < 2\beta < \delta$.

Proof.
Clearly we have $0 < \alpha' = \alpha$ and $0 < \beta' = \beta$. In order to have $0 < \gamma < 2\alpha$ we require $-\frac{\gamma'}{2\alpha'} < n < 1 - \frac{\gamma'}{2\alpha'}$. Similarly, in order to have $\delta < 2\beta$ we need $n < \frac{\delta'}{2\beta'} - 1$.
Now observe that $0 < \delta' \leqslant 2\beta'$ implies $\frac{\delta'}{2\beta'} - 1 \geqslant 0$. Also note that $0 < 2\alpha' \leqslant \gamma'$ implies $\frac{\gamma'}{2\alpha'} \geqslant 1$, however since we have stipulated $\gamma' \not\equiv 0 \bmod 2\alpha'$ it follows that $\frac{\gamma'}{2\alpha'}$ is not an integer. Thus $1 - \frac{\gamma'}{2\alpha'} < 0$. Hence we see that there is a unique integer $n \in \left(-\frac{\gamma'}{2\alpha'}, 1 - \frac{\gamma'}{2\alpha'}\right)$. □

Corollary 3.6.9.
The set $X_1 \setminus (X_1 \cap Y_1) = \Theta \cup \bigcup_{n \in \mathbb{Z}_{<0}} C_n$ is a finite disjoint union, where

$$C_n = \left\{ (\alpha', \beta', \gamma', \delta') \in X_1 \setminus (X_1 \cap Y_1) \mid n \in \left(-\frac{\gamma'}{2\alpha'}, 1 - \frac{\gamma'}{2\alpha'} \right), \gamma' \not\equiv 0 \bmod 2\alpha' \right\}.$$

Proof.
By Observation 3.6.3 we have $\Theta \subseteq X_1 \setminus (X_1 \cap Y_1)$. By Lemma 3.6.8 for any form in $X_1 \setminus ((X_1 \cap Y_1) \cup \Theta)$ there exists a unique integer n such that $n \in \left(-\frac{\gamma'}{2\alpha'}, 1 - \frac{\gamma'}{2\alpha'}\right)$, so we may partition according to n. Hence $X_1 \setminus (X_1 \cap Y_1) = \Theta \cup \bigcup_{n \in \mathbb{Z}_{<0}} C_n$. This is a disjoint union since $\Theta \cap \bigcup C_n = \emptyset$ as γ' cannot simultaneously be congruent to 0 modulo $2\alpha'$ and also not congruent to 0 modulo $2\alpha'$. Lastly, it is a finite disjoint union since in Corollary 3.4.6 we showed X_1 is a finite set. □

Lemma 3.6.10.
The map

$$\begin{aligned} \omega_m : B_m &\longrightarrow C_m \\ \omega_m(\alpha, \beta, \gamma, \delta) &\longmapsto (\alpha, \beta, \gamma - 2m\alpha, \delta + 2m\beta) = (\alpha', \beta', \gamma', \delta') \end{aligned}$$

is well-defined and is a bijection.

Proof.
Well-defined: By Lemma 3.6.4 we know that ω_m preserves the quantity $\alpha^2 + \alpha\delta + \beta\gamma = D$. By Lemma 3.6.5 we know $\omega_m(\alpha, \beta, \gamma, \delta)$ satisfies $\gamma' \not\equiv 0 \bmod 2\alpha'$, thus $(\alpha', \beta', \gamma', \delta') \notin \Theta$. We shall show $(\alpha', \beta', \gamma', \delta')$ lies in $X_1 \setminus (X_1 \cap Y_1)$. We clearly have $\alpha' = \alpha > 0$ and $\beta' = \beta > 0$, further by Lemma 3.6.6 we know m was chosen so that $(\alpha', \beta', \gamma', \delta')$ satisfies $0 < \delta' \leqslant 2\beta'$ and $0 < 2\alpha' \leqslant \gamma'$. Hence ω_m maps into $X_1 \setminus ((X_1 \cap Y_1) \cup \Theta)$.
In Corollary 3.6.9 we showed $X_1 \setminus ((X_1 \cap Y_1) \cup \Theta) = \bigcup_{n \in \mathbb{Z}_{<0}} C_n$. Suppose there exist

$(\alpha,\beta,\gamma,\delta)$, $\left(\hat{\alpha},\hat{\beta},\hat{\gamma},\hat{\delta}\right) \in B_m$ such that $\omega_m(\alpha,\beta,\gamma,\delta) \in C_{n_1}$ and $\omega_m\left(\hat{\alpha},\hat{\beta},\hat{\gamma},\hat{\delta}\right) \in C_{n_2}$ for some $n_1,\, n_2 \in \mathbb{Z}_{<0}$. Then Lemma 3.6.8 implies $n_1,\, n_2 \in \left(-\frac{\gamma'}{2\alpha'}, 1-\frac{\gamma'}{2\alpha'}\right)$ and since this interval contains a unique integer it follows that $n_1 = n_2$.
Next, in C_n we know $n \in \left(-\frac{\gamma'}{2\alpha'}, 1-\frac{\gamma'}{2\alpha'}\right)$, this yields $m - \frac{\gamma}{2\alpha} < n \leqslant m+1-\frac{\gamma}{2\alpha}$. However, in B_m we have $0 < \gamma < 2\alpha$, that is $0 < \frac{\gamma}{2\alpha} < 1$, it follows from this that m is the unique integer in the interval $\left(m-\frac{\gamma}{2\alpha}, m+1-\frac{\gamma}{2\alpha}\right)$. Consequently we have $n = m$ as n is an integer.
Hence we have shown $\omega_m : B_m \longrightarrow C_m$.
Injectivity: Suppose $\omega_m(\alpha,\beta,\gamma,\delta) = \omega_m\left(\hat{\alpha},\hat{\beta},\hat{\gamma},\hat{\delta}\right)$.
Then we have $(\alpha,\beta,\gamma-2m\alpha,\delta+2m\beta) = \left(\hat{\alpha},\hat{\beta},\hat{\gamma}-2m\hat{\alpha},\hat{\delta}+2m\hat{\beta}\right)$. By equating the entries it follows that $\alpha = \hat{\alpha}$, $\beta = \hat{\beta}$, $\gamma = \hat{\gamma}$ and $\delta = \hat{\delta}$. Hence ω_m is injective.
Surjectivity: Let $(\alpha',\beta',\gamma',\delta') \in C_m$ be arbitrary.
Consider $(\alpha,\beta,\gamma,\delta) = (\alpha',\beta',\gamma'+2m\alpha',\delta'-2m\beta')$. We will show that this lies in B_m. Observe $\alpha^2+\alpha\delta+\beta\gamma = \alpha'^2+\alpha'(\delta'-2m\beta')+\beta'(\gamma'+2m\alpha') = \alpha'^2+\alpha'\delta'+\beta'\gamma' = D$. By Lemma 3.6.8 we know this satisfies $0 < \gamma < 2\alpha$ and $0 < 2\beta < \delta$ due to how we partitioned using m. Thus the form lies in $Y_1 \backslash (X_1 \cap Y_1)$. Next, observe $\frac{\delta}{2\beta} = \frac{\delta'-2m\beta'}{2\beta'} = \frac{\gamma'}{2\beta'} - m$. Thus by Lemma 3.6.6 we have there exists a unique integer $p \in \left(-\frac{\delta}{2\beta}, 1-\frac{\delta}{2\beta}\right]$. This becomes $p \in \left(m-\frac{\delta'}{2\beta'}, m+1-\frac{\delta'}{2\beta'}\right]$. Recalling that $0 < \frac{\delta'}{2\beta'} < 1$ we have m is the unique integer in this interval and it follows that $p = m$. Consequently $(\alpha,\beta,\gamma,\delta)$ lies in B_m. Lastly, we observe

$$\begin{aligned}\omega_m(\alpha,\beta,\gamma,\delta) &= \omega_m(\alpha',\beta',\gamma'+2m\alpha',\delta'-2m\beta') \\ &= (\alpha',\beta',\gamma'+2m\alpha'-2m\alpha',\delta'-2m\beta'+2m\beta') \\ &= (\alpha',\beta',\gamma',\delta').\end{aligned}$$

Hence ω_m is a surjection and thus a bijection. □

Theorem 3.6.11.
The map

$$\begin{aligned} W : Y_1 \backslash (X_1 \cap Y_1) &\longrightarrow X_1 \backslash ((X_1 \cap Y_1) \cup \Theta) \\ (\alpha,\beta,\gamma,\delta) &\longmapsto \omega_m(\alpha,\beta,\gamma,\delta), \end{aligned}$$

where m is uniquely determined by $(\alpha,\beta,\gamma,\delta)$, is a bijection.

Proof.
Corollary 3.6.7 shows that $Y_1 \backslash (X_1 \cap Y_1)$ is a finite disjoint union thus m is uniquely determined by $(\alpha,\beta,\gamma,\delta)$. Corollary 3.6.9 shows that $X_1 \backslash ((X_1 \cap Y_1) \cup \Theta)$ is a finite disjoint union. By Lemma 3.6.10 the map $\omega_m : B_m \to C_m$ is a bijection and the disjoint unions imply $\omega_m(\alpha,\beta,\gamma,\delta) \neq \omega_{\hat{m}}\left(\hat{\alpha},\hat{\beta},\hat{\gamma},\hat{\delta}\right)$, thus W is injective. Since each ω_m is a bijection and $X_1 \backslash ((X_1 \cap Y_1) \cup \Theta)$ is a disjoint union it follows that W is surjective.
Hence W is a bijection. □

Corollary 3.6.12.
We have $P_1 = K + R_1$, where K is the cardinality of the set

$$\Theta = \left\{(\alpha, \beta, \gamma, \delta) \mid \alpha^2 + \alpha\delta + \beta\gamma = D, 0 < 2\alpha \leqslant \gamma, 0 < \delta \leqslant 2\beta, \gamma \equiv 0 \bmod 2\alpha\right\}.$$

Proof.
Recall that $P_1 = |I_{0,>}|$, $K = |\Theta|$ and $R_1 = |J_{0,>}|$. Apply Theorem 3.6.11 to observe

$$\begin{aligned} P_1 &= |X_1 \cap Y_1| + |\Theta| + |X_1 \setminus ((X_1 \cap Y_1) \cup \Theta)| \\ &= |X_1 \cap Y_1| + |\Theta| + |Y_1 \setminus (X_1 \cap Y_1)| \text{ (by Theorem 3.6.11)} \\ &= |\Theta| + |Y_1| \\ &= K + R_1. \end{aligned}$$

□

We now perform a similar investigation to determine the relationship between P_2 and S_1.

Definition 3.6.13.
Fix $D \in \mathbb{Z}_{>0}$. Recall from Definitions 3.4.7 and 3.4.19 that the sets X_2 and Y_2 are defined by:

$$X_2 = \left\{(\alpha, \beta, \gamma, \delta) \mid \alpha^2 + \alpha\delta + \beta\gamma = D, 0 < \alpha, 0 < \gamma, 0 \leqslant \delta < 2\beta\right\} \text{ and}$$
$$Y_2 = \left\{(\alpha, \beta, \gamma, \delta) \mid \alpha^2 + \alpha\delta + \beta\gamma = D, 0 < \beta, 0 \leqslant \delta, 0 < \gamma < 2\alpha\right\}.$$
$$\text{Let } \Theta' = \left\{(\alpha, \beta, \gamma, \delta) \mid \alpha^2 + \alpha\delta + \beta\gamma = D, 0 < \alpha, 0 < \gamma, 0 \leqslant \delta < 2\beta, \gamma \not\equiv 0 \bmod 2\alpha\right\}.$$

Let L denote the cardinality of the set Θ'.

Observation 3.6.14.
Recall from Corollaries 3.4.8 and 3.4.20 that X_2 and Y_2 are finite sets. Observe $\Theta' \subseteq X_2$ and thus is also a finite set.
Note that $X_2 \cap Y_2 = \{(\alpha, \beta, \gamma, \delta) \mid \alpha^2 + \alpha\delta + \beta\gamma = D, 0 \leqslant \delta < 2\beta, 0 < \gamma < 2\alpha\}$ and hence $\Theta' \cap (X_2 \cap Y_1) = \emptyset$.

We now give a description of the sets $X_2 \setminus (X_2 \cap Y_2)$ and $Y_2 \setminus (X_2 \cap Y_2)$:

$$X_2 \setminus (X_2 \cap Y_2) = \left\{(\alpha, \beta, \gamma, \delta) \mid \alpha^2 + \alpha\delta + \beta\gamma = D, 0 < 2\beta \leqslant \delta, 0 < \gamma < 2\alpha\right\}, \quad (3.17)$$
$$Y_2 \setminus (X_2 \cap Y_2) = \left\{(\alpha, \beta, \gamma, \delta) \mid \alpha^2 + \alpha\delta + \beta\gamma = D, 0 \leqslant \delta < 2\beta, 0 < 2\alpha \leqslant \gamma\right\}. \quad (3.18)$$

Observation 3.6.15.
We now use the set Θ' to partition $X_2 \setminus (X_2 \cap Y_2)$ as

$$X_2 \setminus (X_2 \cap Y_2) = \Theta' \cup (X_2 \setminus ((X_2 \cap Y_2) \cup \Theta')).$$

For clarity we have

$$X_2 \setminus ((X_2 \cap Y_2) \cup \Theta') = \{\ (\alpha, \beta, \gamma, \delta) \mid \alpha^2 + \alpha\delta + \beta\gamma = D, 0 \leqslant \delta < 2\beta, 0 < 2\alpha \leqslant \gamma,$$

$$\gamma \not\equiv 0 \bmod 2\alpha \,\}\,.$$

Our goal is to construct a bijection $W' : Y_2 \backslash (X_2 \cap Y_2) \longrightarrow X_2 \backslash ((X_2 \cap Y_2) \cup \Theta')$.

We will use the map ω_m redefined to the appropriate sets. As such it is important to note that Lemmas 3.6.4 and 3.6.5 still hold true.

We begin by examining the set $Y_2 \backslash (X_2 \cap Y_2)$.

Lemma 3.6.16.
For any form $(\alpha, \beta, \gamma, \delta) \in Y_2 \backslash (X_2 \cap Y_2)$ there exists a unique integer m such that

$$\omega_m (\alpha, \beta, \gamma, \delta) = (\alpha, \beta, \gamma - 2m\alpha, \delta + 2m\beta) = (\alpha', \beta', \gamma', \delta')$$

satisfies $0 \leqslant \delta' < 2\beta'$ and $0 < 2\alpha' \leqslant \gamma'$.

Proof.
Recall that forms in $Y_2 \backslash (X_2 \cap Y_2)$ satisfy $0 < 2\beta \leqslant \delta$ and $0 < \gamma < 2\alpha$. Clearly we have $\alpha' = \alpha > 0$ and $\beta' = \beta > 0$. In order to have $2\alpha' \leqslant \gamma'$ we required $m \leqslant \frac{\gamma}{2\alpha} - 1$. Notice that $0 \frac{\gamma}{2\alpha} < 1$ implies $m < 0$. Next, in order to have $0 \leqslant \delta' < 2\beta'$ we require $-\frac{\delta}{2\beta} \leqslant m < 1 - \frac{\delta}{2\beta}$. Thus we have $-\frac{\delta}{2\beta} \leqslant m < \min\left\{1 - \frac{\delta}{2\beta}, \frac{\gamma}{2\alpha} - 1\right\}$. We observe that $0 < \frac{\gamma}{2\alpha} < 1$ and $1 \leqslant \frac{\delta}{2\beta}$ imply $1 - \frac{\delta}{2\beta} < 0$ and $-1 < \frac{\gamma}{2\alpha} - 1$. Hence if $1 - \frac{\delta}{2\beta} \leqslant \frac{\gamma}{2\alpha} - 1$ then clearly there is a unique integer $m \in \left[-\frac{\delta}{2\beta}, 1 - \frac{\delta}{2\beta}\right)$. So suppose $\frac{\gamma}{2\alpha} - 1 < 1 - \frac{\delta}{2\beta}$, then $-1 < \min\left\{1 - \frac{\delta}{2\beta}, \frac{\gamma}{2\alpha} - 1\right\}$. Further, $-1 < 1 - \frac{\delta}{2\beta}$ implies $-\frac{\delta}{2\beta} < -1$ so we see that $m = -1$ is the unique integer such that $-\frac{\delta}{2\beta} \leqslant m < \min\left\{1 - \frac{\delta}{2\beta}, \frac{\gamma}{2\alpha} - 1\right\}$. □

Corollary 3.6.17.
The set $Y_2 \backslash (X_2 \cap Y_2) = \bigcup_{m \in \mathbb{Z}_{<0}} {B_m}'$ is a finite disjoint union, where

$${B_m}' = \left\{ (\alpha, \beta, \gamma, \delta) \in Y_2 \backslash (X_2 \cap Y_2) \;\middle|\; -\frac{\delta}{2\beta} \leqslant m < 1 - \frac{\delta}{2\beta} \right\}.$$

Proof.
By Lemma 3.6.16 for each $(\alpha, \beta, \gamma, \delta) \in Y_2 \backslash (X_2 \cap Y_2)$ there exists a unique integer $m \in \left[-\frac{\delta}{2\beta}, 1 - \frac{\delta}{2\beta}\right)$. We use this to partition into a union of sets ${B_m}'$. This is a disjoint union due to the uniqueness of m. By Corollary 3.4.20 we know the set Y_2 is finite and hence it follows that $Y_2 \backslash (X_2 \cap Y_2)$ is finite. □

We now examine $X_2 \backslash (X_2 \cap Y_2)$ in a similar manner.

Lemma 3.6.18.
For any form $(\alpha', \beta', \gamma', \delta') \in X_2 \backslash (X_2 \cap Y_2)$ such that $\gamma' \not\equiv 0 \bmod 2\alpha'$, there exists a unique integer n such that $\tau (\alpha', \beta', \gamma', \delta') = (\alpha', \beta', \gamma' + 2n\alpha', \delta' - 2n\beta') = (\alpha, \beta, \gamma, \delta)$ satisfies $0 < 2\beta \leqslant \delta$ and $0 < \gamma < 2\alpha$.

Proof.
Recall that $(\alpha', \beta', \gamma', \delta')$ satifies $0 \leqslant \delta' < 2\beta'$ and $0 < 2\alpha' \leqslant \gamma'$ so we clearly have $\beta = \beta' > 0$. Now note that in order to have $2\beta \leqslant \delta$ we require $n \leqslant \frac{\delta'}{2\beta'} - 1$. Similarly, in order to have $0 < \gamma < 2\alpha$ we need $-\frac{\gamma'}{2\alpha'} < n < 1 - \frac{\gamma'}{2\alpha'}$. Hence we have $-\frac{\gamma'}{2\alpha'} < n \leqslant \min\left\{1 - \frac{\gamma'}{2\alpha'}, \frac{\delta'}{2\beta'} - 1\right\}$. Observe that $0 \leqslant \frac{\delta'}{2\beta'} < 1$ implies $-1 \leqslant \frac{\delta'}{2\beta'} - 1 < 0$ and also observe $1 \leqslant \frac{\gamma'}{2\alpha'}$ implies $1 - \frac{\gamma'}{2\alpha'} \leqslant 0$.
Consequently if $1 - \frac{\gamma'}{2\alpha'} \leqslant -1$ then since $\gamma' \not\equiv 0 \bmod 2\alpha'$, $1 - \frac{\gamma'}{2\alpha'}$ cannot equal -1 and it follows that there is a unique integer n in the interval $\left(-\frac{\gamma'}{2\alpha'}, 1 - \frac{\gamma'}{2\alpha'}\right)$. Now suppose that $-1 < \min\left\{1 - \frac{\gamma'}{2\alpha'}, \frac{\delta'}{2\beta'} - 1\right\}$. In particular we see that $-\frac{\gamma'}{2\alpha'} < -1$ and hence $n = -1$ is the unique integer that works. □

Corollary 3.6.19.
The set $X_2 \backslash ((X_2 \cap Y_2) \cup \Theta') = \bigcup_{n \in \mathbb{Z}_{<0}} {C_n}'$ *is a finite disjoint union, where*

$$ {C_n}' = \left\{ (\alpha', \beta', \gamma', \delta') \in X_2 \backslash ((X_2 \cap Y_2) \cup \Theta') \,\middle|\, -\frac{\gamma'}{2\alpha'} < n < 1 - \frac{\gamma'}{2\alpha'} \right\}. $$

Proof.
By Corollary 3.4.8 and Observation 3.6.14 X_2 and Θ' are finite sets, thus the set $X_2 \backslash ((X_2 \cap Y_2) \cup \Theta')$ is finite.
We use Lemma 3.6.18 to partition the set into a disjoint union according to the unique integer n. □

Lemma 3.6.20.
The map

$$ {\omega_m}' : {B_m}' \longrightarrow {C_m}' $$
$$ {\omega_m}'(\alpha, \beta, \gamma, \delta) = (\alpha, \beta, \gamma - 2m\alpha, \delta + 2m\beta) $$

is a well-defined bijection.

Proof.
By Lemma 3.6.4 we observe ω'_m preserves D. By Lemma 3.6.5 we know $\omega'_m(\alpha, \beta, \gamma, \delta)$ satisfies $\gamma' \not\equiv 0 \bmod 2\alpha'$ and thus $\omega'_m(\alpha, \beta, \gamma, \delta) \notin \Theta'$. By Lemma 3.6.16 we know $\omega'_m(\alpha, \beta, \gamma, \delta)$ satisfies $0 \leqslant \delta' < 2\beta'$ and $0 < 2\alpha' \leqslant \gamma'$. So we see that $\omega'_m(\alpha, \beta, \gamma, \delta) \in X_2 \backslash ((X_2 \cap Y_2) \cup \Theta')$.
Now suppose there exist $(\alpha, \beta, \gamma, \delta)$, $\left(\hat{\alpha}, \hat{\beta}, \hat{\gamma}, \hat{\delta}\right) \in B'_m$ such that $\omega'_m(\alpha, \beta, \gamma, \delta) \in C'_{n_1}$ and $\omega'_m\left(\hat{\alpha}, \hat{\beta}, \hat{\gamma}, \hat{\delta}\right) \in C'_{n_2}$ for some integers n_1 and n_2. Then $n_1, n_2 \in \left(-\frac{\gamma'}{2\alpha'}, 1 - \frac{\gamma'}{2\alpha'}\right)$. This contains a unique integer and hence $n_1 = n_2$. Therefore $\omega'_m : B'_m \longrightarrow C'_n$.
Now in C'_n we know $-\frac{\gamma'}{2\alpha'} < n < 1 - \frac{\gamma'}{2\alpha'}$ and this rearranges to yield $m - \frac{\gamma}{2\alpha} < n < m + 1 - \frac{\gamma}{2\alpha}$. Since $0 < \frac{\gamma}{2\alpha} < 1$ it follows that $n = m$. Hence $\omega'_m : B'_m \longrightarrow C'_m$ is well-defined.

Injectivity: This follows immediately by assuming $\omega'_m(\alpha,\beta,\gamma,\delta) = \omega'_m\left(\hat{\alpha},\hat{\beta},\hat{\gamma},\hat{\delta}\right)$ and equating the entries.
Surjectivity: Let $(\alpha',\beta',\gamma',\delta') \in C'_m$ be arbitrary. Consider $f = (\alpha',\beta',\gamma'+2m\alpha',\delta'-2m\beta') = (\alpha,\beta,\gamma,\delta)$. We will show this lies in B'_m.
We have $\alpha^2+\alpha\delta+\beta\gamma = \alpha'^2+\alpha'(\delta'-2m\beta')+\beta'(\gamma'+2m\alpha') = \alpha'^2+\alpha'\delta'+\beta'\gamma' = D$. By Lemma 3.6.18 we know it satisfies $0 < 2\beta \leqslant \delta$ and $0 < \gamma < 2\alpha$ and thus it lies in $X_2\backslash(X_2\cap Y_2)$. Now notice that $\frac{\delta}{2\beta} = \frac{\delta'}{2\beta'} - m$ and by Lemma 3.6.16 there exists a unique integer $p \in \left[-\frac{\delta}{2\beta}, 1-\frac{\delta}{2\beta}\right)$, that is $m - \frac{\delta'}{2\beta'} \leqslant p < m+1-\frac{\delta'}{2\beta'}$. Further, $0 \leqslant \frac{\delta'}{2\beta'} < 1$ implies m is the unique integer in the interval $\left[m-\frac{\delta'}{2\beta'}, 1-\frac{\delta'}{2\beta'}\right)$ and hence $p = m$. Therefore $(\alpha,\beta,\gamma,\delta) \in B'_m$. It is straightforward to verify ${\omega_m}'(f) = (\alpha',\beta',\gamma',\delta')$. Thus ω'_m is surjective and hence a bijection. □

Theorem 3.6.21.
The map

$$\begin{aligned} W' : Y_2\backslash(X_2\cap Y_2) &\longrightarrow X_2\backslash((X_2\cap Y_2)\cup\Theta') \text{ given by} \\ W'(\alpha,\beta,\gamma,\delta) &\longmapsto \omega'_m(\alpha,\beta,\gamma,\delta), \end{aligned}$$

where $(\alpha,\beta,\gamma,\delta)$ uniquely determines m, is a bijection.

Proof.
Corollary 3.6.17 shows we may write $Y_2\backslash(X_2\cap Y_2)$ as a finite disjoint union of sets B'_m. By Lemma 3.6.20 the map $\omega'_m : B'_m \longrightarrow C'_m$ is a bijection for each m. Corollary 3.6.19 shows that $X_2\backslash((X_2\cap Y_2)\cup\Theta')$ is a finite disjoint union of the sets C'_m. The disjoint union implies $\omega'_m(\alpha,\beta,\gamma,\delta) \neq \omega_{\hat{m}}{}'\left(\hat{\alpha},\hat{\beta},\hat{\gamma},\hat{\delta}\right)$ and thus W' is injective.
Since each ω'_m is a bijection and $X_2\backslash((X_2\cap Y_2)\cup\Theta')$ is a disjoint union of the sets C'_m, it follows that W' is surjective.
Hence W' is a bijection. □

Corollary 3.6.22.
$P_2 = L + S_1$.

Proof.
Recall $P_2 = |X_2|$, $L = |\Theta'|$ and $S_1 = |Y_2|$. Using Theorem 3.6.21 we have

$$\begin{aligned} P_2 &= |X_2| \\ &= |X_2\cap Y_2| + |\Theta'| + |X_2\backslash((X_2\cap Y_2)\cup\Theta')| \\ &= |X_2\cap Y_2| + |\Theta'| + |Y_2\backslash(X_2\cap Y_2)| \text{ by Theorem 3.6.21} \\ &= |Y_2| + |\Theta'| \\ &= S_1 + L. \end{aligned}$$

□

Notes on Section 3.6

The statement of our results in this section differ slightly from those of Kronecker. Kronecker states the following two results without proof: $P_1 = K + R_1$ and $Q_1 = L + S_1$. This is due to our proof of $P_1 + P_2 = Q_1 + Q_2 = |X_1| + |X_2|$, whereas Kronecker implied he went further when he stated $P_2 = Q_1$ and $Q_2 = P_1$.

3.7 The Relationships between $\overline{P_1}$ and $\overline{R_1}$, and also between $\overline{P_2}$ and $\overline{S_1}$

Having derived the relations $P_1 = K + R_1$ and $Q_1 = L + S_1$ in Section 3.6 we begin this section by investigating whether similar results hold for the quantities $\overline{P_1}$, $\overline{P_2}$, $\overline{R_1}$ and $\overline{S_1}$. Throughout this section we assume $D \in \mathbb{Z}_{>0}$ and is fixed.

Theorem 3.7.1.
$\overline{P_1} = \overline{R_1}$.

Proof.
We will show that the restriction map,
$W\Big|_{\overline{Y_1}\setminus\left(\overline{X_1}\cap\overline{Y_1}\right)} : \overline{Y_1}\setminus\left(\overline{X_1}\cap\overline{Y_1}\right) \longrightarrow \overline{X_1}\setminus\left(\overline{X_1}\cap\overline{Y_1}\right)$ is well-defined and is a bijection.
Recall $\overline{X_1} \subseteq X_1$ and $\overline{Y_1} \subseteq Y_1$ and consider the set $\overline{Y_1}\setminus\left(\overline{X_1}\cap\overline{Y_1}\right) \subseteq Y_1\setminus(X_1\cap Y_1)$. Applying Theorem 3.6.11 we see

$$W\left(\overline{Y_1}\setminus\left(\overline{X_1}\cap\overline{Y_1}\right)\right) \subseteq X_1\setminus((X_1\cap Y_1)\cup\Theta).$$

Since the map W is defined in terms of the maps ω_m we first show that for any integer m the map ω_m satisfies $\gamma' \equiv \gamma \bmod 2$ and $\delta' \equiv \delta \bmod 2$. This follows easily as $\gamma' = \gamma - 2m\alpha \equiv \gamma \bmod 2$ and $\delta' = \delta + 2m\beta \equiv \delta \bmod 2$. Hence the restriction map maps into $\overline{X_1}$. Further, we have $((X_1\cap Y_1)\cup\Theta)\cap\overline{X_1} = \overline{X_1}\cap\overline{Y_1}$. This follows because any element in Θ satisfies $\gamma \equiv 0 \bmod 2\alpha$ and thus $\gamma \equiv 0 \bmod 2$, so $\Theta\cap\overline{X_1} = \emptyset$.
Hence we see that the restriction map maps into $\overline{X_1}\setminus\left(\overline{X_1}\cap\overline{Y_1}\right)$.
Note that injectivity is inherited from W and so it remains to show surjectivity.
Let $(\alpha',\beta',\gamma',\delta') \in \overline{X_1}\setminus\left(\overline{X_1}\cap\overline{Y_1}\right)$. By Theorem 3.6.11 and Lemma 3.6.10 this lies in some set C_m and under the inverse of the map ω_m maps back to a unique $(\alpha,\beta,\gamma,\delta) \in B_m$. But ω_m preserves "γ" and "δ" mod. 2 and hence $\gamma \equiv 1 \bmod 2$ and $\delta \equiv 0 \bmod 2$. Thus $(\alpha,\beta,\gamma,\delta)$ lies in $B_m \cap \overline{Y_1}\setminus\left(\overline{X_1}\cap\overline{Y_1}\right)$. Hence the restriction map is surjective and so it is a bijection.
It follows then that

$$\begin{aligned}\left|\overline{X_1}\right| &= \left|\overline{X_1}\cap\overline{Y_1}\right| + \left|\overline{X_1}\setminus\left(\overline{X_1}\cap\overline{Y_1}\right)\right| \\ &= \left|\overline{X_1}\cap\overline{Y_1}\right| + \left|\overline{Y_1}\setminus\left(\overline{X_1}\cap\overline{Y_1}\right)\right| \\ &= \left|\overline{Y_1}\right|.\end{aligned}$$

So we have $\overline{P_1} = \left|\overline{X_1}\right| = \left|\overline{Y_1}\right| = \overline{R_1}$. □

Theorem 3.7.2.
$\overline{P_2} = \overline{S_1}$.

Proof.
We will show that the restriction map,
$W'\Big|_{\overline{Y_2}\setminus\left(\overline{X_2}\cap\overline{Y_2}\right)} : \overline{Y_2}\setminus\left(\overline{X_2}\cap\overline{Y_2}\right) \longrightarrow \overline{X_2}\setminus\left(\overline{X_2}\cap\overline{Y_2}\right)$ is well-defined and is a bijection.
Recall $\overline{X_2} \subseteq X_2$ and $\overline{Y_2} \subseteq Y_2$ and consider the set $\overline{Y_2}\setminus\left(\overline{X_2}\cap\overline{Y_2}\right) \subseteq Y_2\setminus(X_2\cap Y_2)$. Applying Theorem 3.6.21 we see

$$W'\left(\overline{Y_2}\setminus\left(\overline{X_2}\cap\overline{Y_2}\right)\right) \subseteq X_2\setminus\left((X_2\cap Y_2)\cup\Theta'\right).$$

Since the map W' is defined in terms of the maps ω'_m, we note that as in the proof of Theorem 3.7.1 we have $\gamma' \equiv \gamma \bmod 2$ and $\delta' \equiv \delta \bmod 2$. Hence the restriction map maps into $\overline{X_2}$. Further, we have $\left((X_2\cap Y_2)\cup\Theta'\right)\cap\overline{X_2} = \overline{X_2}\cap\overline{Y_2}$. This follows because any element in Θ' satisfies $\gamma \equiv 0 \bmod 2\alpha$ and so $\gamma \equiv 0 \bmod 2$. Therefore $\Theta'\cap\overline{X_2} = \emptyset$.
Hence we see that the restriction map maps into $\overline{X_2}\setminus\left(\overline{X_2}\cap\overline{Y_2}\right)$.
Note that injectivity is inherited directly from the map W' and so it remains to show surjectivity.
Let $(\alpha',\beta',\gamma',\delta') \in \overline{X_2}\setminus\left(\overline{X_2}\cap\overline{Y_2}\right)$ be arbitrary. By Theorem 3.6.21 and Lemma 3.6.20 this lies in some set C'_m and under the inverse of the map ω'_m, maps back to a unique $(\alpha,\beta,\gamma,\delta)$ in B'_m. But ω'_m preserves "γ" and "δ" mod. 2 and so $\gamma \equiv 1 \bmod 2$ and $\delta \equiv 0 \bmod 2$. Thus $(\alpha,\beta,\gamma,\delta)$ lies in $B'_m \cap \overline{Y_2}\setminus\left(\overline{X_2}\cap\overline{Y_2}\right)$. Hence the restriction map is surjective and so it is a bijection. It then follows that

$$\begin{aligned}\left|\overline{X_2}\right| &= \left|\overline{X_2}\cap\overline{Y_2}\right| + \left|\overline{X_2}\setminus\left(\overline{X_2}\cap\overline{Y_2}\right)\right| \\ &= \left|\overline{X_2}\cap\overline{Y_2}\right| + \left|\overline{Y_2}\setminus\left(\overline{X_2}\cap\overline{Y_2}\right)\right| \\ &= \left|\overline{Y_2}\right|.\end{aligned}$$

So we have $\overline{P_2} = \left|\overline{X_2}\right| = \left|\overline{Y_2}\right| = \overline{S_1}$. □

We now use the results developed in Sections 3.6 and 3.7 to simplify our class number equations.

Applying $P_1 = K + R_1$ and $P_2 = L + S_1$ in Equation 3.14 we get

$$\begin{aligned}\mathrm{Cl}_c(D) &= m+n+2\left(P_0+Q_0-R_0-S_0+2\left(P_1+P_2-R_1-S_1\right)\right) \\ &= m+n+2\left(P_0+Q_0-R_0-S_0+2\left(K+R_1+L-S_1-R_1-S_1\right)\right) \\ &= m+n+2\left(\left[2K+P_0-R_0\right]+\left[2L+Q_0-S_0\right]\right). \qquad (3.19)\end{aligned}$$

Similarly, applying $\overline{P_1} = \overline{R_1}$ and $\overline{P_2} = \overline{S_1}$ into the equation found in Lemma 3.5.10 we get

$$\begin{aligned}\overline{\mathrm{Cl}}_c(D) &= 3\left(\overline{P_0}+\overline{Q_0}-\overline{R_0}-\overline{S_0}+2\left(\overline{P_1}+\overline{P_2}-\overline{R_1}-\overline{S_1}\right)\right) \\ &= 3\left(\overline{P_0}+\overline{Q_0}-\overline{R_0}-\overline{S_0}\right). \qquad (3.20)\end{aligned}$$

Chapter 4 Enumerating Our Sets Via Divisors of D

> "It's not enough that we do our best; sometimes we have to do what's required."
> - Sir Winston Churchill

In this chapter we develop ways of expressing the cardinalities K, L, P_0, Q_0, R_0 and S_0 in terms of divisors of the determinant $D \in \mathbb{Z}_{>0}$.

4.1 Using Divisors of D to count $K + L$.

In this section we will use divisors of the determinant D to derive an expression for value of $K + L$.

We begin by recalling the definitions of the sets Θ and Θ' from Lemmas 3.6.1 and 3.6.13.

$$\Theta = \left\{(\alpha, \beta, \gamma, \delta) \mid \alpha^2 + \alpha\delta + \beta\gamma = D, 0 < \alpha, 0 < \gamma, 0 < \delta \leqslant 2\beta, \gamma \equiv 0 \bmod 2\alpha\right\},$$
$$\Theta' = \left\{(\alpha, \beta, \gamma, \delta) \mid \alpha^2 + \alpha\delta + \beta\gamma = D, 0 < \alpha, 0 < \gamma, 0 \leqslant \delta < 2\beta, \gamma \equiv 0 \bmod 2\alpha\right\}.$$

In both Θ and Θ' we have $\gamma \equiv 0 \bmod 2\alpha$ and $0 < \gamma$. Therefore we may write $\gamma = 2m\alpha$ for some $m \in \mathbb{Z}_{>0}$ as $0 < \alpha$. We now define two more sets, let

$$\Theta_1 = \{(\partial, \mathrm{d}, m, \beta) \mid \partial\mathrm{d} = D, 0 < \partial < \mathrm{d}, 2m\beta < \mathrm{d} - \partial \leqslant 2(m+1)\beta,\ m, \beta \in \mathbb{N}_{>0}\},$$
$$\Theta_1' = \{(\partial, \mathrm{d}, m, \beta) \mid \partial\mathrm{d} = D, 0 < \partial < \mathrm{d}, 2m\beta \leqslant \mathrm{d} - \partial < 2(m+1)\beta,\ m, \beta \in \mathbb{N}_{>0}\}.$$

Lemma 4.1.1.
The map

$$\tau : \Theta \longrightarrow \Theta_1$$
$$(\alpha, \beta, \gamma, \delta) \longmapsto (\partial, \mathrm{d}, m, \beta),$$

where $\gamma = 2m\alpha$, is a well-defined bijection. From this it follows that $|\Theta_1| = |\Theta| = K$.

Proof.
Well-defined: For each $(\alpha, \beta, \gamma, \delta) \in \Theta$ there exists a unique $m \in \mathbb{N}_{>0}$ such that $\gamma = 2m\alpha$. Then $0 < \alpha$ and $0 < \delta \leqslant 2\beta$ implies $0 < \partial = \alpha < \alpha + \delta \leqslant \alpha + \delta + 2m\beta = \mathrm{d}$. Now notice that $\mathrm{d} - \partial - 2m\beta = \delta$, thus $0 < \delta \leqslant 2\beta$ implies $0 < \mathrm{d} - \partial - 2m\beta \leqslant 2\beta$ and so $2m\beta < \mathrm{d} - \partial \leqslant 2(m+1)\beta$. Hence τ maps into Θ_1.
Injectivity: Suppose $\tau(\alpha, \beta, \gamma, \delta) = \tau(\alpha', \beta', \gamma', \delta')$, then
$(\alpha, \alpha + \delta + 2m\beta, m, \beta) = (\alpha', \alpha' + \delta' + 2m'\beta', m', \beta')$. Equating the entries yields $\alpha = \alpha'$, $\beta = \beta'$, $m = m'$ and $\delta = \delta'$. Therefore τ is injective.
Surjectivity: Let $g = (\partial, \mathrm{d}, m, \beta) \in \Theta_1$ be arbitrary.
Consider $f = (\partial, \beta, 2m\partial, \mathrm{d} - \partial - 2m\beta) = (\alpha, \beta, \gamma, \delta)$, we will show this lies in Θ and

$\tau(f) = g$. We have $0 < \partial = \alpha$ and $\gamma = 2m\partial$ as $\partial > 0$ and $m \in \mathbb{N}_{>0}$. Further, $\gamma \equiv 0 \bmod 2\alpha$. Next, $2m\beta < \mathrm{d} - \partial \leqslant 2(m+1)\beta$ implies $0 < \mathrm{d} - \partial - 2m\beta \leqslant 2(m+1)\beta - 2m\beta = 2\beta$. Therefore $0 < \delta \leqslant 2\beta$. Finally we have

$$\begin{aligned} \alpha^2 + \alpha\delta + \beta\gamma &= \partial^2 + \partial(\mathrm{d} - \partial - 2m\beta) + 2m\partial\beta \\ &= \partial\mathrm{d} \\ &= D. \end{aligned}$$

Hence f lies in Θ and we note that $\gamma = 2m\partial = 2m\alpha$. Then we see
$\tau(f) = (\partial, \partial + (\mathrm{d} - \partial - 2m\beta) + 2m\beta, m, \beta) = (\partial, \mathrm{d}, m, \beta)$. Therefore τ is surjective and hence τ is a bijection.
It follows that $|\Theta_1| = |\Theta| = K$. □

Lemma 4.1.2.
The map

$$\begin{aligned} \tau' : \Theta' &\longrightarrow \Theta'_1 \\ (\alpha, \beta, \gamma, \delta) &\longmapsto (\alpha, \alpha + \delta + 2m\beta, m, \beta) = (\partial, \mathrm{d}, m, \beta), \end{aligned}$$

where $\gamma = 2m\alpha$, is a well-defined bijection.
It follows that $|\Theta'_1| = |\Theta'| = L$.

Proof.
Well-defined: For each $(\alpha, \beta, \gamma, \delta) \in \Theta'$ there exists a unique $m \in \mathbb{N}_{>0}$ such that $\gamma = 2m\alpha$. Then $0 < \alpha$ implies $\partial = \alpha > 0$, further $0 \leqslant \delta, 2\beta$ then implies $0 < \partial = \alpha \leqslant \alpha + \delta < \alpha + \delta + 2m\beta = \mathrm{d}$ as $m \in \mathbb{N}_{>0}$ and $\beta > 0$. Next observe $\delta = \mathrm{d} - \partial - 2m\beta$ and so $0 \leqslant \delta < 2\beta$ yields $0 \leqslant \mathrm{d} - \partial - 2m\beta < 2\beta$. Hence $2m\beta \leqslant \mathrm{d} - \partial < 2(m+1)\beta$. It follows that τ' maps into Θ'_1.
Injectivity: Suppose $\tau'(\alpha, \beta, \gamma, \delta) = \tau'(\alpha', \beta', \gamma', \delta')$, then we have
$(\alpha, \alpha + \delta + 2m\beta, m, \beta) = (\alpha', \alpha' + \delta' + 2m'\beta', m', \beta')$. Equating the entries yields τ' is injective.
Surjectivity: Let $g = (\partial, \mathrm{d}, m\beta) \in \Theta'_1$ be arbitrary.
Consider $f = (\partial, \beta, 2m\partial, \mathrm{d} - \partial - 2m\beta) = (\alpha, \beta, \gamma, \delta)$, we will show this lies in Θ' and $\tau'(f) = g$. We have $\alpha = \partial > 0$ and $\gamma = 2m\partial > 0$ as $m \in \mathbb{N}_{>0}$. Further it is clear that $\gamma \equiv 0 \bmod 2\alpha$. Next the inequality $2m\beta \leqslant \mathrm{d} - \partial < 2(m+1)\beta$ implies $0 \leqslant \mathrm{d} - \partial - 2m\beta < 2\beta$, that is, $0 \leqslant \delta < 2\beta$. Lastly observe

$$\begin{aligned} \alpha^2 + \alpha\delta + \beta\gamma &= \partial^2 + \partial(\mathrm{d} - \partial - 2m\beta) + 2m\partial\beta \\ &= \partial\mathrm{d} \\ &= D. \end{aligned}$$

Hence f lies in Θ'. We note that f satisfies $\gamma = 2m\partial = 2m\alpha$.
Then $\tau'(f) = (\partial, \partial + \mathrm{d} - \partial - 2m\beta, m, \beta) = (\partial, \mathrm{d}, m, \beta)$. Therefore τ' is surjective and thus τ' is a bijection.
It follows that $|\Theta'_1| = |\Theta'| = L$. □

We now place conditions on β in the sets Θ_1 and Θ'_1.

Lemma 4.1.3.
Let $(\partial, \mathrm{d}, m, \beta) \in \Theta_1$. *If* $\mathrm{d} - \partial \equiv 1 \bmod 2$. *then we have* $1 \leqslant \beta \leqslant \frac{1}{2}(\mathrm{d} - \partial - 1)$. *Otherwise we have* $1 \leqslant \beta \leqslant \frac{1}{2}(\mathrm{d} - \partial) - 1$.

Proof.
Any form $(\partial, \mathrm{d}, m, \beta) \in \Theta_1$ must satisfy $2m\beta < \mathrm{d} - \partial \leqslant 2(m+1)\beta$. First we assume $\mathrm{d} - \partial$ is odd, then it follows that $2\beta + 1 \leqslant 2m\beta + 1 \leqslant \mathrm{d} - \partial$. In turn this implies $2\beta \leqslant \mathrm{d} - \partial - 1$, that is $\beta \leqslant \frac{1}{2}(\mathrm{d} - \partial - 1)$.
Now assume $\mathrm{d} - \partial$ is even, then it follows that $2m\beta + 2 \leqslant \mathrm{d} - \partial$ thus $m \in \mathbb{N}_{>0}$ implies $2\beta + 2 \leqslant 2m\beta + 2 \leqslant \mathrm{d} - \partial$. Hence $2\beta \leqslant \mathrm{d} - \partial - 2$ and so $\beta \leqslant \frac{1}{2}(\mathrm{d} - \partial) - 1$. □

Lemma 4.1.4.
Let $(\partial, \mathrm{d}, m, \beta) \in \Theta_1'$, *then* $1 \leqslant \beta \leqslant \frac{1}{2}(\mathrm{d} - \partial - 1)$ *if* $\mathrm{d} - \partial \equiv 1 \bmod 2$. *Otherwise,* $1 \leqslant \beta \leqslant \frac{1}{2}(\mathrm{d} - \partial)$.

Proof.
Any form $(\partial, \mathrm{d}, m, \beta) \in \Theta_1'$ must satisfy $2m\beta \leqslant \mathrm{d} - \partial < 2(m+1)\beta$. First we assume $\mathrm{d} - \partial$ is odd, then it follows that $2\beta + 1 \leqslant 2m\beta + 1 \leqslant \mathrm{d} - \partial$, thus $\beta \leqslant \frac{1}{2}(\mathrm{d} - \partial - 1)$.
Now assume $\mathrm{d} - \partial$ is even. Then $2\beta \leqslant 2m\beta \leqslant \mathrm{d} - \partial$, which yields $\beta \leqslant \frac{1}{2}(\mathrm{d} - \partial)$. □

Lemma 4.1.5.
Consider the set Θ_1. *If* $\mathrm{d} - \partial \equiv 1 \bmod 2$ *then* $\beta \in \mathbb{Z} \cap \left[1, \frac{1}{2}(\mathrm{d} - \partial - 1)\right]$. *Otherwise,* $\beta \in \mathbb{Z} \cap \left[1, \frac{1}{2}(\mathrm{d} - \partial) - 1\right]$. *Further,* β *may take any one of these values.*

Proof.
Recall forms in Θ_1 satisfy $0 < \partial < \mathrm{d}$ and $2m\beta < \mathrm{d} - \partial \leqslant 2(m+1)\beta$. Observe for any integer $\beta > 0$ we have

$$\bigcup_{m \in \mathbb{N}_{>0}} (2m\beta, 2(m+1)\beta] = \mathbb{R}_{>2\beta},$$

where this is clearly a disjoint union.
Since $0 < \mathrm{d} - \partial$ it follows that there exists a unique $m \in \mathbb{N}_{>0}$ such that $\mathrm{d} - \partial \in (2m\beta, 2(m+1)\beta]$, unless $\mathrm{d} - \partial \leqslant 2\beta$. However, Lemma 4.1.3 shows $\beta \leqslant \frac{1}{2}(\mathrm{d} - \partial - 1)$ if $\mathrm{d} - \partial \equiv 1 \bmod 2$ or $\beta \leqslant \frac{1}{2}(\mathrm{d} - \partial) - 1$ if $\mathrm{d} - \partial \equiv 0 \bmod 2$. Hence $2\beta < 2\beta + 1 \leqslant \mathrm{d} - \partial$ in the first case, while in the second case $2\beta < 2\beta + 2 \leqslant \mathrm{d} - \partial$. Thus such a unique m always exists for any d, ∂ and β, where $0 < \partial < \mathrm{d}$, $\partial\mathrm{d} = D$ and either $\beta \in \mathbb{Z} \cap \left[1, \frac{1}{2}(\mathrm{d} - \partial - 1)\right]$ if $\mathrm{d} - \partial \equiv 1 \bmod 2$ or $\beta \in \mathbb{Z} \cap \left[1, \frac{1}{2}(\mathrm{d} - \partial) - 1\right]$ if $\mathrm{d} - \partial \equiv 0 \bmod 2$. □

Corollary 4.1.6.

$$K = |\Theta_1| = \sum_{\substack{0<\partial<\mathrm{d} \\ \partial\mathrm{d}=D \\ \mathrm{d}-\partial \equiv 1 \bmod 2}} \frac{1}{2}(\mathrm{d} - \partial - 1) + \sum_{\substack{0<\partial<\mathrm{d} \\ \partial\mathrm{d}=D \\ \mathrm{d}-\partial \equiv 0 \bmod 2}} \left(\frac{1}{2}(\mathrm{d} - \partial) - 1\right).$$

Proof.
By Lemma 4.1.1 we have $K = |\Theta| = |\Theta_1|$. By Lemma 4.1.5 we know that for a fixed pair d, ∂ where $0 < \partial < \mathrm{d}$ and $\partial \mathrm{d} = D$, there exists a unique $m \in \mathbb{N}_{>0}$ for each β. Thus for fixed ∂, d we may split the elements in Θ_1 with those fixed ∂ and d values according to whether $\mathrm{d} - \partial \equiv 1 \bmod 2$ or not. Lemma 4.1.5 implies for each fixed pair ∂, d with $\mathrm{d} - \partial \equiv 1 \bmod 2$ there are $\frac{1}{2}(\mathrm{d} - \partial - 1)$ forms in Θ_1 and for each fixed pair ∂, d with $\mathrm{d} - \partial \equiv 0 \bmod 2$ there are $\frac{1}{2}(\mathrm{d} - \partial) - 1$ forms in Θ_1. Summing over all ∂, d such that $0 < \partial < \mathrm{d}$ and $\partial \mathrm{d} = D$ then yields:

$$K = \sum_{\substack{0<\partial<\mathrm{d} \\ \partial\mathrm{d}=D \\ \mathrm{d}-\partial\equiv 1 \bmod 2}} \frac{1}{2}(\mathrm{d} - \partial - 1) + \sum_{\substack{0<\partial<\mathrm{d} \\ \partial\mathrm{d}=D \\ \mathrm{d}-\partial\equiv 0 \bmod 2}} \left(\frac{1}{2}(\mathrm{d} - \partial) - 1\right).$$

□

Lemma 4.1.7.
Consider the set Θ_1'. If $\mathrm{d} - \partial \equiv 1 \bmod 2$ then $\beta \in \mathbb{Z} \cap \left[1, \frac{1}{2}(\mathrm{d} - \partial - 1)\right]$. Otherwise $\beta \in \mathbb{Z} \cap \left[1, \frac{1}{2}(\mathrm{d} - \partial)\right]$. Further, β may take any one of these values.

Proof.
Recall that forms in Θ_1' satisfy $0 < \partial < \mathrm{d}$ and $2m\beta \leqslant \mathrm{d} - \partial < 2(m+1)\beta$. Observe that for any integer $\beta > 0$ we have

$$\bigcup_{m \in \mathbb{N}_{>0}} [2m\beta, 2(m+1)\beta) = \mathbb{R}_{\geqslant 2\beta}.$$

Since $0 < \mathrm{d} - \partial$ it follows that there exists a unique $m \in \mathbb{N}_{>0}$ such that $\mathrm{d} - \partial \in [2m\beta, 2(m+1)\beta)$ unless $\mathrm{d} - \partial < 2\beta$. However, Lemma 4.1.4 shows regardless of whether $\mathrm{d} - \partial$ is odd or even, that $2\beta \leqslant \mathrm{d} - \partial$. Hence such a unique $m \in \mathbb{N}_{>0}$ always exists for any d, ∂ and β, where $0 < \partial < \mathrm{d}$, $\partial \mathrm{d} = D$ and either $\beta \in \mathbb{Z} \cap \left[1, \frac{1}{2}(\mathrm{d} - \partial - 1)\right]$ if $\mathrm{d} - \partial \equiv 1 \bmod 2$ or $\beta \in \mathbb{Z} \cap \left[1, \frac{1}{2}(\mathrm{d} - \partial)\right]$ if $\mathrm{d} - \partial \equiv 0 \bmod 2$. □

Corollary 4.1.8.

$$L = |\Theta_1'| = \sum_{\substack{0<\partial<\mathrm{d} \\ \partial\mathrm{d}=D \\ \mathrm{d}-\partial\equiv 1 \bmod 2}} \frac{1}{2}(\mathrm{d} - \partial - 1) + \sum_{\substack{0<\partial<\mathrm{d} \\ \partial\mathrm{d}=D \\ \mathrm{d}-\partial\equiv 0 \bmod 2}} \frac{1}{2}(\mathrm{d} - \partial).$$

Proof.
By Lemma 4.1.2 we have $L = |\Theta'| = |\Theta_1'|$. By Lemma 4.1.7 we know that for a fixed pair ∂, d where $0 < \partial < \mathrm{d}$ and $\partial \mathrm{d} = D$, there exists a unique $m \in \mathbb{N}_{>0}$ for each β. Thus for fixed ∂, d we may split the elements in Θ_1' with those ∂ and d values according to whether $\mathrm{d} - \partial \equiv 1 \bmod 2$ or not. Lemma 4.1.7 implies that for each fixed pair d, ∂ with $\mathrm{d} - \partial \equiv 1 \bmod 2$ there are $\frac{1}{2}(\mathrm{d} - \partial - 1)$ forms in Θ_1' and for each fixed pair d, ∂ with $\mathrm{d} - \partial \equiv 0 \bmod 2$ there are $\frac{1}{2}(\mathrm{d} - \partial)$ forms in Θ_1'. Summing over all d, ∂ such that $0 < \partial < \mathrm{d}$ and $\partial \mathrm{d} = D$ then yields:

$$L = \sum_{\substack{0<\partial<\mathrm{d} \\ \partial\mathrm{d}=D \\ \mathrm{d}-\partial\equiv 1 \bmod 2}} \frac{1}{2}(\mathrm{d} - \partial - 1) + \sum_{\substack{0<\partial<\mathrm{d} \\ \partial\mathrm{d}=D \\ \mathrm{d}-\partial\equiv 0 \bmod 2}} \frac{1}{2}(\mathrm{d} - \partial).$$

□

Theorem 4.1.9.
$K + L = \sum_{\substack{\partial \mathrm{d} = D \\ 0 < \partial < \mathrm{d}}} (\mathrm{d} - \partial - 1).$

Proof.
Note that $\frac{1}{2}(\mathrm{d} - \partial) = \left(\frac{1}{2}(\mathrm{d} - \partial) - 1\right) + 1$. Applying Corollaries 4.1.6 and 4.1.8 we see:

$$\begin{aligned}
K + L = & \sum_{\substack{0<\partial<\mathrm{d} \\ \partial \mathrm{d} = D \\ \mathrm{d}-\partial \equiv 1 \bmod 2}} \frac{1}{2}(\mathrm{d} - \partial - 1) + \sum_{\substack{0<\partial<\mathrm{d} \\ \partial \mathrm{d} = D \\ \mathrm{d}-\partial \equiv 0 \bmod 2}} \left(\frac{1}{2}(\mathrm{d} - \partial) - 1\right) + \\
& \sum_{\substack{0<\partial<\mathrm{d} \\ \partial \mathrm{d} = D \\ \mathrm{d}-\partial \equiv 1 \bmod 2}} \frac{1}{2}(\mathrm{d} - \partial - 1) + \sum_{\substack{0<\partial<\mathrm{d} \\ \partial \mathrm{d} = D \\ \mathrm{d}-\partial \equiv 0 \bmod 2}} \frac{1}{2}(\mathrm{d} - \partial) \\
= & \sum_{\substack{0<\partial<\mathrm{d} \\ \partial \mathrm{d} = D \\ \mathrm{d}-\partial \equiv 1 \bmod 2}} \frac{1}{2}(\mathrm{d} - \partial - 1) + \sum_{\substack{0<\partial<\mathrm{d} \\ \partial \mathrm{d} = D \\ \mathrm{d}-\partial \equiv 0 \bmod 2}} \left(\frac{1}{2}(\mathrm{d} - \partial) - 1\right) + \\
& \sum_{\substack{0<\partial<\mathrm{d} \\ \partial \mathrm{d} = D \\ \mathrm{d}-\partial \equiv 1 \bmod 2}} \frac{1}{2}(\mathrm{d} - \partial - 1) + \sum_{\substack{0<\partial<\mathrm{d} \\ \partial \mathrm{d} = D \\ \mathrm{d}-\partial \equiv 0 \bmod 2}} \left(\frac{1}{2}(\mathrm{d} - \partial) - 1\right) + \sum_{\substack{0<\partial<\mathrm{d} \\ \partial \mathrm{d} = D \\ \mathrm{d}-\partial \equiv 0 \bmod 2}} 1 \\
= & \sum_{\substack{0<\partial<\mathrm{d} \\ \partial \mathrm{d} = D \\ \mathrm{d}-\partial \equiv 1 \bmod 2}} (\mathrm{d} - \partial - 1) + \sum_{\substack{0<\partial<\mathrm{d} \\ \partial \mathrm{d} = D \\ \mathrm{d}-\partial \equiv 0 \bmod 2}} ((\mathrm{d} - \partial) - 2) + \sum_{\substack{0<\partial<\mathrm{d} \\ \partial \mathrm{d} = D \\ \mathrm{d}-\partial \equiv 0 \bmod 2}} 1 \\
= & \sum_{\substack{0<\partial<\mathrm{d} \\ \partial \mathrm{d} = D \\ \mathrm{d}-\partial \equiv 1 \bmod 2}} (\mathrm{d} - \partial - 1) + \sum_{\substack{0<\partial<\mathrm{d} \\ \partial \mathrm{d} = D \\ \mathrm{d}-\partial \equiv 0 \bmod 2}} (\mathrm{d} - \partial - 1) \\
= & \sum_{\substack{0<\partial<\mathrm{d} \\ \partial \mathrm{d} = D}} (\mathrm{d} - \partial - 1).
\end{aligned}$$

□

4.2 Using divisors of D to count $m + n$

In this section we will use divisors of D to derive an expression for the value $m + n$. We continue to let $D \in \mathbb{Z}_{>0}$ represent the determinant of the bilinear forms.

Recall from Definition 3.2.2 that we are interested in the quantities m and n, which are the respective cardinalities of the following two sets:

$$M = \left\{ (A_{11}, A_{12}, A_{21}, A_{22}) \,\middle|\, A_{11}A_{22} - A_{12}A_{21} = D, 0 < \frac{A_{12} + A_{21}}{2} \leqslant A_{11}, \right.$$

$$0 < \frac{A_{12}+A_{21}}{2} \leqslant A_{22}, A_{11}-A_{12}-A_{21}+A_{22} > 0, A_{11} = A_{12}-A_{21}+A_{22}\Bigg\},$$

$$N = \Bigg\{(A_{11},A_{12},A_{21},A_{22}) \,\Big|\, A_{11}A_{22}-A_{12}A_{21} = D, 0 \leqslant \frac{A_{12}+A_{21}}{2} < A_{11},$$

$$0 \leqslant \frac{A_{12}+A_{21}}{2} < A_{22}, A_{11}-A_{12}-A_{21}+A_{22} > 0, A_{11} = A_{12}-A_{21}+A_{22}\Bigg\}.$$

Observation 4.2.1.
Any bilinear form in M or N satisfies $A_{11} = A_{12} - A_{21} + A_{22}$. Rewriting this as $A_{22} = A_{11} - A_{12} + A_{21}$ and substituting into the expression for D yields

$$\begin{aligned} D &= A_{11}A_{22} - A_{12}A_{21} \\ &= A_{11}\left(A_{11} - A_{12} + A_{21}\right) - A_{12}A_{21} \\ &= A_{11}^2 - A_{11}A_{12} + A_{11}A_{21} - A_{12}A_{21} \\ &= \left(A_{11} - A_{12}\right)\left(A_{11} + A_{21}\right). \end{aligned}$$

Lemma 4.2.2.
Any bilinear form in the set $M \cup N$ satisfies $A_{11} - A_{12} > 0$ and $A_{11} + A_{21} > 0$.

Proof.
Bilinear forms in the set $M \cup N$ satisfy $A_{22} = A_{11} - A_{12} - A_{21}$ and $A_{11} - A_{12} - A_{21} + A_{22} > 0$ (see Observation 3.2.1). Substituting the former into the latter yields $2(A_{11} - A_{12}) > 0$. Applying Observation 4.2.1 and recalling $D \in \mathbb{Z}_{>0}$ then yields $A_{11} + A_{21} > 0$. □

Lemma 4.2.3.
Let

$$Z_M = \left\{(\partial, \mathrm{d}, A_{11}) \,\Big|\, \partial\mathrm{d} = D, 0 < \partial < \mathrm{d}, \frac{\mathrm{d}-\partial}{2} \leqslant A_{11} \leqslant \frac{1}{2}\mathrm{d} + \frac{3}{2}\partial\right\}.$$

Then the map

$$\begin{aligned} \tau : M &\longrightarrow Z_M \\ (A_{11},A_{12},A_{21},A_{22}) &\longmapsto (A_{11}-A_{12}, A_{11}+A_{21}, A_{11}) = (\partial, \mathrm{d}, A_{11}) \end{aligned}$$

is a well-defined bijection. It follows that $m = |M| = |Z_M|$.

Proof.
Well-defined: By Observation 4.2.1 we have $D = (A_{11} - A_{12})(A_{11} + A_{21}) = \partial\mathrm{d}$. By Lemma 4.2.2 we know $0 < A_{11} - A_{12} = \partial$ and $0 < A_{11} + A_{21} = \mathrm{d}$. Thus $0 < A_{11} - A_{12} = \partial < A_{11} - A_{12} + A_{12} + A_{21} = \mathrm{d}$ as $0 < \frac{1}{2}(A_{12} + A_{21})$. Hence $0 < \partial < \mathrm{d}$. Further, observe $0 < \frac{1}{2}(\mathrm{d} - \partial) = \frac{1}{2}((A_{11} + A_{21}) - (A_{11} - A_{12})) = \frac{1}{2}(A_{12} + A_{21}) \leqslant A_{11}$.
Next, recall $A_{11} - A_{12} + A_{21} = A_{22} \geqslant \frac{1}{2}(A_{12} + A_{21})$. Rearranging this for A_{11} produces:

$$\begin{aligned} \frac{1}{2}\mathrm{d} + \frac{3}{2}\partial &= \frac{1}{2}\left(A_{11} + A_{21}\right) + \frac{3}{2}\left(A_{11} - A_{12}\right) \\ &= A_{11} + A_{11} + \frac{1}{2}A_{21} - \frac{3}{2}A_{12} \end{aligned}$$

$$\geqslant A_{11} + \left(A_{12} - A_{21} + \frac{1}{2}(A_{12} + A_{21})\right) + \frac{1}{2}A_{21} - \frac{3}{2}A_{12}$$
$$= A_{11}.$$

Hence we have $\frac{1}{2}(\mathrm{d} - \partial) \leqslant A_{11} \leqslant \frac{1}{2}\mathrm{d} + \frac{3}{2}\partial$ and so τ maps into Z_M.
Injectivity: Suppose $\tau(A_{11}, A_{12}, A_{21}, A_{22}) = \tau(A'_{11}, A'_{12}, A'_{21}, A'_{22})$, then we have $(A_{11} - A_{12}, A_{11} + A_{21}, A_{11}) = (A'_{11} - A'_{12}, A'_{11} + A'_{21}, A'_{11})$. Equating the entries from right to left yields $A_{11} = A'_{11}$, $A_{12} = A'_{12}$ and $A_{21} = A'_{21}$. Then using $A_{11}A_{22} - A_{12}A_{21} = D = A'_{11}A'_{22} - A'_{12}A'_{21}$ yields $A_{22} = A'_{22}$ and so τ is injective.
Surjectivity: Let $g = (\partial, \mathrm{d}, A_{11}) \in Z_M$ be arbitrary and consider $f = (A_{11}, A_{11} - \partial, \mathrm{d} - A_{11}, \partial + \mathrm{d} - A_{11}) = (a_{11}, a_{12}, a_{21}, a_{22})$, we will show this lies in M and $\tau(f) = g$. We observe $A_{11} \neq 0$ in Z_{m_1} since $0 < \partial < \mathrm{d}$ implies $0 < \mathrm{d} - \partial$ and we have $\frac{1}{2}(\mathrm{d} - \partial) \leqslant A_{11}$. Then we have

$$\begin{aligned} a_{11}a_{22} - a_{12}a_{21} &= A_{11}(\partial + \mathrm{d} - A_{11}) - (A_{11} - \partial)(\mathrm{d} - A_{11}) \\ &= \partial A_{11} + \mathrm{d}A_{11} - A_{11}^2 - \left(\mathrm{d}A_{11} - \partial\mathrm{d} + \partial A_{11} - A_{11}^2\right) \\ &= \partial\mathrm{d}. \end{aligned}$$

Next, we have $0 < \frac{1}{2}(\mathrm{d} - \partial) = \frac{1}{2}(A_{11} - \partial + \mathrm{d} - A_{11}) = \frac{1}{2}(a_{12} + a_{21}) \leqslant A_{11} = a_{11}$. Further, $A_{11} \leqslant \frac{1}{2}\mathrm{d} + \frac{3}{2}\partial$ rearranges to $A_{11} \leqslant \partial + \mathrm{d} - \frac{1}{2}(\mathrm{d} - \partial)$, which implies $\frac{1}{2}(\mathrm{d} - \partial) \leqslant \partial + \mathrm{d} + A_{11} = \partial + \mathrm{d} + a_{11} = a_{22}$. Thus $0 < \frac{1}{2}(A_{12} + A_{21}) = \frac{1}{2}(\mathrm{d} - \partial) \leqslant A_{22}$. Next, we have

$$\begin{aligned} a_{12} - a_{21} + a_{22} &= A_{11} - \partial - (\mathrm{d} - A_{11}) + (\partial + \mathrm{d} - A_{11}) \\ &= A_{11} \\ &= a_{11}. \end{aligned}$$

Hence $a_{11} = a_{12} - a_{21} + a_{22}$. Lastly we see that $a_{11} - a_{12} - a_{21} + a_{22} = A_{11} - (A_{11} - \partial) - (\mathrm{d} - A_{11}) + (\partial + \mathrm{d} - A_{11}) = 2\partial > 0$.
Thus we see f lies in M. Now observe $\tau(f) = (A_{11} - [A_{11} - \partial], A_{11} + [\mathrm{d} - A_{11}], A_{11}) = (\partial, \mathrm{d}, A_{11})$. So we see that τ is surjective and hence a bijection. Therefore it follows that $m = |M| = |Z_M|$. □

Lemma 4.2.4.
Let

$$Z_N = \left\{(\partial, \mathrm{d}, A_{11}) \,\middle|\, \partial\mathrm{d} = D, 0 < \partial \leqslant \mathrm{d}, \frac{\mathrm{d} - \partial}{2} < A_{11} < \frac{1}{2}\mathrm{d} + \frac{3}{2}\partial\right\}.$$

Then the map

$$\tau' : N \longrightarrow Z_N \text{ by}$$
$$(A_{11}, A_{12}, A_{21}, A_{22}) \longmapsto (A_{11} - A_{12}, A_{11} + A_{21}, A_{11}) = (\partial, \mathrm{d}, A_{11})$$

is a well-defined bijection. It follows that $n = |N| = |Z_N|$.

Proof.
By Observation 4.2.1 we know $\partial\mathrm{d} = (A_{11} - A_{12})(A_{11} + A_{21}) = D$. By Lemma 4.2.2

we know $0 < A_{11} - A_{12} = \partial$ and $0 < A_{11} + A_{21} = \mathrm{d}$. Thus $0 < A_{11} - A_{12} = \partial \leqslant A_{11} - A_{12} + A_{12} + A_{21} = \mathrm{d}$ since $0 \leqslant \frac{1}{2}(A_{12} + A_{21})$. Thus $0 < \partial \leqslant \mathrm{d}$. Next, note that $\frac{1}{2}(\mathrm{d} - \partial) = \frac{1}{2}(A_{12} + A_{21}) < A_{11}$ and also

$$\begin{aligned}
\frac{1}{2}\mathrm{d} + \frac{3}{2}\partial &= \frac{1}{2}(A_{11} + A_{21}) + \frac{3}{2}(A_{11} - A_{12}) \\
&= 2A_{11} + \frac{1}{2}(A_{12} + A_{21}) - 2A_{12} \\
&= A_{11} + A_{11} + \frac{1}{2}(A_{12} + A_{21}) - 2A_{12} \\
&> A_{11} + \frac{1}{2}(A_{12} + A_{21}) + \frac{1}{2}(A_{12} + A_{21}) - 2A_{12} \\
&= A_{11} + 2\left(\underbrace{A_{11} - A_{12}}_{} > 0\right) \\
&> A_{11}.
\end{aligned}$$

Hence we see $\frac{1}{2}(\mathrm{d} - \partial) < A_{11} < \frac{1}{2}\mathrm{d} + \frac{3}{2}\partial$ and thus τ' maps into Z_N.
Injectivity: Suppose $\tau'(A_{11}, A_{12}, A_{21}, A_{22}) = \tau'(A'_{11}, A'_{12}, A'_{21}, A'_{22})$. Then we have $(A_{11} - A_{12}, A_{11} + A_{21}, A_{11}) = (A'_{11} - A'_{12}, A'_{11} + A'_{21}, A'_{11})$. Equating the entries from right to left and then using $A_{11}A_{22} - A_{12}A_{21} = D = A'_{11}A'_{22} - A'_{12}A'_{21}$ yields injectivity.
Surjectivity: Let $g = (\partial, \mathrm{d}, A_{11}) \in Z_N$ be arbitrary and consider the form $f = (A_{11}, A_{11} - \partial, \mathrm{d} - A_{11}, \mathrm{d} + \partial - A_{11}) = (a_{11}, a_{12}, a_{21}, a_{22})$. We will show f lies in N and $\tau'(f) = g$.
In the same manner as in the proof of Lemma 4.2.3 we have

$$\begin{aligned}
a_{11}a_{22} - a_{12}a_{21} &= A_{11}(\mathrm{d} + \partial - A_{11}) - (A_{11} - \partial)(\mathrm{d} - A_{11}) \\
&= \partial\mathrm{d} \\
&= D.
\end{aligned}$$

Next, $\partial \leqslant \mathrm{d}$ implies $0 \leqslant \frac{1}{2}(\mathrm{d} - \partial) = \frac{1}{2}(a_{12} + a_{21})$. Further, $\frac{1}{2}(\mathrm{d} - \partial) < A_{11} = a_{11}$ and so $0 \leqslant \frac{1}{2}(a_{12} + a_{21}) < a_{11}$.
Next, $A_{11} < \frac{1}{2}\mathrm{d} + \frac{3}{2}\partial = \mathrm{d} + \partial - \frac{1}{2}(\mathrm{d} - \partial)$, which implies $\frac{1}{2}(\mathrm{d} - \partial) < \mathrm{d} + \partial - A_{11} = a_{22}$. Hence we have $0 \leqslant \frac{1}{2}(a_{12} + a_{21}) < a_{22}$. Then in the same manner as in the proof of Lemma 4.2.3 it follows that $a_{12} - a_{21} + a_{22} = a_{11}$ and $a_{11} - a_{12} - a_{21} + a_{22} = 2\partial > 0$. Thus we see f lies in Z_N. Now observe
$\tau'(f) = (A_{11} - [A_{11} - \partial], A_{11} + [d - A_{11}], A_{11}) = (\partial, \mathrm{d}, A_{11})$. So we see that τ' is surjective and hence a bijection. Therefore it follows that $n = |N| = |Z_N|$. □

We now prove a lemma and a couple of corollaries to make it easier for us to determine the cardinalities of the sets Z_M and Z_N.

Lemma 4.2.5.
Let $a, b \in \mathbb{R}\backslash\mathbb{Z}$, $a \leqslant b$ then there are $\lfloor b - a \rfloor$ integers in $[a, b]$.

Proof.
Let $a, b, \in \mathbb{R}\backslash\mathbb{Z}$, $a \leqslant b$. Let t be the unique integer such that $0 < a + t < 1$ and

consider the translated interval $[a+t, b+t]$. We recall that translating an interval by an integer quantity does not change the number of integers in it. Next, $b+t = n+\epsilon$ for some $0 < \epsilon < 1$ and it is clear that the interval $[a+t, b+t]$ contains n integers. Then we have $n = \lfloor (b+t) - (a+t) \rfloor = \lfloor b-a \rfloor$. □

Corollary 4.2.6.
There are $\lfloor b-a \rfloor$ integers in the interval (a,b), where $a, b, \in \mathbb{R}\backslash\mathbb{Z}$, $a \leqslant b$.

Proof.
This follows immediately from Lemma 4.2.5 as we have narrowed our interval by $0 < \epsilon < 1$. □

Corollary 4.2.7.
If the a, b in Lemma 4.2.5 are integers then there are $b-a+1$ integers in the interval $[a,b]$.

Proof.
Translate the interval so that the left end point is at 0. Then it is clear that the interval contains n non-zero integers, plus 0 and thus contains a total of $n+1$ integers. By the translation we have $b-a = n$ and thus there are $b-a+1$ integers in the interval. □

Lemma 4.2.8.

$$m = \sum_{\substack{\partial \mathrm{d} = D \\ 0 < \partial < \mathrm{d} \\ \mathrm{d} - \partial \equiv 1 \bmod 2}} 2\partial + \sum_{\substack{\partial \mathrm{d} = D \\ 0 < \partial < \mathrm{d} \\ \mathrm{d} - \partial \equiv 0 \bmod 2}} (2\partial + 1).$$

Proof.
From Lemma 4.2.3 we know $m = |Z_M|$. Fix ∂, d so that $0 < \partial < \mathrm{d}$ and $\partial \mathrm{d} = D$. We first assume that $\mathrm{d} - \partial$ is odd. Then the relations on the set Z_M imply $\frac{1}{2}(\mathrm{d} - \partial) < A_{11} < \frac{1}{2}\mathrm{d} + \frac{3}{2}\partial$. This is because $\mathrm{d} - \partial$ is odd and therefore so is $\mathrm{d} + 3\partial$. Consequently, $\frac{1}{2}(\mathrm{d} - \partial)$ and $\frac{1}{2}\mathrm{d} + \frac{3}{2}\partial$ cannot be integers. Applying Corollary 4.2.6 we see $A_{11} \in \mathbb{Z} \cap \left(\frac{1}{2}(\mathrm{d} - \partial), \frac{1}{2}\mathrm{d} + \frac{3}{2}\partial\right)$ and this interval contains 2∂ integers. Hence there are 2∂ possible values of A_{11} for each fixed pair (∂, d).
Now assume $\mathrm{d} - \partial$ is even. It follows that $\frac{1}{2}(\mathrm{d} - \partial)$ and $\frac{1}{2}\mathrm{d} + \frac{3}{2}\partial$ are both non-zero integers as $0 < \partial < \mathrm{d}$. Note that $A_{11} \in \mathbb{Z} \cap \left[\frac{1}{2}(\mathrm{d} - \partial), \frac{1}{2}\mathrm{d} + \frac{3}{2}\partial\right]$. Thus applying Corollary 4.2.7 we see that there are $2\partial + 1$ possible values for A_{11} given a fixed pair (∂, d).
Combining these results together yields

$$m = \sum_{\substack{\partial \mathrm{d} = D \\ 0 < \partial < \mathrm{d} \\ \mathrm{d} - \partial \equiv 1 \bmod 2}} 2\partial + \sum_{\substack{\partial \mathrm{d} = D \\ 0 < \partial < \mathrm{d} \\ \mathrm{d} - \partial \equiv 0 \bmod 2}} (2\partial + 1).$$

□

Lemma 4.2.9.

$$n = \sum_{\substack{\partial \mathrm{d}=D \\ 0<\partial\leqslant \mathrm{d} \\ \mathrm{d}-\partial\equiv 1 \bmod 2}} 2\partial + \sum_{\substack{\partial \mathrm{d}=D \\ 0<\partial\leqslant \mathrm{d} \\ \mathrm{d}-\partial\equiv 0 \bmod 2}} (2\partial - 1)\,.$$

Proof.
From Lemma 4.2.4 we know $n = |Z_N|$. Fix ∂ and d so that $0 < \partial \leqslant \mathrm{d}$ and $\partial\mathrm{d} = D$. We first assume that $\mathrm{d} - \partial$ is odd. Then $\frac{1}{2}(\mathrm{d} - \partial)$ and $\frac{1}{2}\mathrm{d} + \frac{3}{2}\partial$ cannot be integers. Applying Corollary 4.2.6 we see that $A_{11} \in \mathbb{Z} \cap \left(\frac{1}{2}(\mathrm{d} - \partial), \frac{1}{2}\mathrm{d} + \frac{3}{2}\partial\right)$ and this interval contains 2∂ integers. Hence there are 2∂ possible values for A_{11} given a fixed pair (∂, d) with $\mathrm{d} - \partial \equiv 1 \bmod 2$.
Now assume $\mathrm{d} - \partial$ is even. Observe that $A_{11} \in \mathbb{Z} \cap \left(\frac{1}{2}(\mathrm{d} - \partial), \frac{1}{2}\mathrm{d} + \frac{3}{2}\partial\right)$ and that $\left(\frac{1}{2}(\mathrm{d} - \partial), \frac{1}{2}\mathrm{d} + \frac{3}{2}\partial\right) \subset \left[\frac{1}{2}(\mathrm{d} - \partial), \frac{1}{2}\mathrm{d} + \frac{3}{2}\partial\right]$. By Corollary 4.2.7 $\left[\frac{1}{2}(\mathrm{d} - \partial), \frac{1}{2}\mathrm{d} + \frac{3}{2}\partial\right]$ contains $2\partial + 1$ integers and since we must exclude only the two end points it follows that given a fixed pair (∂, d) satisfying $\mathrm{d} - \partial \equiv 0 \bmod 2$, there are $2\partial - 1$ possible values for A_{11}.
Combining these results yields:

$$n = \sum_{\substack{\partial \mathrm{d}=D \\ 0<\partial\leqslant \mathrm{d} \\ \mathrm{d}-\partial\equiv 1 \bmod 2}} 2\partial + \sum_{\substack{\partial \mathrm{d}=D \\ 0<\partial\leqslant \mathrm{d} \\ \mathrm{d}-\partial\equiv 0 \bmod 2}} (2\partial - 1)\,.$$

□

Theorem 4.2.10.
Let $\omega = \begin{cases} -1 + 2\sqrt{D} & \text{if } D = k^2 \text{ for some } k \in \mathbb{Z}_{>0} \\ 0 & \text{otherwise} \end{cases}$ *, then*

$$m + n = \omega + 4 \sum_{\substack{\partial \mathrm{d}=D \\ 0<\partial<\mathrm{d}}} \partial.$$

Proof.
By Lemmas 4.2.8 and 4.2.9 we have

$$\begin{aligned} m + n &= \sum_{\substack{\partial \mathrm{d}=D \\ 0<\partial<\mathrm{d} \\ \mathrm{d}-\partial\equiv 1 \bmod 2}} 2\partial + \sum_{\substack{\partial \mathrm{d}=D \\ 0<\partial<\mathrm{d} \\ \mathrm{d}-\partial\equiv 0 \bmod 2}} (2\partial + 1) + \sum_{\substack{\partial \mathrm{d}=D \\ 0<\partial\leqslant \mathrm{d} \\ \mathrm{d}-\partial\equiv 1 \bmod 2}} 2\partial + \sum_{\substack{\partial \mathrm{d}=D \\ 0<\partial\leqslant \mathrm{d} \\ \mathrm{d}-\partial\equiv 0 \bmod 2}} (2\partial - 1) \\ &= \sum_{\substack{\partial \mathrm{d}=D \\ 0<\partial<\mathrm{d} \\ \mathrm{d}-\partial\equiv 1 \bmod 2}} 2\partial + \sum_{\substack{\partial \mathrm{d}=D \\ 0<\partial<\mathrm{d} \\ \mathrm{d}-\partial\equiv 0 \bmod 2}} (2\partial + 1) + \sum_{\substack{\partial \mathrm{d}=D \\ 0<\partial<\mathrm{d} \\ \mathrm{d}-\partial\equiv 1 \bmod 2}} 2\partial + \\ &\qquad \sum_{\substack{\partial \mathrm{d}=D \\ 0<\partial<\mathrm{d} \\ \mathrm{d}-\partial\equiv 0 \bmod 2}} (2\partial - 1) + \sum_{\substack{\partial \mathrm{d}=D \\ 0<\partial=\mathrm{d} \\ \mathrm{d}-\partial\equiv 1 \bmod 2}} 2\partial + \sum_{\substack{\partial \mathrm{d}=D \\ 0<\partial=\mathrm{d} \\ \mathrm{d}-\partial\equiv 0 \bmod 2}} (2\partial - 1) \\ &= 2 \sum_{\substack{\partial \mathrm{d}=D \\ 0<\partial=\mathrm{d} \\ \mathrm{d}-\partial\equiv 1 \bmod 2}} 2\partial + \sum_{\substack{\partial \mathrm{d}=D \\ 0<\partial<\mathrm{d} \\ \mathrm{d}-\partial\equiv 0 \bmod 2}} (2\partial + 1 + 2\partial - 1) + \end{aligned}$$

$$\sum_{\substack{\partial \mathrm{d}=D \\ 0<\partial=\mathrm{d} \\ \mathrm{d}-\partial\equiv 1 \bmod 2}} 2\partial + \sum_{\substack{\partial \mathrm{d}=D \\ 0<\partial=\mathrm{d} \\ \mathrm{d}-\partial\equiv 0 \bmod 2}} (2\partial - 1)$$
$$= \sum_{\substack{\partial \mathrm{d}=D \\ 0<\partial<\mathrm{d}}} 4\partial + \sum_{\substack{\partial \mathrm{d}=D \\ 0<\partial=\mathrm{d} \\ \mathrm{d}-\partial\equiv 1 \bmod 2}} 2\partial + \sum_{\substack{\partial \mathrm{d}=D \\ 0<\partial=\mathrm{d} \\ \mathrm{d}-\partial\equiv 0 \bmod 2}} (2\partial - 1).$$

First observe that if D is not a perfect square, i.e. $D \neq k^2$ for some $k \in \mathbb{Z}_{>0}$ then we cannot have $\partial = \mathrm{d} = \sqrt{D} = k$. Thus the last two sums are zero in this case.
Secondly we observe if $\mathrm{d} = \partial = \sqrt{D}$ then $\mathrm{d} - \partial \equiv 1 \bmod 2$ is a contradiction. Consequently the second summation is always equal to zero.
Thus in the case where $D = k^2$ for some $k \in \mathbb{Z}_{>0}$ we have the first and third sums remain. Further, the third sum is just $2\partial - 1 = -1 + 2\sqrt{D}$.
Hence we have

$$m + n = \omega + 4 \sum_{\substack{\partial \mathrm{d}=D \\ 0<\partial<\mathrm{d}}} \partial,$$

where $\omega = \begin{cases} -1 + 2\sqrt{D} & \text{if } D = k^2 \text{ for some } k \in \mathbb{Z}_{>0} \\ 0 & \text{otherwise.} \end{cases}$

□

4.3 Determining values for P_0, Q_0, R_0 and S_0.

In this section we determine the values of P_0, Q_0, R_0 and S_0. We continue to let $D \in \mathbb{Z}_{>0}$ be the determinant of our bilinear forms.

Definition 4.3.1.
Let $\sigma(n) = \sum_{\mathrm{d}|n} d$, be the sum of all positive (integer) divisors of n. Observe this includes $d = 1$ and $d = n$.

Recall the sets $I_{0,=}$ and $I_{1,=}$ from Definition 3.4.1:

$$I_{0,=} = \{(A_{11}, A_{11}, A_{21}, A_{22}) \,|\, A_{11}(A_{22} - A_{21}) = D, -A_{11} < A_{21} \leqslant A_{11}, 0 < A_{22} - A_{21}\},$$
$$I_{1,=} = \{(A_{11}, A_{11}, A_{21}, A_{22}) \,|\, A_{11}(A_{22} - A_{21}) = D, -A_{11} \leqslant A_{21} < A_{11}, 0 < A_{22} - A_{21}\}.$$

Definition 4.3.2.
Let $U = \{(\partial, \mathrm{d}) \mid \partial\mathrm{d} = D, \partial, \mathrm{d} \in \mathbb{Z}_{>0}\}$.

Lemma 4.3.3.
The map $\tau : I_{0,=} \longrightarrow U$, given by $\tau(A_{11}, A_{11}, A_{21}, A_{22}) = (A_{11}, A_{22} - A_{21}) = (\partial, \mathrm{d})$ is a surjection. Further, each element $(\partial, \mathrm{d}) \in U$ is mapped to under τ exactly 2∂ times.

Proof.
Well-defined: In the set $I_{0,=}$ we have $0 < A_{22} - A_{21}$, $D = A_{11}(A_{22} - A_{21}) > 0$ and these are integers. Therefore it follows that $\partial = A_{11} \in \mathbb{Z}_{>0}$ and $\mathrm{d} = A_{22} - A_{21} \in \mathbb{Z}_{>0}$.

Lastly, $\partial \mathrm{d} = A_{11}(A_{22} - A_{21}) = D$ and so τ maps into the set U.
Surjectivity: Let $(\partial, \mathrm{d}) \in U$ be arbitrary and consider
$f = (\partial, \partial, 0, \mathrm{d}) = (A_{11}, A_{11}, A_{21}, A_{22})$. We will show this always exists and lies in $I_{0,=}$. We have $A_{11} = \partial > 0$ and $A_{22} - A_{21} = \mathrm{d} - 0 = \mathrm{d} > 0$. Further, $A_{11}(A_{22} - A_{21}) = \partial \mathrm{d} = D$ and $-\partial = -A_{11} < 0 < A_{11} = \partial$, hence f lies in $I_{0,=}$. Lastly, $\tau(\partial, \partial, 0, \mathrm{d}) = (\partial, \mathrm{d} - 0) = (\partial, \mathrm{d})$. Thus we see τ is surjective.
We now observe τ is not injective. This follows because $A_{11} \geqslant 1$, so both 0 and 1 lie in $(-A_{11}, A_{11}]$ always. Consequently we see that $(\partial, \partial, 0, \mathrm{d})$ and $(\partial, \partial, 1, \mathrm{d} + 1)$ both lie in $I_{0,=}$ and map under τ to (∂, d). Therefore we will partition the set U according to ∂. For a fixed $\partial \in \mathbb{N}_{>0}$ such that $D = \partial \mathrm{d}$, we consider the pre-image of (∂, d) under τ in $F_{1,=}$. This is the set of all forms in $F_{1,=}$ that have the same A_{11} term, which equals ∂. Then for each integer A_{21} such that $-\partial = -A_{11} < A_{21} \leqslant A_{11} = \partial$ we see that there is a unique value of A_{22} such that $0 < A_{22} - A_{21}$ and $A_{22} - A_{21} = \mathrm{d}$ where $D = \partial \mathrm{d}$. By Corollary 4.2.7 the interval $(-\partial, \partial]$ contains 2∂ integers, so we see that for a fixed value of ∂ there are 2∂ forms in $I_{0,=}$ that map under τ to (∂, d). Hence τ is a 2∂-to-one surjection. □

Corollary 4.3.4.
$P_0 = 2\sigma(D)$.

Proof.
By Lemma 4.3.3 we know that for a fixed $\partial \in \mathbb{Z}_{>0}$ there are 2∂ elements in $I_{0,=}$ mapping under τ to (∂, d). Further, if two elements in $I_{0,=}$ have distinct A_{11} values then they cannot map under τ to the same (∂, d). Consequently we see

$$\begin{aligned} P_0 &= \sum_{\substack{\partial \\ \partial \mathrm{d} = D}} 2\partial \\ &= 2 \sum_{\substack{\partial \\ \partial | D}} \partial \\ &= 2\sigma(D). \end{aligned}$$

□

Lemma 4.3.5.
The map $\hat{\tau} : I_{1,=} \longrightarrow U$, given by $\hat{\tau}(A_{11}, A_{11}, A_{21}, A_{22}) = (A_{11}, A_{22} - A_{21}) = (\partial, \mathrm{d})$ is a surjection. Further, each element in $(\partial, \mathrm{d}) \in U$ is mapped to exactly 2∂ times under $\hat{\tau}$.

Proof.
We observe that the only difference between the sets $I_{0,=}$ and $I_{1,=}$ is the location of the equality condition within the inequality $-A_{11} < A_{21} < A_{11}$. In the first set it is on the second inequality, while in the second set it is on the first inequality. Consequently the same proof applied to $I_{1,=}$ yields the desired result. □

Corollary 4.3.6.
$Q_0 = 2\sigma(D)$.

Proof.
By Lemma 4.3.5, for a fixed $\partial \in \mathbb{Z}_{>0}$ there are 2∂ elements in $I_{1,=}$ that map under $\hat{\tau}$ to (∂, d). Further, if two elements in $I_{1,=}$ have distinct A_{11} values then they cannot map under $\hat{\tau}$ to the same (∂, d). Consequently we see

$$\begin{aligned} Q_0 &= \sum_{\substack{\partial \\ \partial \mathrm{d} = D}} 2\partial \\ &= 2 \sum_{\substack{\partial \\ \partial | D}} \partial \\ &= 2\sigma(D). \end{aligned}$$

□

Corollary 4.3.7.
$P_0 + Q_0 = 4\sigma(D)$.

Proof.
By Corollaries 4.3.4 and 4.3.6 we have $P_0 + Q_0 = 2\sigma(D) + 2\sigma(D) = 4\sigma(D)$. □

We now will investigate the values of R_0 and S_0. Recall $R_0 = |J_{0,=}|$ and $S_0 = |J_{1,=}|$, where

$$\begin{aligned} J_{0,=} = \{(A_{11}, A_{12}, A_{21}, 0) \,\big|\, \det = D = -A_{12}A_{21}, 0 < \frac{A_{12} + A_{21}}{2} < A_{11}, \\ A_{21} < -|A_{11} - A_{12}|\}, \\ J_{1,=} = \{(A_{11}, A_{12}, A_{21}, 0) \,\big|\, \det = D = -A_{12}A_{21}, 0 \leqslant \frac{A_{12} + A_{21}}{2} < A_{11}, \\ A_{21} < -|A_{11} - A_{12}|\}. \end{aligned}$$

Our next lemma provides a simplification of these two sets.

Lemma 4.3.8.
The sets $J_{0,=}$ and $J_{1,=}$ may be simplified as follows:

$$\begin{aligned} J_{0,=} = \{(A_{11}, A_{12}, A_{21}, 0) \mid \det = D = -A_{12}A_{21}, 0 < A_{12} + A_{21} < A_{11}, \\ A_{21} < -|A_{11} - A_{12}|\}, \\ J_{1,=} = \{(A_{11}, A_{12}, A_{21}, 0) \mid \det = D = -A_{12}A_{21}, 0 \leqslant A_{12} + A_{21} < A_{11}, \\ A_{21} < -|A_{11} - A_{12}|\}. \end{aligned}$$

Proof.
In both $J_{0,=}$ and $J_{1,=}$ we have $A_{21} < 0$ and $A_{12} > 0$, therefore we may write $-A_{21} = |A_{21}|$. Also, elements in $J_{0,=}$ or $J_{1,=}$ satisfy $A_{21} < -|A_{11} - A_{12}|$. This yields $-|A_{21}| < A_{11} - A_{12} < |A_{21}|$ which, is the same as $A_{12} + A_{21} < A_{11} < A_{12} - A_{21}$. Combining this result with $0 < (\leqslant) A_{12} + A_{21} < 2A_{11}$ yields the simplification $0 < A_{12} + A_{21} < A_{11}$. This gives rise to the statements of $J_{0,=}$ and $J_{1,=}$ as given in the lemma. □

We now define two very similar sets that we will use to enumerate the sets $J_{0,=}$ and $J_{1,=}$.

Definition 4.3.9.

$U_1 = \{(\partial, \mathrm{d}, A_{11}) \mid \partial\mathrm{d} = D, 0 < \partial < \mathrm{d}, \partial, \mathrm{d} \in \mathbb{Z}_{>0}, \mathrm{d} - \partial + 1 \leqslant A_{11} \leqslant \mathrm{d} + \partial - 1\}$ and
$U_2 = \{(\partial, \mathrm{d}, A_{11}) \mid \partial\mathrm{d} = D, 0 < \partial \leqslant \mathrm{d}, \partial, \mathrm{d} \in \mathbb{Z}_{>0}, \mathrm{d} - \partial + 1 \leqslant A_{11} \leqslant \mathrm{d} + \partial - 1\}$.

Lemma 4.3.10.
The map

$$\begin{aligned} \nu : J_{0,=} &\longrightarrow U_1 \\ (A_{11}, A_{12}, A_{21}, A_{22}) &\longmapsto (-A_{21}, A_{12}, A_{11}) = (\partial, \mathrm{d}, A_{11}) \end{aligned}$$

is a well-defined bijection.

Proof.
Well-defined: Observe $\partial\mathrm{d} = (-A_{21}) \cdot A_{12} = -A_{12}A_{21} = D$ and that $\partial = -A_{21}$, $\mathrm{d} = A_{12}$ and A_{11} are all strictly positive integers. Also, $0 < A_{12} + A_{21} < A_{11}$ implies $0 < \mathrm{d} - \partial < A_{11}$ and so $0 < \partial < \mathrm{d}$. Next, $A_{21} < -|A_{11} - A_{12}|$ implies $\partial > |A_{11} - \mathrm{d}|$. Hence $-\partial < A_{11} - \mathrm{d} < \partial$, i.e. $\mathrm{d} - \partial < A_{11} < \mathrm{d} + \partial$. Since A_{11}, ∂ and d are integers it follows that $\mathrm{d} - \partial + 1 \leqslant A_{11} \leqslant \mathrm{d} + \partial - 1$. Thus ν is well-defined.
Injectivity: This follows naturally.
Surjectivity: Let $(\partial, \mathrm{d}, A_{11}) \in U_1$ be arbitrary. Consider
$(A_{11}, \mathrm{d}, -\partial, 0) = (a_{11}, a_{12}, a_{21}, 0) = g$. Then $\det(g) = A_{11} \cdot 0 - (\mathrm{d})(-\partial) = \partial\mathrm{d} = D$. Note that $A_{12} + A_{21} = \mathrm{d} - \partial > 0$ as $0 < \partial < \mathrm{d}$. Further, $\mathrm{d} - \partial + 1 \leqslant A_{11}$ implies $A_{12} + A_{21} = \mathrm{d} - \partial < A_{11}$. Lastly, we have $\mathrm{d} - \partial + 1 \leqslant A_{11} \leqslant \mathrm{d} + \partial - 1$ implies $-\partial < A_{11} - \mathrm{d} < \partial$ and thus $|A_{11} - \mathrm{d}| < \partial = -A_{21}$. Therefore $A_{21} < -|A_{11} - A_{12}|$ and thus $g \in J_{0,=}$. We note that $\nu(g) = (-a_{21}, a_{12}, a_{11}) = (\partial, \mathrm{d}, A_{11})$.
Hence ν is surjective and therefore ν is a bijection. □

Corollary 4.3.11.

$$R_0 = \sum_{\substack{\partial \in \mathbb{Z}_{>0} \\ 0 < \partial < \mathrm{d} \\ \partial\mathrm{d} = D}} (2\partial - 1)\,.$$

Proof.
By Lemma 4.3.10 we have $R_0 = |U_1|$. By the construction of U_1 we can pick any pair (∂, d) such that $0 < \partial < \mathrm{d}$ and $\partial\mathrm{d} = D$, and then $1 < \mathrm{d} - \partial + 1 \leqslant A_{11} \leqslant \mathrm{d} + \partial - 1$ implies there is at least one value for A_{11}. So for each such pair ∂, d there is always at least one $(\partial, \mathrm{d}, A_{11}) \in U_1$. Further, by Corollary 4.2.7 there are $(\mathrm{d}+\partial-1)-(\mathrm{d}-\partial+1)+1 = 2\partial-1$ choices for A_{11} given a pair ∂, d.
Hence we have $R_0 = |U_1| = \sum_{\substack{\partial \\ 0 < \partial < \mathrm{d} \\ \partial\mathrm{d} = D}} (2\partial - 1)$. □

Lemma 4.3.12.
The map

$$\begin{aligned} \hat{\nu} : J_{1,=} &\longrightarrow U_2 \\ (A_{11}, A_{12}, A_{21}, 0) &\longmapsto (-A_{21}, A_{12}, A_{11}, 0) = (\partial, \mathrm{d}, A_{11}) \end{aligned}$$

is a well-defined bijection.

Proof.
Well-defined: Observe $\partial \mathrm{d} = (-A_{21}) \cdot A_{12} = -A_{12}A_{21} = D$ and that $\partial = -A_{21}$, $\mathrm{d} = A_{12}$ and A_{11} are all strictly positive integers. Also, $0 \leqslant A_{12} + A_{21} < A_{11}$ implies $0 \leqslant \mathrm{d} - \partial < A_{11}$, thus $0 < \partial \leqslant \mathrm{d}$. Next, $A_{21} < -|A_{12} + A_{21}|$ implies $-\partial < A_{11} - \mathrm{d} < \partial$. This yields $\mathrm{d} - \partial < A_{11} < \mathrm{d} + \partial$ and since A_{11} is an integer we have $\mathrm{d} - \partial + 1 \leqslant A_{11} \leqslant \mathrm{d} + \partial - 1$. Hence $\hat{\nu}$ maps into U_2 and so is well-defined.
Injectivity: This follows naturally.
Surjectivity: Let $(\partial, \mathrm{d}, A_{11}) \in U_2$ be arbitrary. Then consider $g = (A_{11}, \mathrm{d}, -\partial, 0) = (a_{11}, a_{12}, a_{21}, 0)$. We have $\det(g) = A_{11} \cdot 0 - (\mathrm{d})(-\partial) = \partial \mathrm{d} = D$. Next, $0 < \partial \leqslant \mathrm{d}$ implies $0 \leqslant \mathrm{d} - \partial$ so $0 \leqslant a_{12} + a_{21}$. Further, $\mathrm{d} - \partial + 1 \leqslant A_{11} - \mathrm{d} \leqslant \mathrm{d} + \partial - 1$ implies $\mathrm{d} - \partial < A_{11} < \mathrm{d} + \partial$ and so $|A_{11} - \mathrm{d}| < \partial$. Using $a_{21} = -\partial$, $a_{12} = \mathrm{d}$ and $a_{11} = A_{11}$ yields $a_{21} < -|a_{11} - a_{12}|$. Thus g lies in $J_{1,=}$. We note that $\hat{\nu}(g) = (-a_{21}, a_{12}, a_{11}) = (\partial, \mathrm{d}, A_{11})$.
Hence $\hat{\nu}$ is surjective and therefore is a bijection. □

Corollary 4.3.13.
Let $\omega = \begin{cases} -1 + 2\sqrt{D} & D = k^2 \text{ for some } k \in \mathbb{Z}_{>0} \\ 0 & \text{otherwise} \end{cases}$ *, as found in the proof of Theorem 4.2.10. Then*

$$S_0 = \omega + \sum_{\substack{\partial \\ 0 < \partial \leqslant \mathrm{d} \\ \partial \mathrm{d} = D}} (2\partial - 1)\,.$$

Proof.
By Lemma 4.3.12 we have $S_0 = |U_2|$. By the construction of U_2 we can pick any pair (∂, d) such that $\partial \mathrm{d} = D$ and $0 < \partial \leqslant \mathrm{D}$, and then $1 \leqslant \mathrm{d} - \partial + 1 \leqslant A_{11} \leqslant \mathrm{d} + \partial - 1$ implies there is at least one value of A_{11} for each such pair. By Corollary 4.2.7 we see that there are $2\partial - 1$ possible choices for A_{11} for each pair (∂, d).
Hence we have $S_0 = |U_2| = \sum_{\substack{\partial \in \mathbb{Z}_{>0} \\ 0 < \partial \leqslant \mathrm{d} \\ \partial \mathrm{d} = D}} (2\partial - 1)$.
Applying our definition for ω we get

$$S_0 = \omega + \sum_{\substack{\partial \in \mathbb{Z}_{>0} \\ 0 < \partial < \mathrm{d} \\ \partial \mathrm{d} = D}} (2\partial - 1)\,.$$

□

4.4 A Formula for the Complete Class Number of Bilinear Forms with Determinant D

In this section we finish our derivation of Kronecker's formula for the complete class number of positive definite bilinear forms with determinant D.
Recall from earlier $\omega = \begin{cases} -1+2\sqrt{D} & \text{if } D = k^2 \\ 0 & \text{otherwise} \end{cases}$ and $\sigma(D) = \sum_{d|D} d$.

Definition 4.4.1.
Let $\partial, \mathrm{d} \in \mathbb{Z}_{>0}$ be such that $\partial\mathrm{d} = D$. Then we define $\Psi(D) = \sum_{\substack{0<\partial<\mathrm{d} \\ \partial\mathrm{d}=D}} (\mathrm{d}-\partial)$.

Lemma 4.4.2.
Let $D \in \mathbb{Z}_{>0}$, then $2\sum_{\substack{0<\partial<\mathrm{d} \\ \partial\mathrm{d}=D}} \partial = \begin{cases} \sigma(D)-\Psi(D)-\sqrt{D} & \textit{if } D=k^2 \\ \sigma(D)-\Psi(D) & \textit{otherwise.} \end{cases}$

Proof.
Let $D \in \mathbb{Z}_{>0}$, we split the proof into two cases, when D is a perfect square, and otherwise.
First suppose D is a perfect square, then we have

$$\begin{aligned}
\sigma(D)-\Psi(D)-\sqrt{D} &= \sum_{\mathrm{d}|D} \mathrm{d} - \sum_{\substack{0<\partial<\mathrm{d} \\ \partial\mathrm{d}=D}} (\mathrm{d}-\partial) - \sqrt{D} \\
&= \sum_{\substack{\sqrt{D}<\mathrm{d} \\ \partial\mathrm{d}=D}} \mathrm{d} + \sum_{\substack{\mathrm{d}<\sqrt{D} \\ \partial\mathrm{d}=D}} \mathrm{d} + \sqrt{D} - \sum_{\substack{0<\partial<\mathrm{d} \\ \partial\mathrm{d}=D}} \mathrm{d} + \sum_{\substack{0<\partial<\mathrm{d} \\ \partial\mathrm{d}=D}} \partial - \sqrt{D} \\
&= 2\sum_{\substack{0<\partial<\mathrm{d} \\ \partial\mathrm{d}=D}} \partial.
\end{aligned}$$

Now suppose D is not a perfect square, then we never have $\partial = \mathrm{d} = \sqrt{D}$. So we have

$$\begin{aligned}
\sigma(D)-\Psi(D) &= \sum_{\mathrm{d}|D} \mathrm{d} - \sum_{\substack{0<\partial<\mathrm{d} \\ \partial\mathrm{d}=D}} (\mathrm{d}-\partial) \\
&= \sum_{\substack{0<\mathrm{d}<\sqrt{D} \\ d|D}} \mathrm{d} + \sum_{\substack{0<\partial<\sqrt{D} \\ \partial|D}} \partial \\
&= 2\sum_{\substack{0<\partial<\mathrm{d} \\ \partial\mathrm{d}=D}} \partial.
\end{aligned}$$

□

Theorem 4.4.3.
Let $D \in \mathbb{Z}_{>0}$, then

$$\mathrm{Cl}_c(D) = \begin{cases} 6\Psi(D)+6\sigma(D)+1 & \textit{if } D=k^2 \\ 6\Psi(D)+6\sigma(D) & \textit{otherwise.} \end{cases}$$

Proof.
From Equation 3.19 we have

$$\begin{aligned}
\mathrm{Cl}_c(D) &= M + N + 2(2(K+L) + P_0 + Q_0 - R_0 - S_0) \\
&= \omega + 4\sum_{\substack{\partial \mathrm{d}=D \\ 0<\partial<\mathrm{d}}} \partial + 2(2(K+L) + P_0 + Q_0 - R_0 - S_0) \text{ by Theorem 4.2.10} \\
&= \omega + 4\sum_{\substack{\partial \mathrm{d}=D \\ 0<\partial<\mathrm{d}}} \partial + 2\left[\underbrace{2\sum_{\substack{\partial \mathrm{d}=D \\ 0<\partial<\mathrm{d}}} (\mathrm{d}-\partial-1)}_{\text{Theorem 4.1.9}}\right] + \\
&\qquad 2\left[\underbrace{4\sigma(D)}_{\text{Corollary 4.3.7}} - \underbrace{\sum_{\substack{\partial \mathrm{d}=D \\ 0<\partial<\mathrm{d}}} (2\partial-1)}_{\text{Corollary 4.3.11}} - \underbrace{\left(\omega + \sum_{\substack{\partial \mathrm{d}=D \\ 0<\partial<\mathrm{d}}} (2\partial-1)\right)}_{\text{Corollary 4.3.13}}\right] \\
&= \omega - 2\omega + 4\sum_{\substack{\partial \mathrm{d}=D \\ 0<\partial<\mathrm{d}}} \partial + 2\left[2\left(\sum_{\substack{\partial \mathrm{d}=D \\ 0<\partial<\mathrm{d}}} [(\mathrm{d}-\partial-1)-(2\partial-1)]\right) + 4\sigma(D)\right] \\
&= -\omega + 4\sum_{\substack{\partial \mathrm{d}=D \\ 0<\partial<\mathrm{d}}} \partial + 4\sum_{\substack{\partial \mathrm{d}=D \\ 0<\partial<\mathrm{d}}} (\mathrm{d}-3\partial) + 8\sigma(D) \\
&= -\omega + 4\sum_{\substack{\partial \mathrm{d}=D \\ 0<\partial<\mathrm{d}}} \partial + 4\sum_{\substack{\partial \mathrm{d}=D \\ 0<\partial<\mathrm{d}}} (\mathrm{d}-\partial) - 4\sum_{\substack{\partial \mathrm{d}=D \\ 0<\partial<\mathrm{d}}} 2\partial + 8\sigma(D) \\
&= -\omega + 4\sum_{\substack{\partial \mathrm{d}=D \\ 0<\partial<\mathrm{d}}} (\mathrm{d}-\partial) - 4\sum_{\substack{\partial \mathrm{d}=D \\ 0<\partial<\mathrm{d}}} \partial + 8\sigma(D) \\
&= -\omega + 4\Psi(D) - 2\left(\begin{cases} \sigma(D) - \Psi(D) - \sqrt{D} \\ \sigma(D) - \Psi(D) \end{cases}\right) + 8\sigma(D) \text{ by Lemma 4.4.2} \\
&= \begin{cases} 1 - 2\sqrt{D} + 6\Psi(D) + 6\sigma(D) + 2\sqrt{D} & \text{if } D = k^2 \\ 6\Psi(D) + 6\sigma(D) & \text{otherwise.} \end{cases} \\
&= \begin{cases} 6\Psi(D) + 6\sigma(D) + 1 & \text{if } D = k^2 \\ 6\Psi(D) + 6\sigma(D) & \text{otherwise} \end{cases}
\end{aligned}$$

□

4.5 An Application of the Complete Class Number Formula

In this section we develop a series of applications of the complete class number formula, Theorem 4.4.3. We first prove a lower bound on the number of proper equivalence classes of positive definite bilinear forms of determinant $D \in \mathbb{Z}_{>0}$. Then we

derive a formula for the proper class number for positive definite bilinear forms of determinant $D \in \mathbb{Z}_{>0}$ and examine a consequence of this. At the end we prove three theorems which strengthen our lower bound based upon the primality and congruence modulo 12 of the determinant.

We first develop a couple of well-known lemmas and a theorem that will be needed to prove our results in this section.

Lemma 4.5.1.
Let p be a prime such that $p \geqslant 3$. Then -3 is a square mod$p$ *if and only if $p = 3$ or $p \equiv 1 \bmod 3$.*

Proof.
($\Rightarrow$) First suppose $p = 3$, then $m^2 \equiv -3 \bmod p$ is equivalent to $m^2 \equiv 0 \bmod 3$ and it is straightforward to see $m = 0$ is one such solution. Now assume $p \equiv 1 \bmod 3$, then since the multiplicative group of $\mathbb{Z}/p\mathbb{Z}$ is a cyclic group of order $p-1$, there exists an element a of multiplicative order $p-1$. Let $b = a^{\frac{p-1}{3}}$, then $b \not\equiv 1 \bmod p$ yet $b^3 \equiv 1 \bmod 3$. Since $b^3 - 1 = (b-1)(b^2+b+1)$ it follows that $b^2+b+1 \equiv 0 \bmod p$. Now observe $(2b+1)^2 + 3 = 4b^2 + 4b + 4 = 4(b^2+b+1) \equiv 0 \bmod p$ and thus $(2b+1)^2 \equiv -3 \bmod p$. That is, -3 is a square mod$p$.
($\Leftarrow$) Assume $m^2 \equiv -3 \bmod p$. If m is even then observe $p - m$ is odd (as p is a prime and not 2) and satisfies $(p-m)^2 = p^2 - 2mp + m^2 \equiv -3 \bmod p$. Therefore without loss of generality we may assume m is odd. Write $m = 2l+1$ and first deal with $l = 1$. Then $3^2 \equiv -3 \bmod p$, so $p|12$ and since $p > 2$ it follows that $p = 3$. Now assume $l > 1$ as $l = 0$ corresponds to $p = 2$. We have $(2l+1)^2 + 3 \equiv 0 \bmod p$ and thus $4l^2 + 4l + 4 \equiv 0 \bmod p$. This implies $4(l^2+l+1) \equiv 0 \bmod p$, consequently $l^2 + l + 1 \equiv 0 \bmod p$. However, $l^3 - 1 = (l-1)(l^2+l+1)$ and thus $l^3 - 1 \equiv 0 \bmod p$. Since $l \neq 1$, $|l| = 3$ follows immediately. Hence we have an element l of order 3, and this forms a subgroup within a group of order $p-1$. Therefore $3|(p-1)$ and thus $p \equiv 1 \bmod 3$. □

Theorem 4.5.2.
Let p be a prime. Then $p = x^2 + xy + y^2$ for some integers x, y if and only if $p = 3$ or $p \equiv 1 \bmod 3$.

Proof.
($\Rightarrow$) Suppose p is a prime and $p = x^2 + xy + y^2$ for some integers x and y. Recall $t^2 \equiv 0, 1 \bmod 3$, with 0 occurring if and only if $3 \mid t$. Since p is prime, it follows that at least one of x, y is not divisible by 3. Therefore without loss of generality we have $x^2 \equiv 1 \bmod 3$. We immediately see if $3 \mid y$ then $p \equiv 1 \bmod 3$. Thus we now suppose $3 \nmid y$ and hence $y^2 \equiv 1 \bmod 3$. It follows that $xy \equiv 1 \bmod 3$ or $xy \equiv 2 \bmod 3$. In the first instance we have $p \equiv 0 \bmod 3$ however, p is prime and hence $p = 3$. In the second instance it is straightforward to verify $p \equiv 1 \bmod 3$.
($\Leftarrow$) Suppose p is a prime such that $p \equiv 1 \bmod 3$. By Lemma 4.5.1 there exists an integer m such that $m^2 \equiv -3 \bmod p$. We may assume m is odd as we may replace m with $p - m$ if needed. Writing $m^2 + 3 = pn$ we see $4 \mid pn$ as m is odd. Since p is prime,

it follows that $4 \mid n$ and we let $n = 4r$. Thus $m^2 + 3 = 4pr$. Consider the binary quadratic form, $px^2 + mxy + ry^2$, which has discriminant $m^2 - 4pr = -3$ (Note this is the usual definition of the discriminant - not the one due to Kronecker). Since the proper class number is 1 for binary quadratic forms with discriminant -3, it follows that $x^2 + xy + y^2$ and $px^2 + mxy + ry^2$ represent the same integers. In particular, there exist integers x and y such that $p = x^2 + xy + y^2$. □

We now develop our first application of Kronecker's formula for the complete class number.

Lemma 4.5.3.
The proper class number satisfies $\mathrm{Cl}_c(D) \leqslant 6\mathrm{Cl}_+(D)$*, with equality if and only if there are no proper automorphs for any bilinear form of determinant* D*.*

Proof.
By Lemma 2.5.22 and Lemma 2.5.26 we know if there are no proper automorphs of a bilinear form, then its proper equivalence class contains exactly six complete equivalence classes. From Summary 2.5.27 if at least one proper automorph exists then there are less than six complete equivalence classes within the proper equivalence class.
Hence $\mathrm{Cl}_c(D) \leqslant 6\mathrm{Cl}_+(D)$.
We now prove when equality holds.
($\Rightarrow$). Assume $\mathrm{Cl}_c(D) = 6\mathrm{Cl}_+(D)$, then every proper equivalence class must contain exactly six complete equivalence classes. Lemma 2.5.22 and Summary 2.5.27 then imply no proper automorphs exist for any bilinear form with determinant D.
($\Leftarrow$) Assume there are no bilinear forms of determinant D that have a proper automorph. Then Lemma 2.5.22 and Summary 2.5.27 imply every proper equivalence class contains exactly six complete equivalence classes. Therefore $\mathrm{Cl}_c(D) = 6\mathrm{Cl}_+(D)$. □

Lemma 4.5.4.
Let $D > 1$ *then the complete class number satisfies* $12D \leqslant \mathrm{Cl}_c(D)$*, with equality if and only if* D *is prime.*
When $D = 1$ *we have* $\mathrm{Cl}_c(D) = 7$*.*

Proof.
Firstly, let $D = 1$, then $\mathrm{Cl}_c(D) = 6\Psi(D) + 6\sigma(D) + 1 = 7$. Now assume $D > 1$ and apply Theorem 4.4.3 as follows:

$$\begin{aligned}
\mathrm{Cl}_c(D) &= \begin{cases} 6\Psi(D) + 6\sigma(D) + 1 & \text{if } D = k^2 \\ 6\Psi(D) + 6\sigma(D) & \text{otherwise} \end{cases} \\
&\geqslant 6\Psi(D) + 6\sigma(D) \\
&= 6 \sum_{\substack{\partial \mathrm{d} = D \\ 0 < \partial < \mathrm{d}}} (\mathrm{d} - \partial) + 6 \sum_{\mathrm{d} \mid D} \mathrm{d} \\
&= 6 \sum_{\substack{\partial \mathrm{d} = D \\ 0 < \partial < \mathrm{d}}} (\mathrm{d} - \partial) + 6 \sum_{\substack{\mathrm{d} \mid D \\ 0 < \mathrm{d} < \sqrt{D}}} \mathrm{d} + 6 \sum_{\substack{\mathrm{d} \mid D \\ \sqrt{D} < \mathrm{d}}} \mathrm{d} + 6 \sum_{\substack{\mathrm{d} \mid D \\ \mathrm{d} = \sqrt{D}}} \mathrm{d}
\end{aligned}$$

$$\geqslant 6 \sum_{\substack{\partial \mathrm{d}=D \\ 0<\partial<\mathrm{d}}} (\mathrm{d}-\partial) + 6 \sum_{\substack{\mathrm{d}|D \\ 0<\mathrm{d}<\sqrt{D}}} \mathrm{d} + 6 \sum_{\substack{\mathrm{d}|D \\ \sqrt{D}<\mathrm{d}}} \mathrm{d}$$

$$= 6 \sum_{\substack{\partial \mathrm{d}=D \\ 0<\partial<\mathrm{d}}} 2\mathrm{d}$$

$\geqslant 12D$ as $\mathrm{d} = D$ is always included in the summation.

We now examine when equality holds.
($\Rightarrow$) Suppose $\mathrm{Cl}_c(D) = 12D$, then equality holds throughout above. This means D cannot be a perfect square. It also implies $6 \sum_{\substack{\partial \mathrm{d}=D \\ 0<\partial<\mathrm{d}}} 2\mathrm{d} = 12D$ and so the only divisor we may sum over is $\mathrm{d} = D$ itself. Therefore D is prime.
($\Leftarrow$) Suppose D is prime, it is straightforward to check equality holds throughout our application of Theorem 4.4.3, thus $\mathrm{Cl}_c(D) = 12D$. □

Corollary 4.5.5.
The proper class number satisfies $\mathrm{Cl}_+(D) \geqslant 2D$.

Proof.
Applying Lemmas 4.5.3 and 4.5.4 we get $12D \leqslant \mathrm{Cl}_c(D) \leqslant 6\mathrm{Cl}_+(D)$. Hence $2D \leqslant \mathrm{Cl}_+(D)$. □

Theorem 4.5.6.
The proper class number satisfies $\mathrm{Cl}_+(D) = 2D$ *if and only if* D *is a prime and* $D \equiv 11 \bmod 12$.

Proof.
From Corollary 4.5.5 we have $\mathrm{Cl}_+(D) \geqslant 2D$.
($\Rightarrow$) Assume $\mathrm{Cl}_+(D) = 2D$, then equality must hold throughout the proof of Corollary 4.5.5. Thus Lemma 4.5.4 yields D is prime and Lemma 4.5.3 implies there are no proper automorphs for any bilinear form with determinant D. Therefore D must be a prime such that D does not fall into one of the first four rows of Summary 2.3. Thus D is a prime and cannot be written as either $D = A_{11}^2$, $D = 3A_{11}^2$, $D = A_{11}^2 + A_{12}^2$, or $D = (A_{12} + A_{21})^2 - A_{12}A_{21} = A_{12}^2 + A_{12}A_{21} + A_{21}^2$.
Clearly, D being prime and $D = A_{11}^2$ or $D = 3A_{11}^2$ is an impossibility except when $D = 3$. Further, a prime p may be expressed as a sum of two integer squares if and only if $p \equiv 1 \bmod 4$ ("*Fermat's Theorem on Sums of Two Squares*", see [Za1990]). Therefore we must have $D = 2$, $D = 3$ or $D \equiv 3 \bmod 4$.
Next, Theorem 4.5.2 implies a prime D such that $D = A_{12}^2 + A_{12}A_{21} + A_{21}^2$ occurs if and only if $D = 3$ or $D \equiv 1 \bmod 3$. However, the only way to write $D = 3$ as $D = A_{12}^2 + A_{12}A_{21} + A_{21}^2$ is using $A_{12} = A_{21} = 1$. This breaks the condition found in row three of Summary 2.3 for a proper automorph to exist. Therefore $D = 3$ is a special case to be checked; from Example 2.4.40 we see $\mathrm{Cl}_+(3) = 8 = 2 \cdot D + 2$. Thus we must have $D \equiv 2 \bmod 3$. Using this along with $D = 2$ or $D \equiv 3 \bmod 4$ implies $D = 2$ or $D \equiv 11 \bmod 12$. Example 2.4.39 shows $\mathrm{Cl}_+(2) = 5 = 2 \cdot D + 1$ and hence we must have $D \equiv 11 \bmod 12$.

($\Leftarrow$) Assume D is a prime number such that $D \equiv 11 \bmod 12$. Then any reduced bilinear form with this determinant, cannot fall into one of the first four rows of Summary 2.3. This is because the first row requires $D \equiv 1 \bmod 4$ or $D = 2$, the third requires $D \equiv 1 \bmod 3$ or $D = 3$, and the second and fourth imply D is not prime. Therefore there are no proper automorphs and thus every proper equivalence class contains exactly six complete equivalence classes. Hence $\mathrm{Cl}_c(D) = 6\mathrm{Cl}_+(D)$. Since D is prime, Lemma 4.5.4 yields $12D = \mathrm{Cl}_c(D)$ and thus we have $\mathrm{Cl}_+(D) = 2D$. □

We now develop a couple of well-known results in order to easily explore the proper class number via Theorem 4.4.3.

Theorem 4.5.7 (Ireland & Rosen Proposition 17.6.1)**.**
Let n be a positive integer, then the number of integral solutions (x, y), $x > 0$, $y \geqslant 0$ to the equation $x^2 + y^2 = n$ is $\sum_{d|n} \chi(d)$, where $\chi(d) = \begin{cases} 1 & \text{if } d \equiv 1 \bmod 4 \\ 0 & \text{if } d \equiv 0 \bmod 2 \\ -1 & \text{if } d \equiv 3 \bmod 4. \end{cases}$

Proof.
See Theorem A.1.9 or Ireland & Rosen pages 279-280, [IR1990]. □

Corollary 4.5.8.
The number of integral solutions (x, y), $x > 0$, $y \in \mathbb{Z}$ to the equation $x^2 + y^2 = n$ is given by

$$\begin{cases} 2\big(\sum_{d|n} \chi(d)\big) - 1 & \text{if } n \text{ is a perfect square} \\ 2\sum_{d|n} \chi(d) & \text{otherwise.} \end{cases}$$

Proof.
First suppose n is not a perfect square, thus $\neq x^2 + 0^2$ so $y \neq 0$. Let (x, y) be a solution to $n = x^2 + y^2$ with $x > 0$, $y > 0$. Then the map $(x, y) \mapsto (x, -y)$ is a bijection between this set and the set of solutions where $x > 0$ and $y < 0$. Hence when n is not a perfect square, we apply Theorem 4.5.7 to get the number of integral solutions is $2\sum_{d|n} \chi(d)$.
Now suppose n is a perfect square. Observe the only solution for which $y = 0$ is the solution $(\sqrt{n}, 0)$ as we are restricting to $x > 0$. Therefore, all other solutions have $y \neq 0$ and we may apply the same argument as in the case where n is not a perfect square. Under this counting argument we will have counted $(\sqrt{n}, 0)$ twice and so we get the number of integral solutions is just $2\big(\sum_{d|n} \chi(d)\big) - 1$. □

We now show χ is a multiplicative function.

Lemma 4.5.9.
Let $m, n \in \mathbb{Z}$ then $\chi(mn) = \chi(m)\chi(n)$.

Proof.
Let $m, n \in \mathbb{Z}$ and consider the integral function χ as defined in Theorem 4.5.7. Clearly if $2|mn$ then $2|m$ or $2|n$ (or both). Consequently $\chi(mn) = 0 = \chi(m)\chi(n)$.
Now suppose $mn \equiv 1 \bmod 4$. Then it follows $m \equiv n \bmod 4$ and thus $\chi(m) = \chi(n)$. Hence $\chi(mn) = 1 = \chi(m)\chi(n)$.
Lastly, if $mn \equiv 3 \bmod 4$ then $2 \nmid m$, $2 \nmid n$ and $m \not\equiv n \bmod 4$. Hence $\chi(m) \neq \chi(n)$ and thus $\chi(mn) = -1 = \chi(m)\chi(n)$.
Hence it follows that χ is a multiplicative function. □

Our next result is a rephrasing of LeVeque's Theorem 1-6. Note that LeVeque uses proper to mean $\gcd(x, y) = 1$.

Theorem 4.5.10 (LeVeque Theorem 1-6)**.**
Let $\omega(f)$ be the number of automorphs [proper and improper] of $f = ax^2+bxy+cy^2$, an integral positive form of discriminant $\Delta = b^2 - 4ac$. Let n be a positive integer. Then the number of proper representations of n by f is $\omega(f)$ times the number of forms g that are equivalent to f. In particular, if there is only one class of discriminant Δ, the number of proper representations is $\omega(f)$ times the number of solutions to the congruence $m^2 \equiv -\Delta \bmod 4n$, $0 \leqslant m < 2n$.

Proof.
See LeVeque pages 20-21, [LeV1956]. □

We now introduce a definition and prove a theorem that is directly derived from LeVeque's result above.

Definition 4.5.11.
Let $N \in \mathbb{Z}_{>0}$ and write $N = 2^a \cdot 3^b \cdot \left(\prod_{i=1}^{r} p_i^{e_i}\right)\left(\prod_{j=1}^{s} q_j^{f_j}\right)$, where p_i, q_j are primes such that $p_i \equiv 1 \bmod 3$, $q_j \equiv 2 \bmod 3$.
We define the quantity n_N as follows:

$$n_N = \begin{cases} 2^r & \text{if } a = 0, 0 \leqslant b \leqslant 1, s = 0 \\ 0 & \text{otherwise.} \end{cases}$$

We present a quick proof that n_N is a multiplicative function.

Lemma 4.5.12.
The function n_N as defined in Theorem 4.5.13 is a multiplicative function.

Proof.
First observe $n_1 = 2^0 = 1$. Now let $a, b \in \mathbb{N}$ be such that $\gcd(a, b) = 1$. Then if $2 \mid a$ or $2 \mid b$ we get $n_{ab} = 0 = n_a \cdot n_b$. Also, if $9 \mid a$ or $9 \mid b$ then $9 \mid ab$ and we have $n_{ab} = 0 = n_a \cdot n_b$. Further, due to $\gcd(a, b) = 1$ we cannot have $9 \mid ab$ where $3 \mid a$ and $3 \mid b$. Now note if p_j is a prime such that $p_j \equiv 2 \bmod 3$ and it divides either a or b, then $p_j \mid ab$ and we have $n_{ab} = 0 = n_a \cdot n_b$.

Lastly, suppose $\gcd(a,b)=1$ and a, b are products of primes satisfying $p_i \equiv 1 \bmod 3$. Then $ab = p_{a_1}^{e_{a_1}} \cdots p_{a_k}^{e_{a_k}} p_{b_1}^{e_{b_1}} \cdots p_{b_n}^{e_{b_n}}$ and we have

$$\begin{aligned} n_{ab} &= 2^{e_{a_1}+\cdots+e_{a_k}+e_{b_1}+\cdots+e_{b_n}} \\ &= 2^{e_{a_1}+\cdots+e_{a_k}} \cdot 2^{e_{b_1}+\cdots+e_{b_n}} \\ &= n_a \cdot n_b. \end{aligned}$$

Hence n_N is a multiplicative function. □

Theorem 4.5.13.
Let $D \in \mathbb{Z}_{>0}$ and assume $D = x^2+xy+y^2$ for some $x, y \in \mathbb{Z}$, $(x,y) \neq (0,0)$. Then the number of representations of D in this manner is given by

$$\sum_{\substack{N=\frac{D}{a^2} \\ a>0, a^2 \mid D}} 6n_N,$$

where n_N is defined in Definition 4.5.11.

Proof.
Let D be as above and $(x,y) \neq (0,0)$ such that $D = x^2+xy+y^2$. Let $\gcd(x,y) = a \geqslant 1$, then $x = as$ and $y = at$ where $\gcd(s,t) = 1$. Thus $D = (as)^2 + (as)(at) + (at)^2 = a^2(s^2+st+t^2)$ and consequently (s,t) is a proper representation of $\frac{D}{a^2}$.
Theorem 4.5.10 informs us that the number of proper representations of a positive integer N as $N = s^2+st+t^2$ is six times the number of solutions to $m^2 \equiv -3 \bmod 4N$, $0 \leqslant m < 2N$. This is because the binary quadratic form x^2+xy+y^2 has six distinct automorphs, discriminant $b^2-4ac = -3$, and thus proper class number 1 (see Table B2, [Fl1989, p.194]). Let n_N be the number of such solutions. Then the number of representations (proper and improper) of D as x^2+xy+y^2 is given by

$$\sum_{\substack{N=\frac{D}{a^2} \\ a^2 \mid D}} 6n_N.$$

Thus we now let $N = \frac{D}{a^2}$ for some divisor $a \geqslant 1$ such that $a^2 \mid D$ and turn our attention to calculating n_N. Observe that N may or may not be square free depending on its prime factorisation. Also, note $N = 1$ is possible when D is a perfect square. Therefore we consider the equation $m^2 \equiv -3 \bmod 4N$ and for the moment we will ignore the condition $0 \leqslant m < 2N$.
Write $4N = 2^{e_2+2} \cdot 3^{e_3} \cdot \prod_{i=1}^{k} p_i^{e_i}$, where p_i is a prime such that $p_i > 3$, $e_i > 0$, and e_2, e_3 are non-negative. By the Chinese Remainder Theorem there is at least one solution to $m^2 \equiv -3 \bmod 4N$ if and only if there is at least one solution to each of

$$\begin{aligned} m^2 &\equiv -3 \bmod 2^{e_2+2} \\ m^2 &\equiv -3 \bmod 3^{e_3} \\ m^2 &\equiv -3 \bmod p_1^{e_1} \end{aligned}$$

$$\vdots$$
$$m^2 \equiv -3 \bmod p_k^{e_k}.$$

We first consider $m^2 \equiv -3 \bmod 2^{e_2+2}$ by examining $m^2 \equiv -3 \bmod 2$. This has a single solution, namely $m = 1, 0 \leqslant m < 2$. Now we utilise Hensel's Lemma with $f(x) = x^2 + 3$ and $p = 2$. We have $f(1) = 1^2 + 3 = 4 \equiv 0 \bmod 2$ and $f'(1) = 2 \cdot 1 \equiv 0 \bmod 2$. Thus $m = 1$ is not a simple root. We now consider $m^2 \equiv -3 \bmod 4$, $0 \leqslant m < 4$ and observe both $m = 1$ and $m = 3$ work. That is, $f(1) = 4 \equiv 0 \bmod 4$ and $f(3) = 12 \equiv 0 \bmod 4$, and further we have $f'(1) = 2 \equiv 0 \bmod 2$ and $f'(3) = 6 \equiv 0 \bmod 2$. Therefore we attempt to lift these two solutions to mod8. Consider $m^2 \equiv -3 \bmod 8$, $0 \leqslant m < 8$. We have $f(1) = f(5) = f(3) = f(7) \equiv 4 \bmod 8 \not\equiv 0 \bmod 8$ and therefore we cannot lift to a solution mod8. Consequently the equation $m^2 \equiv -3 \bmod 2^{e_2+2}$ will only have solutions when $e_2 = 0$. When $e_2 = 0$ there are precisely two solutions, namely $m = 1$ and $m = 3$. From this it follows that in order for there to be a solution to our system, we require $2 \nmid N$. Therefore $\gcd(4, N) = 1$.

Hence, by the Chinese Remainder Theorem it is sufficient to consider the number of solutions to $m^2 \equiv -3 \bmod N$ and then multiply our answer by 2 when $2 \nmid N$. Otherwise there are no solutions to the system.

Since we deduced $2 \nmid N$ we now consider $p = 3$. Then the equation $m^2 \equiv -3 \bmod 3^{e_3}$ has a solution if $e_1 = 1$ (only $m = 0$ works), and vacuously has a solution (the empty solution) if $e_3 = 0$. We now apply Hensel's Lemma to attempt to lift our solutions to mod9. We have $f(0) = 3 \equiv 3 \bmod 9 \not\equiv 0 \bmod 9$ and so we cannot lift our only solution. Hence the equation $m^2 \equiv -3 \bmod 3^{e_3}$ has a solution if and only if $e_3 = 0$ or $e_3 = 1$ and thus $9 \nmid N$.

Finally, let p_i be a prime such that $p_i > 3$ and consider $m^2 \equiv -3 \bmod p_i^{e_i}$. Since $p_i > 3$, Lemma 4.5.1 implies the equation $m^2 \equiv -3 \bmod p_i$ has a solution if and only if $p_i \equiv 1 \bmod 3$. Hence we require each p_i that divides N to satisfy $p_i \equiv 1 \bmod 3$ in order for a solution to our system to exist. Let m be such that $m^2 \equiv -3 \bmod p_i$, $0 \leqslant m < p_i$ and apply Hensel's Lemma with $f(x) = x^2 + 3$. We have $f(m) = m^2 + 3 \equiv 0 \bmod p_i$ and $m \neq 0$ else we have $-3 \equiv 0 \bmod p_i$, contradicting $p_i > 3$. Thus $f'(m) = 2 \cdot m \equiv (2 \bmod p_i)(m \bmod p_i) \not\equiv 0 \bmod p_i$ as $2 \not\equiv 0 \bmod p_i$ and $0 < m < p$. Thus by Hensel's Lemma we will have a solution to $m^2 \equiv -3 \bmod p_i^{e_i}$ for any $e_i > 0$. However, we note $p_i - m$ is also a solution to $m^2 \equiv -3 \bmod p_i$. Applying Hensel's Lemma we have $f'(p_i - m) = 2p_i - 2m \equiv -2m \bmod p_i \not\equiv 0 \bmod p_i$ as we observed already $2m \not\equiv 0 \bmod p_i$. Hence this solution is also lifted to solutions for $m^2 \equiv -3 \bmod p_i^{e_i}$. Therefore we will have 2 solutions to $m^2 \equiv -3 \bmod p_i^{e_i}$ whenever $p_1 \equiv 1 \bmod 3$.

Consequently we have $2^{\#p_i \equiv 1 \bmod 3}$ solutions to $m^2 \equiv -3 \bmod N$ if and only if N has no prime divisors $p_i \equiv 2 \bmod 3$, $2 \nmid N$ and $9 \nmid N$. Otherwise there are no solutions.

We now reinstate the condition $0 \leqslant m < 2N$ and note that all solutions m we have found so far satisfy $0 \leqslant m < N$. Observe that we may obtain another solution by adding N to m since $(N + m)^2 = N^2 + 2Nm + m^2 \equiv -3 \bmod N$. Further, this new solution satisfies $N \leqslant N + m < 2N$ by construction. Therefore each solution m such that $0 \leqslant m < N$ produces another solution k in the range $N \leqslant k < 2N$. By the reverse logic, any solution k such that $k^2 \equiv -3 \bmod N$ where $N \leqslant k < 2N$ can

produce a solution m where $0 \leqslant m < N$. Therefore there are $2 \cdot 2^{\#p_i \equiv 1 \bmod 3}$ solutions to $m^2 \equiv -3 \bmod N$, $0 \leqslant m < 2N$.
Finally we use the Chinese Remainder Theorem to consider the number of solutions to $m^2 \equiv -3 \bmod 4N$ where $0 \leqslant m < 2N$. This equation immediately implies m must be odd. Therefore since we deduced $2 \nmid N$ in order for solutions to exist to $m^2 \equiv -3 \bmod N$, we see that the solutions to $m^2 \equiv -3 \bmod 4N$ are precisely the odd solutions to $m^2 \equiv -3 \bmod N$. Since $2 \nmid N$ and m is odd, it follows that only one of m, $N + m$ is odd and therefore exactly half of the solutions to $m^2 \equiv -3 \bmod N$, $0 \leqslant m < 2N$ are solutions to $m^2 \equiv -3 \bmod 4N$, $0 \leqslant m < 2N$.
Hence the number of solutions to $m^2 \equiv -3 \bmod 4N$, $0 \leqslant m < 2N$ is given by n_N where n_N is as defined in Definition 4.5.11.
This completes the proof. □

Our goal now is to determine a formula for the proper class number for positive definite bilinear forms of determinant $D > 0$. We let $D \in \mathbb{Z}_{>0}$ and assume we know the prime factorisation for D. Then we can use Theorem 4.4.3 to compute $\mathrm{Cl}_c(D)$ directly. However, we also know every proper equivalence class contains a unique reduced positive definite bilinear form and that the proper equivalence class of such a bilinear form contains exactly six complete equivalence classes unless the reduced bilinear form has a non-trivial proper automorph. Thus we let u_1, u_2, u_3 and u_4 denote the number of reduced bilinear forms with automorphs in rows 1 through 4 of Summary 2.3 for a given determinant D. Then we have

$$\mathrm{Cl}_c(D) = 6\left[\mathrm{Cl}_+(D) - u_1 - u_2 - u_3 - u_4\right] + 3(u_1 + u_2) + 2(u_3 + u_4).$$

This is because only bilinear forms in rows 1 through 4 do not have 6 complete equivalence classes within their proper equivalence class, and every proper equivalence class contains a unique reduced bilinear form. Thus we multiply $\mathrm{Cl}_+(D)$ by 6 and subtract multiples of 6 for those reduced bilinear forms having a non-trivial proper automorph. Lastly, we add on the correct number of complete equivalence classes within the respective proper equivalence class, based upon our results in Summary 2.3.
Rearranging this equation then yields

$$6\mathrm{Cl}_+(D) = \mathrm{Cl}_c(D) + 3(u_1 + u_2) + 4(u_3 + u_4). \tag{4.1}$$

We now demonstrate how to count the quantities $u_1 + u_2$ and $u_3 + u_4$.

Lemma 4.5.14.
The number of positive definite reduced bilinear forms of determinant $D > 0$ having a non-trivial proper automorph in either row 1 or row 2 of Summary 2.3 is given by

$$u_1 + u_2 = \begin{cases} 2\big(\sum_{d|D} \chi(d)\big) - 1 & \text{if } D = k^2 \\ 2\sum_{d|D} \chi(d) & \text{if } D \neq k^2. \end{cases}$$

Proof.
We need to investigate those positive definite reduced bilinear forms which look like $\begin{pmatrix} x & y \\ -y & x \end{pmatrix}$ where $x > 0$. When $y \neq 0$ we have a row 1 bilinear form and when $y = 0$ we have a row 2 bilinear form. Observe that there cannot be a bilinear form which lies in both row 1 and row 2. Further, the determinant of these bilinear forms is $D = x^2 + y^2$ where $y = 0$ is permitted. By Corollary 4.5.8 we get our result. □

The next two lemmas will yield useful results about the quantity $u_1 + u_2$.

Lemma 4.5.15.
Let $D > 0$ be an integer and χ be defined as in Theorem 4.5.7. Then $\sum_{d|D} \chi(d) \geqslant 0$.

Proof.
It is straightforward to observe χ is a (completely) multiplicative function on the integers. Consequently it follows that $g(n) = \sum_{d|n} \chi(d)$ is a multiplicative function as well.
Let $D \in \mathbb{Z}_{>0}$ and write $D = 2_0^e p_1^{e_1} \cdots p_k^{e_k}$ where $e_0 \geqslant 0$ and $e_i \geqslant 1$. Then

$$\sum_{d|D} \chi(d) = \left(\sum_{d|2^{e_0}} \chi(d) \right) \left(\sum_{d|p_1^{e_1}} \chi(d) \right) \cdots \left(\sum_{d|p_k^{e_k}} \chi(d) \right). \tag{4.2}$$

We observe

$$\sum_{d|2^{e_0}} \chi(d) = 1 \text{ as only } d = 1 \text{ is not divisible by } 2$$

$$\sum_{d|p_i^{e_i}} \chi(d) = \begin{cases} e_i + 1 & \text{if } p_i \equiv 1 \bmod 4 \text{ as all divisors are } 1 \bmod 4 \\ 1 & \text{if } p_i \equiv 3 \bmod 4 \text{ and } e_i \equiv 0 \bmod 2 \\ 0 & \text{if } p_i \equiv 3 \bmod 4 \text{ and } e_i \equiv 1 \bmod 2. \end{cases}$$

Hence we see $\sum_{d|D} \chi(D) \geqslant 0$. □

Lemma 4.5.16.
Let $D > 0$ be an integer and χ be defined as in Theorem 4.5.7. Then $\sum_{d|D} \chi(d)$ is odd if and only if D is a perfect square or two times a perfect square.

Proof.
From Lemma 4.5.15 we may write $D = 2_0^e p_1^{e_1} \cdots p_k^{e_k}$ and thus

$$\sum_{d|D} \chi(d) = \left(\sum_{d|2^{e_0}} \chi(d) \right) \left(\sum_{d|p_1^{e_1}} \chi(d) \right) \cdots \left(\sum_{d|p_k^{e_k}} \chi(d). \right).$$

Then clearly we cannot have any odd powers of primes congruent to 3 mod 4 else the sum is zero. Similarly, we require all primes $p_i \equiv 1 \bmod 4$ to satisfy $e_i + 1 \equiv 1 \bmod 2$.

Thus $e_i \equiv 0 \bmod 2$. Thus we cannot have any odd powers of primes congruent to 1 mod 4.
Consequently $D = k^2$ or $D = 2k^2$ as powers of 2 make no difference to the summation. □

We now investigate the quantity $u_3 + u_4$ in a similar manner.

Lemma 4.5.17.
The number of positive definite reduced bilinear forms of determinant $D > 0$ having a non-trivial proper automorph in either row 3 or row 4 of Summary 2.3 is given by

$$u_3 + u_4 = \begin{cases} \big(\sum\limits_{\substack{N=\frac{D}{a^2} \\ a>0}} 3n_N \big) - 1 & \text{if } D = k^2 \\ \sum\limits_{\substack{N=\frac{D}{a^2} \\ a>0}} 3n_N & \text{if } D \neq k^2. \end{cases}$$

Proof.
We need to investigate those positive definite reduced bilinear forms that look like $\begin{pmatrix} x+y & x \\ y & x+y \end{pmatrix}$ where $x + y > 0$. When $x = y$ we have a row 4 automorph, otherwise we have a row 3 automorph. Observe these bilinear forms have determinant $D = (x+y)^2 - xy = x^2 + xy + y^2$. By Theorem 4.5.13 there are $\sum\limits_{\substack{N=\frac{D}{a^2} \\ a>0}} 6n_N$ ways to do this with $(x, y) \neq (0, 0)$. Therefore if $x + y \neq 0$, that is $D \neq k^2$, then exactly half of the solutions satisfy $x + y > 0$ while the remainder satisfy $x + y < 0$. Therefore $u_3 + u_4 = \sum\limits_{\substack{N=\frac{D}{a^2} \\ a>0}} 3n_N$ if D is not a perfect square.
Thus we now assume D is a perfect square and consequently we have the non-trivial solutions $(x, -x)$ and $(-x, x)$. These are counted by our summation and are the only pairs (x, y) that satisfy $x + y = 0$. However, we want only positive definite bilinear forms, so we must subtract two before applying the same argument as in the $D \neq k^2$ case. Hence when D is a perfect square we have $u_3 + u_4 = 3\big(\sum\limits_{\substack{N=\frac{D}{a^2} \\ a>0}} 3n_N \big) - 1$. □

We can now derive a formula for the proper class number for reduced positive definite bilinear forms with determinant D.

Theorem 4.5.18.
Let $D > 0$ be an integer. Then the number of proper equivalence classes of positive

definite bilinear forms with determinant D is given by

$$\mathrm{Cl}_+(D) = \begin{cases} \Psi(D) + \sigma(D) + \sum_{d|D} \chi(d) + 2 \sum_{\substack{N=\frac{D}{a^2} \\ a>0}} n_N & \text{if } D \neq k^2 \\ \Psi(D) + \sigma(D) + \sum_{d|D} \chi(d) + 2\big(\sum_{\substack{N=\frac{D}{a^2} \\ a>0}} n_N\big) - 1 & \text{if } D = k^2. \end{cases}$$

Proof.
We use Equation 4.1 and apply Lemmas 4.5.14 and 4.5.17 to get:

$$\begin{aligned} 6\mathrm{Cl}_+(D) = 6\mathrm{Cl}_+(D) &= \mathrm{Cl}_c(D) + 3(u_1+u_2) + 4(u_3+u_4). \\ &= \begin{cases} 6\Psi(D) + 6\sigma(D) + 3\cdot 2\sum_{d|D}\chi(d) + 4\cdot 3 \sum_{\substack{N=\frac{D}{a^2} \\ a>0}} n_N & \text{if } D \neq k^2 \\ 6\Psi(D) + 6\sigma(D) + 1 + & \\ 3\cdot\big(2\big(\sum_{d|D}\chi(d)\big) - 1\big) + 4\big(3\big(\sum_{\substack{N=\frac{D}{a^2} \\ a>0}} n_N\big) - 1\big) & \text{if } D = k^2 \end{cases} \\ &= \begin{cases} 6\Psi(D) + 6\sigma(D) + 6\sum_{d|D}\chi(d) + 6\cdot 2\sum_{\substack{N=\frac{D}{a^2} \\ a>0}} n_N & \text{if } D \neq k^2 \\ 6\Psi(D) + 6\sigma(D) + 6\sum_{d|D}\chi(d) + 6\cdot 2\big(\sum_{\substack{N=\frac{D}{a^2} \\ a>0}} n_N\big) - 6 & \text{if } D = k^2. \end{cases} \end{aligned}$$

Consequently,

$$\mathrm{Cl}_+(D) = \begin{cases} \Psi(D) + \sigma(D) + \sum_{d|D} \chi(d) + 2 \sum_{\substack{N=\frac{D}{a^2} \\ a>0}} n_N & \text{if } D \neq k^2 \\ \Psi(D) + \sigma(D) + \sum_{d|D} \chi(d) + 2\big(\sum_{\substack{N=\frac{D}{a^2} \\ a>0}} n_N\big) - 1 & \text{if } D = k^2. \end{cases}$$

□

Corollary 4.5.19.
The proper class number for positive definite bilinear forms of determinant D, $\mathrm{Cl}_+(D)$, is odd if and only if $D = 2k^2$ or $D = q^2$ where $k, q \in \mathbb{Z}$, $q \equiv 1 \bmod 2$.

Proof.
We split into two cases depending on whether or not D is a perfect square.
Case 1: $D \neq k^2$. Then Theorem 4.5.18 yields

$$\mathrm{Cl}_+(D) = \Psi(D) + \sigma(D) + \sum_{d|D} \chi(d) + 2 \sum_{\substack{N=\frac{D}{a^2} \\ a>0}} n_N$$

$$= 2 \sum_{\substack{\partial \mathrm{d} = D \\ 0 < \partial < \mathrm{d}}} \mathrm{d} + \sum_{d|D} \chi(d) + 2 \sum_{\substack{N = \frac{D}{a^2} \\ a > 0}} n_N.$$

Thus $\mathrm{Cl}_+(D) \equiv 1 \bmod 2$ if and only if $\sum_{d|D} \chi(D) \equiv 1 \bmod 2$. Applying Lemma 4.5.16 and recalling $D \neq k^2$, this is if and only if $D = 2k^2$.
Case 2: $D = k^2$. Then Theorem 4.5.18 yields

$$\begin{aligned} \mathrm{Cl}_+(D) &= \Psi(D) + \sigma(D) + \sum_{d|D} \chi(d) + 2\Big(\sum_{\substack{N = \frac{D}{a^2} \\ a > 0}} n_N \Big) - 1 \\ &= 2 \sum_{\substack{\partial \mathrm{d} = D \\ 0 < \partial < \mathrm{d}}} \mathrm{d} + \sqrt{D} + \sum_{d|D} \chi(d) + 2\Big(\sum_{\substack{N = \frac{D}{a^2} \\ a > 0}} n_N \Big) - 1. \end{aligned}$$

Since $D = k^2$ by Lemma 4.5.16 we know $\sum_{d|D} \chi(d) \equiv 1 \bmod 2$ and thus $\mathrm{Cl}_+(D) \equiv 1 \bmod 2$ if and only if $\sqrt{D} - 1 \equiv 0 \bmod 2$. Yet this is if and only if $\sqrt{D} \equiv 1 \bmod 2$ and hence $D = q^2$ for some $q \in \mathbb{Z}$ such that $q \equiv 1 \bmod 2$. □

Theorem 4.5.20.
Let D be an odd square then $\mathrm{Cl}_+(D) = 2D + L$ where $L \equiv 1 \bmod 4$.

Proof.
Let $D = q^2$ where $q \in \mathbb{Z}_{>0}$, $q \equiv 1 \bmod 2$. By Lemma 4.5.19 we know $\mathrm{Cl}_+(D)$ is odd and thus $L \equiv 1$ or $3 \bmod 4$. We examine the formula for $\mathrm{Cl}_+(D)$ given in Theorem 4.5.18.
Observe $\Psi(D) \equiv 0 \bmod 4$ since $D \equiv 1 \bmod 4$ implies $\partial \equiv \mathrm{d} \bmod 4$ and so $(\mathrm{d} - \partial) \equiv 0 \bmod 4$. Now write $D = \prod_{i=1}^{k} p_i^{e_i} \prod_{j=1}^{m} q_j^{f_j}$ where $p_i \equiv 1 \bmod 4$ and $q_j \equiv 3 \bmod 4$. Note each e_i and f_j is even because D is a square. We also note σ is a multiplicative function and thus

$$\sigma(D) = \prod_{i=1}^{n} \sigma\left(p_i^{e_i}\right) \prod_{j=1}^{m} \sigma\left(q_j^{f_j}\right).$$

Observe $\sigma\left(p_i^{e_i}\right) \equiv e_i + 1 \bmod 4$ since $p_i^{e_i} \equiv 1 \bmod 4$. Similarly, $\sigma\left(q_j^{f_j}\right) = 1$ because we have an alternating sequence of 1's and -1's, starting and finishing with 1. Hence

$$\begin{aligned} \sigma(D) &\equiv \prod_{i=1}^{n} (e_i + 1) \bmod 4 \\ &= \sum_{d|D} \chi(d) \bmod 4. \end{aligned}$$

This follows from Equation 4.2 found in Lemma 4.5.15.
Further, since $D = q^2$, by Lemma 4.5.16 we have $\sum_{d|D} \chi(d) \equiv 1 \bmod 2$ and thus $\sigma(D) + \sum_{d|D} \chi(d) \equiv 2 \bmod 4$.

Now consider the term $2\sum_{\substack{N=\frac{D}{a^2}\\ a>0}} n_N$. By the definition of n_N (see Definition 4.5.11) we know n_N is either 0 or a power of 2 unless $N = 1$ or $N = 3$. Consequently $2\sum_{\substack{N=\frac{D}{a^2}\\ a>0}} n_N \equiv 0 \bmod 4$ unless we have $N = 1$ or $N = 3$. In order to have $N = 1$ this means D is a square which we certainly have; while in order to have $N = 3$ this means $D = 3t^2$, which cannot happen as $D = q^2$. Therefore we deduce $2\sum_{\substack{N=\frac{D}{a^2}\\ a>0}} n_N \equiv 2 \bmod 4$.

Hence we deduce $\mathrm{Cl}_+(D) \equiv 2 + 2 - 1 = 3 \bmod 4$, where it is important to recall the -1 comes from D being square.
Since $D \equiv 1 \bmod 4$ and we are writing $\mathrm{Cl}_+(D) = 2D + L$, it follows that $2D + L \equiv 3 \bmod 4$ and therefore $L \equiv 1 \bmod 4$. □

Having demonstrated $\mathrm{Cl}_+(D) \geqslant 2D$ for all $D \in \mathbb{Z}_{>0}$, and derived a formula to compute the proper class number in terms of divisors of the determinant it is natural to ask what the next lower bounds are. We first investigate when $\mathrm{Cl}_+(D) = 2D + 1, 2D + 3, 2D + 5$ and $2D + 7$, and then prove three theorems to address $\mathrm{Cl}_+(D) = 2D + 2, 2D + 4$ and $2D + 6$. Observe the special cases of $D = 1$ and $D = 2$ have already been dealt with separately via Examples 2.4.38 and 2.4.39. In these two cases we have shown $\mathrm{Cl}_+(1) = 3 = 2D + 1$ and $\mathrm{Cl}_+(2) = 5 = 2D + 1$.

To streamline the proofs we will use Lemmas 4.5.14 and 4.5.17 to give a description for the number of non-trivial proper automorphs in the case where $D = p^2$, p a prime.

Lemma 4.5.21.
Let $D = p^2$ where p is prime. Consider the set of positive definite reduced bilinear forms with determinant $D = p^2$, then number of such bilinear forms having a non-trivial proper automorph is:

$$u_1 + u_2 + u_3 + u_4 = \begin{cases} 3 & \text{if } p = 2, 3 \text{ or } p \equiv 11 \bmod 12 \\ 7 & \text{if } p \equiv 5 \bmod 12 \\ 9 & \text{if } p \equiv 7 \bmod 12 \\ 13 & \text{if } p \equiv 1 \bmod 12. \end{cases}$$

Further,

$$3(u_1 + u_2) + 4(u_3 + u_4) = \begin{cases} 11 & \text{if } p = 2, 3 \text{ or } p \equiv 11 \bmod 12 \\ 23 & \text{if } p \equiv 5 \bmod 12 \\ 35 & \text{if } p \equiv 7 \bmod 12 \\ 47 & \text{if } p \equiv 1 \bmod 12. \end{cases}$$

Proof.
The number of reduced bilinear forms with non-trivial proper automorphs is given by $u_1 + u_2 + u_3 + u_4$, see Equation 4.1. We consider the primes mod12 and apply

Lemmas 4.5.14 and 4.5.17.
Observe

$$\chi(1)+\chi(p)+\chi(p^2)=\begin{cases}3 & \text{if } p\equiv 1 \bmod 4\\ 1 & \text{if } p\equiv 3 \bmod 4 \text{ or } p=2.\end{cases}$$

Case 1: $p=2$, then $u_1+u_2+u_3+u_4=2(\chi(1)+\chi(2)+\chi(4))-1+3(0+2^0)-1=3$.
Case 2: $p=3$, then $u_1+u_2+u_3+u_4=2\cdot 1-1+3(0+2^0)-1=3$.
Case 3: $p\equiv 11 \bmod 12$, then $p\equiv 3 \bmod 4$ and $p\equiv 2 \bmod 3$.
Hence $u_1+u_2+u_3+u_4=2\cdot 1-1+3(0+2^0)-1=3$.
Case 4: $p\equiv 5 \bmod 12$, then $p\equiv 1 \bmod 4$ and $p\equiv 2 \bmod 3$.
Hence $u_1+u_2+u_3+u_4=2\cdot 3-1+3(0+2^0)-1=7$.
Case 5: $p\equiv 7 \bmod 12$, then $p\equiv 3 \bmod 4$ and $p\equiv 1 \bmod 3$.
Hence $u_1+u_2+u_3+u_4=2\cdot 1-1+3(2^1+2^0)-1=9$.
Case 6: $p\equiv 1 \bmod 12$, then $p\equiv 1 \bmod 4$ and $p\equiv 1 \bmod 3$.
Hence $u_1+u_2+u_3+u_4=2\cdot 3-1+3(2^1+2^0)-1=13$.
This covers all possibilities for p being prime and hence we have our result.
Applying the same reasoning yields

$$3(u_1+u_2)+4(u_3+u_4)=\begin{cases}11 & \text{if } p=2,3 \text{ or } p\equiv 11 \bmod 12\\ 23 & \text{if } p\equiv 5 \bmod 12\\ 35 & \text{if } p\equiv 7 \bmod 12\\ 47 & \text{if } p\equiv 1 \bmod 12.\end{cases}$$

□

Theorem 4.5.22.
Assume $D=2k^2$ and $\mathrm{Cl}_+(D)=2D+L$ for some $k,L\in\mathbb{Z}_{>0}$, $k>1$. Then $k\leqslant\frac{L}{4}$. Further, if $k=1$ ($D=2$) then $\mathrm{Cl}_+(D)=2D+1$.

Proof.
First note by Corollary 4.5.19 that we must have $L\equiv 1 \bmod 2$
Now let $D=2k^2$, $k>1$ then by Theorem 4.5.18 we have

$$\mathrm{Cl}_+(D)=2D+2\sum_{\substack{0<\partial<\mathrm{d}<D\\ \partial\mathrm{d}=D}}\mathrm{d}+\sum_{d|D}\chi(d)+2\sum_{\substack{N=\frac{D}{a^2}\\ a>0}}n_N. \tag{4.3}$$

Observe $N=\frac{2k^2}{a^2}$ and so $2\mid N$ always. Hence $2\sum_{\substack{N=\frac{D}{a^2}\\ a>0}}n_N=0$. We also know $\sum_{d|D}\chi(d)\geqslant 0$, $2k\mid D$, and in particular $D>2k>\sqrt{2}k=\sqrt{D}$ as $k>1$. Thus $2\sum_{\substack{0<\partial<\mathrm{d}<D\\ \partial\mathrm{d}}}\mathrm{d}\geqslant 2k$.
Hence we have $2D+L=\mathrm{Cl}_+(D)\geqslant 2D+2(2k)$ and so $L\geqslant 4k$. That is, $1<k\leqslant\frac{L}{4}$.
Whereas if $k=1$ (i.e., $D=2$) then the first sum in 4.3 is empty and so $\mathrm{Cl}_+(D)=2D+\sum_{d|2}\chi(d)=2D+1$. □

Corollary 4.5.23.
Let $D = 2k^2$ then $\mathrm{Cl}_+(D) = 2D+1$ only when $D = 2$ and $\mathrm{Cl}_+(D) = 2D+L$ cannot occur for $L \in \{3,5,7\}$.

Proof.
From Theorem 4.5.22 we know when $k = 1$, $D = 2$ and $\mathrm{Cl}_+(D) = 2D+1$. Then observe for $L \in \{1,3,5,7\}$ we have $k \leqslant \frac{L}{4} < 2$. Thus we cannot have $D = 2k^2$ and $\mathrm{Cl}_+(D) = 2D+L$ for $L \in \{3,5,7\}$. □

Theorem 4.5.24.
Let $D = q^2$, $q \in \mathbb{Z}_{>0}$, $q \equiv 1 \bmod 2$ then there are no values of q such that $\mathrm{Cl}_+(q^2) = 2D+3$ or $2D+7$. Further, only $q = 1$ yields $\mathrm{Cl}_+(q^2) = 2D+1$ and only $q = 3$ yields $\mathrm{Cl}_+(q^2) = 2D+5$.

Proof.
First observe from Theorem 4.5.18 that $\mathrm{Cl}_+(1) = 3 = 2D+1$. Now let $D > 1$ and apply the theorem to get

$$2D + L = \mathrm{Cl}_+(D) = 2D + \sum_{\substack{0<\partial<\mathrm{d}<D \\ \partial\mathrm{d}=D}} + \sum_{d|D} \chi(d) + 2 \sum_{\substack{N=\frac{D}{a^2} \\ a>0}} n_N + q - 1. \tag{4.4}$$

We note that each of the summations is greater than or equal to 0.
We now examine $q-1$. For $L = 1$ we see $q - 1 > L$ for $q > 2$ and therefore only $q = 1$ is possible since q is odd. Thus only $q = 1$ satisfies $\mathrm{Cl}_+(q^2) = 2D+1$.
For $L = 3$ we see $q - 1 > 3$ for $q > 4$. Thus $q = 1$ or $q = 3$; however $q \neq 1$ by above so we consider $q = 3$. This is the same as $D = 9$ and applying Theorem 4.5.18 yields $\mathrm{Cl}_+(9) = 2D+5$. Hence no such q exists so that $\mathrm{Cl}_+(q^2) = 2D+5$.
For $L = 5$ we see $q - 1 > 5$ for $q > 6$. Thus $q = 1$, $q = 3$ or $q = 5$. By above we know $q \neq 1$ and $q = 3$ works. Applying Theorem 4.5.18 with $q = 5$ yields $\mathrm{Cl}_+(5^2) = 59 = 2D+9$.
Lastly, for $L = 7$ we see $q - 1 > 7$ for $q > 8$. Thus $q = 1$, $q = 3$, $q = 5$ or $q = 7$. By above we know only $q = 7$ is a possibility. Applying Theorem 4.5.18 yields $\mathrm{Cl}_+(49) = 111 = 2D+13$. Hence no such q exists. □

Corollary 4.5.25.
We have

$$\begin{aligned}
&\mathrm{Cl}_+(D) = 2D+1 \Leftrightarrow D = 1 \text{ or } D = 2 \\
&\mathrm{Cl}_+(D) \neq 2D+3 \\
&\mathrm{Cl}_+(D) = 2D+5 \Leftrightarrow D = 9 \\
&\mathrm{Cl}_+(D) \neq 2D+7.
\end{aligned}$$

Proof.
By Corollary 4.5.19 we have $\mathrm{Cl}_+(D)$ is odd if and only if either $D = 2k^2$ or $D = q^2$, $q \equiv 1 \bmod 2$. Applying Corollary 4.5.23 and Theorem 4.5.24 then gives the result. □

Theorem 4.5.26.
Let $D > 2$ be an integer. Then $\mathrm{Cl}_+(D) = 2D + 2$ if and only if D is a prime such that $D = 3$ or $D \equiv 5 \bmod 12$.

Proof.
($\Leftarrow$) Firstly, if $D = 3$ then Example 2.4.40 shows $\mathrm{Cl}_+(3) = 8 = 2 \cdot 3 + 2$. Thus assume D is a prime such that $D \equiv 5 \bmod 12$. We now examine Summary 2.3 for the existence of reduced bilinear forms with non-trivial proper automorphs. Since D is prime, we cannot have the second or fourth row. Since $D \equiv 5 \bmod 12$ implies $D \equiv 2 \bmod 3$ we cannot have the third row (see Theorem 4.5.2). Therefore if we have such an automorph, it comes from the first row. Therefore we may write $D = a^2 + b^2$ where $a > 0$, $b \neq 0$ and $a, b \in \mathbb{Z}$. By Lemma 4.5.8 there are four ways to do this because $D \equiv 5 \bmod 12$ implies $D \equiv 1 \bmod 4$ and so $\chi(1) = \chi(D) = 1$. Hence there four positive definite reduced bilinear forms with non-trivial (row 1) proper automorphs, each of which will contain three complete equivalence classes within their respective proper equivalence class. Therefore we have

$$\begin{aligned}\mathrm{Cl}_c(D) &= 6[\mathrm{Cl}_+(D) - 4] + 4 \cdot 3 \\ &= 6\mathrm{Cl}_+(D) - 12.\end{aligned}$$

By Lemma 4.5.4, D prime implies $12D = \mathrm{Cl}_c(D)$ and so $12D = 6\mathrm{Cl}_+(D) - 12$. Hence $\mathrm{Cl}_+(D) = 2D + 2$.

($\Rightarrow$) Assume $\mathrm{Cl}_+(D) = 2D + 2$, then $6\mathrm{Cl}_+(D) - 12 = 12D$. First suppose D is not a perfect square. Then by Lemma 4.5.4 we have $\mathrm{Cl}_c(D) \geqslant 12D$ with equality if and only if D is prime. Therefore if D is not prime then we have $\mathrm{Cl}_c(D) = 12 \sum_{\substack{\partial \mathrm{d} = D \\ 0 < \partial < \mathrm{d}}} \mathrm{d} > 12D + 12\sqrt{D}$ as there must exist a divisor x of D such that $\sqrt{D} < x < D$. Thus we have

$$6\mathrm{Cl}_+(D) - 12 = 12D < 12D + 12\sqrt{D} < \mathrm{Cl}_c(D) \leqslant 6\mathrm{Cl}_+(D).$$

However, this is a contradiction because D not prime implies $D > 3$ and thus $12\sqrt{D} > 12$. Therefore the interval $[6\mathrm{Cl}_+(D) - 12, 6\mathrm{Cl}_+(D)]$ contains the subinterval $[12D, \mathrm{Cl}_c(D)]$, which had width at least 13. Therefore D is either a prime or a perfect square.
Now assume $D = k^2$, then if $D = (pq)^2$ for some $p, q \in \mathbb{Z}_{>1}$, $p \neq q$, applying Lemma 4.5.4 we see $\mathrm{Cl}_c(D) = 12 \sum_{\substack{\partial \mathrm{d} = D \\ 0 < \partial < \mathrm{d}}} \mathrm{d} + 6\sqrt{D} + 1 > 12D + 12\sqrt{D} + 6\sqrt{D} + 1$. This is because without loss of generality we may assume $p < q$ and we have $\sqrt{D} < pq^2 < D$, $pq^2 \mid D$. This implies

$$6\mathrm{Cl}_+(D) - 12 = 12D < 12D + 18\sqrt{D} + 1 < \mathrm{Cl}_c(D) \leqslant 6\mathrm{Cl}_+(D),$$

which is clearly a contradiction as $D > 2$. Therefore if D is a perfect square then $D = p^2$, where p is a prime. In this situation Lemma 4.5.4 implies Kronecker's

complete class number formula is $\mathrm{Cl}_c(D) = 12D + 6\sqrt{D} + 1$ and we apply Lemma 4.5.21 to this result. Thus

$$\begin{aligned} 6\mathrm{Cl}_+(D) - 12 &= 12D \\ &< 12D + 6\sqrt{D} + 1 \\ &= \mathrm{Cl}_c(D) \\ &= 6\mathrm{Cl}_+(D) - 3(u_1 + u_2) - 4(u_3 + u_4) \leqslant 6\mathrm{Cl}_+(D) - 11. \end{aligned}$$

Observe we have an immediate contradiction when the last inequality is strict. That is we have a contradiction unless $p = 2, 3$ or $p \equiv 11 \bmod 12$. However, if $p = 2$, $p = 3$ or $p \equiv 11 \bmod 12$ then $12D + 6\sqrt{D} + 1 \geqslant 12D + 6 \cdot 2 + 1 = 12D + 13$, giving a contradiction. Thus $D \neq p^2$ and consequently D is a prime.
By Theorem 4.5.6 we know $D \not\equiv 11 \bmod 12$ since $\mathrm{Cl}_+(D) = 2D + 2 \neq 2D$. Further, $D > 2$ implies either $D = 3$, $D \equiv 5 \bmod 12$, or $D \equiv 1 \bmod 3$. From Example 2.4.40 we know $\mathrm{Cl}_+(3) = 2 \cdot 3 + 2$. Thus we may assume $D > 3$. Now assume $D \equiv 1 \bmod 3$. Then $u_3 + u_4 > 0$ and we calculate its value via Lemma 4.5.17. We have $u_3 + u_4 = 6 \sum_{\substack{N = \frac{D}{a^2} \\ a > 0}} n_N = 6(n_D + n_1) = 6(2^1 + 2^0) = 18$. Thus we get $6\mathrm{Cl}_+(D) - 12 = 12D = \mathrm{Cl}_c(D) = 6\mathrm{Cl}_+(D) - 3(u_1 + u_2) - 18$ which is clearly a contradiction as $u_1 + u_2 \geqslant 0$. Therefore $D > 3$ and prime implies $D \equiv 2 \bmod 3$ and so either $D \equiv 5 \bmod 12$ or $D \equiv 11 \bmod 12$. Yet we have ruled out $D \equiv 11 \bmod 12$ and so it follows that $D \equiv 5 \bmod 12$.

□

Theorem 4.5.27.
Let D be an integer such that $D > 2$. Then $\mathrm{Cl}_+(D) = 2D + 4$ if and only if $D = 4$ or D is a prime such that $D \equiv 7 \bmod 12$.

Proof.
($\Leftarrow$) Firstly, if $D = 4$ the Example 2.4.41 shows $\mathrm{Cl}_+(4) = 12 = 2 \cdot 4 + 4$. Thus assume D is a prime such that $D \equiv 7 \bmod 12$ and thus $D \equiv 3 \bmod 4$. We examine Summary 2.3 for the existence of reduced bilinear forms with non-trivial proper automorphs. Since D is prime, we cannot have the second or fourth row. Since $D \equiv 3 \bmod 4$, Corollary 4.5.8 implies there are no row 1 automorphs and so only row 3 remains. By Theorem 4.5.13 there are $6n_D$ ways to do this, and we have $n_D = 1$ because D is a prime such that $D \equiv 3 \bmod 4$. Hence since D is prime we have $12D = \mathrm{Cl}_c(()\, D) = 6[\mathrm{Cl}_+(D) - 6] + 6 \cdot 2 = 6\mathrm{Cl}_+(D) - 24$. Thus $\mathrm{Cl}_+(D) = 2D + 4$.

($\Rightarrow$) Assume $\mathrm{Cl}_+(D) = 2D + 4$ which, implies $6\mathrm{Cl}_+(D) - 24 = 12D$. First suppose D is not a perfect square or a prime. Then we have $\mathrm{Cl}_c(D) = 12 \sum_{\substack{\partial \mathrm{d} = D \\ 0 < \partial < \mathrm{d}}} \mathrm{d} > 12D + 12\sqrt{D} > 12D + 24$ since $D > 2$ and not a perfect square or prime implies $D > 5$. Thus $\mathrm{Cl}_c(D) \geqslant 12D + 25$ and we get

$$6\mathrm{Cl}_+(D) - 24 = 12D < 12D + 25 \leqslant \mathrm{Cl}_c(D) \leqslant 6\mathrm{Cl}_+(D).$$

This is a contradiction because it implies the interval $[6\mathrm{Cl}_+(D)-24, 6\mathrm{Cl}_+(D)]$ contains the subinterval $[12D, 12D+25]$. Therefore either D is a prime or a perfect square.
Suppose D is a perfect square, then if $D=(pq)^2$ where without loss of generality $1<p\leqslant q$, we have $\mathrm{Cl}_c(D)=12\sum_{\substack{\partial \mathrm{d}=D\\ 0<\partial<\mathrm{d}}}\mathrm{d}+6\sqrt{D}+1>12D+12\sqrt{D}+6\sqrt{D}+1\geqslant 12D+37$. This is because there exists at least one integer x such that $x\mid D$ and $\sqrt{D}<x<D$, and we use the fact $D\geqslant 4$ as D is a perfect square. Thus we have the following contradiction

$$6\mathrm{Cl}_+(D)-24=12D<12D+37\leqslant \mathrm{Cl}_c(D)\leqslant 6\mathrm{Cl}_+(D).$$

Therefore if D is a perfect square then $D=p^2$ where p is a prime. By Equation 4.1 we have $\mathrm{Cl}_c(D)=6\mathrm{Cl}_+(D)-3(u_1+u_2)-4(u_3+u_4)$ and thus we have

$$6\mathrm{Cl}_+(D)-24=12D<12D+6\sqrt{D}+1=\mathrm{Cl}_c(D)=6\mathrm{Cl}_+(D)-3(u_1+u_2)-4(u_3+u_4).$$

By Lemma 4.5.21 we have a contradiction unless $3(u_1+u_2)+4(u_3+u_4)=11$ or 23. Further, $3(u_1+u_2)+4(u_3+u_4)=23$ then $p\equiv 7 \bmod 12$ and thus $D\geqslant 49$. This implies the interval $[6\mathrm{Cl}_+(D)-24, 6\mathrm{Cl}_+(D)-23]$ contains the subinterval $[12D, 12D+43]$, which is a contradiction. So we have $6\mathrm{Cl}_+(D)-24=12D<12D+6\sqrt{D}+1=\mathrm{Cl}_c(D)=6\mathrm{Cl}_+(D)-11$ and in the same vein, this is a contradiction unless $D=4$. Therefore if D is a perfect square then $D=4$. In Example 2.4.41 we show directly $\mathrm{Cl}_+(4)=12=2\cdot 4+4$.
Thus we now are left with the case when D is a prime. By Theorems 4.5.6 and 4.5.26 we know that D must satisfy either $D\equiv 7 \bmod 12$ or $D\equiv 1 \bmod 12$. Suppose $D\equiv 1 \bmod 12$, then $D\equiv 1 \bmod 4$ and $D\equiv 1 \bmod 3$. Applying Lemmas 4.5.14 and 4.5.17 we see $3(u_1+u_2)+4(u_3+u_4)=3(2(\chi(1)+\chi(D)))+4(3n_D)=3\cdot 4+12\cdot 2=36$. Therefore we have the following contradiction:

$$6\mathrm{Cl}_+(D)-24=12D=\mathrm{Cl}_c(D)=6\mathrm{Cl}_+(D)-3(u_1+u_2)-4(u_3+u_4)=6\mathrm{Cl}_+(D)-36.$$

Hence D is a prime such that $D\equiv 7 \bmod 12$.
Thus we have show if $\mathrm{Cl}_+(D)=2\cdot D+4$ then either $D=4$ or D is a prime such that $D\equiv 7 \bmod 12$. □

Theorem 4.5.28.
Let D be an integer such that $D>2$. Then $\mathrm{Cl}_+(D)=2D+6$ if and only if $D=6$ or D is a prime such that $D\equiv 1 \bmod 12$.

Proof.
($\Leftarrow$) Firstly, if $D=6$ then Example 2.4.42 demonstrates $\mathrm{Cl}_+(6)=18=2\cdot 6+6$. Thus now suppose D is a prime such that $D\equiv 1 \bmod 12$. By Lemma 4.5.4 this implies $12D=\mathrm{Cl}_c(D)$. We now consider the existence of non-trivial proper automorphs. Since $D\equiv 1 \bmod 4$ and $D\equiv 1 \bmod 3$ we have both row 1 and row3 automorphs. By Equation 4.1, Lemma 4.5.14 and Lemma 4.5.17 we have

$$12D=\mathrm{Cl}_c(D)=6\mathrm{Cl}_+(D)-3(u_1+u_2)-4(u_3+u_4)=6\mathrm{Cl}_+(D)-36.$$

Hence $\mathrm{Cl}_+(D) = 2D + 6$.

($\Rightarrow$) Let $\mathrm{Cl}_+(D) = 2D + 6$, which implies $12D = 6\mathrm{Cl}_+(D) - 36$. First assume D is neither a perfect square nor a prime. Then $\mathrm{Cl}_c(D) = 12 \sum_{\substack{\partial \mathrm{d} = D \\ 0 < \partial < \mathrm{d}}} \mathrm{d} > 12D + 12\sqrt{D}$. Since D is not a perfect square nor a prime, it follows that either $D = 6$ or $D \geqslant 8$. The case $D = 6$ is examined in Example 2.4.42, where we have $\mathrm{Cl}_+(6) = 18 = 2 \cdot 6 + 6$. So we now suppose $D \geqslant 8$. In fact, if $D > 8$ then we have $6\mathrm{Cl}_+(D) - 36 = 12D < 12D + 12\sqrt{D} \leqslant \mathrm{Cl}_c(D) \leqslant 6\mathrm{Cl}_+(D)$, which is a contraction as $12D + 12\sqrt{D} > 12D + 37$ as we assume D is not a perfect square. Thus we consider $D = 8$ carefully by itself. We have $\mathrm{Cl}_c(8) \geqslant 12D + 12\sqrt{8} > 12D + 33$ and since $12 \mid \mathrm{Cl}_c(8)$ it follows that $12D + 36 \leqslant \mathrm{Cl}_c(8)$. By applying Lemmas 4.5.14 and 4.5.17 to Equation 4.1 we have $\mathrm{Cl}_c(8) = 6\mathrm{Cl}_+(8) - 3 \cdot 2 - 4 \cdot 0 = 6\mathrm{Cl}_+(8) - 6$. Therefore we get the following contradiction:

$$6\mathrm{Cl}_+(8) - 36 = 12D < 12D + 36 \leqslant \mathrm{Cl}_c(8) = 6\mathrm{Cl}_+(8) - 6.$$

Therefore if D is not a perfect square or prime then only $D = 6$ satisfies $\mathrm{Cl}_+(D) = 2D + 6$.
Now suppose D is a perfect square ,then if $D = (pq)^2$ where $1 < p \leqslant q$ we have $\mathrm{Cl}_c(D) \geqslant 12D + 12\sqrt{D} + 6\sqrt{D} + 1$ as there is a divisor x of D such that $\sqrt{D} < x < D$. Further, D is at least 16 and so we get the following contradiction:

$$6\mathrm{Cl}_+(D) - 36 = 12D < 12D + 73 \leqslant \mathrm{Cl}_c(D) \leqslant 6\mathrm{Cl}_+(D).$$

Therefore if D is a perfect square then $D = p^2$ where p is a prime. Then we have $6\mathrm{Cl}_+(D) - 36 = 12D < 12D + 6\sqrt{D} + 1 = \mathrm{Cl}_c(D) = 6\mathrm{Cl}_+(D) - 3(u_1 + u_2) - 4(u_3 + u_4)$. Applying Lemma 4.5.21 we see we have an immediate contradiction if $p \geqslant 5$. Further, we note that $p = 2$ ($D = 4$) has already been considered, thus only $p = 3$ ($D = 9$) remains. Applying Lemmas 4.5.14 and 4.5.17 along with Theorem 4.5.18 when $D = 9$ yields $\mathrm{Cl}_+(9) = 23 = 2 \cdot 9 + 5 \neq 2D + 6$. Thus D cannot be a perfect square and consequently is a prime.
Since D is a prime and we have already considered $D = 2, 3$ along with when $D \equiv 5, 7, 11 \bmod 12$, it immediately follows that D is a prime such that $D \equiv 1 \bmod 12$. $\square$

We now give an observation which demonstrates the utility of being able to calculate the complete class number via an independent method.

Observation 4.5.29.
Let $D = pq$ where $p < q$ are primes. Then D is not a perfect square. Apply Theorem 4.4.3 to get

$$\begin{aligned} \mathrm{Cl}_c(D) &= 6\Psi(D) + 6\sigma(D) \\ &= 6 \sum_{\substack{\partial \mathrm{d} = D \\ 0 < \partial < \mathrm{d}}} (\mathrm{d} - \partial) + 6 \sum_{\mathrm{d} \mid D} \mathrm{d} \end{aligned}$$

$$= 12 \sum_{\substack{\partial \mathrm{d} = D \\ 0 < \partial < \mathrm{d}}} \mathrm{d}.$$

However, we know $D = pq$ and so the divisors of D are 1, p, q, pq. Therefore $\mathrm{Cl}_c(D) = 12pq + 12q = 12D + 12q$. Hence if we know the complete class number for D, or have the time to calculate it via the computation of all positive definite reduced bilinear forms with determinant D, then we may recover q and thus p. That is, we have a method for factorising D in the case where $D = pq$, $p < q$ primes.

Remark 4.5.30.
Currently we have three independent ways to compute $\mathrm{Cl}_c(D)$ for any given positive integer D. The first method is to use Kronecker's formula found in Theorem 4.4.3. This method is efficient but relies upon knowing the factors of D. The second method is to compute the set of reduced bilinear forms with determinant D and then use our knowledge of non-trivial proper automorphs to recount the complete class number. This is currently a finite but lengthy process involving the bounds for A_{11}, A_{12}, A_{21} and A_{22} found in Lemmas 2.4.27 to 2.4.32.
Our third method comes from enumerating the sets B^0 and B^1 found in Theorem 3.1.29. It remains to calculate new bounds for A_{11}, A_{12}, A_{21} and A_{22} in this situation. Thus it may be more efficient to compute $\mathrm{Cl}_c(D)$ using the third method than second.

Having proven $\mathrm{Cl}_+(D) \geqslant 2D$ it is somewhat reasonable to investigate when $\mathrm{Cl}_+(D) = 3D$. This problem turns out to be trickier than hoped for, as the following two results demonstrate.

Lemma 4.5.31.
Assume $D = 1$, $D = 4$ or $D = 2p$ where p is a prime such that $p \equiv 3 \bmod 4$, then $\mathrm{Cl}_+(D) = 3D$.

Proof.
For $D = 1$ and $D = 4$ we calculated $\mathrm{Cl}_+(1) = 3$ and $\mathrm{Cl}_+(4) = 12$ respectively in Examples 2.4.38 and 2.4.41. So assume $D = 2p$ where p is a prime such that $p \equiv 3 \bmod 4$. Applying Theorem 4.5.18 we get

$$\begin{aligned}
\mathrm{Cl}_+(D) &= \mathrm{Cl}_+(2p) \\
&= \Psi(2p) + \sigma(2p) + \sum_{d \mid 2p} \chi(d) + 2 \sum_{\substack{N = \frac{2p}{a^2} \\ a > 0}} n_N \\
&= (2p-1) + (p-2) + 1 + 2 + p + 2p + \underbrace{\chi(1) + \chi(2) + \chi(p) + \chi(2p)}_{=0 \text{ as } p \equiv 3 \bmod 4} + 2n_{2p} \\
&= 6p - 3 + 3 + 2n_{2p} \\
&= 6p \text{ as } 2 \mid 2p \\
&= 3(2p) \\
&= 3D.
\end{aligned}$$

□

Attempting the converse however is much more difficult. It requires careful consideration of several cases. The following lemma is a partial result for the converse.

Lemma 4.5.32.
Assume D is a positive integer such that $\mathrm{Cl}_+(D) = 3D$. Then either $D = 1$, $D = 4$, or $D = 2p$ where p is a prime such that $p \equiv 3 \bmod 4$, or perhaps, $D = k^2$ where k is an odd composite integer.

Proof.
First suppose $D \neq k^2$, $D \neq 2k^2$ for some integer k. By Lemma 4.5.16 we know $\sum_{d|D} \chi(d)$ is even and we have

$$\begin{aligned} 3D = \mathrm{Cl}_+(D) &= \Psi(D) + \sigma(D) + \sum_{d|D} \chi(d) + 2 \sum_{\substack{N = \frac{D}{a^2} \\ a>0}} n_N \\ &= 2 \sum_{\substack{\partial \mathrm{d} = D \\ 0 < \partial < \mathrm{d}}} \mathrm{d} + \sum_{d|D} \chi(d) + 2 \sum_{\substack{N = \frac{D}{a^2} \\ a>0}} n_N. \end{aligned}$$

Thus it follows the right hand side of the above is even. Hence D must be even.
Then $D = 2q$ for some integer q and we have D, q are divisors of D such that D, $q > \sqrt{D}$. Thus $2 \sum_{\substack{\partial \mathrm{d} = D \\ 0 < \partial < \mathrm{d}}} \mathrm{d} \geqslant 2(D + q) = 2(D + \frac{D}{2}) = 3D$.
Consequently, in order to avoid a contradiction (as the left hand side is $3D$), we must have equality throughout. This is because $2 \sum_{\substack{N = \frac{D}{a^2} \\ a>0}} n_N \geqslant 0$ and we have shown in Lemma 4.5.15 that $\sum_{d|D} \chi(d) \geqslant 0$. Hence q must be a prime, else we would have more terms in $2 \sum_{\substack{\partial \mathrm{d} = D \\ 0 < \partial < \mathrm{d}}} \mathrm{d}$.
Since q is prime and we must have $\chi(1) + \chi(2) + \chi(q) + \chi(2q) = \sum_{d|D} \chi(d) = 0$, it follows that $\chi(q) = -1$ and thus $q \equiv 3 \bmod 4$. It is then straightforward to check $2 \sum_{\substack{N = \frac{D}{a^2} \\ a>0}} n_N = 2n_{2q} = 0$ as $2 \mid 2q$.
Therefore if $D \neq k^2$, $D \neq 2k^2$ and $\mathrm{Cl}_+(D) = 3D$ then $D = 2p$ where p is a prime such that $p \equiv 3 \bmod 4$.
Now suppose $D = 2k^2$ for some integer k. By Lemma 4.5.16 it follows that $\sum_{d|D} \chi(d)$ is odd and we have

$$3D = \mathrm{Cl}_+(D) = 2 \sum_{\substack{\partial \mathrm{d} = D \\ 0 < \partial < \mathrm{d}}} \mathrm{d} + \sum_{d|D} \chi(d) + 2 \sum_{\substack{N = \frac{D}{a^2} \\ a>0}} n_N.$$

Observe since $D = 2k^2$, the left hand side is even, whilst $\sum_{d|D} \chi(d)$ being odd makes the right hand side odd. This is a contradiction. Hence $D \neq 2k^2$.
Lastly suppose $D = k^2$. We already know by direct calculation that $\mathrm{Cl}_+(1) = 3$ and $\mathrm{Cl}_+(4) = 12$. Therefore we will assume $k \geqslant 3$. Lemma 4.5.16 implies $\sum_{d|D} \chi(d)$ is odd and applying Theorem 4.5.18 we get

$$\begin{aligned} 3D = \mathrm{Cl}_+(D) &= \Psi(D) + \sigma(D) + \sum_{d|D} \chi(d) + 2\Big(\sum_{\substack{N=\frac{D}{a^2} \\ a>0}} n_N \Big) - 1 \\ &= 2 \sum_{\substack{\partial \mathrm{d} + d \\ 0<\partial<\mathrm{d}}} \mathrm{d} + \sqrt{D} + \sum_{d|D} \chi(d) + 2\Big(\sum_{\substack{N=\frac{D}{a^2} \\ a>0}} n_N \Big) - 1. \end{aligned}$$

We split into two cases according to whether k is odd or even.
Case 1: k is even.
Write $k = 2j$ and thus $D = 4j^2$. Observe both D and $\frac{D}{2} = 2j^2$ are divisors of D that are larger than $\sqrt{D}$ and hence we have $2 \sum_{\substack{\partial \mathrm{d} = D \\ 0<\partial<\mathrm{d}}} \mathrm{d} \geqslant 2(D + \frac{D}{2}) = 3D$. Therefore we have a contradiction because $\sqrt{D} - 1 \; 1$ (since $D = k^2$, $k > 2$), $\sum_{d|D} \chi(d) \geqslant 0$ and $2 \sum_{\substack{N=\frac{D}{a^2} \\ a>0}} n_N \geqslant 0$.
Thus k must be odd.
Case 2: k is odd.
Suppose further that k is a prime. Then it follows that $2 \sum_{\substack{\partial \mathrm{d} = D \\ 0<\partial<\mathrm{d}}} \mathrm{d} = 2D$. Thus we wish to show $D \neq \sqrt{D} + \sum_{d|D} \chi(d) + 2\Big(\sum_{\substack{N=\frac{D}{a^2} \\ a>0}} n_N \Big) - 1$. We examine the two summations separately. We have

$$\begin{aligned} \sum_{d|D} \chi(d) &= \chi(1) + \chi(k) + \chi(k^2) \\ &= \begin{cases} 3 & \text{if } k \equiv 1 \bmod 4 \\ 1 & \text{if } k \equiv 3 \bmod 4. \end{cases} \end{aligned}$$

Similarly we have

$$\begin{aligned} 2 \sum_{\substack{N=\frac{D}{a^2} \\ a>0}} n_N &= 2(n_{k^2} + n_1) \\ &= \begin{cases} 2 & \text{if } k = 3 \text{ as } n_9 = 0 \\ 2 & \text{if } k \equiv 2 \bmod 3 \\ 6 & \text{if } k \equiv 1 \bmod 3. \end{cases} \end{aligned}$$

Combining these two results together yields

$$\sqrt{D}+\sum_{d|D}\chi(d)+2\Big(\sum_{\substack{N=\frac{D}{a^2}\\ a>0}}n_N\Big)-1=\begin{cases}5 & \text{if } k=3\\ k+4 & \text{if } k\equiv 5 \bmod 12\\ k+8 & \text{if } k\equiv 1 \bmod 12\\ k+2 & \text{if } k\equiv 11 \bmod 12\\ k+6 & \text{if } k\equiv 7 \bmod 12.\end{cases}$$

In each case, setting it equal to $D=k^2$ and solving the resulting quadratic never yields an integer value greater than or equal to 3 for k. Hence we deduce if $D=k^2$ and $\mathrm{Cl}_+(D)=3D$ then either $D=1$, $D=4$, or perhaps $D=k^2$ where k is an odd composite integer. □

Observation 4.5.33.
At this stage in time I am unable to rule out the case $D=k^2$ where k is an odd composite integer. This is despite numerical evidence suggesting that this case should not arise. This case is particularly difficult to prove because one can find values for k where $\mathrm{Cl}_+(k^2)>3k^2$, but also find (many) values for k where $\mathrm{Cl}_+(k^2)<3k^2$. In general, the more distinct prime factors k has, the more likely it is that $\mathrm{Cl}_+(k^2)>3k^2$.

Notes on Section 4.5

This section is not found in [Kr1897] or [We1974].

4.6 Determining values for $\overline{P_0}$, $\overline{Q_0}$, $\overline{R_0}$ and $\overline{S_0}$

We now return our attention to determining values for $\overline{P_0}$, $\overline{Q_0}$, $\overline{R_0}$ and $\overline{S_0}$. We will do this in an analogous way to that of Section 4.3.
Recall the sets $\overline{I_{0,=}}$ and $\overline{I_{1,=}}$ from Definition 3.5.1:

$$\begin{aligned}\overline{I_{0,=}}=\{(A_{11},A_{11},A_{21},A_{22})\mid{}&\det(A)=D,-A_{11}<A_{21}\leqslant A_{11},\\ &A_{11}+A_{22}\equiv 1 \bmod 2, A_{11}+A_{21}\equiv 0 \bmod 2\},\\ \overline{I_{1,=}}=\{(A_{11},A_{11},A_{21},A_{22})\mid{}&\det(A)=D,-A_{11}\leqslant A_{21}<A_{11},\\ &A_{11}+A_{22}\equiv 1 \bmod 2, A_{11}+A_{21}\equiv 0 \bmod 2\}.\end{aligned}$$

Further, remember $\overline{P_0}=|\overline{I_{0,=}}|$ and $\overline{Q_0}=|\overline{I_{1,=}}|$.

Lemma 4.6.1.
Any bilinear form in the set $\overline{I_{0,=}}$ satisfies $A_{11}\equiv D \bmod 2$ and $A_{22}-A_{21}\equiv 1 \bmod 2$.

Proof.
In $\overline{I_{0,=}}$ we have $A_{11}+A_{22}\equiv 1 \bmod 2$ and $A_{11}+A_{21}\equiv 0 \bmod 2$. Adding these together yields $A_{22}-A_{21}\equiv A_{22}+A_{21}\equiv 1 \bmod 2$. Now $D=A_{11}(A_{22}-A_{21})$ and $A_{22}-A_{21}\equiv 1 \bmod 2$ imply if D is odd then $A_{11}\equiv 1 \bmod 2$, and if D is even then $A_{11}\equiv 0 \bmod 2$. Consequently we have $A_{11}\equiv D \bmod 2$. □

Lemma 4.6.2.
Let $V = \{(s,t,A_{21}) \mid s,t \in \mathbb{Z}_{>0}, st = D, t \equiv 1 \bmod 2, s \equiv A_{21} \bmod 2, -s < A_{21} \leqslant s\}$. *Then the map*

$$\begin{aligned} \chi : \overline{I_{0,=}} &\longrightarrow V \\ (A_{11}, A_{11}, A_{21}, A_{22}) &\longmapsto (A_{11}, A_{22} - A_{21}, A_{21}) \end{aligned}$$

is a well-defined bijection.

Proof.
Well-defined: We have $st = A_{11}(A_{22} - A_{21}) = D$ and since $D > 0$ and $0 < A_{22} - A_{21}$ it follows that $s,t \in \mathbb{Z}_{>0}$. By Lemma 4.6.1 we have $t = A_{22} - A_{21} \equiv 1 \bmod 2$. Also $s = A_{11} \equiv A_{21} \bmod 2$ because in $\overline{I_{0,=}}$ we have $A_{11} + A_{21} \equiv 0 \bmod 2$. Lastly, we have $-s = -A_{11} < A_{21} \leqslant A_{11} = s$. Therefore χ is well-defined.
Injectivity: This is straightforward to verify.
Surjectivity: Let $(s,t,A_{21}) \in V$ be arbitrary and consider
$g = (s, s, A_{21}, t + A_{21}) = (A_{11}, A_{11}, A_{21}, A_{22})$. Then $\det(g) = s(t + A_{21}) - sA_{21} = st = D$. Next, $-A_{11} = -s < A_{21} \leqslant s = A_{11}$ and $t \in \mathbb{Z}_{>0}$ implies $t = A_{22} - A_{21} > 0$. Now $A_{11} + A_{22} = s + t + A_{21} \equiv t \bmod 2$ as $s \equiv A_{21} \bmod 2$, however $t \equiv 1 \bmod 2$ and thus $A_{11} + A_{22} \equiv 1 \bmod 2$. Lastly, $A_{11} + A_{21} = s + A_{21} \equiv 0 \bmod 2$ as $s \equiv A_{21} \bmod 2$. Hence $g \in \overline{I_{0,=}}$. Finally we note $\chi(g) = (s, t + A_{21} - A_{21}, A_{21}) = (s,t,A_{21})$.
Thus χ is a surjection and hence a bijection. □

Theorem 4.6.3.

$$\overline{P_0} = \sum_{\substack{t \mid D \\ t \text{ odd}}} \frac{D}{t}.$$

Proof.
By Lemma we have $\overline{P_0} = \left|\overline{I_{0,=}}\right| = |V|$. We calculate $|V|$. Since t is odd, pick any pair of divisors s,t of D where t is odd. By Corollary 4.2.7 we have $(-s,s]$ contains $(2s+1)-1 = 2s$ integers and then the condition $A_{21} \equiv s \bmod 2$ implies there are only s possible choices for A_{21}. Since $s \neq 0$, we can find s forms (s,t,A_{21}) for any $s,t \in \mathbb{Z}_{>0}$ where $st = D$ and t is odd. Noting $s = \frac{D}{t}$ then yields $\overline{P_0} = |V| = \sum_{\substack{t \mid D \\ t\text{odd}}} \frac{D}{t}$. □

Lemma 4.6.4.
$\overline{Q_0} = \overline{P_0} = \sum_{\substack{t \mid D \\ t\text{odd}}} \frac{D}{t}$.

Proof.
Let $Z = \overline{I_{0,=}} \cap \overline{I_{1,=}}$ and consider

$$\overline{I_{0,=}} \backslash Z = \{(A_{11}, A_{11}, A_{21}, A_{22}) \mid \det(A) = D, A_{21} = A_{11}, A_{11} + A_{22} \bmod 2, \\ 0 < A_{22} - A_{21}\},$$

$$\overline{I_{1,=}}\backslash Z = \{(A_{11}, A_{11}, A_{21}, A_{22}) \mid \det(A) = D, A_{21} = -A_{11}, A_{11} + A_{22} \bmod 2, \\ 0 < A_{22} - A_{21}\}.$$

We note that in both of these sets we automatically have $A_{11}+A_{21} \equiv 0 \bmod 2$. Define the map

$$\hat{\chi} : \overline{I_{0,=}}\backslash Z \longrightarrow \overline{I_{1,=}}\backslash Z$$
$$(A_{11}, A_{11}, A_{21}, A_{22}) \longmapsto (A_{11}, A_{11}, -A_{21}, A_{22} - 2A_{21}) = (a_{11}, a_{11}, a_{21}, a_{22}).$$

We now show that $\hat{\chi}$ is well-defined and is a bijection.
Well-defined: We have $\det(a_{11}, a_{11}, a_{21}, a_{22}) = A_{11}(A_{22}-2A_{21})-A_{11}(-A_{11}) = A_{11}(A_{22}-A_{21}) = D$. Next, $a_{21} = -A_{21} = -A_{11} = -a_{11}$ as $A_{21} = -A_{11}$ in $\overline{F_{1,=}}\backslash Z$. Further, $a_{11} + a_{22} = A_{22} - 2A_{21} + A_{11} \equiv A_{11} + A_{22} \equiv 1 \bmod 2$. Lastly, $a_{22} - a_{21} = A_{22} - 2A_{21} - (-A_{21}) = A_{22} - A_{21} > 0$. Hence $\hat{\chi}$ is well-defined.
Injectivity: This is straightforward to verify.
Surjectivity: Let $(a_{11}, a_{11}, a_{21}, a_{22}) \in \overline{I_{1,=}}\backslash Z$ be arbitrary and consider $g = (a_{11}, a_{11}, -a_{21}, a_{22} - 2a_{21}) = (A_{11}, A_{11}, A_{21}, A_{22})$. Then $\det(g) = a_{11}(a_{22} - 2a_{21}) - a_{11}(-a_{21}) = a_{11}(a_{22} - a_{21}) = D$. Further, $A_{21} = -a_{21} = -(-a_{11}) = a_{11} = A_{11}$, $A_{11}+A_{22} = a_{11}+a_{22}-2a_{21} \equiv a_{11}+a_{22} \equiv 1 \bmod 2$, and $A_{22}-A_{21} = a_{22}-2a_{21}-(-a_{21}) = a_{22} - a_{21} > 0$. Thus $\hat{\chi}$ is surjective and hence a bijection.
From this and Theorem 4.6.3 it follows that $\overline{Q_0} = \overline{P_0} = \sum_{\substack{t|D \\ t\text{odd}}} \frac{D}{t}$. □

Definition 4.6.5.
Let $\sigma_{\text{odd}}(D) = \sum_{\substack{\text{d}|D \\ \text{d odd}}} \text{d}$.

Lemma 4.6.6.
Let $D \in \mathbb{Z}_{>0}$ and let m be the largest odd divisor of D. Then $D = 2^k m$ and we have

$$\overline{P_0} = 2^k \sigma_{\text{odd}}(D).$$

Proof.
Let $D \in \mathbb{Z}_{>0}$ and m be the largest odd divisor of D. Using $D = 2^k m$, Definition 4.6.5 and Lemma 4.6.3 we have

$$\begin{aligned}
\overline{P_0} &= \sum_{\substack{t|D \\ t \text{ odd}}} \frac{D}{t} \\
&= \sum_{\substack{\text{t}|D \\ \text{t odd}}} \frac{2^k m}{t} \\
&= 2^k \sum_{\substack{t|D \\ t \text{ odd}}} \frac{m}{t} \text{ as } t \nmid 2^k
\end{aligned}$$

$$= 2^k \sum_{\substack{\mathrm{d}|D \\ \mathrm{d\ odd}}} \mathrm{d} \text{ as } m \text{ and } t \text{ are odd implies } \tfrac{m}{t} \text{ is odd}$$
$$= 2^k \sigma_{\mathrm{odd}}(D).$$

□

We now derive an expression for $\overline{R_0}$.

Lemma 4.6.7.
Let

$$V = \{(s,t,A_{11}) \mid s,t \in \mathbb{Z}_{>0}, st = D, s > t, s-t+1 \leqslant A_{11} \leqslant s+t-1, s \equiv t \bmod 2, A_{11} \equiv 1 \bmod 2\}.$$

Then the map

$$\gamma : \overline{J_{0,=}} \longrightarrow V$$
$$(A_{11}, A_{12}, A_{21}, 0) \longmapsto (A_{12}, -A_{21}, A_{11})$$

is a well-defined bijection.

Proof.
Well-defined: We have $A_{21} < 0$ in $\overline{J_{0,=}}$ and $0 < D = -A_{12}A_{21} = st$ implies $s = A_{12} \in \mathbb{Z}_{>0}$ and $t = -A_{21} \in \mathbb{Z}_{>0}$. Next, we note $A_{21} < 0 < A_{12}$ and $0 < \frac{1}{2}(A_{12} + A_{21})$ implies $s = A_{12} > -A_{21} = t$. Also, $s = A_{12} \equiv -A_{21} = t \bmod 2$ since $A_{12}+A_{21} \equiv 0 \bmod 2$ in $\overline{J_{0,=}}$. Since $A_{22} = 0$ we automatically get $A_{11} \equiv 1 \bmod 2$. Combining these results yields $s - t \equiv s + t \equiv 0 \bmod 2$. Lastly, $A_{21} < -|A_{11} - A_{12}|$ implies $A_{12} + A_{21} < A_{11} < A_{12} - A_{21}$ (remember $A_{21} < 0$) and so $s - t < A_{11} < s + t$. However, A_{11} is odd and $s \pm t$ are even and so we have $s - t + 1 \leqslant A_{11} \leqslant s + t - 1$. Hence γ is well-defined.
Injectivity: This is straightforward to verify.
Surjectivity: Let $(s,t,A_{11}) \in V$ be arbitrary and consider $g = (A_{11}, s, -t, 0) = (a_{11}, a_{12}, a_{21}, 0)$. Then $\det(g) = A_{11} \cdot 0 - s(-t) = st = D$. Further, $\frac{1}{2}(a_{12} + a_{21}) = \frac{1}{2}(s-t) > 0$ as $s > t$. We also have $\frac{1}{2}(a_{12} + a_{21}) = \frac{1}{2}(s-t) < s - t + 1 \leqslant A_{11} = a_{11}$. Thus $0 < \frac{1}{2}(a_{12} + a_{21}) \leqslant a_{11}$. Next, $s-t+1 \leqslant A_{11} \leqslant s+t-1$ implies $s-t < A_{11} < s+t$, which in turn yields $-t < A_{11} - s < t$. Hence $|A_{11} - s| < t$. Using $t = -a_{21}$ and $s = a_{12}$ then gives $a_{21} < -|a_{11} - a_{12}|$.
Lastly, observe $a_{11} = A_{11} \equiv 1 \bmod 2$ and $a_{12} + a_{21} = s - t \equiv 0 \bmod 2$. Thus $g \in \overline{J_{0,=}}$. Finally, we have $\gamma(g) = (s, -(-t), A_{11}) = (s,t,A_{11})$.
Hence γ is surjective and thus a bijection. □

Corollary 4.6.8.

$$\overline{R_0} = \sum_{\substack{st=D \\ s>t \\ s \equiv 1 \bmod 2}} t.$$

Proof.
By Lemma 4.6.7 we have $\overline{R_0} = |V|$. Pick any pair of divisors, s, t of D such that $s > t$ and $s \equiv t \bmod 2$. The conditions on the set V then imply $A_{11} \in [s-t+1, s+t-1]$. Since $s > t$ and $s - t + 1$ is odd, it follows that $s - t + 1 > 0$. Further, by Corollary 4.2.7 there are $2t - 1$ integers in this interval, of which t of them are odd because both $s - t + 1$ and $s + t - 1$ are odd.
Thus we have $\overline{R_0} = |V| = \sum_{\substack{st=D \\ s>t \\ s \equiv t \bmod 2}} t.$ □

In our next few results we will be required to take special care with the case when the determinant is a perfect square.

Lemma 4.6.9.
Let $D \in \mathbb{Z}_{>0}$ then

$$\overline{S_0} = \begin{cases} \overline{R_0} + \sqrt{D} & \text{if } D \text{ is a perfect square} \\ \overline{R_0} & \text{otherwise.} \end{cases}$$

Proof.
Let $D \in \mathbb{Z}_{>0}$ and recall $\overline{R_0} = |J_{0,=}|$ and $\overline{S_0} = |J_{1,=}|$, where

$$\begin{aligned} J_{0,=} = \{(A_{11}, A_{12}, A_{21}, 0) \,|\, \det(A) = D, 0 < \frac{1}{2}(A_{12} + A_{21}) \leqslant A_{11}, \\ A_{21} < -|A_{11} - A_{12}|, A_{11} \equiv 1 \bmod 2, A_{12} + A_{21} \equiv 0 \bmod 2\}, \\ J_{1,=} = \{(A_{11}, A_{12}, A_{21}, 0) \mid \det(A) = D, 0 \leqslant \frac{1}{2}(A_{12} + A_{21}) < A_{11}, \\ A_{21} < -|A_{11} - A_{12}|, A_{11} \equiv 1 \bmod 2, A_{12} + A_{21} \equiv 0 \bmod 2\}. \end{aligned}$$

Let $Z = \overline{J_{0,=}} \cap \overline{J_{1,=}}$, then

$$\begin{aligned} \overline{J_{0,=}} \backslash Z = \{(A_{11}, A_{12}, A_{21}, 0) \mid \det(A) = D, A_{12} + A_{21} = 2A_{11}, A_{21} < -|A_{11} - A_{12}|, \\ A_{11} \equiv 1 \bmod 2\}, \\ \overline{J_{1,=}} \backslash Z = \{(A_{11}, A_{12}, A_{21}, 0) \mid \det(A) = D, 0 = A_{12} + A_{21}, A_{21} < -|A_{11} - A_{12}|, \\ A_{11} \equiv 1 \bmod 2\}. \end{aligned}$$

We note the condition $A_{12} + A_{21} \equiv 0 \bmod 2$ is automatically fulfilled in the sets $\overline{J_{0,=}} \backslash Z$ and $\overline{J_{1,=}} \backslash Z$ and so is omitted from the description.
Observe both $\overline{J_{0,=}} \backslash Z$ and $\overline{J_{1,=}} \backslash Z$ contain the relation $A_{21} < -|A_{11} - A_{12}|$, which implies $A_{12} + A_{21} < A_{11} < A_{12} + |A_{21}|$. Consequently $\overline{J_{0,=}} \backslash Z = \emptyset$ since the set $\overline{J_{0,=}} \backslash Z$ requires $2A_{11} = A_{12} + A_{21} < A_{11}$.
Let $(A_{11}, A_{12}, A_{21}, 0) \in \overline{J_{1,=}} \backslash Z$, this satisfies $0 = A_{12} + A_{21}$ and thus $A_{21} = -A_{12}$. This yields $D = \det(A) = -A_{12}A_{21} = A_{12}^2$ and hence if D is not a perfect square then $\overline{J_{1,=}} \backslash Z = \emptyset$ and thus $\overline{R_0} = |Z| = \overline{S_0}$.
We now assume D is a perfect square, it is still true that $\overline{J_{1,=}} \backslash Z = \emptyset$ but we will show $\overline{J_{1,=}} \backslash Z \neq \emptyset$. Let $(A_{11}, A_{12}, A_{21}, 0) \in \overline{J_{1,=}} \backslash Z$ be arbitrary, then by above $D = A_{12}^2$.

Since $A_{12} > 0$ it follows that $A_{12} = \sqrt{D}$ and $A_{21} = -\sqrt{D}$. Then $A_{21} < -|A_{11} - A_{12}|$ implies $A_{12} + A_{21} < A_{11} < A_{12} + |A_{21}|$ and so $0 < A_{11} < 2\sqrt{D}$. There are $2\sqrt{D} - 1$ integers in the interval $\left[1, 2\sqrt{D} - 1\right]$ and since 1 and $2\sqrt{D} - 1$ are odd, it follows that precisely $\sqrt{D}$ of them are odd.
Therefore there are $\sqrt{D}$ choices for A_{11} and consequently $\left|\overline{J_{1,=}} \backslash Z\right| = \sqrt{D}$.
Hence

$$\begin{aligned}
\overline{S_0} &= \left|\overline{J_{1,=}}\right| \\
&= \left|\overline{J_{1,=}} \backslash Z\right| + |Z| \\
&= \left|\overline{J_{1,=}} \backslash Z\right| + \underbrace{\left|\overline{J_{0,=}} \backslash Z\right|}_{=0} + |Z| \\
&= \left|\overline{J_{1,=}} \backslash Z\right| + \left|\overline{J_{0,=}}\right| \\
&= \sqrt{D} + \overline{R_0}.
\end{aligned}$$

Hence we have our result, $\overline{S_0} = \begin{cases} \overline{R_0} + \sqrt{D} & \text{if } D = k^2 \\ \overline{R_0} & \text{otherwise} \end{cases}$. □

Lemma 4.6.10.
Let $D \in \mathbb{Z}_{>0}$ and assume $D \equiv 2 \bmod 4$, then $\overline{R_0} = \overline{S_0} = 0$.

Proof.
Since $D \equiv 2 \bmod 4$, the prime factorisation of D contains a single power of 2. Thus D cannot be a perfect square and so Lemma 4.6.9 yields $\overline{S_0} = \overline{R_0}$. Further, since D contains a single power of 2, there are no divisors s, t of D such that $st = D$ and $s \equiv t \equiv 1 \bmod 2$. Thus at least one of s, t is divisible by 2. However, $D \equiv 2 \bmod 4$ implies that we cannot have $2 \mid s$ and $2 \mid t$.
Hence $s \not\equiv t \bmod 2$ and thus $\overline{S_0} = \overline{R_0} = \sum_{\substack{0<t<s \\ st=D \\ s \equiv t \bmod 2}} t = 0$. □

Lemma 4.6.11. *Let $D \in \mathbb{Z}_{>0}$ be such that $D \equiv 1 \bmod 2$. Then*

$$\overline{R_0} = \begin{cases} \frac{1}{2}\left(\sigma(D) - \Psi(D) - \sqrt{D}\right) & \text{if } D = k^2 \\ \frac{1}{2}\left(\sigma(D) - \Psi(D)\right) & \text{otherwise} \end{cases} \quad \text{and}$$

$$\overline{S_0} = \begin{cases} \frac{1}{2}\left(\sigma(D) - \Psi(D) + \sqrt{D}\right) & \text{if } D = k^2 \\ \frac{1}{2}\left(\sigma(D) - \Psi(D)\right) & \text{otherwise.} \end{cases}$$

Proof.
Let $D \in \mathbb{Z}_{>0}$ and $D \equiv 1 \bmod 2$. First suppose that D is not a perfect square, then Lemma 4.4.2 yields $2 \sum_{\substack{0<\partial<\mathrm{d} \\ \partial \mathrm{d}=D}} \partial = \sigma(D) - \Psi(D)$. Since D is odd it follows that ∂ and d are always odd and so $\partial \equiv \mathrm{d} \bmod 2$. Since D is not a perfect square we cannot have

$\partial = \mathrm{d} = \sqrt{D}$. By Lemmas 4.6.8 and 4.6.9 we have

$$\overline{S_0} = \overline{R_0} = \sum_{\substack{0<\partial<\mathrm{d} \\ \partial\mathrm{d}=D \\ \partial\equiv\mathrm{d} \bmod 2}} \partial = \frac{1}{2}\left(2\sum_{\substack{0<\partial<\mathrm{d} \\ \partial\mathrm{d}=D}} \partial\right) = \frac{1}{2}\left(\sigma(D) - \Psi(D)\right).$$

Now suppose D is a perfect square, then Lemma 4.4.2 yields $2\sum_{\substack{0<\partial<\mathrm{d} \\ \partial\mathrm{d}=D}} \partial = \sigma(D) - \Psi(D) - \sqrt{D}$. It is still true that $\partial \equiv \mathrm{d} \equiv 1 \bmod 2$. Lemmas 4.6.8 and 4.6.9 then yield

$$\overline{R_0} = \sum_{\substack{0<\partial<\mathrm{d} \\ \partial\mathrm{d}=D}} \partial = \frac{1}{2}\left(2\sum_{\substack{0<\partial<\mathrm{d} \\ \partial\mathrm{d}=D \\ \partial\equiv\mathrm{d} \bmod 2}} \partial\right) = \frac{1}{2}\left(\sigma(D) - \Psi(D) - \sqrt{D}\right) \text{ and}$$

$$\overline{S_0} = \overline{R_0} + \sqrt{D} = \tfrac{1}{2}\left(\sigma(D) - \Psi(D) - \sqrt{D}\right) + \sqrt{D} = \tfrac{1}{2}\left(\sigma(D) - \Psi(D) + \sqrt{D}\right). \qquad \square$$

Lemma 4.6.12.
Let $D \in \mathbb{Z}_{>0}$ be such that $D \equiv 0 \bmod 4$. Then

$$\overline{R_0} = \begin{cases} \sigma\left(\frac{D}{4}\right) - \Psi\left(\frac{D}{4}\right) - \sqrt{\frac{D}{4}} & \text{if } D = k^2 \\ \sigma\left(\frac{D}{4}\right) - \Psi\left(\frac{D}{4}\right) & \text{otherwise} \end{cases}$$

$$\overline{S_0} = \begin{cases} \sigma\left(\frac{D}{4}\right) - \Psi\left(\frac{D}{4}\right) + \sqrt{\frac{D}{4}} & \text{if } D = k^2 \\ \sigma\left(\frac{D}{4}\right) - \Psi\left(\frac{D}{4}\right) & \text{otherwise} \end{cases}.$$

Proof.
Let $D \in \mathbb{Z}_{>0}$ be such that $D \equiv 0 \bmod 4$, we first assume that D is not a perfect square. Then $\overline{R_0} = \sum_{\substack{0<t<s \\ st=D \\ s\equiv t \bmod 2}} t$ implies $2 \mid s$ and $2 \mid t$ as otherwise $s \not\equiv t \bmod 2$. We note that $D \equiv 0 \bmod 4$ implies there is no pair of divisors S, t of D such that $s \equiv t \equiv 1 \bmod 2$. Now let (s,t) be a pair of divisors of D and write $s = 2\hat{s}$ and $t = 2\hat{t}$. It follows that $D = 4\hat{s}\hat{t}$ and so $\hat{s}, \hat{t}$ are divisors of $\frac{D}{4}$. Then Lemmas 4.4.2, 4.6.8 and 4.6.9 yield

$$\overline{S_0} = \overline{R_0} = \sum_{\substack{0<2\hat{t}<2\hat{s} \\ 4\hat{s}\hat{t}=D \\ 2\hat{s}\equiv 2\hat{t} \bmod 2}} 2\hat{t} = 2\sum_{\substack{0<\hat{t}<\hat{s} \\ \hat{s}\hat{t}=\frac{D}{4}}} \hat{t} = \sigma\left(\frac{D}{4}\right) - \Psi\left(\frac{D}{4}\right).$$

Now assume D is a perfect square, we note that $D \equiv 0 \bmod 4$ implies $\frac{D}{4}$ is also a perfect square. We also note that the requirement $s \equiv t \bmod 2$ for any pair of divisors we consider, means $2 \mid s$ and $2 \mid t$. Again, we write $s = 2\hat{s}$ and $t = 2\hat{t}$. Then Lemmas 4.4.2, 4.6.8 and 4.6.9 yield

$$\overline{R_0} = \sum_{\substack{0<2\hat{t}<2\hat{s} \\ 4\hat{s}\hat{t}=D \\ 2\hat{s}\equiv 2\hat{t} \bmod 2}} 2\hat{t} = 2\sum_{\substack{0<\hat{t}<\hat{s} \\ \hat{s}\hat{t}=\frac{D}{4}}} \hat{t} = \sigma\left(\frac{D}{4}\right) - \Psi\left(\frac{D}{4}\right) - \sqrt{\frac{D}{4}}.$$

Further, we have

$$\overline{S_0} = \overline{R_0} + \sqrt{D} = \sigma\left(\frac{D}{4}\right) - \Psi\left(\frac{D}{4}\right) - \sqrt{\frac{D}{4}} + \sqrt{D} = \sigma\left(\frac{D}{4}\right) - \Psi\left(\frac{D}{4}\right) + \sqrt{\frac{D}{4}}.$$

□

4.7 A Formula for the Single Bar Complete Class Number for Bilinear Forms

In this section we utilise our expressions for $\overline{P_0}$, $\overline{Q_0}$, $\overline{R_0}$ and $\overline{S_0}$ to develop a formula for $\overline{\mathrm{Cl}}_c(D)$. We remind the reader that D is a fixed positive integer corresponding to the determinant of the bilinear form.

Lemma 4.7.1.
Let $D \in \mathbb{Z}_{>0}$ be such that $D \equiv 1 \bmod 2$.
Then $2\sigma_{odd}(D) - \sigma(D) + \Psi(D) = \sigma(D) + \Psi(D)$.

Proof.
Recall from Definition 4.6.5 the definition of σ_{odd}. Note that $D \equiv 1 \bmod 2$ implies every divisor d of D satisfies $d \equiv 1 \bmod 2$. Thus when D is odd we have $2\sigma_{\mathrm{odd}}(D) = 2\sigma(D)$.
Hence $2\sigma_{\mathrm{odd}}(D) - \sigma(D) + \Psi(D) = \sigma(D) + \Psi(D)$. □

Lemma 4.7.2.
Let $D \in \mathbb{Z}_{>0}$ be such that $D \equiv 0 \bmod 2$. Then $D = 2^k \cdot m$ where $k \geqslant 1$ and $m \equiv 1 \bmod 2$ and we have $\sigma_{odd}\left(\frac{D}{2^q}\right) = \sigma\left(\frac{D}{2^k}\right)$ for $0 \leqslant q \leqslant k$.

Proof.
$D \equiv 0 \bmod 2$ implies $D = 2^k \cdot m$ where $k \geqslant 1$ and $m \equiv 1 \bmod$. We note for $0 \leqslant q \leqslant k$ the set of odd divisors of $\frac{D}{2^q}$ is precisely the set of odd divisors of $m = \frac{D}{2^k}$. By Definition 4.6.5 this means $\sigma_{\mathrm{odd}}\left(\frac{D}{2^q}\right) = \sigma\left(\frac{D}{2^k}\right)$ for $0 \leqslant q \leqslant k$. □

Lemma 4.7.3.
Let $D \in \mathbb{Z}_{>0}$ be such that $D \equiv 0 \bmod 4$. Then writing $D = 2^k \cdot m$ where $m \equiv 1 \bmod 2$ yields $2^{k+1}\sigma_{odd}(D) = 4\sigma_{odd}\left(\frac{D}{4}\right) + 4\sigma\left(\frac{D}{4}\right)$.

Proof.
First recall $\sigma(D)$ is a multiplicative arithmetic function. That is, for $D = a \cdot b$ where $\gcd(a, b) = 1$ we have $\sigma(D) = \sigma(a) \cdot \sigma(b)$.
Writing $D = 2^k \cdot m$ where $m \equiv 1 \bmod 2$ and consequently $k \geqslant 2$ yields

$$\begin{aligned}
\sigma\left(\frac{D}{4}\right) &= \sigma\left(2^{k-2} \cdot m\right) \\
&= \sigma\left(2^{k-2}\right) \cdot \sigma(m) \; m \equiv 1 \bmod 2 \\
&= \sigma(m) \sum_{q=0}^{k-2} 2^q
\end{aligned}$$

$$= \left(2^{k-1} - 1\right) \sigma(m).$$

We note $\sigma_{\text{odd}}(m) = \sigma_{\text{odd}}\left(\frac{D}{4}\right) = \sigma_{\text{odd}}(D)$ and further $\sigma(m) = \sigma_{\text{odd}}(m)$ since $m \equiv 1 \bmod 2$. Therefore

$$\begin{aligned} 4\sigma_{\text{odd}}\left(\frac{D}{4}\right) + 4\sigma\left(\frac{D}{4}\right) &= 4\sigma(m) + 4\left(2^{k-1} - 1\right)\sigma(m) \\ &= 4 \cdot 2^{k-1}\sigma(m) \\ &= 2^{k+1}\sigma(m) \\ &= 2^{k+1}\sigma_{\text{odd}}(D). \end{aligned}$$

□

We now state and prove the key theorem of Kronecker's section 18, see [Kr1897, p. 476].

Theorem 4.7.4.
Let $D \in \mathbb{Z}_{>0}$, then

$$\frac{1}{3}\overline{\text{Cl}}_c(D) = \begin{cases} \sigma(D) + \Psi(D) & \text{if } D \equiv 1 \bmod 2 \\ 4\sigma\left(\frac{D}{2}\right) & \text{if } D \equiv 2 \bmod 4 \\ 4\sigma_{odd}\left(\frac{D}{4}\right) + 2\sigma\left(\frac{D}{4}\right) + 2\Psi\left(\frac{D}{4}\right) & \text{if } D \equiv 0 \bmod 4. \end{cases}$$

Proof.
From Section 3.7, Equation 3.20 we have $\overline{\text{Cl}}_c(D) = 3\left(\overline{P_0} + \overline{Q_0} - \overline{R_0} - \overline{S_0}\right)$.
We will split this proof into two cases, when D is a perfect square and otherwise.
First assume that D is not a perfect square.
Using our results from Section 4.6 plus Lemmas 4.7.1, 4.7.2 and 4.7.3 we have

$$\begin{aligned} \frac{1}{3}\overline{\text{Cl}}_c(D) &= \begin{cases} 2\overline{P_0} - 2\overline{R_0} & \text{if } D \equiv 1 \bmod 2 \\ 2\overline{P_0} & \text{if } D \equiv 2 \bmod 4 \\ 2\overline{P_0} - 2\overline{R_0} & \text{if } D \equiv 0 \bmod 4 \end{cases} \\ &= \begin{cases} 2 \cdot 2^0\sigma_{\text{odd}}(D) - 2 \cdot \frac{1}{2}\left(\sigma(D) - \Psi(D)\right) & \text{if } D \equiv 1 \bmod 2 \\ 2 \cdot 2\sigma_{\text{odd}}(D) & \text{if } D \equiv 2 \bmod 4 \\ 2 \cdot 2^k\sigma_{\text{odd}}(D) - 2\left(\sigma\left(\frac{D}{4}\right) + \Psi\left(\frac{D}{4}\right)\right) & \text{if } D \equiv 0 \bmod 4 \end{cases} \\ &= \begin{cases} 4\sigma_{\text{odd}}(D) - \sigma(D) + \Psi(D) & \text{if } D \equiv 1 \bmod 2 \\ 4\sigma_{\text{odd}}(D) & \text{if } D \equiv 2 \bmod 4 \\ 2^{k+1}\sigma_{\text{odd}}(D) - 2\sigma\left(\frac{D}{4}\right) + 2\Psi\left(\frac{D}{4}\right) & \text{if } D \equiv 0 \bmod 4 \end{cases} \\ &= \begin{cases} \sigma(D) + \Psi(D) & \text{if } D \equiv 1 \bmod 2 \\ 4\sigma\left(\frac{D}{2}\right) & \text{if } D \equiv 2 \bmod 4 \\ 4\sigma_{\text{odd}}\left(\frac{D}{4}\right) + 2\sigma\left(\frac{D}{4}\right) + 2\Psi\left(\frac{D}{4}\right) & \text{if } D \equiv 0 \bmod 4. \end{cases} \end{aligned}$$

We now suppose that D is a perfect square. Note D being a perfect square means we cannot have $D \equiv 2, 3 \bmod 4$. Recall when $D \equiv 1 \bmod 2$ we have $\sigma_{\text{odd}}(D) = \sigma(D)$ and

also note that in the proof of Lemma 4.7.3 we made no assumptions as to whether D was a perfect square or not. Thus we get

$$\begin{aligned}
\frac{1}{3}\overline{\mathrm{Cl}}_c(D) &= \begin{cases} 2\overline{P_0} - \overline{R_0} - \overline{S_0} & \text{if } D \equiv 1 \bmod 2 \\ 2\overline{P_0} - \overline{R_0} - \overline{S_0} & \text{if } D \equiv 0 \bmod 4 \end{cases} \\
&= \begin{cases} 2 \cdot 2^0 \sigma_{\mathrm{odd}}(D) - \frac{1}{2}\left(\sigma(D) - \Psi(d) - \sqrt{D}\right) - \frac{1}{2}\left(\sigma(D) - \Psi(D) + \sqrt{D}\right) \\ 2 \cdot 2^k \sigma_{\mathrm{odd}}(D) - \left(\sigma\left(\frac{D}{4}\right) - \Psi\left(\frac{D}{4}\right) - \sqrt{\frac{D}{4}}\right) - \left(\sigma\left(\frac{D}{4}\right) - \Psi\left(\frac{D}{4}\right) + \sqrt{\frac{D}{4}}\right) \end{cases} \\
&= \begin{cases} 2\sigma_{\mathrm{odd}}(D) - \sigma(D) + \Psi(D) & \text{if } D \equiv 1 \bmod 2 \\ 2^{k+1}\sigma_{\mathrm{odd}}(D) - 2\sigma\left(\frac{D}{4}\right) + 2\Psi\left(\frac{D}{4}\right) & \text{if } D \equiv 0 \bmod 4 \end{cases} \\
&= \begin{cases} \sigma(D) + \Psi(D) & \text{if } D \equiv 1 \bmod 2 \\ 4\sigma_{\mathrm{odd}}\left(\frac{D}{4}\right) + 2\sigma\left(\frac{D}{4}\right) + 2\Psi\left(\frac{D}{4}\right) & \text{if } D \equiv 0 \bmod 4. \end{cases}
\end{aligned}$$

□

It is quite remarkable the results are the same regardless of whether D is a perfect square or not.

Notes on Section 4.7

The following lemma is given in Kronecker but is not used in our work.

Lemma 4.7.5.
Let $D \in \mathbb{Z}_{>0}$ be such that $D \equiv 0 \bmod 4$. Write $D = 2^k \cdot m$ where $m \equiv 1 \bmod 2$ and consequently $k \geqslant 2$. Then $\sigma\left(2^{k-2} \cdot m\right) = \left(2^{k-1} - 1\right)\sigma_{odd}(m)$.

Proof.
We first note $m \equiv 1 \bmod 2$ implies $\sigma(m) = \sigma_{\mathrm{odd}}(m)$. Therefore $\left(2^{k-1} - 1\right)\sigma(m) = \left(2^{k-1} - 1\right)\sigma_{\mathrm{odd}}(m)$.
We have $\sigma(2^{k-2} \cdot m) = \sum_{\mathrm{d} \mid 2^{k-2} \cdot m} \mathrm{d}$. Any divisor d of $2^{k-2} \cdot m$ may be written as $2^q \cdot t$ where $t \equiv 1 \bmod 2$, $t \mid m$ and $0 \leqslant q \leqslant k-2$. Further, for every such q and any divisor t of m we get $2^q \cdot t$ is a divisor of $2^{k-2} \cdot m$. Let $d_1, d_2, \ldots, d_r$ be the divisors of m. From this it follows

$$\begin{aligned}
\sum_{\mathrm{d} \mid 2^{k-2} \cdot m} \mathrm{d} &= d_1 + 2d_1 + 2^2 d_1 + \ldots + 2^{k-2} d_1 + \ldots + 2^{k-2} d_r \\
&= d_1 \sum_{q=0}^{k-2} 2^q + \ldots + d_r \sum_{q=0}^{k-2} 2^q \\
&= (d_1 + \ldots + d_r) \sum_{q=0}^{k-2} 2^q \\
&= \sigma(m) \sum_{q=0}^{k-2} 2^q
\end{aligned}$$

$$= \left(2^{k-1} - 1\right) \sigma(m)$$
$$= \left(2^{k-1} - 1\right) \sigma_{\text{odd}}(m).$$

□

In Lemma 4.7.3 we note Kronecker stated it as $2^{k+1}\sigma_{\text{odd}}(D) = 4\sigma_{\text{odd}}(D) + 4\sigma\left(\frac{D}{4}\right)$. This is not an error of his part, but a reflection of the fact that $\sigma_{\text{odd}}(D) = \sigma_{\text{odd}}\left(\frac{D}{4}\right)$.

Theorem 4.7.4 differs by a factor of two when compared with Kronecker's original work. This is still due to Kronecker considering definite bilinear forms.

4.8 Introducing $\overline{\overline{\text{Cl}}}_c(D)$.

We now turn our attention to introducing one further refinement of the complete class number for positive definite bilinear forms. As before, $D \in \mathbb{Z}_{>0}$ is the determinant of our bilinear forms.
We single out the following two subsets of the set of complete equivalence classes of bilinear forms.

Definition 4.8.1.
Let $\overline{\overline{\text{Cl}}}_c(D)$ be the cardinality of the subset of complete equivalence classes of bilinear forms satisfying the following two conditions:

1. At least one of A_{11} and A_{22} is odd, and
2. $A_{12} - A_{21} \equiv 0 \bmod 4$.

Definition 4.8.2.
Let $\text{Cl}_c''(D)$ be the cardinality of the subset of complete equivalence classes of bilinear forms satisfying the following two conditions:

1. Exactly one of A_{11} and A_{22} is odd (that is, $A_{11} + A_{22} \equiv 1 \bmod 2$), and
2. $A_{12} - A_{21} \equiv 0 \bmod 4$.

Observation 4.8.3.
Definitions 4.8.1 and 4.8.2 are well defined on complete equivalence classes because any two completely equivalent bilinear forms must be congruent to each other modulo 2 (see Lemma 2.4.7). Consequently modulo two they must have the same sum of their outer coefficients. Further, by Lemma 2.4.6 we know $A_{12} - A_{21}$ is invariant under proper equivalence, it is invariant under complete equivalence and thus all forms within a complete equivalence class satisfy $A_{12} - A_{21} \equiv 0 \bmod 4$.

Observation 4.8.4.
Observe any bilinear form which is counted in $\text{Cl}_c''(D)$ is also counted in $\overline{\overline{\text{Cl}}}_c(D)$. However, if a bilinear form has both outer coefficients odd then it is counted in $\overline{\overline{\text{Cl}}}_c(D)$ but not in $\text{Cl}_c''(D)$. Further, any form satisfying $A_{12} - A_{21} \equiv 0 \bmod 4$ automatically satisfies $A_{12} - A_{21} \equiv 0 \bmod 2$ but not vice versa.
Hence $\text{Cl}_c''(D) \leqslant \overline{\overline{\text{Cl}}}_c(D) \leqslant \overline{\text{Cl}}_c(D) \leqslant \text{Cl}_c(D)$.

Our first goal is to deduce the following result: $\overline{\overline{\mathrm{Cl}}}_c(D) = 3(\overline{\overline{P}} + \overline{\overline{Q}} - \overline{\overline{R}} - \overline{\overline{S}})$.
To do so, we will give a similar argument to that of Section 3.3, where we proved $\overline{\mathrm{Cl}}_c(D) = 3(\overline{P} + \overline{Q} - \overline{R} - \overline{S})$.

We begin with the following theorem.

Theorem 4.8.5.
Let $\mathcal{A}$ be a bilinear form with matrix representation A, $M \in \mathrm{SL}_2(\mathbb{Z})$ and $B = M^t AM$. Then $A_{11} \equiv A_{22} \equiv 0 \bmod 2$ and $A_{12} - A_{21} \equiv 0 \bmod 4$ if and only if $B_{11} \equiv B_{22} \equiv 0 \bmod 2$ and $B_{12} - B_{21} \equiv 0 \bmod 4$.

Proof.
($\Rightarrow$) Assume $A_{11} \equiv A_{22} \equiv 0 \bmod 2$ and $A_{12} - A_{21} \equiv 0 \bmod 4$. From Lemma 2.4.6 we have $B_{12} - B_{21} = A_{12} - A_{21} \equiv 0 \bmod 4$ as $M \in \mathrm{SL}_2(\mathbb{Z})$. Further, note that $A_{12} + A_{21} \equiv 0 \bmod 2$ and $B_{12} + B_{21} \equiv 0 \bmod 2$. Applying Observation 2.4.5 (I) with $M \in \mathrm{SL}_2(\mathbb{Z})$ yields

$$\begin{aligned} B_{11} &= \alpha^2 A_{11} + \alpha\gamma(A_{12} + A_{21}) + \gamma^2 A_{22} \equiv 0 \bmod 2 \text{ and} \\ B_{22} &= \beta^2 A_{11} + \beta\delta(A_{12} + A_{21}) + \delta^2 A_{22} \equiv 0 \bmod 2. \end{aligned}$$

($\Leftarrow$) Since $M \in \mathrm{GL}_2(\mathbb{Z})$ it is invertible. Write $A = (M^{-1})^t BM^{-1}$ and apply ($\Rightarrow$). □

Corollary 4.8.6.
There is no Kronecker reduced form, $\begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix}$ satisfying $A_{12} - A_{21} \equiv 0 \bmod 4$ and at least one of A_{11}, A_{22} odd, that is properly equivalent to the reduced form $\begin{pmatrix} a_{12} + a_{21} & a_{12} \\ a_{21} & a_{12} + a_{21} \end{pmatrix}$, where $a_{12} + a_{21} > 0$.

Proof.
Recall Kronecker reduced forms are positive definite and every positive definite form is properly equivalent to a unique reduced form. Let $A = \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix}$ be a Kronecker reduced form with $A_{12} - A_{21} \equiv 0 \bmod 4$ and at least one of its outer coefficients odd. Assume $B = M^t AM = \begin{pmatrix} a_{12} + a_{21} & a_{12} \\ a_{21} & a_{12} + a_{21} \end{pmatrix}$ where $a_{12} + a_{21} > 0$ and $M \in \mathrm{SL}_2(\mathbb{Z})$.
Then Lemma 2.4.6 implies the reduced form satisfies $a_{12} - a_{21} = A_{12} - A_{21} \equiv 0 \bmod 4$ and so $a_{12} + a_{21} \equiv 0 \bmod 2$, thus $a_{11} \equiv a_{22} \equiv 0 \bmod 2$. Next, the matrix M^{-1} transforms the reduced form back to the Kronecker reduced form A. However, Theorem 4.8.5 implies $A_{11} \equiv A_{22} \equiv 0 \bmod 2$, contradicting at least one of A_{11}, A_{22} is odd.
Hence there does not exist a Kronecker reduced form with $A_{12} - A_{21} \equiv 4 \bmod 2$ and at least one of its outer coefficients odd which is properly equivalent to the reduced form $\begin{pmatrix} a_{12} + a_{21} & a_{12} \\ a_{21} & a_{12} + a_{21} \end{pmatrix}$, where $a_{12} + a_{21} > 0$. □

For a given reduced bilinear form we now consider the structure of the complete equivalence classes in its proper equivalence class with respect to $\overline{\overline{\mathrm{Cl}}}_c(D)$ and $\mathrm{Cl}''_c(D)$.

We will continue to use the representatives found in Equation 2.16 to describe the transformation matrices used to generate the complete equivalence classes.

Lemma 4.8.7.
Let $\mathcal{A}$ be a bilinear form with matrix representation A. Assume the proper equivalence class of $\mathcal{A}$ contains six distinct representatives for the complete equivalence classes of $\mathcal{A}$ and let $\mathcal{A} \sim_+ \mathcal{B}$. If B satisfies $B_{11} \equiv B_{22} \equiv 0 \bmod 2$ and $B_{12} - B_{21} \equiv 0 \bmod 4$ then all six complete equivalence classes satisfy $a_{11} + a_{22} \equiv 0 \bmod 2$. While if $B_{12} - B_{21} \equiv 0 \bmod 4$ and at least one of B_{11}, B_{22} is odd then only two of the complete equivalence classes have forms satisfying $a_{11} + a_{22} \equiv 0 \bmod 2$.

Proof.
Let B satisfy $B_{12} - B_{21} \equiv 0 \bmod 4$, then any bilinear form properly equivalent to B also has this property. We apply Lemma 3.3.9 as $B_{12} - B_{21} \equiv 0 \bmod 4$ implies $B_{12} - B_{21} \equiv 0 \bmod 2$. Thus we know any bilinear form that is properly equivalent to B satisfies $a_{11} + a_{22}$ is congruent to either $B_{11} + B_{22}$, B_{11} or $B_{22} \bmod 2$.
Now recall completely equivalent bilinear forms have the same entries mod2 in their matrix representations. Thus using Observation 2.4.5 (I) along with each of the 6 complete equivalence class representatives found in S, we see exactly two complete equivalence classes yield bilinear forms satisfying $a_{11} + a_{22} \equiv B_{11} \bmod 2$, two more satisfy $a_{11} + a_{22} \equiv B_{22} \bmod 2$, while the remaining two satisfy $a_{11} + a_{22} \equiv B_{11} + B_{22} \bmod 2$.
The only way for all of these to be $0 \bmod 2$ is if $B_{11} \equiv B_{22} \equiv 0 \bmod 2$. We now observe if exactly one of B_{11}, B_{22} is odd then only one of B_{11}, B_{22} and $B_{11} + B_{22}$ is even. Whilst if both B_{11} and B_{22} are odd then only $B_{11} + B_{22}$ is even.
Hence either all six complete equivalence classes of bilinear forms within the proper equivalence class satisfy $a_{11} + a_{22} \equiv 0 \bmod 2$ (when $B_{11} \equiv B_{22} \equiv 0 \bmod 2$); otherwise only two complete equivalence classes within the proper equivalence class have this property. □

Our next lemma and theorem prove a key result implied by Kronecker.

Lemma 4.8.8.
Consider the subset of positive definite Kronecker reduced bilinear forms $\mathcal{A}$ satisfying the following two conditions:

1. *At least one of their outer coefficients is odd, and*
2. $A_{12} - A_{21} \equiv 0 \bmod 4$.

Then within the proper equivalence class of such a bilinear form, there is a 2:1 ratio of the number of complete equivalence classes with the property $A_{11} + A_{22} \equiv 1 \bmod 2$ to those with the property $A_{11} + A_{22} \equiv 0 \bmod 2$.

Proof.
Consider the set of Kronecker reduced bilinear forms with the properties as given in the statement of the lemma. Recall every Kronecker reduced bilinear form is properly equivalent to a unique reduced bilinear form. Consequently, Lemma 2.4.6 implies this

reduced bilinear form also satisfies $a_{12} - a_{21} \equiv 0 \bmod 4$. Further, Theorem 4.8.5 implies the reduced form must have at least one of its outer coefficients odd because the Kronecker reduced form has at least one odd outer coefficient. Further still, Theorem 4.8.5 implies all bilinear forms within the proper equivalence class have this property. If the proper equivalence class of the reduced bilinear form contains 6 distinct representatives for the complete equivalence classes, then Lemma 4.8.7 implies that exactly two of the six complete equivalence classes have forms satisfying $A_{11}+A_{22} \equiv 0 \bmod 2$. This is because our reduced form does not satisfy $A_{11} \equiv A_{22} \equiv 0 \bmod 2$. Consequently in this case we have a 2:1 ratio of complete equivalence classes with the property $A_{11} + A_{22} \equiv 1 \bmod 2$ to those that have $A_{11} + A_{22} \equiv 0 \bmod 2$.

We now deal with the situation when the proper equivalence class of the reduced bilinear form contains less than 6 distinct complete equivalence classes. This means the reduced form has a proper automorph. Therefore we must consider reduced bilinear forms of the types found in the first four rows of Summary 2.5.27.

Observe that the form in the fourth row is a special case of the form in the third row, where $A_{21} = A_{21}$. By Corollary 4.8.6 we know there is no Kronecker reduced form with at least one odd outer coefficient odd, and the sum of its inner coefficients even that reduces to $\begin{pmatrix} a_{12}+a_{21} & a_{12} \\ a_{21} & a_{12}+a_{21} \end{pmatrix}$. Hence the third and fourth types of reduced bilinear form cannot arise when we reduce our Kronecker reduced bilinear form. We investigate rows one and two separately.

Suppose our Kronecker reduced bilinear form is properly equivalent to the reduced bilinear form $\begin{pmatrix} A_{11} & A_{12} \\ -A_{12} & A_{11} \end{pmatrix}$, where $A_{11} \equiv 1 \bmod 2$. Then the set of complete equivalence classes within its proper equivalence class is given by

$$\left\{ \begin{pmatrix} A_{11} & A_{12} \\ -A_{12} & A_{11} \end{pmatrix}, \begin{pmatrix} 2A_{11} & A_{11}+A_{12} \\ A_{11}-A_{12} & A_{11} \end{pmatrix}, \begin{pmatrix} A_{11} & A_{11}+A_{12} \\ A_{11}-A_{12} & 2A_{11} \end{pmatrix} \right\}.$$

Since we began with a Kronecker reduced bilinear form that satisfies $A_{12} - A_{21} \equiv 0 \bmod 4$ and this is invariant under $\mathrm{SL}_2(\mathbb{Z})$, we know all of the above three forms must satisfy $a_{12} - a_{21} \equiv 0 \bmod 4$. It is straightforward to check that only the first form satisfies $a_{11} + a_{22} \equiv 0 \bmod 2$ and hence we have a 2:1 ratio.

Now suppose our Kronecker reduced bilinear form is properly equivalent to the reduced bilinear form $\begin{pmatrix} A_{11} & 0 \\ 0 & A_{11} \end{pmatrix}$, where $A_{11} \equiv 1 \bmod 2$. Then the set of complete equivalence classes within its proper equivalence class is given by

$$\left\{ \begin{pmatrix} A_{11} & 0 \\ 0 & A_{11} \end{pmatrix}, \begin{pmatrix} 2A_{11} & A_{11} \\ A_{11} & A_{11} \end{pmatrix}, \begin{pmatrix} A_{11} & A_{11} \\ A_{11} & 2A_{11} \end{pmatrix} \right\}.$$

It is clear all of these complete equivalence classes contain bilinear forms satisfying $a_{12} - a_{21} \equiv 0 \bmod 4$ and straightforward to verify only the first form satisfies $a_{11} + a_{22} \equiv 0 \bmod 2$. Hence we have a 2:1 ratio.

Thus we always have a 2:1 ratio of complete equivalence classes where $a_{11} + a_{22} \equiv 1 \bmod 2$ to those where $a_{11} + a_{22} \equiv 0 \bmod 2$ within the proper equivalence class of

any Kronecker reduced bilinear form that satisfies $A_{12} - A_{21} \equiv 0 \bmod 4$ and has at least one odd outer coefficient. □

Theorem 4.8.9.
Let $D \in \mathbb{Z}_{>0}$ then $3\mathrm{Cl}_c''(D) = 2\overline{\overline{\mathrm{Cl}}}_c(D)$.

Proof.
The set of complete equivalence classes of bilinear forms that are counted by $\mathrm{Cl}_c''(D)$ are contained within the set of complete equivalence classes of bilinear forms counted by $\overline{\overline{\mathrm{Cl}}}_c(D)$. Also recall the bilinear forms in a complete equivalence class that are counted by $\mathrm{Cl}_c''(D)$ all have the property $A_{11} + A_{22} \equiv 1 \bmod 2$. Then Lemma 4.8.8 shows that within a proper equivalence class of a Kronecker reduced form which has at least one odd outer coefficient and $A_{12} - A_{21} \equiv 0 \bmod 4$, we have a 2:1 ratio of complete equivalence classes that satisfy $A_{11} + A_{22} \equiv 1 \bmod 2$ to those satisfying $A_{11} + A_{22} \equiv 0 \bmod 2$. Hence $\mathrm{Cl}_c''(D) = \frac{2}{3}\overline{\overline{\mathrm{Cl}}}_c(D)$ and thus $3\mathrm{Cl}_c''(D) = 2\overline{\overline{\mathrm{Cl}}}_c(D)$. □

We now extend the ideas developed in Section 3.3.

Definition 4.8.10.
We define four subsets, $\overline{\overline{\Theta_i}} \subseteq \overline{\Theta_i}$ where $\Theta \in \{I, J\}$ and $i \in \{0, 1\}$, by strengthening the condition $A_{12} - A_{21} \equiv 0 \bmod 2$ to $A_{12} - A_{21} \equiv 0 \bmod 4$.
We then partition our new sets further using $=, >, <$ in accordance with Definitions 3.4.1, 3.4.2 and 3.5.1. We use the following notation for the cardinalities of these sets: $\overline{\overline{P}} = \left|\overline{\overline{I}}_0\right|$, $\overline{\overline{Q}} = \left|\overline{\overline{I}}_1\right|$, $\overline{\overline{R}} = \left|\overline{\overline{J}}_0\right|$ and $\overline{\overline{S}} = \left|\overline{\overline{J}}_1\right|$.

It is important to note we are still retaining the condition $A_{11} + A_{22} \equiv 1 \bmod 2$. Also since $\overline{\overline{\Theta_i}} \subseteq \overline{\Theta_i}$, it follows immediately that these new sets are finite.

Theorem 4.8.11.
Let $D \in \mathbb{Z}$ then $\overline{\overline{\mathrm{Cl}}}_c(D) = 3\left(\overline{\overline{P}} + \overline{\overline{Q}} - \overline{\overline{R}} - \overline{\overline{S}}\right)$.

Proof.
We are considering subsets of the sets B^0 and B^1 from Section 3.2. Since the sets M and N were in fact the empty set when we considered $\overline{\mathrm{Cl}}_c(D)$, they are in fact still empty. Therefore, in the same manner as we constructed $\mathrm{Cl}_c(D)$, we have

$$\mathrm{Cl}_c''(D) = 2\left(\overline{\overline{P}} + \overline{\overline{Q}} - \overline{\overline{R}} - \overline{\overline{S}}\right).$$

(One should recall the map γ found in Lemma 3.2.3 preserves the quantity $A_{12} - A_{21}$.)
Applying Theorem 4.8.9 then yields

$$\begin{aligned}\overline{\overline{\mathrm{Cl}}}_c(D) &= \frac{3}{2}\mathrm{Cl}_c''(D) \\ &= 3\left(\overline{\overline{P}} + \overline{\overline{Q}} - \overline{\overline{R}} - \overline{\overline{S}}\right).\end{aligned}$$

□

Our next goal is to derive an expression for $\frac{1}{3}\overline{\overline{\mathrm{Cl}}}_c(D) = \overline{\overline{P}} + \overline{\overline{Q}} - \overline{\overline{R}} - \overline{\overline{S}}$.

We will give a detailed proof of the result $\overline{\overline{P}} + \overline{\overline{Q}} - \overline{\overline{R}} - \overline{\overline{S}} = \overline{\overline{P_0}} + \overline{\overline{Q_0}} - \overline{\overline{R_0}} - \overline{\overline{S_0}}$. Readers wishing to omit the technical details may skip ahead to Section 4.9.
The following summary will be a key reference point for this subsection.

Summary 4.8.12.
Throughout, det $= D$ will be used to denote $A_{11}A_{22} - A_{12}A_{21} = D$.

$$\overline{\overline{I_{0,>}}} = \{\,(A_{11},A_{12},A_{21},A_{22}) \big|\, \det = D, A_{11} > A_{12}, 0 < \frac{1}{2}(A_{12}+A_{21}) \leqslant A_{11},$$
$$|A_{11}-A_{12}| < A_{22}-A_{21}, A_{11}+A_{22} \equiv 1 \bmod 2, A_{12}-A_{21} \equiv 0 \bmod 4\}$$

$$\overline{\overline{I_{0,<}}} = \{\,(A_{11},A_{12},A_{21},A_{22}) \big|\, \det = D, A_{11} < A_{12}, 0 < \frac{1}{2}(A_{12}+A_{21}) \leqslant A_{11},$$
$$|A_{11}-A_{12}| < A_{22}-A_{21}, A_{11}+A_{22} \equiv 1 \bmod 2, A_{12}-A_{21} \equiv 0 \bmod 4\}$$

$$\overline{\overline{I_{1,>}}} = \{\,(A_{11},A_{12},A_{21},A_{22}) \big|\, \det = D, A_{11} > A_{12}, 0 \leqslant \frac{1}{2}(A_{12}+A_{21}) < A_{11},$$
$$|A_{11}-A_{12}| < A_{22}-A_{21}, A_{11}+A_{22} \equiv 1 \bmod 2, A_{12}-A_{21} \equiv 0 \bmod 4\}$$

$$\overline{\overline{I_{1,<}}} = \{\,(A_{11},A_{12},A_{21},A_{22}) \big|\, \det = D, A_{11} < A_{12}, 0 \leqslant \frac{1}{2}(A_{12}+A_{21}) < A_{11},$$
$$|A_{11}-A_{12}| < A_{22}-A_{21}, A_{11}+A_{22} \equiv 1 \bmod 2, A_{12}-A_{21} \equiv 0 \bmod 4\}$$

$$\overline{\overline{J_{0,>}}} = \{\,(A_{11},A_{12},A_{21},A_{22}) \big|\, \det = D, 0 < A_{22} < \frac{1}{2}(A_{12}+A_{21}) < A_{11},$$
$$|A_{11}-A_{12}| < A_{22}-A_{21}, A_{11}+A_{22} \equiv 1 \bmod 2, A_{12}-A_{21} \equiv 0 \bmod 4\}$$

$$\overline{\overline{J_{0,<}}} = \{\,(A_{11},A_{12},A_{21},A_{22}) \big|\, \det = D, A_{22} < 0 < \frac{1}{2}(A_{12}+A_{21}) < A_{11},$$
$$|A_{11}-A_{12}| < A_{22}-A_{21}, A_{11}+A_{22} \equiv 1 \bmod 2, A_{12}-A_{21} \equiv 0 \bmod 4\}$$

$$\overline{\overline{J_{1,>}}} = \{\,(A_{11},A_{12},A_{21},A_{22}) \big|\, \det = D, 0 < A_{22} \leqslant \frac{1}{2}(A_{12}+A_{21}) < A_{11},$$
$$|A_{11}-A_{12}| < A_{22}-A_{21}, A_{11}+A_{22} \equiv 1 \bmod 2, A_{12}-A_{21} \equiv 0 \bmod 4\}$$

$$\overline{\overline{J_{1,<}}} = \{\,(A_{11},A_{12},A_{21},A_{22}) \big|\, \det = D, A_{22} < 0 \leqslant \frac{1}{2}(A_{12}+A_{21}) < A_{11},$$
$$|A_{11}-A_{12}| < A_{22}-A_{21}, A_{11}+A_{22} \equiv 1 \bmod 2, A_{12}-A_{21} \equiv 0 \bmod 4\}$$

Observation 4.8.13.
Readers may recall from Section 3.5 the manner in which we proved results such as $\overline{P_1}+\overline{P_2} = \overline{Q_1}+\overline{Q_2}$ (Lemma 3.5.3). Unfortunately, restricting these maps further fails to yield any bijections and so a different approach is required. The restriction maps of the maps W and W' (see Theorems 3.7.1 and 3.7.2) will be further restricted after we have laid the groundwork.

The following lemma will prove useful along the way.

Lemma 4.8.14.
Assume $A_{12} - A_{21} \equiv 0 \bmod 4$ *then* $2A_{12} \equiv 2A_{21} \equiv A_{12}+A_{21} \equiv 0, 2 \bmod 4$.

Proof.
Note that $A_{12} - A_{21} \equiv 0 \bmod 4$ implies $A_{12} + A_{21} \equiv 0 \bmod 2$ and thus $A_{12} + A_{21} \equiv 0$ or $2 \bmod 4$. If $A_{12} + A_{21} \equiv 0 \bmod 4$ then it is straightforward to see that A_{12} and A_{21} are both even. Consequently $4 \mid 2A_{12}$, $4 \mid 2A_{21}$ and $4 \mid (A_{12} + A_{21})$. If $A_{12} + A_{21} \equiv 2 \bmod 4$ then it is straightforward to see that both A_{12} and A_{21} are odd. Consequently $2A_{12} \equiv 2A_{21} \equiv (A_{12} + A_{21}) \equiv 2 \bmod 4$. □

Consider the set $\overline{\overline{I_{0,>}}}$ and partition it into $\overline{\overline{I_{0,>}}} = \overline{\overline{I_{0,>,e}}} \cup \overline{\overline{I_{0,<,o}}}$, where

$$\overline{\overline{I_{0,>,e}}} = \left\{ A \in \overline{\overline{I_{0,>}}} | A_{11} \equiv 0 \bmod 2 \right\} \text{ and}$$
$$\overline{\overline{I_{0,<,o}}} = \left\{ A \in \overline{\overline{I_{0,>}}} | A_{11} \equiv 1 \bmod 2 \right\}.$$

Recall the set $\overline{X_1}$ and its associated map $\phi\Big|_{\overline{X_1}}$ from Lemma 3.5.4. Now consider the subsets $\overline{\overline{X_{1,e}}}$, $\overline{\overline{X_{1,o}}} \subseteq \overline{X_1}$, where

$$\overline{\overline{X_{1,e}}} = \left\{ (\alpha, \beta, \gamma, \delta) \in \overline{X_1} \mid \beta \equiv 0 \bmod 2, 2\alpha \equiv \delta \bmod 4 \right\} \text{ and}$$
$$\overline{\overline{X_{1,o}}} = \left\{ (\alpha, \beta, \gamma, \delta) \in \overline{X_1} \mid \beta \equiv 1 \bmod 2, 2\alpha \not\equiv \delta \bmod 4 \right\}.$$

Lemma 4.8.15.
The restriction map $\phi\Big|_{\overline{\overline{X_{1,e}}}} : \overline{\overline{X_{1,e}}} \longrightarrow \overline{\overline{I_{0,>,e}}}$ *is a bijection.*

Proof.
Well-defined: It is enough to show $A_{12} - A_{21} \equiv 0 \bmod 4$ and $A_{11} \equiv 0 \bmod 2$. We have $A_{12} - A_{21} = (\beta - \alpha) - (\alpha - \beta + \delta) = 2(\beta - \alpha) - \delta \equiv 2\alpha - \delta \equiv 0 \bmod 4$ as $2\beta \equiv 0 \bmod 4$ and $2\alpha \equiv \delta \bmod 4$. Also, $A_{11} = \beta \equiv 0 \bmod 2$ and so the restriction is well-defined.
Injectivity: Inherited.
Surjectivity: Let $f = (A_{11}, A_{12}, A_{21}, A_{22}) \in \overline{\overline{I_{0,>,e}}}$ be arbitrary and let
$g = (A_{11} - A_{12}, A_{11}, -A_{11} + A_{12} - A_{21} + A_{22}, A_{12} + A_{21})$. Then $g \in \overline{X_1}$ and satisfies $\beta = A_{11} \equiv 0 \bmod 2$ and $2\alpha - \delta = 2A_{11} - 2A_{12} - (A_{12} + A_{21}) \equiv 2A_{11} + 2A_{12} - (A_{12} + A_{21}) \equiv 0 \bmod 4$ due to Lemma 4.8.14 and $A_{11} \equiv 0 \bmod 2$.
Finally observe $\phi\Big|_{\overline{\overline{X_{1,e}}}}(g) = f$. Thus the restriction map is surjective and hence we have the desired bijection. □

Lemma 4.8.16.
The restriction map, $\phi\Big|_{\overline{\overline{X_{1,o}}}} : \overline{\overline{X_{1,o}}} \longrightarrow \overline{\overline{I_{0,>,o}}}$ *is a bijection.*

Proof.
Well-defined: It is enough to show $A_{12} - A_{21} \equiv 0 \bmod 4$ and $A_{11} \equiv 1 \bmod 2$. We have $A_{12} - A_{21} = 2(\beta - \alpha) - \delta \equiv 0 \bmod 4$ as $\beta \equiv 1 \bmod 2$ and then if $\alpha \equiv 1 \bmod 2$ we have $\delta \equiv 0 \bmod 4$, whilst if $\alpha \equiv 0 \bmod 2$ then $\delta \equiv 2 \bmod 4$. We also have $A_{11} = \beta \equiv 1 \bmod 2$.
Injectivity: This is inherited.

Surjectivity: Let $f = (A_{11}, A_{12}, A_{21}, A_{22}) \in \overline{\overline{I_{0,>,o}}}$ be arbitrary and g be the same as in the proof of Lemma 4.8.15. Then $g \in \overline{X_1}$ and satisfies $\beta = A_{11} \equiv 1 \bmod 2$ and by Lemma 4.8.14 we have $2\alpha - \delta = 2A_{11} - 2A_{12} - (A_{12} + A_{21}) \equiv 2A_{11} + 2A_{12} - (A_{12} + A_{21}) \equiv 2 \bmod 4$ as $A_{11} \equiv 1 \bmod 2$. Thus $2\alpha \not\equiv \delta \bmod 4$.
Finally note that $\phi\Big|_{\overline{\overline{X_{1,o}}}}(g) = f$. Thus the restriction map is surjective and hence we have the desired bijection. □

Corollary 4.8.17.
$\overline{\overline{P_1}} = \left|\overline{\overline{X_{1,e}}}\right| + \left|\overline{\overline{X_{1,o}}}\right|$. □

Next, consider the set $\overline{\overline{I_{0,<}}} \subseteq \overline{I_{0,<}} \subseteq I_{0,<}$, expressing it as a disjoint union of $\overline{\overline{I_{0,<,e}}}$ and $\overline{\overline{I_{0,<,o}}}$, where

$$\overline{\overline{I_{0,<,e}}} = \left\{ A \in \overline{\overline{I_{0,<}}} \,\middle|\, A_{11} \equiv 0 \bmod 2 \right\} \text{ and}$$
$$\overline{\overline{I_{0,<,o}}} = \left\{ A \in \overline{\overline{I_{0,<}}} \,\middle|\, A_{11} \equiv 1 \bmod 2 \right\}.$$

Recall from Lemma 3.4.7 the set X_2 and the map $\psi : X_2 \longrightarrow I_{0,<}$. Further, recall the set $\overline{X_2} \subseteq X_2$ as defined in Lemma 3.5.5.
Thus we consider the subsets $\overline{\overline{X_{2,e}}}, \overline{\overline{X_{2,o}}} \subseteq \overline{X_2} \subseteq X_2$, where
$\overline{\overline{X_{2,e}}} = \{(\alpha, \beta, \gamma, \delta) \in \overline{X_2} \mid \beta \equiv 0 \bmod 2, 2\alpha \equiv \delta \bmod 4\}$ and
$\overline{\overline{X_{2,o}}} = \{(\alpha, \beta, \gamma, \delta) \in \overline{X_2} \mid \beta \equiv 1 \bmod 2, 2\alpha \equiv \delta \bmod 4\}$.

The following observation will help streamline a couple of forthcoming proofs.

Observation 4.8.18.
Under the assumption $2\alpha \equiv \delta \bmod 4$, δ is even and so $\delta \equiv -\delta \bmod 4$.
Hence $2\alpha + \delta \equiv 2\alpha - \delta \equiv 0 \bmod 4$.

Note Observation 4.8.18 shows $2\alpha \equiv \delta \bmod 4$ is the same as $2\alpha \equiv -\delta \bmod 4$ when $\delta \equiv 0 \bmod 2$.

Lemma 4.8.19.
The restriction map, $\psi\Big|_{\overline{\overline{X_{2,e}}}} : \overline{\overline{X_{2,e}}} \longrightarrow \overline{\overline{I_{0,<,e}}}$ *is a bijection.*

Proof.
Well-defined: It is enough to show $A_{11} \equiv 0 \bmod 2$ and $A_{12} - A_{21} \equiv 0 \bmod 4$. We have $A_{11} = \beta \equiv 0 \bmod 2$, and by Observation 4.8.18 $A_{12} - A_{21} = \alpha + \beta - (\beta - \alpha - \delta) = 2\alpha + \delta \equiv 0 \bmod 4$.
Injectivity: This is inherited.
Surjectivity: Let $f = (A_{11}, A_{12}, A_{21}, A_{22}) \in \overline{\overline{I_{0,<,e}}}$ be arbitrary and consider $g = (A_{12} - A_{11}, A_{11}, A_{11} - A_{12} - A_{21} + A_{22}, 2A_{11} - A_{12} - A_{21})$. Then $g \in X_2$ and satisfies $\beta = A_{11} \equiv 0 \bmod 2$ and by Lemma 4.8.14 $2\alpha - \delta = 2A_{12} - 2A_{11} - (2A_{11} - A_{12} - A_{21}) \equiv 2A_{12} + (A_{12} + A_{21}) \equiv 0 \bmod 4$.

Finally, note $\psi\Big|_{\overline{\overline{X_{2,e}}}}(g) = f$, so the restriction map is surjective and hence is a bijection. □

Lemma 4.8.20.
The restriction map, $\psi\Big|_{\overline{\overline{X_{2,o}}}} : \overline{\overline{X_{2,o}}} \longrightarrow \overline{\overline{I_{0,<,o}}}$ *is a bijection.*

Proof.
Well-defined: It is sufficient to show $A_{11} \equiv 1 \bmod 2$ and $A_{12} - A_{21} \equiv 0 \bmod 4$. We have $A_{11} = \beta \equiv 1 \bmod 2$ and $A_{12} - A_{21} = 2\alpha + \delta \equiv 0 \bmod 4$ by Observation 4.8.18.
Injectivity: Inherited.
Surjectivity: Let $f = (A_{11}, A_{12}, A_{21}, A_{22}) \in \overline{\overline{I_{0,<,o}}}$ be arbitrary and let g be the same as in Lemma 4.8.19. The $g \in X_2$ and satisfies $\beta = A_{11} \equiv 1 \bmod 2$ as well as $\delta - 2\alpha = (2A_{11} - A_{12} - A_{21}) - 2(A_{12} - A_{11}) = 4A_{11} - (A_{12} + A_{21}) - 2A_{12} \equiv 0 \bmod 4$ by Lemma 4.8.14.
Lastly, $\psi\Big|_{\overline{\overline{X_{2,o}}}}(g) = f$, so the restriction map surjective and thus is a bijection. □

Corollary 4.8.21.
$\overline{\overline{P_2}} = \left|\overline{\overline{X_{2,e}}}\right| + \left|\overline{\overline{X_{2,o}}}\right|$. □

Next, consider the set $\overline{\overline{I_{1,>}}} \subseteq \overline{I_{1,>}}$, partitioning it into the sets $\overline{\overline{I_{1,>,e}}}$ and $\overline{\overline{I_{1,>,o}}}$, where

$$\overline{\overline{I_{1,>,e}}} = \left\{A \in \overline{\overline{I_{1,>}}} \mid A_{11} \equiv 0 \bmod 2\right\} \text{ and}$$
$$\overline{\overline{I_{1,>,o}}} = \left\{A \in \overline{\overline{I_{1,>}}} \mid A_{11} \equiv 1 \bmod 2\right\}.$$

Then recall the map $\hat{\phi}\big|_{\overline{X_2}}$ from Corollary 3.5.11 and consider the following subsets of $\overline{X_2}$, namely $\overline{\overline{X_{2,e}}}$ (from Lemma 4.8.19) and
$\overline{\overline{X'_{2,o}}} = \left\{(\alpha, \beta, \gamma, \delta) \in \overline{X_2} \mid \beta \equiv 1 \bmod 2, 2\alpha \not\equiv \delta \bmod 4\right\}$.

Lemma 4.8.22.
The restriction map, $\hat{\phi}\big|_{\overline{\overline{X_{2,e}}}} : \overline{\overline{X_{2,e}}} \longrightarrow \overline{\overline{I_{1,>,e}}}$ *is a bijection.*

Proof.
Well-defined: It is enough to show $A_{11} \equiv 0 \bmod 2$ and $A_{12} - A_{21} \equiv 0 \bmod 4$. We have $A_{11} = \beta \equiv 0 \bmod 2$ and $A_{12} - A_{21} = (\beta - \alpha) - (\alpha - \beta + \delta) = 2(\beta - \alpha) - \delta \equiv 2\alpha - \delta \equiv 0 \bmod 4$ as $\beta \equiv 0 \bmod 2$.
Injectivity: This is inherited.
Surjectivity: Let $f = (A_{11}, A_{12}, A_{21}, A_{22}) \in \overline{\overline{I_{1,>,e}}}$ be arbitrary and let $g = (A_{11} - A_{12}, A_{11}, -A_{11} + A_{12} - A_{21} + A_{22}, A_{12} + A_{21})$. Then $g \in \overline{X_2}$ and satisfies $\beta = A_{11} \equiv 0 \bmod 2$ and $2\alpha - \delta = 2A_{11} - 2A_{12} - (A_{12} + A_{21}) \equiv -2A_{12} - (A_{12} + A_{21}) \equiv 0 \bmod 4$ by using Lemma 4.8.14 and $A_{11} \equiv 0 \bmod 2$.
Lastly we note $\hat{\phi}\Big|_{\overline{\overline{X_{2,e}}}}(g) = f$, so the restriction map is surjective and hence is a bijection. □

Lemma 4.8.23.
The restriction map, $\hat{\phi}\big|_{\overline{\overline{X'_{2,o}}}} : \overline{\overline{X'_{2,o}}} \longrightarrow \overline{\overline{I_{1,>,o}}}$ *is a bijection.*

Proof.
Well-defined: It is enough to show $A_{11} \equiv 1 \bmod 2$ and $A_{12} - A_{21} \equiv 0 \bmod 4$. We have $A_{11} = \beta \equiv 1 \bmod 2$ and $A_{12} - A_{21} = 2(\beta - \alpha) - \delta \equiv 0 \bmod 4$. The last result follows from $\delta \equiv 0 \bmod 2$ in $\overline{X_2}$ and $2\alpha - \delta \equiv 2 \bmod 4$ since $2\alpha \not\equiv \delta \bmod 4$.
Injectivity: This is inherited.
Surjectivity: Let $f = (A_{11}, A_{12}, A_{21}, A_{22}) \in \overline{\overline{I_{1,>,o}}}$ be arbitrary and consider g as in the proof of Lemma 4.8.22. Then $g \in \overline{X_2}$ and satisfies $\beta = A_{11} \equiv 1 \bmod 2$ as well as $2\alpha - \delta = 2A_{11} - 2A_{12} - (A_{12} + A_{21}) \equiv 2A_{11} \equiv 2 \bmod 4$ by Lemma 4.8.14. Thus $2\alpha \not\equiv \delta \bmod 4$.
Lastly, we observe $\hat{\phi}\big|_{\overline{\overline{X'_{2,o}}}}(g) = f$, so the restriction map is surjective and hence is a bijection. □

Corollary 4.8.24.
$\overline{\overline{Q_1}} = \left|\overline{\overline{I_{1,>}}}\right| = \left|\overline{\overline{I_{1,>,e}}}\right| + \left|\overline{\overline{I_{1,>,o}}}\right| = \left|\overline{\overline{X_{2,e}}}\right| + \left|\overline{\overline{X'_{2,o}}}\right|$. □

Next, consider the set $\overline{\overline{I_{1,<}}} \subseteq \overline{I_{1,<}}$, partitioning it into the sets $\overline{\overline{I_{1,<,e}}}$ and $\overline{\overline{I_{1,<,o}}}$, where

$$\overline{\overline{I_{1,<,e}}} = \left\{ A \in \overline{\overline{I_{1,<}}} \mid A_{11} \equiv 0 \bmod 2 \right\} \text{ and}$$
$$\overline{\overline{I_{1,<,o}}} = \left\{ A \in \overline{\overline{I_{1,<}}} \mid A_{11} \equiv 1 \bmod 2 \right\}.$$

Recall the map $\hat{\psi}$ from Corollary 3.5.12 and the set $\overline{X_1}$ from Lemma 3.5.4.
Thus we consider the subsets $\overline{\overline{X_{1,e}}}$, $\overline{\overline{X'_{1,o}}} \subseteq \overline{X_1}$ where $\overline{\overline{X_{1,e}}}$ is the same as in Lemma 4.8.15 and $\overline{\overline{X'_{1,o}}} = \left\{(\alpha, \beta, \gamma, \delta) \in \overline{X_1} \mid \beta \equiv 1 \bmod 2, 2\alpha \equiv \delta \bmod 4\right\}$.

Lemma 4.8.25.
The restriction map, $\hat{\psi}\big|_{\overline{\overline{X_{1,e}}}} : \overline{\overline{X_{1,e}}} \longrightarrow \overline{\overline{I_{1,<,e}}}$ *is a bijection.*

Proof.
Well-defined: It is enough to show $A_{11} \equiv 0 \bmod 2$ and $A_{12} - A_{21} \equiv 0 \bmod 4$. We have $A_{11} = \beta \equiv 0 \bmod 2$,then using $\beta \equiv 0 \bmod 2$ and applying Observation 4.8.18 we have $A_{12} - A_{21} = (\alpha + \beta) - (\beta - \alpha - \delta) = 2\alpha + \delta \equiv 2\alpha - \delta \equiv 0 \bmod 4$. Thus the restriction map is well-defined.
Injectivity: This is inherited.
Surjectivity: Let $f = (A_{11}, A_{12}, A_{21}, A_{22}) \in \overline{\overline{I_{1,<,e}}}$ be arbitrary and let
$g = (A_{12} - A_{11}, A_{11}, A_{11} - A_{12} - A_{21} + A_{22}, 2A_{11} - A_{12} - A_{21})$. Then $g \in \overline{X_1}$ and it satisfies $\beta = A_{11} \equiv 0 \bmod 2$ as well as $2\alpha - \delta = 2A_{12} - 2A_{11} - 2A_{11} + A_{12} + A_{21} \equiv 2A_{12} + (A_{12} + A_{21}) \equiv 0 \bmod 4$ by Lemma 4.8.14. Lastly, we observe $\hat{\psi}\big|_{\overline{\overline{X_{1,e}}}}(g) = f$, so the restriction map is surjective and hence is a bijection. □

Lemma 4.8.26.
The restriction map $\hat{\psi}\big|_{\overline{\overline{X'_{1,o}}}} : \overline{\overline{X'_{1,o}}} \longrightarrow \overline{\overline{I_{1,<,o}}}$ *is a bijection.*

Proof.
Well-defined: It is enough to show $A_{11} \equiv 1 \bmod 2$ and $A_{12} - A_{21} \equiv 0 \bmod 4$. We have $A_{11} = \beta \equiv 1 \bmod 2$ and $A_{12} - A_{21} = (\alpha+\beta) - (\beta - \alpha - \delta) = 2\alpha + \delta \equiv 2\alpha - \delta \equiv 0 \bmod 4$ by Observation 4.8.18 and $2\alpha \equiv \delta \bmod 4$.
Injectivity: This is inherited.
Surjectivity: Let $f = (A_{11}, A_{12}, A_{21}, A_{22}) \in \overline{\overline{I_{1,<,o}}}$ be arbitrary and consider g as given in the proof of Lemma 4.8.25. Then $g \in \overline{X_1}$ and satisfies $\beta = A_{11} \equiv 1 \bmod 2$ as well as $2\alpha - \delta = 2A_{12} - 2A_{11} - 2A_{11} + A_{12} + A_{21} \equiv 2A_{12} + (A_{12} + A_{21}) \equiv 0 \bmod 4$ by Lemma 4.8.14. Therefore the restriction map is a surjection and hence is a bijection. □

Corollary 4.8.27.
$\overline{\overline{Q_2}} = \left|\overline{\overline{I_{1,<}}}\right| = \left|\overline{\overline{I_{1,<,e}}}\right| + \left|\overline{\overline{I_{1,<,o}}}\right| = \left|\overline{\overline{X_{1,e}}}\right| + \left|\overline{\overline{X'_{1,o}}}\right|$. □

Now consider the set $\overline{\overline{J_{0,>}}}$, partitioning it into and disjoint union of the sets $\overline{\overline{J_{0,>,e}}}$ and $\overline{\overline{J_{0,>,o}}}$, where

$$\overline{\overline{J_{0,>,e}}} = \left\{ A \in \overline{\overline{J_{0,>}}} \mid A_{22} \equiv 0 \bmod 2 \right\} \text{ and}$$
$$\overline{\overline{J_{0,>,o}}} = \left\{ A \in \overline{\overline{J_{0,>}}} \mid A_{22} \equiv 1 \bmod 2 \right\}.$$

Recall the map $\iota\big|_{\overline{Y_1}}$ from Lemma 3.5.7 and consider the subsets $\overline{\overline{Y_{1,e}}}, \overline{\overline{Y_{1,o}}} \subseteq \overline{Y_1}$ where,
$\overline{\overline{Y_{1,e}}} = \{(\alpha, \beta, \gamma, \delta) \mid \beta \equiv 0 \bmod 2, 2\alpha \equiv \delta \bmod 4\}$ and
$\overline{\overline{Y_{1,o}}} = \{(\alpha, \beta, \gamma, \delta) \mid \beta \equiv 1 \bmod 2, 2\alpha \equiv \delta \bmod 4\}$.

Lemma 4.8.28.
The restriction of the map $\iota\big|_{\overline{Y_1}}$ *to the set* $\overline{\overline{Y_{1,e}}}$*, given by* $\iota\big|_{\overline{\overline{Y_{1,e}}}} : \overline{\overline{Y_{1,e}}} \longrightarrow \overline{\overline{J_{0,>,e}}} \subseteq \overline{J_{0,>}}$ *is a bijection.*

Proof.
Well-defined: It is enough to show $A_{22} \equiv 0 \bmod 2$ and $A_{12} - A_{21} \equiv 0 \bmod 4$. We have $A_{22} = \beta \equiv 0 \bmod 2$ and by applying Observation 4.8.18 we see $A_{12} - A_{21} = (\alpha + \beta + \delta) - (\beta - \alpha) \equiv 2\alpha + \delta \equiv 0 \bmod 4$.
Injectivity: This is inherited.
Surjectivity: Let $f = (A_{11}, A_{12}, A_{21}, A_{22}) \in \overline{\overline{J_{0,>,e}}}$ and let
$g = (A_{22} - A_{21}, A_{22}, A_{11} - A_{12} - A_{21} + A_{22}, A_{12} + A_{21} - 2A_{22})$. Then $g \in \overline{Y_1}$ and it satisfies $\beta = A_{22} \equiv 0 \bmod 2$ and also $2\alpha - \delta = (2A_{22} - 2A_{21}) - (A_{12} + A_{21} - 2A_{22}) \equiv -2A_{21} - (A_{12} + A_{21}) \equiv 0 \bmod 4$ by Observation 4.8.18.
It is straightforward to verify $\iota\big|_{\overline{\overline{Y_{1,e}}}}(g) = f$, thus the restriction map is a surjection and hence is a bijection. □

Lemma 4.8.29.
The restriction of the map $\iota\big|_{\overline{Y_1}}$ to the set $\overline{\overline{Y_{1,o}}}$, given by $\iota\big|_{\overline{\overline{Y_{1,o}}}} : \overline{\overline{Y_{1,o}}} \longrightarrow \overline{\overline{J_{0,>,o}}} \subseteq \overline{J_{0,>}}$ is a bijection.

Proof.
Well-defined: It is enough to show $A_{22} \equiv 1 \bmod 2$ and $A_{12} - A_{21} \equiv 0 \bmod 4$. We have $A_{22} = \beta \equiv 1 \bmod 2$ and further, $A_{12} - A_{21} = 2\alpha + \delta \equiv 0 \bmod 4$ by Observation 4.8.18.
Injectivity: This is inherited.
Surjectivity: Let $f = (A_{11}, A_{12}, A_{21}, A_{22}) \in \overline{\overline{J_{0,>,o}}}$ be arbitrary and g be the same as in the proof of Lemma 4.8.28. Then $g \in \overline{Y_1}$ and it satisfies $\beta = A_{22} \equiv 1 \bmod 2$ and also $2\alpha - \delta = 2A_{22} - 2A_{21} - (A_{12} + A_{21} - 2A_{22}) = 4A_{22} - 2A_{21} - (A_{12} + A_{21}) \equiv -2A_{21} - (A_{12} + A_{21}) \equiv 0 \bmod 4$ by Lemma 4.8.14.
Lastly, we note that $\iota\big|_{\overline{\overline{Y_{1,o}}}}(g) = f$ and so the restriction map is surjective and hence is a bijection. □

Corollary 4.8.30.
$\overline{\overline{R_1}} = \left|\overline{\overline{J_{0,>}}}\right| = \left|\overline{\overline{J_{0,>,e}}}\right| + \left|\overline{\overline{J_{0,>,o}}}\right| = \left|\overline{\overline{Y_{1,e}}}\right| + \left|\overline{\overline{Y_{1,o}}}\right|$. □

Now consider $\overline{\overline{J_{0,<}}}$, partitioning it into a disjoint union of the sets $\overline{\overline{J_{0,<,e}}}$ and $\overline{\overline{J_{0,<,o}}}$, where

$$\overline{\overline{J_{0,<,e}}} = \left\{A \in \overline{\overline{J_{0,<}}} \mid A_{22} \equiv 0 \bmod 2\right\} \text{ and}$$
$$\overline{\overline{J_{0,<,o}}} = \left\{A \in \overline{\overline{J_{0,<}}} \mid A_{22} \equiv 1 \bmod 2\right\}.$$

Recall the map $\hat{\iota}\big|_{\overline{Y_1}}$ from Corollary 3.5.13 and consider the following subsets of $\overline{Y_1}$, namely $\overline{\overline{Y_{1,e}}}$ (from Lemma 4.8.28) and $\overline{\overline{Y'_{1,o}}} = \{(\alpha, \beta, \gamma, \delta) \mid \beta \equiv 1 \bmod 2, 2\alpha \not\equiv \delta \bmod 4\}$.

Lemma 4.8.31.
The restriction map $\hat{\iota}\big|_{\overline{\overline{Y_{1,e}}}} : \overline{\overline{Y_{1,e}}} \longrightarrow \overline{\overline{J_{0,<,e}}}$ is a bijection.

Proof.
Well-defined: It is sufficient to show $A_{22} \equiv 0 \bmod 2$ and $A_{12} - A_{21} \equiv 0 \bmod 4$. We have $A_{22} = -\beta \equiv 0 \bmod 2$ and by Observation 4.8.18 we have $A_{12} - A_{21} = (\alpha + \beta + \delta) - (-\beta - \alpha) = 2(\beta + \alpha) + \delta \equiv 2\alpha + \delta \equiv 0 \bmod 4$.
Injectivity: This is inherited.
Surjectivity: Let $f = (A_{11}, A_{12}, A_{21}, A_{22}) \in \overline{\overline{J_{0,<,e}}}$ be arbitrary and let
$g = (A_{22} - A_{21}, -A_{22}, -A_{11} + A_{12} - A_{21} + A_{22}, A_{12} + A_{21})$. Then $g \in \overline{Y_1}$ and it satisfies $\beta = -A_{22} \equiv 0 \bmod 2$ as well as $2\alpha - \delta = 2A_{22} - 2A_{21} - (A_{12} + A_{21}) \equiv -2A_{21} - (A_{12} + A_{21}) \equiv 0 \bmod 4$ by Lemma 4.8.14.
Lastly it is straightforward to note $\hat{\iota}\big|_{\overline{\overline{Y_{1,e}}}}(g) = f$, so the restriction is surjective and thus is a bijection. □

Lemma 4.8.32.
The restriction map $\hat{\imath}\big|_{\overline{\overline{Y_{1,o'}}}} : \overline{\overline{Y'_{1,o}}} \longrightarrow \overline{\overline{J_{0,<,o}}}$ *is a bijection.*

Proof.
Well-defined: It is enough to show $A_{22} \equiv 1 \bmod 2$ and $A_{12} - A_{21} \equiv 0 \bmod 4$. We have $A_{22} = -\beta \equiv 1 \bmod 2$. Further, $A_{12} - A_{21} = 2(\beta + \alpha) + \delta \equiv 0 \bmod 4$ since in $\overline{Y_1}$ we have $\delta \equiv 0 \bmod 2$ and we also have $2\alpha \not\equiv \delta \bmod 4$. Using Observation 4.8.18 then gives the result.
Injectivity: This is inherited.
Surjectivity: Let $f = (A_{11}, A_{12}, A_{21}, A_{22}) \in \overline{\overline{J_{0,<,o}}}$ be arbitrary and consider g as in the proof of Lemma 4.8.31. Then $g \in \overline{Y_1}$ and satisfies $\beta = -A_{22} \equiv 1 \bmod 2$. Further, by Lemma 4.8.14 we have $2\alpha - \delta = 2A_{22} - 2A_{21} - (A_{12} + A_{21}) \equiv 2A_{22} \equiv 2 \bmod 4$, thus $2\alpha \not\equiv \delta \bmod 4$.
Lastly it is straightforward to check $\hat{\imath}\big|_{\overline{\overline{Y'_{1<o}}}}(g) = f$, so the restriction map is surjective and hence is a bijection. □

Corollary 4.8.33.
$\overline{\overline{R_2}} = \left|\overline{\overline{J_{0,<}}}\right| = \left|\overline{\overline{J_{0,<,e}}}\right| + \left|\overline{\overline{J_{0,<,o}}}\right| = \left|\overline{\overline{Y_{1,e}}}\right| + \left|\overline{\overline{Y'_{1,o}}}\right|$. □

Now consider $\overline{\overline{J_{1,>}}}$, partitioning it into a disjoint union of the sets $\overline{\overline{J_{1,>,e}}}$ and $\overline{\overline{J_{1,>,o}}}$, where

$$\overline{\overline{J_{1,>,e}}} = \left\{ A \in \overline{\overline{J_{1,>}}} \mid A_{22} \equiv 0 \bmod 2 \right\}$$
$$\overline{\overline{J_{1,>,o}}} = \left\{ A \in \overline{\overline{J_{1,>}}} \mid A_{22} \equiv 1 \bmod 2 \right\}.$$

Recall the map $\Gamma\big|_{\overline{Y_2}}$ from Lemma 3.5.9 and consider the subsets $\overline{\overline{Y_{2,e}}}$, $\overline{\overline{Y_{2,o}}} \subseteq \overline{Y_2}$, where

$$\overline{\overline{Y_{2,e}}} = \left\{ (\alpha, \beta, \gamma, \delta) \in \overline{Y_2} \mid \beta \equiv 0 \bmod 2, 2\alpha \equiv \delta \bmod 4 \right\} \text{ and}$$
$$\overline{\overline{Y_{2,o}}} = \left\{ (\alpha, \beta, \gamma, \delta) \in \overline{Y_2} \mid \beta \equiv 1 \bmod 2, 2\alpha \equiv \delta \bmod 4 \right\}.$$

Lemma 4.8.34.
The restriction of the map $\Gamma\big|_{\overline{Y_2}}$ *to the subset* $\overline{\overline{Y_{2,e}}}$ *given by* $\Gamma\big|_{\overline{\overline{Y_{2,e}}}} : \overline{\overline{Y_{2,e}}} \longrightarrow \overline{\overline{J_{1,>,e}}} \subseteq \overline{J_{1,>}}$ *is a bijection.*

Proof.
Well-defined: It is enough to show $A_{22} \equiv 0 \bmod 2$ and $A_{12} - A_{21} \equiv 0 \bmod 4$. We have $A_{22} = \beta \equiv 0 \bmod 2$ and $A_{12} - A_{21} = (\alpha + \beta + \delta) - (\beta - \alpha) = 2\alpha + \delta \equiv 2\alpha - \delta \equiv 0 \bmod 4$ by Observation 4.8.18.
Injectivity: This is inherited.
Surjectivity: Let $f = (A_{11}, A_{12}, A_{21}, A_{22}) \in \overline{\overline{J_{1,>,e}}}$ be arbitrary and let
$g = (A_{22} - A_{21}, A_{22}, A_{11} - A_{12} - A_{21} + A_{22}, A_{12} + A_{21} - 2A_{22})$. Then $g \in \overline{Y_2}$ and it satisfies $\beta = A_{22} \equiv 0 \bmod 2$ as well as $2\alpha - \delta = 2A_{22} - 2A_{21} - (A_{12} + A_{21}) + 2A_{22} \equiv -2A_{21} - (A_{12} + A_{21}) \equiv 0 \bmod 4$ by Lemma 4.8.14.

Lastly, it is straightforward to verify $\Gamma\big|_{\overline{\overline{Y_{2,e}}}}(g) = f$ and thus the restriction map is surjective. It follows that the restriction map is a bijection. □

Lemma 4.8.35.
The restriction of the map $\Gamma\big|_{\overline{Y_2}}$ to the subset $\overline{\overline{Y_{2,o}}}$, given by $\Gamma\big|_{\overline{\overline{Y_{2,o}}}} : \overline{\overline{Y_{2,o}}} \longrightarrow \overline{\overline{J_{1,>,o}}}$, is a well-defined bijection.

Proof.
Well-defined: It is enough to show $A_{22} \equiv 1 \bmod 2$ and $A_{12} - A_{21} \equiv 0 \bmod 4$. We have $A_{22} = \beta \equiv 1 \bmod 2$ and $A_{12} - A_{21} = 2\alpha + \delta \equiv 2\alpha - \delta \equiv 0 \bmod 4$ by Observation 4.8.18.
Injectivity: This is inherited.
Surjectivity: Let $f = (A_{11}, A_{12}, A_{21}, A_{22}) \in \overline{\overline{J_{1,>,o}}}$ be arbitrary and consider g as in the proof of Lemma 4.8.34. Then $g \in \overline{Y_2}$ and it satisfies $\beta = A_{22} \equiv 1 \bmod 2$ as well as $2\alpha - \delta = 2A_{22} - 2A_{21} - (A_{12} + A_{21}) + 2A_{22} \equiv -2A_{21} - (A_{12} + A_{21}) \equiv 0 \bmod 4$ due to Lemma 4.8.14.
Lastly, it is straightforward to see $\Gamma\big|_{\overline{\overline{Y_{2,o}}}}(g) = f$ and thus the restriction map is surjective. Therefore the restriction map is a bijection. □

Corollary 4.8.36.
$\overline{\overline{S_1}} = \left|\overline{\overline{J_{1,>}}}\right| = \left|\overline{\overline{J_{1,>,e}}}\right| + \left|\overline{\overline{J_{1,>,o}}}\right| = \left|\overline{\overline{Y_{2,e}}}\right| + \left|\overline{\overline{Y_{2,o}}}\right|$. □

Lastly, consider the set $\overline{\overline{J_{1,<}}}$, partitioning it into a disjoint union of the subsets $\overline{\overline{J_{1,<,e}}}$ and $\overline{\overline{J_{1,<,o}}}$, where

$$\overline{\overline{J_{1,<,e}}} = \left\{A \in \overline{\overline{J_{1,<}}} \mid A_{22} \equiv 0 \bmod 2\right\} \text{ and}$$
$$\overline{\overline{J_{1,<,o}}} = \left\{A \in \overline{\overline{J_{1,<}}} \mid A_{22} \equiv 1 \bmod 2\right\}.$$

Now recall the map $\hat{\Gamma}$ from Corollary 3.5.14 and consider the following subsets of $\overline{Y_2}$, $\overline{\overline{Y_{2,e}}}$ (from Lemma 4.8.34) and $\overline{\overline{Y'_{2,o}}} = \{(\alpha, \beta, \gamma, \delta) \mid \beta \equiv 1 \bmod 2, 2\alpha \not\equiv \delta \bmod 4\}$.

Lemma 4.8.37.
The restriction of the map $\hat{\Gamma}$ to the subset $\overline{\overline{Y_{2,e}}}$, given by $\hat{\Gamma}\big|_{\overline{\overline{Y_{2,e}}}} : \overline{\overline{Y_{2,e}}} \longrightarrow \overline{\overline{J_{1,<,e}}} \subseteq \overline{J_{1,<}}$ is a well-defined bijection.

Proof.
Well-defined: It is enough to show $A_{22} \equiv 0 \bmod 2$ and $A_{12} - A_{21} \equiv 0 \bmod 4$. We have $A_{22} = -\beta \equiv 0 \bmod 4$ and $A_{12} - A_{21} = (\alpha + \beta + \delta) - (-\beta - \alpha) = 2(\beta + \alpha) + \delta \equiv 2\alpha + \delta \equiv 0 \bmod 4$ by Observation 4.8.18.
Injectivity: This is inherited.
Surjectivity: Let $f = (A_{11}, A_{12}, A_{21}, A_{22}) \in \overline{\overline{J_{1,<,e}}}$ be arbitrary and let
$g = (A_{22} - A_{21}, -A_{22}, -A_{11} + A_{12} - A_{21} + A_{22}, A_{12} + A_{21})$. Then $g \in \overline{Y_2}$ and it satisfies $\beta = -A_{22} \equiv 0 \bmod 2$ as well as $2\alpha - \delta = 2A_{22} - 2A_{21} - (A_{12} + A_{21}) \equiv -2A_{21} - (A_{12} + A_{21}) \equiv 0 \bmod 4$ by Observation 4.8.18.

Lastly, it is straightforward to check that $\hat{\Gamma}\big|_{\overline{\overline{Y_{2,e}}}}(g) = f$ and so the restriction map is surjective and thus is a bijection. □

Lemma 4.8.38.
The restriction of the map $\hat{\Gamma}$ to the subset $\overline{\overline{Y'_{2,o}}}$, given by $\hat{\Gamma}\big|_{\overline{\overline{Y'_{2,o}}}} : \overline{\overline{Y'_{2,o}}} \longrightarrow \overline{\overline{J_{1,<,o}}}$ is a well-defined bijection.

Proof.
Well-defined: It is enough to show $A_{22} \equiv 1 \bmod 2$ and $A_{12} - A_{21} \equiv 0 \bmod 4$. We have $A_{22} = -\beta \equiv 1 \bmod 2$ and $A_{12} - A_{21} = 2(\beta + \alpha) + \delta \equiv 2\beta + 2\alpha - \delta \equiv 0 \bmod 4$ by Observation 4.8.18.
Injectivity: This is inherited.
Surjectivity: Let $f = (A_{11}, A_{12}, A_{21}, A_{22}) \in \overline{\overline{J_{1,<,o}}}$ be arbitrary and let g be the same as in the proof of Lemma 4.8.37. Then $g \in \overline{Y_2}$ and it satisfies $\beta = -A_{22} \equiv 1 \bmod 2$ as well as $A_{12} - A_{21} = 2A_{22} - 2A_{21} - (A_{12} + A_{21}) \equiv 2A_{22} \equiv 2 \bmod 4$ by the use of Lemma 4.8.14.
Lastly it is straightforward to show $\hat{\Gamma}\big|_{\overline{\overline{Y'_{2,o}}}}(g) = f$, so the restriction map is surjective and thus is a bijection. □

Corollary 4.8.39.
$\overline{\overline{S_2}} = \left|\overline{\overline{J_{1,<}}}\right| = \left|\overline{\overline{J_{1,<,e}}}\right| + \left|\overline{\overline{J_{1,<,o}}}\right| = \left|\overline{\overline{Y_{2,e}}}\right| + \left|\overline{\overline{Y'_{2,o}}}\right|$. □

Summary 4.8.40.
By using Corollaries 4.8.17, 4.8.21, 4.8.24, 4.8.27, 4.8.30, 4.8.33, 4.8.36 and 4.8.39 we are able to deduce:

$$\begin{aligned}
\overline{\overline{P_1}} + \overline{\overline{P_2}} + \overline{\overline{Q_1}} + \overline{\overline{Q_2}} - \overline{\overline{R_1}} - \overline{\overline{R_2}} - \overline{\overline{S_1}} - \overline{\overline{S_2}} = {} & \left|\overline{\overline{X_{1,e}}}\right| + \left|\overline{\overline{X_{1,o}}}\right| + \left|\overline{\overline{X_{2,e}}}\right| + \left|\overline{\overline{X_{2,o}}}\right| + \\
& \left|\overline{\overline{X_{2,e}}}\right| + \left|\overline{\overline{X'_{2,o}}}\right| + \left|\overline{\overline{X_{1,e}}}\right| + \left|\overline{\overline{X'_{1,o}}}\right| - \\
& \left|\overline{\overline{Y_{1,e}}}\right| - \left|\overline{\overline{Y_{1,o}}}\right| - \left|\overline{\overline{Y_{1,e}}}\right| - \left|\overline{\overline{Y'_{1,o}}}\right| - \\
& \left|\overline{\overline{Y_{2,e}}}\right| - \left|\overline{\overline{Y_{2,o}}}\right| - \left|\overline{\overline{Y_{2,e}}}\right| - \left|\overline{\overline{Y'_{2,o}}}\right| \\
= {} & 2\left|\overline{\overline{X_{1,e}}}\right| + 2\left|\overline{\overline{X_{2,e}}}\right| + \left|\overline{\overline{X_{1,o}}}\right| + \left|\overline{\overline{X'_{1,o}}}\right| + \\
& \left|\overline{\overline{X_{2,o}}}\right| + \left|\overline{\overline{X'_{2,o}}}\right| - 2\left|\overline{\overline{Y_{1,e}}}\right| - 2\left|\overline{\overline{Y_{2,e}}}\right| - \\
& \left|\overline{\overline{Y_{1,o}}}\right| - \left|\overline{\overline{Y'_{1,o}}}\right| - \left|\overline{\overline{Y_{2,o}}}\right| - \left|\overline{\overline{Y'_{2,o}}}\right|.
\end{aligned}$$

Lemma 4.8.41.
There is a bijection between the sets $\overline{\overline{X_{1,e}}}$ and $\overline{\overline{Y_{1,e}}}$. Thus $\left|\overline{\overline{X_{1,e}}}\right| = \left|\overline{\overline{Y_{1,e}}}\right|$.

Proof.
First note that $\overline{\overline{X_{1,e}}} \subseteq \overline{X_1}$, $\overline{\overline{Y_{1,e}}} \subseteq \overline{Y_1}$ and that these are finite sets. Clearly we have $\overline{\overline{X_{1,e}}} \cap \overline{\overline{Y_{1,e}}} \subseteq \overline{X_1} \cap \overline{Y_1}$. Thus we recall the restriction map found in Theorem 3.7.1 and

show that $W\big|_{\overline{\overline{Y_{1,e}}}\setminus(\overline{\overline{X_{1,e}}}\cap\overline{\overline{Y_{1,e}}})} : \overline{\overline{Y_{1,e}}}\setminus(\overline{\overline{X_{1,e}}}\cap\overline{\overline{Y_{1,e}}}) \longrightarrow \overline{\overline{X_{1,e}}}\setminus(\overline{\overline{X_{1,e}}}\cap\overline{\overline{Y_{1,e}}})$ is a bijection.
Recall $W(\alpha,\beta,\gamma,\delta) = \omega_m(\alpha,\beta,\gamma,\delta) = (\alpha,\beta,\gamma-2m\alpha,\delta+2m\beta) = (\alpha',\beta',\gamma',\delta')$.
Well-defined: It is sufficient to show $\beta' \equiv 0 \bmod 2$ and $2\alpha' \equiv \delta' \bmod 4$. We have $\beta' = \beta \equiv 0 \bmod 2$ and also $2\alpha' - \delta' = 2\alpha - \delta - 2m\beta \equiv 2m\beta \equiv 0 \bmod 4$ since $2\alpha \equiv \delta \bmod 4$ and $\beta \equiv 0 \bmod 2$. Therefore the restriction map is well-defined.
Injectivity: This is inherited from the previous restriction of the map W in Theorem 3.7.1.
Surjectivity: Let $(\alpha',\beta',\gamma',\delta') \in \overline{\overline{X_{1,e}}}\setminus(\overline{\overline{X_{1,e}}}\cap\overline{\overline{Y_{1,e}}})$ be arbitrary and let $(\alpha,\beta,\gamma,\delta) = (\alpha',\beta',\gamma'+2m\alpha',\delta'-2m\beta')$. It is enough to show $\beta \equiv 0 \bmod 2$ and $2\alpha \equiv \delta \bmod 4$. This is because of the proof of surjectivity in Theorem 3.7.1.
We have $\beta = \beta' \equiv 0 \bmod 2$ and also $2\alpha - \delta = 2\alpha' - \delta' + 2m\beta' \equiv 0 \bmod 4$ due to $\beta' \equiv 0 \bmod 2$.
Hence the restriction map is surjective and therefore is a bijection.
Thus it follows that $\left|\overline{\overline{X_{1,e}}}\right| = \left|\overline{\overline{Y_{1,e}}}\right|$. □

Lemma 4.8.42.
There is a bijection between the sets $\overline{\overline{X_{2,e}}}$ and $\overline{\overline{Y_{2,e}}}$. Thus $\left|\overline{\overline{X_{2,e}}}\right| = \left|\overline{\overline{Y_{2,e}}}\right|$.

Proof.
First note that $\overline{\overline{X_{2,e}}} \subseteq \overline{X_2}$, $\overline{\overline{Y_{2,e}}} \subseteq \overline{Y_2}$ and these are finite sets. Clearly we have $\overline{\overline{X_{2,e}}} \cap \overline{\overline{Y_{2,e}}} \subseteq \overline{X_2} \cap \overline{Y_2}$. Hence we recall the restriction map W' from Theorem 3.7.2 and show that $W'\big|_{\overline{\overline{Y_{2,e}}}\setminus(\overline{\overline{X_{2,e}}}\cap\overline{\overline{Y_{2,e}}})} : \overline{\overline{Y_{2,e}}}\setminus(\overline{\overline{X_{2,e}}}\cap\overline{\overline{Y_{2,e}}}) \longrightarrow \overline{\overline{X_{2,e}}}\setminus(\overline{\overline{X_{2,e}}}\cap\overline{\overline{Y_{2,e}}})$ is a bijection.
Recall $W'(\alpha,\beta,\gamma,\delta) = \omega'_m(\alpha,\beta,\gamma,\delta) = (\alpha,\beta,\gamma-2m\alpha,\delta+2m\beta) = (\alpha',\beta',\gamma',\delta')$.
Well-defined: It is sufficient to show $\beta' \equiv 0 \bmod 2$ and $2\alpha' \equiv \delta' \bmod 4$. We have $\beta' = \beta \equiv 0 \bmod 2$ and $2\alpha' - \delta' = 2\alpha - \delta - 2m\beta \equiv 0 \bmod 4$ since $2\alpha \equiv \delta \bmod 4$ and $\beta \equiv 0 \bmod 2$. Thus the restriction map is well-defined.
Injectivity: This is inherited from the prior restriction of the map W' in Theorem 3.7.2.
Surjectivity: Let $(\alpha',\beta',\gamma',\delta') \in \overline{\overline{X_{2,e}}}\setminus(\overline{\overline{X_{2,e}}}\cap\overline{\overline{Y_{2,e}}})$ be arbitrary and consider $(\alpha,\beta,\gamma,\delta) = (\alpha',\beta',\gamma'+2m\alpha',\delta'-2m\beta')$. It is sufficient to show $\beta \equiv 0 \bmod 2$ and $2\alpha \equiv \delta \bmod 4$. We have $\beta = \beta' \equiv 0 \bmod 2$ and $2\alpha - \delta = 2\alpha' - \delta + 2m\beta' \equiv 0 \bmod 4$ since $2\alpha' \equiv \delta' \bmod 4$ and $\beta' \equiv 0 \bmod 2$.
Hence the restriction map is surjective and therefore is a bijection.
Thus it follows that $\left|\overline{\overline{X_{2,e}}}\right| = \left|\overline{\overline{Y_{2,e}}}\right|$. □

Lemma 4.8.43.
There is a bijection between the sets U and V, where $U = \overline{\overline{Y_{1,o}}} \cup \overline{\overline{Y'_{1,o}}}$ and $V = \overline{\overline{X_{1,o}}} \cup \overline{\overline{X'_{1,o}}}$. Consequently $\left|\overline{\overline{Y_{1,o}}}\right| + \left|\overline{\overline{Y'_{1,o}}}\right| = \left|\overline{\overline{X_{1,o}}}\right| + \left|\overline{\overline{X'_{1,o}}}\right|$.

Proof.
First note that $\overline{\overline{Y_{1,o}}}, \overline{\overline{Y'_{1,o}}} \subseteq \overline{Y_1}$ and $\overline{\overline{X_{1,o}}}, \overline{\overline{X'_{1,o}}} \subseteq \overline{X_1}$, so these are finite subsets and thus U and V are finite sets. Note that by construction $\overline{\overline{Y_{1,o}}} \cap \overline{\overline{Y'_{1,o}}} = \emptyset$ and $\overline{\overline{X_{1,o}}} \cap \overline{\overline{X'_{1,o}}} = \emptyset$. Lastly, observe $U \cap V \subseteq \overline{X_1} \cap \overline{Y_1}$.

Now we further restrict the restriction of the map W found in Theorem 3.7.1 to the subset $U\backslash(U\cap V)$. We will show that this maps to $V\backslash(U\cap V)$ and is in fact a bijection. To show that this restriction is well-defined it is sufficient to show $\beta' \equiv 1 \bmod 2$ due to the proof of Theorem 3.7.1. We have $\beta' = \beta \equiv 1 \bmod 2$ and therefore the restriction is well-defined.
Note that injectivity is inherited and so it remains to show surjectivity. Again, it is sufficient to consider $(\alpha, \beta, \gamma, \delta)$ from the surjectivity part of the proof of Theorem 3.7.1 and show $\beta \equiv 1 \bmod 2$. We have $\beta = \beta' \equiv 1 \bmod 2$ and hence the restriction map is surjective.
It follows that this restriction map gives a bijection between $U\backslash(U\cap V)$ and $V\backslash(U\cap V)$. Using this bijection and the finiteness of the sets we have $\left|\overline{\overline{Y_{1,o}}}\right| + \left|\overline{\overline{Y'_{1,o}}}\right| = \left|\overline{\overline{X_{1,o}}}\right| + \left|\overline{\overline{X'_{1,o}}}\right|$. □

Lemma 4.8.44.
There is a bijection between the sets U' and V', where $U' = \overline{\overline{Y_{2,o}}} \cup \overline{\overline{Y'_{2,o}}}$ and $V' = \overline{\overline{X_{2,o}}} \cup \overline{\overline{X'_{2,o}}}$. Consequently $\left|\overline{\overline{Y_{2,o}}}\right| + \left|\overline{\overline{Y'_{2,o}}}\right| = \left|\overline{\overline{X_{2,o}}}\right| + \left|\overline{\overline{X'_{2,o}}}\right|$.

Proof.
First note that $\overline{\overline{Y_{2,o}}}, \overline{\overline{Y'_{2,o}}} \subseteq \overline{Y_2}$ and $\overline{\overline{X_{2,o}}}, \overline{\overline{X'_{2,o}}} \subseteq \overline{X_2}$, so these are finite subsets and thus U' and V' are finite sets. Note that by construction $\overline{\overline{Y_{2,o}}} \cap \overline{\overline{Y'_{2,o}}} = \emptyset$ and $\overline{\overline{X_{2,o}}} \cap \overline{\overline{X'_{2,o}}} = \emptyset$. Lastly, observe $U' \cap V' \subseteq \overline{X_2} \cap \overline{Y_2}$.
Now we further restrict the restriction of the map W' found in Theorem 3.7.2 to the subset $U'\backslash(U' \cap V')$. We will show that this maps to $V'\backslash(U' \cap V')$ and is in fact a bijection.
To show that this restriction is well-defined it is sufficient to show $\beta' \equiv 1 \bmod 2$ due to the proof of Theorem 3.7.2. We have $\beta' = \beta \equiv 1 \bmod 2$ and therefore the restriction is well-defined.
Note that injectivity is inherited and so it remains to show surjectivity. Again, it is sufficient to consider $(\alpha, \beta, \gamma, \delta)$ from the surjectivity part of the proof of Theorem 3.7.2 and show $\beta \equiv 1 \bmod 2$. We have $\beta = \beta' \equiv 1 \bmod 2$ and hence the restriction map is surjective.
It follows that this restriction map gives a bijection between $U'\backslash(U'\cap V')$ and $V'\backslash(U'\cap V')$. Using this bijection and the finiteness of the sets we have $\left|\overline{\overline{Y_{2,o}}}\right| + \left|\overline{\overline{Y'_{2,o}}}\right| = \left|\overline{\overline{X_{2,o}}}\right| + \left|\overline{\overline{X'_{2,o}}}\right|$. □

Summary 4.8.45.
We now use Lemmas 4.8.41, 4.8.42, 4.8.43 and 4.8.44 along with Summary 4.8.40 to deduce

$$\overline{\overline{P}} + \overline{\overline{Q}} - \overline{\overline{R}} - \overline{\overline{S}} = \overline{\overline{P_0}} + \overline{\overline{Q_0}} - \overline{\overline{R_0}} - \overline{\overline{S_0}}.$$

Thus we have shown

$$\frac{1}{3}\overline{\overline{\mathrm{Cl}_c}}(D) = \overline{\overline{P}} + \overline{\overline{Q}} - \overline{\overline{R}} - \overline{\overline{S}}$$

$$= \overline{\overline{P_0}} + \overline{\overline{Q_0}} - \overline{\overline{R_0}} - \overline{\overline{S_0}}. \tag{4.5}$$

4.9 Determining the values of $\overline{\overline{P_0}}$, $\overline{\overline{Q_0}}$, $\overline{\overline{R_0}}$ and $\overline{\overline{S_0}}$.

In this section we establish bijections that will permit us to determine the values for $\overline{\overline{P_0}}$, $\overline{\overline{Q_0}}$, $\overline{\overline{R_0}}$ and $\overline{\overline{S_0}}$ in terms of divisors of D.

Lemma 4.9.1.
Let

$$Z_1 = \{(\partial, \mathrm{d}, A_{21}) \mid \partial\mathrm{d} = D, \partial, \mathrm{d} \in \mathbb{Z}_{>0}, \mathrm{d} \equiv 1 \bmod 2, -\partial < A_{21} \leqslant \partial, \partial \equiv A_{21} \bmod 4\}.$$

Then the map

$$\begin{aligned} j : \overline{\overline{I_{0,=}}} &\longrightarrow Z_1 \\ (A_{11}, A_{12}, A_{21}, A_{22}) &\longmapsto (A_{11}, A_{22} - A_{21}, A_{21}) = (\partial, \mathrm{d}, A_{21}) \end{aligned}$$

is a bijection.

Proof.
Well-defined: We have $\partial\mathrm{d} = A_{11}(A_{22} - A_{21}) = D$ and since $A_{11} > 0$ it follows that $A_{22} - A_{21} > 0$, therefore $\mathrm{d}, \partial \in \mathbb{Z}_{>0}$.
Observe $A_{11} + A_{22} \equiv 1 \bmod 2$ and $A_{11} - A_{21} = A_{12} - A_{21} \equiv 0 \bmod 4$ imply $\mathrm{d} = A_{22} - A_{21} \equiv 1 \bmod 2$ as well as $\partial - A_{21} = A_{11} - A_{21} \equiv 0 \bmod 4$. Next, $-A_{11} < A_{21} \leqslant A_{11}$ implies $-\partial < A_{21} \leqslant \partial$ and so the map j is well-defined.
Injectivity: This is straightforward to verify.
Surjectivity: Let $(\partial, \mathrm{d}, A_{21}) \in Z_1$ be arbitrary and
consider $(\partial, \partial, A_{21}, \mathrm{d} + A_{21}) = (a_{11}, a_{12}, a_{21}, a_{22})$. Then it satisfies
$\det(a_{11}, a_{12}, a_{21}, a_{22}) = \partial(\mathrm{d} + A_{21} - A_{21}) = \partial\mathrm{d} = D$ and we note $a_{11} = \partial = a_{12}$. Next, $-\partial < A_{21} \leqslant \partial$ implies $-a_{11} < a_{21} \leqslant a_{11}$. We also have $a_{11} + a_{22} = \partial + \mathrm{d} + A_{21} \equiv \mathrm{d} \equiv 1 \bmod 2$ since $\partial - A_{21} \equiv 0 \bmod 4$. Lastly we have $a_{12} - a_{21} = \partial - A_{21} \equiv 0 \bmod 4$ and therefore $(a_{11}, a_{12}, a_{21}, a_{22}) \in \overline{\overline{I_{0,=}}}$.
It is straightforward to verify $j(a_{11}, a_{12}, a_{21}, a_{22}) = (\partial, \mathrm{d}, A_{21})$, thus the map j is surjective and hence is a bijection. □

Corollary 4.9.2.

$$\overline{\overline{P_0}} = \sum_{\substack{\partial\mathrm{d}=D \\ \mathrm{d}\ odd}} \left[\left(\frac{\partial}{2} + \frac{1}{4} \right) - \frac{(-1)^\partial}{4} \right].$$

Proof.
By Lemma 4.9.1 we know $\left|\overline{\overline{I_{0,=}}}\right| = \overline{\overline{P_0}} = |Z_1|$. It remains to count the set Z_1.
Fix $D \in \mathbb{Z}_{>0}$ and let d be any positive odd divisor of D. This always exists as we may take $\mathrm{d} = 1$. Let ∂ be the unique positive integer such that $\partial\mathrm{d} = D$.
Then A_{21} is such that $-\partial < A_{21} \leqslant \partial$ and $\partial - A_{21} \equiv 0 \bmod 4$. Observe that the interval $(-\partial, \partial]$ contains precisely 2∂ integers of which ∂ are even. We split into two

cases.
Case I: $\partial \equiv 0 \bmod 2$
Then $(-\partial, \partial]$ contains $\frac{\partial}{2}$ integers that are congruent to $i \bmod 4$ for $i \in \{0,1,2,3\}$. Now $\partial - A_{21} \equiv 0 \bmod 4$ gives $A_{21} \equiv \partial \bmod 4$ and since ∂ is fixed it follows that there is only one choice for i. Since we may take $A_{21} = \partial$ it follows that give (∂, d) where $\partial \equiv 0 \bmod 2$, $\mathrm{d} \equiv 1 \bmod 2$ and $\partial \mathrm{d} = D$ then there are exactly $\frac{\partial}{2}$ choices for A_{21}.
Case II: $\partial \equiv 1 \bmod 2$
Again, note that there are 2∂ integers in the interval $(-\partial, \partial]$ and also $2\partial \equiv 2 \bmod 4$. In particular, write $2\partial = 4\left(\frac{\partial-1}{2}\right) + 2$ and thus there are at least $\frac{\partial-1}{2}$ choices for A_{21}, with the possibility of one more.
Next, we have $\partial - A_{21} \equiv 0 \bmod 4$, i.e. $A_{21} \equiv \partial \bmod 4$ and so $A_{21} \neq -\partial + 1$. Observe $\partial - 4\left(\frac{\partial-1}{2}\right) = -\partial + 2 \in (-\partial, \partial]$. Thus there are $\frac{\partial-1}{2} + 1 = \frac{\partial+1}{2}$ possible choices for A_{21}.
Notice that the difference between these two cases is $\frac{1}{2}$, this permits us to condense the result as follows:

$$\left(\frac{\partial}{2} + \frac{1}{4}\right) - \frac{(-1)^{\partial}}{4} = \begin{cases} \frac{\partial}{2} & \text{if } \partial \equiv 0 \bmod 2 \\ \frac{\partial+1}{2} & \text{if } \partial \equiv 1 \bmod 2. \end{cases}$$

Now we are free to sum over all positive odd divisors d of D. This gives

$$\overline{\overline{P_0}} = \sum_{\substack{\partial \mathrm{d} = D \\ \mathrm{d} \text{ odd}}} \left[\left(\frac{\partial}{2} + \frac{1}{4}\right) - \frac{(-1)^{\partial}}{4} \right].$$

□

Lemma 4.9.3.
Let

$$Z_3 = \{\ (\partial, \mathrm{d}, A_{21}) \mid \partial \mathrm{d} = D, \partial, \mathrm{d} \in \mathbb{Z}_{>0}, \mathrm{d} \equiv 1 \bmod 2, \partial - A_{21} \equiv 0 \bmod 4, \\ -\partial \leqslant A_{21} < \partial\ \}.$$

Then the map

$$j : \overline{\overline{I_{1,=}}} \longrightarrow Z_3$$
$$(A_{11}, A_{12}, A_{21}, A_{22}) \longmapsto (\partial, \mathrm{d}, A_{21})$$

is a well-defined bijection.

Proof.
Well-defined: We have $\partial \mathrm{d} = A_{11}(A_{22} - A_{21}) = D$, further $D, A_{11} > 0$ implies $A_{22} - A_{21} > 0$ and so $\partial, \mathrm{d} \in \mathbb{Z}_{>0}$. Next, $A_{11} + A_{22} \equiv 1 \bmod 2$ and $A_{12} - A_{21} \equiv 0 \bmod 4$ imply $\mathrm{d} = A_{22} - A_{21} \equiv 1 \bmod 2$ and $\partial - A_{21} = A_{11} - A_{21} = A_{12} - A_{21} \equiv 0 \bmod 4$. Lastly we have $-A_{11} \leqslant A_{21} < A_{11}$ yields $-\partial \leqslant A_{21} < A_{11}$ and so the map is well-defined.
Injectivity: This is straightforward to verify.
Surjectivity: Let $(\partial, \mathrm{d}, A_{21}) \in Z_3$ be arbitrary and consider $(\partial, \partial, A_{21}, \mathrm{d} + A_{21}) =$

$(a_{11}, a_{12}, a_{21}, a_{22})$.
Then it satisfies $\det(a_{11}, a_{12}, a_{21}, a_{22}) = \partial(\mathrm{d} + A_{21} - A_{21}) = \partial\mathrm{d} = D$, $a_{11} = \partial \in \mathbb{Z}_{>0}$ and $\mathrm{d}, A_{21} \in \mathbb{Z}_{>0}$ implies $a_{11} + a_{22} = \partial + \mathrm{d} - A_{21} \equiv \partial \bmod 4 \equiv 1 \bmod 2$. Lastly we have $a_{12} - a_{21} = \partial - A_{21} \equiv 0 \bmod 4$ and it is straightforward to verify that $j(a_{11}, a_{12}, a_{21}, a_{22}) = (\partial, \mathrm{d}, A_{21})$. Hence the map is surjective and thus is a bijection. □

Corollary 4.9.4.
$\overline{\overline{Q_0}} = \sum_{\substack{\partial\mathrm{d}=D \\ \mathrm{d}\ odd}} \left[\left(\frac{\partial}{2} - \frac{1}{4} \right) + \frac{(-1)^\partial}{4} \right].$

Proof.
By Lemma 4.9.3 we know $\overline{\overline{Q_0}} = \left|\overline{\overline{I_{1,=}}}\right| = |Z_3|$. It remains to count the set Z_3. Fix $D \in \mathbb{Z}_{>0}$ and let d be any positive odd divisor of D. This always exists as we may take $\mathrm{d} = 1$. Let ∂ be the unique positive integer such that $\partial\mathrm{d} = D$. Then A_{21} satisfies $-\partial \leqslant A_{21} < \partial$ and $\partial - A_{21} \equiv 0 \bmod 4$, that is, $A_{21} \equiv \partial \bmod 4$. We note that $[-\partial, \partial)$ contains exactly 2∂ integers of which ∂ are even. We split into cases.
Case I: $\partial \equiv 0 \bmod 2$
Then $\frac{\partial}{2}$ is an integer and thus each class of integers modulo 4 within the interval $[-\partial, \partial)$ contains exactly $\frac{\partial}{2}$ integers. Since $A_{21} \equiv \partial \bmod 4$ we have $\frac{\partial}{2}$ choices for A_{21}.
Case II: $\partial \equiv 1 \bmod 2$
In this case we have $2\partial \equiv 2 \bmod 4$ and we may write $2\partial = 4\left(\frac{\partial-1}{2}\right) + 2$. Thus there are at least $\frac{\partial-1}{2}$ choices for A_{21} with the potential for there to be one more. Now $A_{21} \equiv \partial \bmod 4$ implies $A_{21} \neq -\partial$ and we note that $A_{21} \neq \partial$ since $\partial \notin [-\partial, \partial)$. Therefore since $\partial - 4\left(\frac{\partial-1}{2}\right) = -\partial + 2$ we see $A_{21} \in [-\partial + 2, \partial - 4]$ and this interval contains precisely $\frac{\partial-1}{2}$ congruent to $\partial \bmod 4$.
Combining these results, we may write the number of choices for A_{21} as follows:

$$\left(\frac{\partial}{2} - \frac{1}{4} \right) + \frac{(-1)^\partial}{4}.$$

Now we are free to sum over all positive odd divisors of D. This gives

$$\overline{\overline{Q_0}} = \sum_{\substack{\partial\mathrm{d}=D \\ \mathrm{d}\ \mathrm{odd}}} \left[\left(\frac{\partial}{2} - \frac{1}{4} \right) + \frac{(-1)^\partial}{4} \right].$$

□

Lemma 4.9.5.
$\overline{\overline{P_0}} + \overline{\overline{Q_0}} = 2^k \sigma_{\mathrm{odd}}(D)$, *where* $D = 2^k m$, $m \equiv 1 \bmod 2$.

Proof.

$$\overline{\overline{P_0}} + \overline{\overline{Q_0}} = \sum_{\substack{\partial\mathrm{d}=D \\ \mathrm{d}\ \mathrm{odd}}} \left[\left(\frac{\partial}{2} + \frac{1}{4} \right) - \frac{(-1)^\partial}{4} \right] + \sum_{\substack{\partial\mathrm{d}=D \\ \mathrm{d}\ \mathrm{odd}}} \left[\left(\frac{\partial}{2} - \frac{1}{4} \right) + \frac{(-1)^\partial}{4} \right]$$

$$= \sum_{\substack{\partial \mathrm{d}=D \\ \mathrm{d}\ \text{odd}}} \partial.$$

Now if D is odd we have $k = 0$ and $\displaystyle\sum_{\substack{\partial \mathrm{d}=D \\ \mathrm{d}\ \text{odd}}} \partial = \sigma_{\text{odd}}(D) = 2^k \sigma_{\text{odd}}(D)$.

So suppose D is even, i.e. $D = 2^k m$ for some $k \geqslant 1$ and $m \equiv 1 \bmod 2$. Then $\partial = \frac{D}{\mathrm{d}} = \frac{2^k m}{\mathrm{d}}$ and $\mathrm{d} \mid m$. Therefore we have

$$\begin{aligned} \sum_{\substack{\partial \mathrm{d}=D \\ \mathrm{d}\ \text{odd}}} \partial &= \sum_{\substack{\mathrm{d} \mid m \\ \mathrm{d}\ \text{odd}}} 2^k \frac{m}{\mathrm{d}} \\ &= 2^k \sigma_{\text{odd}}(m) \\ &= 2^k \sigma_{\text{odd}}(D). \end{aligned}$$

Hence $\overline{\overline{P_0}} + \overline{\overline{Q_0}} = 2^k \sigma_{\text{odd}}(D)$, where $D = 2^k m$, $m \equiv 1 \bmod 2$. □

Next we investigate the cardinalities of the sets $\overline{\overline{J_{0,=}}}$ and $\overline{\overline{J_{1,=}}}$. Recall from Lemma 4.3.8 we have

$$\begin{aligned} J_{0,=} &= \{(A_{11}, A_{12}, A_{21}, 0) \mid \det(A) = D, 0 < A_{12} + A_{21} < A_{11}, A_{21} < -|A_{11} - A_{12}|\} \\ J_{1,=} &= \{(A_{11}, A_{12}, A_{21}, 0) \mid \det(A) = D, 0 \leqslant A_{12} + A_{21} < A_{11}, A_{21} < -|A_{11} - A_{12}|\}. \end{aligned}$$

Note that $\overline{\overline{J_{0,=}}} \subseteq J_{0,=}$ and $\overline{\overline{J_{1,=}}} \subseteq J_{1,=}$.

From Lemma 4.6.7 recall the bijection $\gamma : \overline{J_{0,=}} \longrightarrow V$. We give a restriction of this map.

Lemma 4.9.6.
The following restriction of the map γ from Lemma 4.6.7 is a bijection.
$\gamma|_{\overline{\overline{J_{0,=}}}} : \overline{\overline{J_{0,=}}} \longrightarrow \overline{\overline{V}}$, *where* $\overline{\overline{V}} = \{(s, t, A_{11}) \in V \mid s + t \equiv 0 \bmod 4\}$.

Proof.
Observe $\overline{\overline{J_{0,=}}} \subseteq \overline{J_{0,=}}$ and $\overline{\overline{V}} \subseteq V$. Therefore it is enough to show $s + t \equiv 0 \bmod 4$ for well-definedness. We have $s + t = A_{12} + (-A_{21}) \equiv 0 \bmod 4$.
We note injectivity is inherited and so it remains to show surjectivity. Let $(s, t, A_{11}) \in \overline{\overline{V}}$ be arbitrary and consider $g = (A_{11}, s, -t, 0) = (a_{11}, a_{12}, a_{21}, a_{22})$. By Lemma 4.6.7 we know g lies in $\overline{J_{0,=}}$ and so it is enough to show $a_{12} - a_{21} = s - (-t) = s + t \equiv 0 \bmod 4$. Hence the restriction is surjective and it is straightforward to verify $\gamma|_{\overline{\overline{J_{0,=}}}}(g) = (s, t, A_{11})$. Therefore we have a bijection. □

Corollary 4.9.7.
$\overline{\overline{R_0}} = \left|\overline{\overline{J_{0,=}}}\right| = \left|\overline{\overline{V}}\right|$.

We now recall $\overline{\overline{S_0}} = \left|\overline{\overline{J_{1,=}}}\right|$ and examine the similarities between the sets $\overline{\overline{J_{0,=}}}$ and $\overline{\overline{J_{1,=}}}$.

Lemma 4.9.8.
$\overline{\overline{S_0}} = \begin{cases} \overline{\overline{R_0}} + \sqrt{D} & \text{if } D = 4k^2 \\ \overline{\overline{R_0}} & \text{otherwise.} \end{cases}$

Proof.
Let

$$\begin{aligned} Z &= \overline{\overline{J_{1,=}}} \cap \overline{\overline{J_{0,=}}} \\ &= \{(A_{11}, A_{12}, A_{21}, 0) \mid \det(A) = D, 0 < A_{12} + A_{21} < A_{11}, A_{21} < -|A_{11} - A_{12}|, \\ &\qquad A_{11} \equiv 1 \bmod 2, A_{12} - A_{21} \equiv 0 \bmod 4\}. \end{aligned}$$

It is then clear that $\overline{\overline{J_{0,=}}} \backslash Z = \emptyset$ and

$$\overline{\overline{J_{1,=}}} \backslash Z = \{(A_{11}, A_{12}, A_{21}, 0) \mid \det(A) = D, 0 = A_{12} + A_{21} < A_{11}, A_{21} < -|A_{11} - A_{12}|, \\ A_{11} \equiv 1 \bmod 2, A_{12} - A_{21} \equiv 0 \bmod 4\}.$$

It follows that $\overline{\overline{S_0}} = \overline{\overline{R_0}} + \left|\hat{V}\right|$, where

$$\hat{V} = \{(A_{11}, A_{12}, A_{21}, 0) \mid -A_{12}A_{21} = D, 0 = A_{12} + A_{21} < A_{11}, A_{21} < -|A_{11} - A_{12}|, \\ A_{11} \equiv 1 \bmod 2, A_{12} - A_{21} \equiv 0 \bmod 4\}.$$

We note $A_{12} + A_{21} = 0$ implies $A_{21} = -A_{12}$ and so $2A_{12} = A_{12} - A_{21} \equiv 0 \bmod 4$ and hence both A_{12} and A_{21} must be even. Further, $A_{21} = -A_{12}$ implies $D = A_{12}^2$ and so we have $\overline{\overline{S_0}} = \overline{\overline{R_0}}$ unless $D = 4k^2$ for some integer k.

Now suppose $D = 4k^2$, then in the set $\hat{V}$ we have $D = -A_{12}A_{21} = A_{12}^2 = 4k^2$ as $A_{12} \equiv 0 \bmod 2$. Using $A_{21} = -A_{21}$ and $A_{21} < -|A_{11} - A_{12}|$ yields $-A_{12} < A_{11} - A_{12} < A_{12}$ and so $0 < A_{11} < 2A_{12}$. Therefore we have $A_{11} \in [1, 2A_{12} - 1]$ as $A_{11} \equiv 1 \bmod 2$, and this interval contains $(2A_{12}-1)-1+1 = 2A_{12}-1$ integers, of which $A_{12} = \sqrt{D}$ are odd.

Therefore when $D = 4k^2$ for some integer k we have $\overline{\overline{S_0}} = \overline{\overline{R_0}} + \sqrt{D}$.

Hence $\overline{\overline{S_0}} = \begin{cases} \overline{\overline{R_0}} + \sqrt{D} & \text{if } D = 4k^2 \\ \overline{\overline{R_0}} & \text{otherwise.} \end{cases}$ □

Our goal now is to derive an expression for $\overline{\overline{R_0}} + \overline{\overline{S_0}}$. We will do this via a series of four lemmas. Note that by Corollary 4.9.7 we have $\left|\overline{\overline{J_{0,=}}}\right| = \left|\overline{\overline{V}}\right|$ and therefore $\overline{\overline{V}}$ is a finite set since $\overline{\overline{J_{0,=}}} \subseteq J_{0,=}$, which is finite.

Lemma 4.9.9.
Let $D \equiv 1 \bmod 4$ *then* $\overline{\overline{R_0}} = \overline{\overline{S_0}} = 0$.

Proof.
Let $D \equiv 1 \bmod 4$, then in the definition of the set $\overline{\overline{V}}$ we have $D = st$ and $s + t \equiv$

0 mod 4. Using $D = st$ we see that either $s \equiv t \equiv 1 \bmod 4$ or $s \equiv t \equiv 3 \bmod 4$ and in either case we have $s+t \equiv 2 \bmod 4$. This is a contradiction and so $\overline{\overline{R_0}} = 0$. Applying Lemma 4.9.8 we get $\overline{\overline{S_0}} = \overline{\overline{R_0}}$ as $D \equiv 1 \bmod 4$ implies $D \neq 4k^2$. □

Lemma 4.9.10.
If $D \equiv 2 \bmod 4$ *then* $\overline{\overline{R_0}} = \overline{\overline{S_0}} = 0$.

Proof.
Let $D \equiv 2 \bmod 4$, from the definition of the set $\overline{\overline{V}}$ we have $D = st$ and precisely one of s, t must be odd. It follows that $s + t \not\equiv 0 \bmod 4$, a contradiction. Since $D \equiv 2 \bmod 4$ implies $D \neq 4k^2$, applying Lemma 4.9.8 yields $\overline{\overline{R_0}} = \overline{\overline{S_0}} = 0$. □

Lemma 4.9.11.
If $D \equiv 3 \bmod 4$ *then* $\overline{\overline{R_0}} = \overline{\overline{S_0}} = \frac{1}{2}(\sigma(D) - \Psi(D))$.

Proof.
Let $D \equiv 3 \bmod 4$, then in particular $D \neq 4k^2$. We have $D = st \equiv 3 \bmod 4$ implies s and t are both odd as well as $s \equiv -t \bmod 4$. Thus $s + t \equiv 0 \bmod 4$ as desired. So we may pick any pair of divisors s, t of D with $s > t$. Then there are t choices for $A_{11} \in [s - t + 1, s + t - 1]$ because there are $2t - 1$ integers in this interval and both $s - t + 1$ and $s + t - 1$ are odd due to $s + t \equiv 0 \bmod 4$.
Applying Lemmas 4.4.2 and 4.9.8 we have $\overline{\overline{S_0}} = \overline{\overline{R_0}} = \left|\overline{\overline{V}}\right| = \sum_{\substack{D=st \\ s>t}} t = \frac{1}{2}(\sigma(D) - \Psi(D))$.
□

We now examine the case when $D \equiv 0 \bmod 4$. Regardless of whether D is a perfect square or not, we must satisfy both $st \equiv 0 \bmod 4$ and $s + t \equiv 0 \bmod 4$. Thus both s and t must be even, and further we require $s \equiv t \equiv 2 \bmod 4$ or $s \equiv t \equiv 0 \bmod 4$. The first implies $D \equiv 4 \bmod 8$ while the latter implies $D \equiv 0 \bmod 16$. This motivates us to break down the $D \equiv 0 \bmod 4$ case into three subcases: $D \equiv 4 \bmod 8$, $D \equiv 8 \bmod 16$ and $D \equiv 0 \bmod 16$.

Lemma 4.9.12.
If $D \equiv 8 \bmod 16$ *then* $\overline{\overline{R_0}} = \overline{\overline{S_0}} = 0$.

Proof.
Let $D \equiv 8 \bmod 16$, then $2^3 \mid D$ but $2^4 \nmid D$. Thus D is not a perfect square; consequently Lemma 4.9.8 implies $\overline{\overline{S_0}} = \overline{\overline{R_0}}$. Further, since $\overline{\overline{R_0}} = \left|\overline{\overline{V}}\right|$ and elements of $\overline{\overline{V}}$ satisfy either $s \equiv t \equiv 2 \bmod 4$ or $s \equiv t \equiv 0 \bmod 4$, it is clear that $D = st \equiv 8 \bmod 16$ is impossible.
Thus $\overline{\overline{V}} = \emptyset$ and hence $\overline{\overline{R_0}} = \overline{\overline{S_0}} = 0$. □

Lemma 4.9.13.
Assume $D \equiv 4 \bmod 8$ *and write* $D = 4n$ *where* $n \equiv 1 \bmod 2$. *Then*
$$\overline{\overline{R_0}} = \begin{cases} \sigma(n) - \Psi(n) - \sqrt{n} & \text{if } n = k^2 \\ \sigma(n) - \Psi(n) & \text{otherwise} \end{cases} \quad \text{and} \quad \overline{\overline{S_0}} = \begin{cases} \sigma(n) - \Psi(n) + \sqrt{n} & \text{if } n = k^2 \\ \sigma(n) - \Psi(n) & \text{otherwise.} \end{cases}$$

Proof.
Let $D = 4n$, $n \equiv 1 \bmod 2$. From the definition of D and the set $\overline{\overline{V}}$ we have $s \equiv t \equiv 2 \bmod 4$ because $16 \nmid D$. If $D > 4$ then there always exists a pair (s,t) with $0 < t < s$ as we may take $(\hat{s}, \hat{t})$ to be any pair of divisors of $\frac{D}{4} > 1$ such that $0 < \hat{t} < \hat{s}$ and then let $s = 2\hat{s}$, $t = 2\hat{t}$. Hence in this situation, given a pair (s,t) we count the choices for A_{11}. We note $A_{11} \in [s - t + 1, s + t - 1]$ and since $2 \mid (s \pm t)$ it follows that of the $2t - 1$ integers in this interval, precisely t of them are odd. Thus there are t choices for A_{11}.
Hence when $D \equiv 4 \bmod 8$, $D > 4$ we have

$$\begin{aligned}
\overline{\overline{R_0}} = \left|\overline{\overline{V}}\right| &= \sum_{\substack{D=st \\ 0<t<s \\ s\equiv t\equiv 2 \bmod 4}} t \\
&= 2 \sum_{\substack{D=4\hat{s}\hat{t} \\ 0<\hat{t}<\hat{s} \\ \hat{s}\equiv\hat{t}\equiv 1 \bmod 2}} \hat{t} \\
&= 2 \sum_{\substack{D=4\hat{s}\hat{t} \\ 0<\hat{t}<\hat{s}}} \hat{t} \text{ as } D \equiv 4 \bmod 8 \text{ implies no even } \hat{s}, \hat{t} \text{ exist} \\
&= \begin{cases} \sigma\left(\frac{D}{4}\right) - \Psi\left(\frac{D}{4}\right) - \sqrt{\frac{D}{4}} & \text{if } D = 4k^2 \\ \sigma\left(\frac{D}{4}\right) - \Psi\left(\frac{D}{4}\right) & \text{otherwise} \end{cases} \quad \text{by Lemma 4.4.2} \\
&= \begin{cases} \sigma(n) - \Psi(n) - \sqrt{n} & \text{if } n = k^2 \\ \sigma(n) - \Psi(n) & \text{otherwise.} \end{cases}
\end{aligned}$$

In the case where $D = 4$ we have $s \equiv t \equiv 2 \bmod 4$ implies $s = t = 2$ and this contradicts $t < s$. Consequently $\overline{\overline{V}} = \emptyset$ and it is elementary to verify $\sigma(1) - \Psi(1) - \sqrt{1} = 0$, thus the above formula holds for all $D \equiv 4 \bmod 8$. Applying Lemma 4.9.8 we get

$$\begin{aligned}
\overline{\overline{S_0}} &= \begin{cases} \sigma(n) - \Psi(n) - \sqrt{n} + \sqrt{D} & \text{if } D = 4k^2 \\ \sigma(n) - \Psi(n) & \text{otherwise} \end{cases} \\
&= \begin{cases} \sigma(n) - \Psi(n) + \sqrt{n} & \text{if } n = k^2 \\ \sigma(n) - \Psi(n) & \text{otherwise.} \end{cases}
\end{aligned}$$

□

Lemma 4.9.14.
Assume $D = 4n \equiv 0 \bmod 16$, *then* $\overline{\overline{R_0}} = 2 \begin{cases} \sigma\left(\frac{n}{4}\right) - \Psi\left(\frac{n}{4}\right) - \sqrt{\frac{n}{4}} & \text{if } n = 4k^2 \\ \sigma\left(\frac{n}{4}\right) - \Psi\left(\frac{n}{4}\right) & \text{otherwise} \end{cases}$ *and* $\overline{\overline{S_0}} = 2 \begin{cases} \sigma\left(\frac{n}{4}\right) - \Psi\left(\frac{n}{4}\right) + \sqrt{\frac{n}{4}} & \text{if } n = 4k^2 \\ \sigma\left(\frac{n}{4}\right) - \Psi\left(\frac{n}{4}\right) & \text{otherwise.} \end{cases}$

Proof.
Let $D = 4n \equiv 0 \bmod 16$, note that $4 \mid n$. From the definition of the set $\overline{\overline{V}}$ we have s and t satisfy either $s \equiv t \equiv 2 \bmod 4$ or $s \equiv t \equiv 0 \bmod 4$. From $D \equiv 0 \bmod 16$ it

follows we may only have $s \equiv t \equiv 0 \bmod 16$. Since $16 \mid D$, for $D > 16$ we may find a pair (s,t) such that $D = st$ and $0 < t < s$ by letting $s = 4\hat{s}$, $t = 4\hat{t}$ where $0 < \hat{t} < \hat{s}$ and $1 < \frac{D}{16} = \hat{s}\hat{t}$.
Hence in this situation, given a pair (s,t) we count the possibilities for A_{11}. As in the proof of Lemma 4.9.13 there are t choices for A_{11}.
Hence when $D = 4n \equiv 0 \bmod 16$, $D > 16$ we have

$$\begin{aligned}
\overline{\overline{R_0}} = \left|\overline{\overline{V}}\right| &= \sum_{\substack{D=st \\ 0<t<s \\ s\equiv t\equiv 0 \bmod 4}} t \\
&= 2 \cdot 2 \sum_{\substack{D=16\hat{s}\hat{t} \\ 0<\hat{t}<\hat{s}}} \hat{t} \\
&= 2 \begin{cases} \sigma\left(\frac{D}{16}\right) - \Psi\left(\frac{D}{16}\right) - \sqrt{\frac{D}{16}} & \text{if } D = 16k^2 \\ \sigma\left(\frac{D}{16}\right) - \Psi\left(\frac{D}{16}\right) & \text{otherwise} \end{cases} \quad \text{by Lemma 4.4.2} \\
&= 2 \begin{cases} \sigma\left(\frac{n}{4}\right) - \Psi\left(\frac{n}{4}\right) - \sqrt{\frac{n}{4}} & \text{if } n = 4\hat{k}^2 \\ \sigma\left(\frac{n}{4}\right) - \Psi\left(\frac{n}{4}\right) & \text{otherwise.} \end{cases}
\end{aligned}$$

In the case where $D = 16$ we have $s \equiv t \equiv 0 \bmod 4$ implies $s = t = 4$, contradicting $t < s$. Therefore we have $\overline{\overline{V}} = \emptyset$ and it is straightforward to verify $\sigma(1) - \Psi(1) - \sqrt{1} = 0$. Thus the above formula holds for all $D \equiv 0 \bmod 16$. Applying Lemma 4.9.8 we have

$$\begin{aligned}
\overline{\overline{S_0}} &= 2 \begin{cases} \sigma\left(\frac{n}{4}\right) - \Psi\left(\frac{n}{4}\right) - \sqrt{\frac{n}{4}} + \sqrt{D} & \text{if } D = 16k^2 \\ \sigma\left(\frac{n}{4}\right) - \Psi\left(\frac{n}{4}\right) & \text{otherwise} \end{cases} \\
&= 2 \begin{cases} \sigma\left(\frac{n}{4}\right) - \Psi\left(\frac{n}{4}\right) + \sqrt{\frac{n}{4}} & \text{if } n = 4\hat{k}^2 \\ \sigma\left(\frac{n}{4}\right) - \Psi\left(\frac{n}{4}\right) & \text{otherwise.} \end{cases}
\end{aligned}$$

□

Corollary 4.9.15.

$$\overline{\overline{R_0}} + \overline{\overline{S_0}} = \begin{cases} 0 & \text{if } D \equiv 1 \bmod 4 \\ 0 & \text{if } D \equiv 2 \bmod 4 \\ \sigma(D) - \Psi(D) & \text{if } D \equiv 3 \bmod 4 \\ 2\left(\sigma(n) - \Psi(n)\right) & \text{if } D = 4n \equiv 4 \bmod 8 \\ 0 & \text{if } D = 4n \equiv 8 \bmod 16 \\ 4\left(\sigma\left(\frac{n}{4}\right) - \Psi\left(\frac{n}{4}\right)\right) & \text{if } D = 4n \equiv 0 \bmod 16. \end{cases}$$

Proof.
This follows from carefully combining the results found in Lemmas 4.9.9, 4.9.10, 4.9.11, 4.9.13, 4.9.12 and 4.9.14. □

These results agree exactly with those of Kronecker, found in [Kr1897, p. 480].
We now prove a lemma stated but not proved in Kronecker's section 19.

Lemma 4.9.16 (Kronecker)**.**
Let $D = 4n = 2^k m$ where $m \equiv 1 \bmod 2$ and $k \geqslant 4$.
Then $2^k \sigma_{\text{odd}}(m) = 8\sigma_{\text{odd}}(m) + 8\sigma\left(2^{k-4}m\right)$.

Proof.

$$\begin{aligned}
8\sigma_{\text{odd}}(m) + 8\sigma\left(2^{k-4}m\right) &= 8\sum_{\substack{d|m \\ d \text{ odd}}} d + 8\sum_{d|2^{k-4}m} d \\
&= 8\sum_{\substack{d|m \\ d\text{odd}}} d + 8\sum_{\substack{d|m \\ d \text{ odd}}} d + 8\sum_{\substack{d=2\hat{d} \\ \hat{d}|m}} d + 8\sum_{\substack{d=4\hat{d} \\ \hat{d}|m}} d + \cdots + 8\sum_{\substack{d=2^{k-4}\hat{d} \\ \hat{d}|m}} d \\
&= 16\sum_{\substack{d|m \\ d\text{odd}}} d + 16\sigma_{\text{odd}}(m)\left(1 + 2 + \cdots 2^{k-5}\right) \\
&= 16\sigma_{\text{odd}}(m) + 2^4\sigma_{\text{odd}}(m) \cdot \left(\frac{2^{k-4}-1}{2-1}\right) \\
&= 16\sigma_{\text{odd}}(m) + 2^k\sigma_{\text{odd}}(m) - 16\sigma_{\text{odd}}(m) \\
&= 2^k\sigma_{\text{odd}}(m).
\end{aligned}$$

□

4.10 A Formula for $\overline{\overline{\text{Cl}}}_c(D)$

In this section we draw upon our results from Section 4.9 to derive a formula for computing $\overline{\overline{\text{Cl}}}_c(D)$ in terms of the divisors of D. We continue to let $D \in \mathbb{Z}_{>0}$ and write $D = 2^k m$ where $k \geqslant 0$ and $m \equiv 1 \bmod 2$.
We begin our derivation with Equation 4.5.

$$\begin{aligned}
\frac{1}{3}\overline{\overline{\text{Cl}}}_c(D) &= \overline{\overline{P_0}} + \overline{\overline{Q_0}} - \overline{\overline{R_0}} - \overline{\overline{S_0}} \\
&= \sum_{\substack{\text{d odd} \\ \partial \text{d}=D}} \partial - \begin{cases} 0 & \text{if } D \equiv 1 \bmod 4 \\ 0 & \text{if } D \equiv 2 \bmod 4 \\ \sigma(D) - \Psi(D) & \text{if } D \equiv 3 \bmod 4 \\ 2\sigma\left(\frac{D}{4}\right) - 2\Psi\left(\frac{D}{4}\right) & \text{if } D \equiv 4 \bmod 8 \\ 0 & \text{if } D \equiv 8 \bmod 16 \\ 4\left(\sigma\left(\frac{D}{16}\right) - \Psi\left(\frac{D}{16}\right)\right) & \text{if } D \equiv 0 \bmod 16 \end{cases} \\
&= 2^k\sigma_{\text{odd}}(D) - \begin{cases} 0 & \text{if } D \equiv 1 \bmod 4 \\ 0 & \text{if } D \equiv 2 \bmod 4 \\ \sigma(D) - \Psi(D) & \text{if } D \equiv 3 \bmod 4 \\ 2^2\sigma_{\text{odd}}\left(\frac{D}{4}\right) - 2\sigma_{\text{odd}}\left(\frac{D}{4}\right) + 2\Psi\left(\frac{D}{4}\right) & \text{if } D \equiv 4 \bmod 8 \\ 8\sigma_{\text{odd}}(m) & \text{if } D \equiv 8 \bmod 16 \\ 2^4\sigma_{\text{odd}}\left(\frac{D}{16}\right) - 4\sigma\left(\frac{D}{16}\right) + 4\Psi\left(\frac{D}{16}\right) & \text{if } D \equiv 0 \bmod 16 \end{cases}
\end{aligned}$$

$$= \begin{cases} \sigma_{\text{odd}}(D) & \text{if } D \equiv 1 \bmod 4 \\ 2\sigma_{\text{odd}}(D) & \text{if } D \equiv 2 \bmod 4 \\ \sigma_{\text{odd}}(D) - (\sigma(D) - \Psi(D)) & \text{if } D \equiv 3 \bmod 4 \\ 2\sigma_{\text{odd}}\left(\frac{D}{4}\right) + 2\Psi\left(\frac{D}{4}\right) & \text{if } D \equiv 4 \bmod 8 \\ 8\sigma_{\text{odd}}(m) & \text{if } D \equiv 8 \bmod 16 \\ 16\sigma_{\text{odd}}\left(\frac{D}{16}\right) - 4\sigma\left(\frac{D}{16}\right) + 4\Psi\left(\frac{D}{16}\right) & \text{if } D \equiv 0 \bmod 16. \end{cases}$$

Applying Lemma 4.9.16, we see $2^4\sigma_{\text{odd}}\left(\frac{D}{16}\right) = 8\sigma_{\text{odd}}\left(\frac{D}{16}\right) + 8\sigma\left(\frac{D}{16}\right)$. Thus we get

$$\frac{1}{3}\overline{\overline{\text{Cl}}}_c(D) = \begin{cases} \sigma_{\text{odd}}(m) & \text{if } D \equiv 1 \bmod 4 \\ 2\sigma_{\text{odd}}(m) & \text{if } D \equiv 2 \bmod 4 \\ \Psi(m) & \text{if } D \equiv 3 \bmod 4 \\ 2\sigma_{\text{odd}}\left(\frac{D}{4}\right) + 2\Psi\left(\frac{D}{4}\right) & \text{if } D \equiv 4 \bmod 8 \\ 8\sigma_{\text{odd}}(m) & \text{if } D \equiv 8 \bmod 16 \\ 8\sigma_{\text{odd}}\left(\frac{D}{16}\right) + 4\sigma\left(\frac{D}{16}\right) + 4\Psi\left(\frac{D}{16}\right) & \text{if } D \equiv 0 \bmod 16. \end{cases} \tag{4.6}$$

Observe we continue to differ from Kronecker's result by a factor of 2. This is still due to the fact the we are only considering positive definite bilinear forms. We also see our result matches (1), (2), (3), (4), (5) and (6) of Kronecker's paper ([Kr1897, p. 480]).

Chapter 5 A Connection between Bilinear Forms and Binary Quadratic Forms

> "Now this is not the end. It is not even the beginning of the end. But it is, perhaps, the end of the beginning."
> - Sir Winston Churchill

In this chapter we develop a connection between the class number for positive definite bilinear forms and the class number for positive definite binary quadratic forms.

5.1 Developing the Connection with Binary Quadratic Forms

A significant milestone in Kronecker's paper [Kr1897] is the development of his formula for $\mathrm{Cl}_c(D)$ in terms of the divisors of D. However, a more important result is his connection between $\mathrm{Cl}_c(D)$ and summing over certain complete equivale nce classes of positive definite binary quadratic forms. We shall develop this notion in this section.

Throughout this chapter (unless explicitly stated otherwise) we will assume any binary quadratic forms given are positive definite and are of the form $f = ax^2 + 2bxy + cy^2$ where a, b and c are integers. Thus we will refer to the determinant of such a binary quadratic form by $\det(f) = ac - b^2$.

It will be useful for the reader to remind themselves of the definition of an associated binary quadratic form (see Definition 2.4.8).

We first give a slightly stronger version of Lemma 2.4.25.

Lemma 5.1.1.
Let $\mathcal{A}$ be a bilinear form, then $\mathcal{A}$ is positive definite if and only if $A_{\mathcal{A}}$ is a positive definite binary quadratic form.

Proof.
Let $\mathcal{A}$ have matrix representation $A = \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix}$ and by definition $A_{\mathcal{A}} = A_{11}x^2 + (A_{12} + A_{21})xy + A_{22}y^2$ is its associated binary quadratic form.
($\Rightarrow$). Suppose $\mathcal{A}$ is a positive definite bilinear form. By Corollary 2.4.19 this implies $A_{11} > 0$ and $4A_{11}A_{22} - (A_{12} + A_{21})^2 > 0$. By Lemma 2.4.11 we wish to show $A_{\mathcal{A}} = ax^2 + rxy + cy^2$ satisfies $a > 0$ and $4\det(A_{\mathcal{A}}) > 0$.
By definition we have $A_{\mathcal{A}} = A_{11}x^2 + (A_{12} + A_{21})xy + A_{22}y^2$. Thus we clearly have $a = A_{11} > 0$. Further, $4\det(A_{\mathcal{A}}) = 4A_{11}A_{22} - (A_{12} + A_{21})^2 > 0$. Therefore $A_{\mathcal{A}}$ is a positive definite binary quadratic form.
($\Leftarrow$) Suppose $A_{\mathcal{A}}$ is a positive definite binary quadratic form. Then it follows that

$A_{11} > 0$ and $0 < 4\det(A_{\mathcal{A}}) = 4A_{11}A_{22} - (A_{12} + A_{21})^2$. Therefore by Corollary 2.4.19, $\mathcal{A}$ is a positive definite bilinear form. □

We also note Kronecker considered only those binary quadratic forms having an even xy coefficient. This is because when working with the definition of complete equivalence we would like the entries to be integers. Our next series of lemmas indicate how we may determine the number of complete equivalence classes for binary quadratic forms with odd xy coefficient.

Lemma 5.1.2.
Let $f = ax^2+rxy+cy^2$ be a positive definite binary quadratic form where $r \equiv 1 \bmod 2$. Then every binary quadratic form in the complete equivalence class of f has the property that its xy coefficient is odd.

Proof.
Let $A_f = \begin{pmatrix} a & \frac{r}{2} \\ \frac{r}{2} & c \end{pmatrix}$ be the matrix representation of f. Let $M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \ker\sigma$ then using Observation 2.4.5 we have

$$M^t A_f M = (\alpha^2 a + \alpha\gamma r + c\gamma^2)x^2 + (2\alpha\beta a + (\alpha\delta + \beta\gamma)r + 2\gamma\delta c)xy + (\beta^2 a + \beta\delta r + \delta^2 c)y^2.$$

Since $M \in \ker\sigma$ we have $\alpha\delta \equiv 1 \bmod 2$ and $\beta\gamma \equiv 0 \bmod 2$. Using this along with $r \equiv 1 \bmod 2$ it follows that the xy coefficient of $M^t A_f M$ is always odd.
Hence if a positive definite binary quadratic form $ax^2 + rxy + cy^2$ has $r \equiv 1 \bmod 2$ then all forms in its complete equivalence class have this property. □

Lemma 5.1.3.
Let $f = ax^2 + 2bxy + cy^2$ be a positive definite binary quadratic form with matrix representation $\mathrm{A}_f = \begin{pmatrix} a & b \\ b & c \end{pmatrix}$ and let $M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \ker\sigma$. If at least one of a, c is odd then at least one of the outer coefficients of $M^t\mathrm{A}_f M$ is odd.

Proof.
First observe that if a and c are both odd then since α and δ are odd, Observation 2.4.5 shows that a' and c' are both odd.
Without loss of generality we may assume a is odd and c is even. Then since M satisfies $\alpha \equiv \delta \equiv 1 \bmod 2$ and $\beta \equiv \gamma \equiv 0 \bmod 2$ it follows that $a' = \alpha^2 a + 2\alpha\gamma b + \gamma^2 c$ is odd. Thus $M^t\mathrm{A}_f M$ has at least one odd outer coefficient. □

We now introduce some of Kronecker's notation (see [Kr1897, p. 445]).

Definition 5.1.4.
Let $n > 0$ be an integer and define the following:
Let $6\mathrm{G}(n)$ be the number of complete equivalence classes of positive definite binary quadratic forms, $ax^2 + 2bxy + cy^2$, with determinant $ac - b^2 = n$.
Let $6\mathrm{F}(n)$ be the number of complete equivalence classes of positive definite binary quadratic forms, $ax^2 + 2bxy + cy^2$, with determinant $ac - b^2 = n$ and where at least one of the outer coefficients (a and/or c) is odd.

The above definition provides the motivation for Lemma 5.1.3, where we proved the property of having at least one odd outer coefficient is preserved within a complete equivalence class.

Lemma 5.1.5.
Let $n \in \mathbb{Z}_{>0}$ be such that $n \equiv 3 \bmod 4$ and consider the following sets of positive definite binary quadratic forms.
Let $\mathcal{Q}_n = \{[f]_c \mid f = ax^2 + rxy + cy^2, n = 4\det(f) = 4ac - r^2\}$ and
$\mathcal{R}_n = \{[g]_c \mid g = Ax^2 + Bxy + Cy^2, A \equiv C \equiv 0 \bmod 2, B \equiv 2 \bmod 4, 4n = 4\det(g)\}$.
Define the map $\pi : \mathcal{Q}_n \longrightarrow \mathcal{R}_n$ by $\pi([f]_c) = [A_f P]_c$, where $P = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$.
Then the map π is a bijection.

Proof.
Well-defined: Since $n \equiv 3 \bmod 4$ and $4\det(f) = 4ac - r^2$, we must have $r \equiv 1 \bmod 2$. By Lemma 5.1.2 we know if $f = ax^2 + rxy + cy^2$ has $r \equiv 1 \bmod 2$ then every binary quadratic form in the complete equivalence class of f has this property. Next, since the determinant is invariant under $\mathrm{SL}_2(\mathbb{Z})$ we note that $4\det(f)$ is also an invariant. Now observe $A_f P = \begin{pmatrix} a & \frac{r}{2} \\ \frac{r}{2} & c \end{pmatrix}\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} 2a & r \\ r & 2c \end{pmatrix}$, which yields the binary quadratic form $2ax^2 + 2rxy + 2cy^2 = Ax^2 + Bxy + Cy^2$. It is then clear that $A = 2a$, $C = 2c$ and $A \equiv C \equiv 0 \bmod 2$. We also see $B = 2r \equiv 2 \bmod 4$ as $r \equiv 1 \bmod 2$. Lastly, $4\det(g) = 4(AC - (\frac{B}{2})^2) = 4((2a)(2c) - (r)^2) = 4(4ac - r^2) = 4n$. It remains to check our map is independent of our choice of representative from within the complete equivalence class. Suppose $f \sim_c \hat{f}$, then there exists $M \in \ker\sigma$ such that $M^t A_f M = A_{\hat{f}}$. Then we have

$$\begin{aligned}
\pi\left([\hat{f}]_c\right) &= \left[A_{\hat{f}} P\right]_c \\
&= \left[M^t A_f M P\right]_c \\
&= \left[M^t A_f P M\right]_c \text{ as } P \text{ and } M \text{ commute} \\
&= [A_f P]_c \text{ as } M \in \ker\sigma \\
&= \pi([f]_c).
\end{aligned}$$

Hence π is well-defined.
Injectivity: Suppose $\pi([f]_c) = \pi\left([\hat{f}]_c\right)$, then $[A_f P]_c = \left[A_{\hat{f}} P\right]_c$. Therefore there exists a matrix $M \in \ker\sigma$ such that $M^t A_f P M = A_{\hat{f}} P$. Since the matrices P and M commute we have $M^t A_f M P = A_{\hat{f}} P$ and it follows that $M^t A_f M = A_{\hat{f}}$. That is $[f]_c = \left[\hat{f}\right]_c$ and therefore π is injective.
Surjectivity: Let $[g]_c \in \mathcal{R}_n$ be arbitrary and consider $\left[\frac{g}{2}\right]_c$. We note the binary quadratic form $\frac{g}{2}$ is well-defined by the following logic. We have $A \equiv C \equiv 0 \bmod 2$, $B \equiv 2 \bmod 4$ implies $r = \frac{B}{2} \equiv 1 \bmod 2$ and thus $a = \frac{A}{2}$, $b = \frac{B}{2}$ and $c = \frac{C}{2}$ are integers. We also have $4\det(\frac{g}{2}) = 4\left(\left(\frac{A}{2}\right)\left(\frac{C}{2}\right) - \left(\frac{B}{2}\right)^2\right) = (AC - B^2) = \det(g) = n$.

Thus $\left[\frac{g}{2}\right]_c \in \mathcal{Q}_n$.
Now observe $\pi\left(\left[\frac{g}{2}\right]_c\right) = \left[A_{\frac{g}{2}}P\right]_c = [A_g]_c = [g]_c$. So π is surjective and hence is a bijection. $\square$

We now give a nearly identical result, this time for when $n \equiv 0 \bmod 4$.

Lemma 5.1.6.
Let $n \in \mathbb{Z}_{>0}$ be such that $n \equiv 0 \bmod 4$ and consider the following sets of positive definite binary quadratic forms.
Let $\mathcal{Q}_n = \{[f]_c \mid f = ax^2 + rxy + cy^2, n = 4\det(f) = 4ac - r^2\}$ and
$\mathcal{R}'_n = \{[g]_c \mid g = Ax^2 + Bxy + Cy^2, A \equiv C \equiv 0 \bmod 2, B \equiv 0 \bmod 4, 4n = 4\det(g)\}$.
Define the map $\pi : \mathcal{Q}_n \longrightarrow \mathcal{R}'_n$ by $\pi([f]_c) = [A_f P]_c$, where $P = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$.
Then the map π is a bijection.

Proof.
Well-defined: Since $n \equiv 0 \bmod 4$ and $4\det(f) = 4ac - r^2$, we must have $r \equiv 0 \bmod 2$. By the complement of Lemma 5.1.2 we know if $f = ax^2 + rxy + cy^2$ has $r \equiv 0 \bmod 2$ then every binary quadratic form in the complete equivalence class of f has this property. Next, since the determinant is invariant under $\mathrm{SL}_2(\mathbb{Z})$ we note that $4\det(f)$ is also an invariant. Now observe $A_f P = \begin{pmatrix} a & \frac{r}{2} \\ \frac{r}{2} & c \end{pmatrix}\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} 2a & r \\ r & 2c \end{pmatrix}$, which yields the binary quadratic form $2ax^2 + 2rxy + 2cy^2 = Ax^2 + Bxy + Cy^2$. It is then clear that $A = 2a$, $C = 2c$ and $A \equiv C \equiv 0 \bmod 2$. We also see $B = 2r \equiv 0 \bmod 4$ as $r \equiv 0 \bmod 2$. Lastly, $4\det(g) = 4(AC - (\frac{B}{2})^2) = 4((2a)(2c) - (r)^2) = 4(4ac - r^2) = 4n$. It remains to check our map is independent of our choice of representative from within the complete equivalence class. Suppose $f \sim_c \hat{f}$, then there exists $M \in \ker\sigma$ such that $M^t A_f M = A_{\hat{f}}$. Then we have

$$\begin{aligned}
\pi\left([\hat{f}]_c\right) &= \left[A_{\hat{f}}P\right]_c \\
&= \left[M^t A_f M P\right]_c \\
&= \left[M^t A_f P M\right]_c \text{ as } P \text{ and } M \text{ commute} \\
&= [A_f P]_c \text{ as } M \in \ker\sigma \\
&= \pi([f]_c).
\end{aligned}$$

Hence π is well-defined.
Injectivity: This is analogous to the proof of injectivity in Lemma 5.1.5.
Surjectivity: Let $[g]_c \in \mathcal{R}'_n$ be arbitrary and consider $\left[\frac{g}{2}\right]_c$. We note the binary quadratic form $\frac{g}{2}$ is well-defined by the following logic. We have $A \equiv C \equiv 0 \bmod 2$, $B \equiv 0 \bmod 4$ implies $r = \frac{B}{2} \equiv 0 \bmod 2$ and thus $a = \frac{A}{2}$, $b = \frac{B}{2}$ and $c = \frac{C}{2}$ are integers. We also have $4\det(\frac{g}{2}) = 4\left(\left(\frac{A}{2}\right)\left(\frac{C}{2}\right) - \left(\frac{B}{2}\right)^2\right) = (AC - B^2) = \det(g) = n$.
Thus $\left[\frac{g}{2}\right]_c \in \mathcal{Q}_n$.
Now observe $\pi\left(\left[\frac{g}{2}\right]_c\right) = \left[A_{\frac{g}{2}}P\right]_c = [A_g]_c = [g]_c$. So π is surjective and hence is a bijection. $\square$

We are now in a position to prove two of Kronecker's statements about the structure of the complete equivalence classes of binary quadratic forms. We begin by proving his third claim on page 444 of [Kr1897].

Lemma 5.1.7.
Let $n > 0$ be a positive integer and consider the set of binary quadratic forms $f = ax^2 + 2bxy + cy^2$ with $\det(f) = n > 0$. Then we have $\mathrm{G}(4n) = \mathrm{F}(4n) + \mathrm{G}(n)$.

Proof.
Recall from Definition 5.1.4 that $6\mathrm{G}(n)$ is the number of complete equivalence classes of positive definite binary quadratic forms with determinant n, and that $6\mathrm{F}(n)$ is the number of complete equivalence classes of positive definite binary quadratic forms with determinant n and where all forms have at least one odd outer coefficient.
Therefore $6\mathrm{G}(4n) - 6\mathrm{F}(4n)$ is the number of complete equivalence classes of positive definite binary quadratic forms with determinant $4n$ and where both outer coefficients are even.
By Lemma 5.1.6 we know there is a bijection between the set of complete equivalence classes of binary quadratic forms with determinant n and the set of complete equivalence classes of binary quadratic forms with determinant $4n$ and the property that both outer coefficients are even. Since we are dealing with finite sets, it follows that $6\mathrm{G}(4n) - 6\mathrm{F}(4n) = 6\mathrm{G}(n)$. Dividing by 6 then yields Kronecker's result. □

We now prove his fourth claim ([Kr1897, p. 444]).

Lemma 5.1.8.
Let $n > 0$ be an integer such that $n \equiv 1$ or $2 \bmod 4$ and consider the set of binary quadratic forms $f = ax^2 + 2bxy + cy^2$ with $\det(f) = n$. Then we have $\mathrm{G}(n) = \mathrm{F}(n)$.

Proof.
By Lemma 5.1.3 if a binary quadratic form within a $\mathrm{GL}_2(\mathbb{Z})$-equivalence class has at least one odd outer coefficient, then every binary quadratic form within this equivalence class has this property.
Let $n \equiv 1$ or $2 \bmod 4$ and $ac - b^2 = n$. Assume $a \equiv c \equiv 0 \bmod 2$ then we have $n \equiv -b^2 \bmod 4$. This implies $n \equiv 0$ or $3 \bmod 4$, a contradiction. Hence when $n \equiv 1$ or $2 \bmod 4$, every binary quadratic form has at least one odd outer coefficient and thus $6\mathrm{G}(n) = 6\mathrm{F}(n)$ and we have Kronecker's result. □

Observation 5.1.9.
It is important to note that $6\mathrm{G}(n)$ and $6\mathrm{F}(n)$ are integers, this is not necessarily true for $\mathrm{G}(n)$ and $\mathrm{F}(n)$.

Our next lemma is particularly important because it establishes the connection between complete equivalence classes of associated binary quadratic forms with the complete equivalence classes of binary quadratic forms in general.

Lemma 5.1.10.
Let $\tau_{D,h}$ be the set of positive definite bilinear forms with determinant $D > 0$ and $h = A_{12} - A_{21} \equiv 0 \bmod 2$. Then the set of complete equivalence classes of associated binary

quadratic forms developed from the set $\tau_{D,h}$ is finite and has the same cardinality as the set of complete equivalence classes of binary quadratic forms with determinant $D - \left(\frac{h}{2}\right)^2$.

Proof.
To begin note that there are finitely many bilinear forms with determinant D and by Lemma 2.4.6 h is invariant under $\mathrm{SL}_2(\mathbb{Z})$. Therefore there are finitely many associated binary quadratic forms. In a similar manner to bilinear forms we see there are a finite number of positive definite binary quadratic forms $f = ax^2 + 2bxy + cy^2$ with determinant $D - (\frac{h}{2})^2$.
Next, by Lemma 2.4.19 the bilinear forms in $\tau_{D,h}$ satisfy $4A_{11}A_{22} - (A_{12} + A_{21})^2 > 0$ and thus $4D - (A_{12} - A_{21})^2 > 0$. Therefore we get $4d - h^2 > 0$ which yields $-2\sqrt{D} < h < 2\sqrt{D}$. Consequently $D - (\frac{h}{2})^2$ is a positive integer.
Now observe the associated binary quadratic forms satisfy $\det(A_{\mathcal{A}}) = A_{11}A_{22} - \left(\frac{A_{12}+A_{21}}{2}\right)^2 = D - \left(\frac{h}{2}\right)^2$, which is an integer as $h \equiv 0 \bmod 2$. Further, every associated binary quadratic form with this determinant is a binary quadratic form with the same determinant. Therefore if we have $A_{\mathcal{A}} \not\sim_c A_{\mathcal{B}}$ then we cannot have $[A_{\mathcal{A}}]_c = [A_{\mathcal{B}}]_c$ without a contradiction. Thus the cardinality of the set of complete equivalence classes of binary quadratic forms with determinant $D - \left(\frac{h}{2}\right)^2$ is greater than or equal to the cardinality of the set of complete equivalence classes of associated binary quadratic forms with this determinant.
Lastly, we will show that every complete equivalence class of positive definite binary quadratic forms contains an associated binary quadratic form that comes from a bilinear form with determinant D and satisfies $h \equiv 0 \bmod 2$.
Let $f = ax^2 + 2bxy + cy^2$ be an arbitrary positive definite binary quadratic form with determinant $D - \left(\frac{h}{2}\right)^2$, thus $ac - b^2 = D - \left(\frac{h}{2}\right)^2$. In particular this means $D = ac - b^2 + \left(\frac{h}{2}\right)^2$. Now consider the bilinear form $\mathcal{A}$ with matrix representation $A = \begin{pmatrix} a & b + \frac{h}{2} \\ b - \frac{h}{2} & c \end{pmatrix}$. Since $h \equiv 0 \bmod 2$ we note both $b + \frac{h}{2}$ and $b - \frac{h}{2}$ are integers. This bilinear form has determinant $ac - \left(b + \frac{h}{2}\right)\left(b - \frac{h}{2}\right) = ac - b^2 + \left(\frac{h}{2}\right)^2 = D$ and satisfies $h' = (b + \frac{h}{2}) - (b - \frac{h}{2}) = h \equiv 0 \bmod 2$. Finally we see $A_{\mathcal{A}} = f$. Thus every binary quadratic form with determinant $D - \left(\frac{h}{2}\right)^2$ is the associated binary quadratic form for some bilinear form with determinant D and fixed value of $h \equiv 0 \bmod 2$.
Therefore we must have equality between the cardinalities of the two sets. □

We now begin to establish the connection between bilinear forms and binary quadratic forms with the following lemma.

Lemma 5.1.11.
Let $\mathcal{A}$ and $\mathcal{B}$ be positive definite bilinear forms satisfying $\det(A) = \det(B)$, $A_{12} - A_{21} \equiv B_{12} - B_{21} \equiv 0 \bmod 2$ and $A_{\mathcal{A}} \sim_c A_{\mathcal{B}}$. Then $\mathcal{A} \sim_c \mathcal{B}$ or $\mathcal{A} \sim_c \mathcal{B}^t$.

Proof.
Since $A_{12} - A_{21} \equiv B_{12} - B_{21} \equiv 0 \bmod 2$ it follows that $A_{\mathcal{A}}$ and $A_{\mathcal{B}}$ are of the form $ax^2 + 2bxy + cy^2$. Therefore we may talk about complete equivalence between these

binary quadratic forms because their matrix representations have integer entries. Therefore there exists a matrix $M \in \ker \sigma$ such that $M^t A_{\mathcal{A}} M = A_{\mathcal{B}}$. We apply Observation 2.4.5 to get

$$\begin{aligned} A_{\mathcal{B}} &= M^t A_{\mathcal{A}} M \\ &= [\alpha^2 A_{11} + \alpha\gamma(A_{12} + A_{21}) + \gamma^2 A_{22}]x^2 + \\ &\qquad [2\alpha\beta A_{11} + (\alpha\delta + \beta\gamma)(A_{12} + A_{21}) + 2\gamma\delta A_{22}]xy + \\ &\qquad [\beta^2 A_{11} + \beta\delta(A_{12} + A_{21}) + \delta^2 A_{22}]y^2. \end{aligned}$$

Equating coefficients yields

$$\begin{aligned} B_{11} &= \alpha^2 A_{11} + \alpha\gamma(A_{12} + A_{21}) + \gamma^2 A_{22} \\ B_{12} + B_{21} &= 2\alpha\beta A_{11} + (\alpha\delta + \beta\gamma)(A_{12} + A_{21}) + 2\gamma\delta A_{22} \\ B_{22} &= \beta^2 A_{11} + \beta\delta(A_{12} + A_{21}) + \delta^2 A_{22}. \end{aligned}$$

Next we calculate $M^t AM$ directly by applying Observation 2.4.5.

$$\begin{aligned} M^t AM &= \begin{pmatrix} \alpha^2 A_{11} + \alpha\gamma(A_{12} + A_{21}) + \gamma^2 A_{22} & \alpha\beta A_{11} + \beta\gamma A_{21} + \alpha\delta A_{12} + \gamma\delta A_{22} \\ \alpha\beta A_{11} + \alpha\delta A_{21} + \beta\gamma A_{12} + \delta\gamma A_{22} & \beta^2 A_{11} + \beta\delta(A_{12} + A_{21}) + \delta^2 A_{22} \end{pmatrix} \\ &= \begin{pmatrix} B_{11} & X_1 \\ X_2 & B_{22} \end{pmatrix}, \end{aligned}$$

where $X_1 = \alpha\beta A_{11} + \beta\gamma A_{21} + \alpha\delta A_{12} + \gamma\delta A_{22}$ and $X_2 = \alpha\beta A_{11} + \alpha\delta A_{21} + \beta\gamma A_{12} + \delta\gamma A_{22}$. We observe $X_1 + X_2 = B_{12} + B_{21}$ and $B_{11}B_{22} - B_{12}B_{21} = \det(B) = \det(A) = \det(M^t AM) = B_{11}B_{22} - X_1X_2$. Consequently $X_1X_2 = B_{12}B_{21}$. Solving this system of equations yields two solutions, namely $(X_1, X_2) = (B_{12}, B_{21})$ or $(X_1, X_2) = (B_{21}, B_{12})$. Thus we get $\mathcal{A} \sim_c \mathcal{B}$ or $\mathcal{A} \sim_c \mathcal{B}^t$. □

Theorem 5.1.12.
Let $\mathcal{A}$ and $\mathcal{B}$ be positive definite bilinear forms such that $\det(A) = \det(B)$ *and* $A_{12} - A_{21} \equiv B_{12} - B_{21} \equiv 0 \bmod 2$. *Then $\mathcal{A} \sim_c \mathcal{B}$ if and only if $A_{\mathcal{A}} \sim_c A_{\mathcal{B}}$ and $A_{12} - A_{21} = B_{12} - B_{21}$.*

Proof.
($\Rightarrow$) Suppose $\mathcal{A} \sim_c \mathcal{B}$ then Lemma 2.4.12 implies $A_{\mathcal{A}} \sim_c A_{\mathcal{B}}$ because complete equivalence implies proper equivalence.
($\Leftarrow$) Suppose $A_{\mathcal{A}} \sim_c A_{\mathcal{B}}$ and $A_{12} - A_{21} = B_{12} - B_{21}$. Then there exists a matrix $M \in \ker \sigma$ such that $M^t A_{\mathcal{A}} M = A_{\mathcal{B}}$. Since $A_{12} - A_{21} \equiv 0 \bmod 2$ we apply Lemma 5.1.11 to see either $\mathcal{A} \sim_c \mathcal{B}$ or $\mathcal{A} \sim_c \mathcal{B}^t$ via the matrix M. By Lemma 2.4.6 we know complete equivalence preserves $A_{12} - A_{21}$. Therefore if $A_{12} - A_{21} \neq 0$ then we have $\mathcal{A} \sim_c \mathcal{B}$ because $\mathcal{B}^t$ satisfies $a_{12} - a_{21} = B_{21} - B_{12} = -(B_{12} - B_{21})$. Now suppose $A_{12} - A_{21} = 0$, then we have $B_{12} - B_{21} = 0$ and thus $B_{12} = B_{21}$. This implies $\mathcal{B} = \mathcal{B}^t$ and therefore we have $\mathcal{A} \sim_c \mathcal{B}$. □

We now present a lemma that determines the relationship between complete equivalence classes of positive definite bilinear forms where $A_{12} - A_{21} \equiv 1 \bmod 2$ and those where $A_{12} - A_{21} \equiv 0 \bmod 2$.

Lemma 5.1.13.
Fix $D \in \mathbb{Z}_{>0}$ and define $\mathcal{X}_D = \{[\mathcal{A}]_c \mid \det(\mathrm{A}) = D, A_{12} - A_{21} \equiv 1 \bmod 2\}$ as well as $\mathcal{Y}_D = \{[\mathcal{B}]_c \mid \det(\mathrm{B}) = 4D, B_{11} \equiv B_{22} \equiv 0 \bmod 2, B_{12} - B_{21} \equiv 2 \bmod 4\}$.
Define $\tau : \mathcal{X}_D \longrightarrow \mathcal{Y}_D$ by $[\mathcal{A}]_c \longmapsto [2\mathcal{A}]_c$.
Then τ is a bijection.

Proof.
Well-defined: We first show $[2\mathcal{B}]_c \in \mathcal{Y}_D$. We have $\det(2I_2 A) = \det(2I_2)\det(A) = 4\det(A) = 4D$. Also $2B_{11} \equiv 2B_{22} \equiv 0 \bmod 2$. Lastly, $2(B_{12} - B_{21}) \equiv 2 \bmod 4$ as $B_{12} - B_{21} \equiv 1 \bmod 2$. Thus τ maps into $\mathcal{R}_D$.
Now we show that τ respects complete equivalence classes. Assume $\mathcal{B} \sim_c \mathcal{B}'$, then there exists $M \in \ker \sigma$ such that $M^t \mathrm{B} M = \mathrm{B}'$. Using this we have $M^t(2I_2\mathrm{B})M = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} M^t \mathrm{B} M = 2\mathrm{B}'$. Thus $2\mathcal{B} \sim_c 2\mathcal{B}'$ and hence τ is well-defined.
Injectivity: Suppose $\tau([\mathcal{B}]_c) = \tau([\mathcal{B}']_c)$, then there exists an $M \in \ker \sigma$ such that $M^t(2\mathrm{B})M = 2\mathrm{B}'$. It follows that $\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \mathrm{B}' = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} M^t \mathrm{B} M = M^t(2\mathrm{B})M$ and so $M^t \mathrm{B} M = \mathrm{B}'$. Therefore $[\mathcal{B}]_c = [\mathcal{B}']_c$.
Surjectivity: Let $[\mathcal{B}]_c \in \mathcal{Y}_D$ be arbitrary and consider $\left[\frac{\mathcal{B}}{2}\right]_c$. The following observations show that $\frac{\mathcal{B}}{2}$ is well-defined. Since $B_{11} \equiv B_{22} \equiv 0 \bmod 2$ and it follows that $\frac{B_{11}}{2}, \frac{B_{22}}{2} \in \mathbb{Z}_{>0}$. Next, $4 \mid \det(\mathrm{B}) = 4D$ and since $B_{11} \equiv B_{22} \equiv 0 \bmod 2$ it follows that $4 \mid B_{12}B_{21}$. Using $B_{12} - B_{21} \equiv 2 \bmod 4$ we have either $B_{12} \equiv 0 \bmod 4$ and $B_{21} \equiv 2 \bmod 4$, or vice versa. Therefore $\frac{B_{12}}{2}, \frac{B_{21}}{2} \in \mathbb{Z}$ and we clearly have $B_{12} - B_{21} = 2k$ where $k \equiv 1 \bmod 2$ and thus $\frac{B_{12} - B_{21}}{2} \equiv 1 \bmod 2$. Lastly, $\det\left(\frac{\mathrm{B}}{2}\right) = \left(\frac{B_{11}}{2}\right)\left(\frac{B_{22}}{2}\right) - \left(\frac{B_{12}}{2}\right)\left(\frac{B_{21}}{2}\right) = \frac{1}{4}(B_{11}B_{22} - B_{12}B_{21}) = \frac{1}{4}(4D) = D$. Hence $\left[\frac{\mathcal{B}}{2}\right]_c \in \mathcal{X}_D$. We observe $\tau\left(\left[\frac{\mathcal{B}}{2}\right]_c\right) = [\mathcal{B}]_c$ and hence τ is a surjection and so is a bijection. □

We now derive Kronecker's result for the complete class number of positive determinant bilinear forms of determinant $D > 0$ in terms of summations of certain complete equivalence classes of binary quadratic forms.

Theorem 5.1.14.
Let $D > 0$ be an integer. Then $\mathrm{Cl}_c(D) = 6 \sum_{-2\sqrt{D} < h < 2\sqrt{D}} \left[\mathrm{G}(4D - h^2) - \mathrm{F}(4D - h^2)\right]$.

Proof.
Fix an integer $D > 0$ and consider the set of all complete equivalence classes of positive definite bilinear forms with determinant D. This set has cardinality $\mathrm{Cl}_c(D)$. By Lemma 2.4.19 any such bilinear form satisfies $4A_{11}A_{22} - (A_{12} + A_{21})^2 > 0$ and this rearranges to give $4D - h^2 > 0$, where $h = A_{12} - A_{21}$. By Lemma 2.4.6 we know this quantity is preserved within a proper equivalence class, so in particular within a complete equivalence class. Further, this rearranges to give $-2\sqrt{D} < h < 2\sqrt{D}$.
We first partition the set of all complete equivalence classes of positive definite bilinear forms with determinant D according to whether $h = A_{12} - A_{21} \equiv 0 \bmod 2$ or not. By Lemma 5.1.13 there is a one-to-one correspondence between the set of complete

equivalence classes of bilinear forms with determinant D that satisfy $A_{12} - A_{21} \equiv 1 \bmod 2$, and the set $\mathcal{Y}_D$. Here

$$\mathcal{Y}_D = \{[\mathcal{B}]_c \mid \det(B) = 4D, B_{11} \equiv B_{22} \equiv 0 \bmod 2, B_{12} - B_{21} \equiv 2 \bmod 4\}.$$

Therefore we have $\mathrm{Cl}_c(D) = \mathrm{Cl}_{c,e}(D) + |\mathcal{Y}_D|$, where
$\mathrm{Cl}_{c,e}(D) = |\{[\mathcal{A}]_c \mid \det(A) = D, A_{12} - A_{21} \equiv 0 \bmod 2\}|$.
Now partition each of these sets according to their value of h, where $-2\sqrt{D} < h < 2\sqrt{D}$. This gives

$$\mathrm{Cl}_c(D) = \sum_{\substack{-2\sqrt{D}<h<2\sqrt{D} \\ h \equiv 0 \bmod 2}} |\tau_{D,h}| + \sum_{\substack{-2\sqrt{D}<h<2\sqrt{D} \\ h \equiv 1 \bmod 2}} |\mathcal{Y}_{D,h}|,$$

where $\mathcal{Y}_{D,h} = \{[\mathcal{A}]_C \mid \det(A) = 4D, a_{11} \equiv a_{22} \equiv 0 \bmod 2, 2h = a_{12} - a_{21} \equiv 2 \bmod 4\}$. This is because all forms $(a_{11}, a_{12}, a_{21}, a_{22}) \in \mathcal{Y}_{D,h}$ are positive definite and so satisfy $4a_{11}a_{22} - (a_{12} + a_{21})^2 > 0$. By construction we have $a_{ij} = 2A_{ij}$ for $1 \leqslant i, j \leqslant 2$ and thus we get $4(2A_{11})(2A_{22}) - (2A_{12} + 2A_{21})^2 > 0$. Hence $4(4D - h^2) > 0$ where $h = A_{12} - A_{21} \equiv 1 \bmod 2$ and thus $-2\sqrt{D} < h < 2\sqrt{D}$.
Next, by Theorem 5.1.12 when $h = A_{12} - A_{21} \equiv 0 \bmod 2$ there is a one-to-one correspondence between complete equivalence classes of binary quadratic forms with determinant D, and the complete equivalence classes of associated binary quadratic forms with determinant $A_{11}A_{22} - \left(\frac{A_{12}+A_{21}}{2}\right)^2 = D - \left(\frac{h}{2}\right)^2$. Further, by Lemma 5.1.10 we know there is a one-to-one correspondence between the complete equivalence classes of associated binary quadratic forms with determinant $D - \left(\frac{h}{2}\right)^2$ and the complete equivalence classes of binary quadratic forms with determinant $D - \left(\frac{h}{2}\right)^2$.
Lastly, by the contrapositive of Lemma 5.1.3 and using the invariance of $A_{12} - A_{21}$ we see that the property of having both outer coefficients even and $A_{12} - A_{21} \equiv 0 \bmod 2$ is preserved within a complete equivalence class of a binary quadratic form having these properties. Therefore, applying Theorem 5.1.12 to the complete equivalence classes in the set $\mathcal{Y}_{D,h}$ yields a one-to-one correspondence with the binary quadratic forms with determinant $4D - (h)^2$ having the property that both outer coefficients are even. To see why the binary quadratic forms have determinant $4D - h^2$, recall a bilinear form $(a_{11}, a_{12}, a_{21}, a_{22}) \in \mathcal{Y}_{D,h}$ has $a_{11} = 2A_{11}$, $a_{22} = 2A_{22}$ and $a_{12} - a_{21} = 2(A_{12} - A_{21})$. Thus its associated binary quadratic form has the following determinant

$$\begin{aligned}
\det(a) &= a_{11}a_{22} - \left(\frac{a_{12} + a_{21}}{2}\right)^2 \\
&= a_{11}a_{22} - a_{12}a_{21} - \left(\frac{a_{12} - a_{21}}{2}\right)^2 \\
&= 4(A_{11}A_{22} - A_{12}A_{21}) - \left(\frac{2(A_{12} - A_{21})}{2}\right)^2 \\
&= 4D - h^2.
\end{aligned}$$

We now apply Kronecker's notation to our result. In particular, note that the set of complete equivalence classes of binary quadratic forms with both outer coefficients

even and determinant n is counted by $6\mathrm{G}(n) - 6\mathrm{F}(n)$. Using this we have

$$\mathrm{Cl}_c(D) = \sum_{\substack{-2\sqrt{D}<h<2\sqrt{D} \\ h\equiv 0 \bmod 2}} 6\mathrm{G}\left(D - \left(\frac{h}{2}\right)^2\right) + \sum_{\substack{-2\sqrt{D}<h<2\sqrt{D} \\ h\equiv 1 \bmod 2}} \left[6\mathrm{G}\left(4D-h^2\right) - 6\mathrm{F}\left(4D-h^2\right)\right].$$

Further, we apply Lemma 5.1.7 in order to observe $6\mathrm{G}\left(D - \left(\frac{h}{2}\right)^2\right) = 6\mathrm{G}(4D-h^2) - 6\mathrm{F}(4D-h^2)$. Using this we get

$$\mathrm{Cl}_c(D) = 6 \sum_{-2\sqrt{D}<h<2\sqrt{D}} \left[\mathrm{G}(4D-h^2) - \mathrm{F}(4D-h^2)\right].$$

□

We now turn our attention to deriving a similar expression for $\overline{\mathrm{Cl}}_c(D)$. Thus we are now interested in the complete equivalence classes of positive definite bilinear forms with determinant D, $B_{12} + B_{21} \equiv 0 \bmod 2$ and where at least one of B_{11} and B_{22} is odd.

In particular this means $h = A_{12} - A_{21}$ is even and thus $\overline{\mathrm{Cl}}_c(D) = \sum_{\substack{-2\sqrt{D}<h<2\sqrt{D} \\ h\equiv 0 \bmod 2}} |\tau_{D,h}|$.

Next, as in the proof of Theorem 5.1.14 we have a one-to-one correspondence between the complete equivalence classes of associated binary forms with determinant $D - \left(\frac{h}{2}\right)^2$ and the complete equivalence classes of binary quadratic forms with determinant $D - \left(\frac{h}{2}\right)^2$ in general. Further, the property that at least one outer coefficient is odd and $A_{12} + A_{21} \equiv 0 \bmod 2$ is preserved in both cases.

Hence we have

$$\begin{aligned}\overline{\mathrm{Cl}}_c(D) &= \sum_{\substack{-2\sqrt{D}<h<2\sqrt{D} \\ h\equiv 0 \bmod 2}} 6\mathrm{F}\left(D - \left(\frac{h}{2}\right)^2\right) \\ &= \sum_{-\sqrt{D}<\hat{h}<\sqrt{D}} 6\mathrm{F}\left(D - \hat{h}^2\right).\end{aligned}$$

Lastly, we wish to determine a similar expression for $\overline{\overline{\mathrm{Cl}}}_c(D)$. Thus we are interested in the complete equivalence classes of positive definite bilinear forms with determinant D, $B_{12} - B_{21} \equiv 0 \bmod 4$, and where at least one of B_{11}, B_{22} is odd. Recalling $h = A_{12} - A_{21}$ is invariant within a complete equivalence class, and following the proof of Theorem 5.1.14 we see

$$\overline{\overline{\mathrm{Cl}}}_c(D) = \sum_{\substack{4|h \\ -2\sqrt{D}<h<2\sqrt{D}}} |\tau_{D,h,o}|$$

$$
\begin{aligned}
&= 6 \sum_{\substack{4|h \\ -2\sqrt{D}<h<2\sqrt{D}}} \mathrm{F}\left(D - \left(\frac{h}{2}\right)^2\right) \\
&= 6 \sum_{\substack{2|\hat{h} \\ -\sqrt{D}<\hat{h}<\sqrt{D}}} \mathrm{F}\left(D - \hat{h}^2\right) \\
&= 6 \sum_{-\sqrt{D}<2\tilde{h}<\sqrt{D}} \mathrm{F}\left(D - 4\tilde{h}^2\right).
\end{aligned}
$$

Summary 5.1.15.
The following summarises the results of this subsection so far:

$$\mathrm{Cl}_c(D) = 6 \sum_{-2\sqrt{D}<h<2\sqrt{D}} \left(\mathrm{G}\left(4D - h^2\right) - \mathrm{F}\left(4D - h^2\right)\right) \tag{5.1}$$

$$\overline{\mathrm{Cl}}_c(D) = 6 \sum_{-\sqrt{D}<\hat{h}<\sqrt{D}} \mathrm{F}\left(D - \hat{h}^2\right) \tag{5.2}$$

$$\overline{\overline{\mathrm{Cl}}}_c(D) = 6 \sum_{-\sqrt{D}<2\tilde{h}<\sqrt{D}} \mathrm{F}\left(D - 4\tilde{h}^2\right). \tag{5.3}$$

It is important to note that h, $\hat{h}$ and $2\tilde{h}$ are integer valued.

We now make connections between the results found in Summary 5.1.15 and those of Sections 4.4 and 4.7.

First we make a seemingly unmotivated definition. Motivation for this will be apparent in the proof of Lemma 5.1.17.

Definition 5.1.16.
Recall the arithmetic functions F and G were defined for $n \in \mathbb{Z}_{>0}$. We extend this definition to $n \in \mathbb{Z}_{\geqslant 0}$ by defining $\mathrm{G}(0) = -\frac{1}{6}$ and $\mathrm{F}(0) = 0$.

Lemma 5.1.17.
Let $D \in \mathbb{Z}_{>0}$ be arbitrary. Then

$$\sigma(D) + \Psi(D) = \sum_{-2\sqrt{D}\leqslant h\leqslant 2\sqrt{D}} \left(\mathrm{G}\left(4D - h^2\right) - \mathrm{F}\left(4D - h^2\right)\right).$$

Proof.
From Theorem 4.4.3 we have

$$
\begin{aligned}
\mathrm{Cl}_c(D) = &\begin{cases} 6\sigma(D) + 6\Psi(D) + 1 & \text{if } D = k^2 \\ 6\sigma(D) + 6\Psi(D) & \text{otherwise} \end{cases} \\
&= 6 \begin{cases} \sigma(D) + \Psi(D) + \frac{1}{6} & \text{if } D = k^2 \\ \sigma(D) + \Psi(D) & \text{otherwise.} \end{cases}
\end{aligned} \tag{5.4}
$$

Next, because h is an integer by construction, we have

$$6 \sum_{-2\sqrt{D}<h<2\sqrt{D}} \left(\mathrm{G}\left(4D-h^2\right)-\mathrm{F}\left(4D-h^2\right)\right) =$$
$$\begin{cases} 6 \sum\limits_{-2\sqrt{D}\leqslant h\leqslant 2\sqrt{D}} \left(\mathrm{G}\left(4D-h^2\right)-\mathrm{F}\left(4D-h^2\right)\right) - 6(\mathrm{G}(0)-\mathrm{F}(0)) & \text{if } D=k^2 \\ 6 \sum\limits_{-2\sqrt{D}\leqslant h\leqslant 2\sqrt{D}} \left(\mathrm{G}\left(4D-h^2\right)-\mathrm{F}\left(4D-h^2\right)\right) & \text{otherwise.} \end{cases} \tag{5.5}$$

We now equate Equations 5.4 and 5.5 in each of our two cases. When $D=k^2$ we have

$$\sigma(D)+\Psi(D)+\frac{1}{6} = \sum_{-2\sqrt{D}\leqslant h\leqslant 2\sqrt{D}} \left(\mathrm{G}\left(4D-h^2\right)-\mathrm{F}\left(4D-h^2\right)\right) - (\mathrm{G}(0)-\mathrm{F}(0)),$$

whilst when $D\neq k^2$ we have

$$\sigma(D)+\Psi(D) = \sum_{-2\sqrt{D}\leqslant h\leqslant 2\sqrt{D}} \left(\mathrm{G}\left(4D-h^2\right)-\mathrm{F}\left(4D-h^2\right)\right).$$

This motivates $\mathrm{G}(0)=-\frac{1}{6}$ and $\mathrm{F}(0)=0$ as found in Definition 5.1.16.
From this we get

$$\sigma(D)+\Psi(D) = \sum_{-2\sqrt{D}\leqslant h\leqslant 2\sqrt{D}} \left(\mathrm{G}\left(4D-h^2\right)-\mathrm{F}\left(4D-h^2\right)\right),$$

which is exactly what Kronecker claimed. □

We now proceed to derive similar results using an argument based upon our results for $\overline{\mathrm{Cl}}_c(D)$.

Lemma 5.1.18.
Let $D\in\mathbb{Z}_{>0}$. Then

$$\frac{1}{2}\left(\sigma(D)+\Psi(D)\right) = \sum_{-\sqrt{D}<\hat{h}<\sqrt{D}} \mathrm{F}\left(D-\hat{h}^2\right) \quad \textit{if } D\equiv 1 \bmod 2 \tag{5.6}$$

$$2\sigma\left(\frac{D}{2}\right) = \sum_{-\sqrt{D}<\hat{h}<\sqrt{D}} \mathrm{F}\left(D-\hat{h}^2\right) \quad \textit{if } D\equiv 2 \bmod 4 \tag{5.7}$$

$$2\sigma_{\mathrm{odd}}\left(\frac{D}{4}\right)+\sigma\left(\frac{D}{4}\right)+\Psi\left(\frac{D}{4}\right) = \sum_{-\sqrt{D}<\hat{h}<\sqrt{D}} \mathrm{F}\left(D-\hat{h}^2\right) \quad \textit{if } D\equiv 0 \bmod 4. \tag{5.8}$$

Proof.
From Theorem 4.7.4 we have

$$\frac{1}{3}\overline{\mathrm{Cl}}_c(D) = \begin{cases} \sigma(D)+\Psi(D) & \text{if } D\equiv 1 \bmod 2 \\ 4\sigma\left(\frac{D}{2}\right) & \text{if } D\equiv 2 \bmod 4 \\ 4\sigma_{\mathrm{odd}}\left(\frac{D}{4}\right)+2\sigma\left(\frac{D}{4}\right)+2\Psi\left(\frac{D}{4}\right) & \text{if } D\equiv 0 \bmod 4. \end{cases}$$

From Summary 5.1.15 we have $\overline{\mathrm{Cl}}_c(D) = 6 \sum_{-\sqrt{D}<\hat{h}<\sqrt{D}} \mathrm{F}\left(D - \hat{h}^2\right)$.

Equating these yields

$$\sum_{-\sqrt{D}<\hat{h}<\sqrt{D}} \mathrm{F}\left(D - \hat{h}^2\right) = \begin{cases} \frac{1}{2}\left(\sigma(D) + \Psi(D)\right) & \text{if } D \equiv 1 \bmod 2 \\ 2\sigma\left(\frac{D}{2}\right) & \text{if } D \equiv 2 \bmod 4 \\ 2\sigma_{\mathrm{odd}}\left(\frac{D}{4}\right) + \sigma\left(\frac{D}{4}\right) + \Psi\left(\frac{D}{4}\right) & \text{if } D \equiv 0 \bmod 4. \end{cases}$$

□

Lastly, we derive similar results by using our knowledge of $\overline{\overline{\mathrm{Cl}}}_c(D)$.

Lemma 5.1.19.
Let $D \in \mathbb{Z}_{>0}$, then:

$$\sum_{-\sqrt{D}<2\tilde{h}<\sqrt{D}} \mathrm{F}\left(D - 4\tilde{h}^2\right) = \frac{1}{2}\sigma_{\mathrm{odd}}(D) \text{ if } D \equiv 1 \bmod 4$$

$$\sum_{-\sqrt{D}<2\tilde{h}<\sqrt{D}} \mathrm{F}\left(D - 4\tilde{h}^2\right) = \sigma_{\mathrm{odd}}(D) \text{ if } D \equiv 2 \bmod 4$$

$$\sum_{-\sqrt{D}<2\tilde{h}<\sqrt{D}} \mathrm{F}\left(D - 4\tilde{h}^2\right) = \frac{1}{2}\Psi(D) \text{ if } D \equiv 3 \bmod 4$$

$$\sum_{-\sqrt{D}<2\tilde{h}<\sqrt{D}} \mathrm{F}\left(D - 4\tilde{h}^2\right) = \sigma_{\mathrm{odd}}\left(\frac{D}{4}\right) + \Psi\left(\frac{D}{4}\right) \text{ if } D \equiv 4 \bmod 8$$

$$\sum_{-\sqrt{D}<2\tilde{h}<\sqrt{D}} \mathrm{F}\left(D - 4\tilde{h}^2\right) = 4\sigma\left(\frac{D}{8}\right) \text{ if } D \equiv 8 \bmod 16$$

$$\sum_{-\sqrt{D}<2\tilde{h}<\sqrt{D}} \mathrm{F}\left(D - 4\tilde{h}^2\right) = 4\sigma_{\mathrm{odd}}\left(\frac{D}{16}\right) + 2\sigma\left(\frac{D}{16}\right) + 2\Psi\left(\frac{D}{16}\right) \text{ if } D \equiv 0 \bmod 16.$$

Proof.
From Section 4.10 we have

$$\frac{1}{3}\overline{\overline{\mathrm{Cl}}}_c(D) = \begin{cases} \sigma_{\mathrm{odd}}(D) & \text{if } D \equiv 1 \bmod 4 \\ 2\sigma_{\mathrm{odd}}(D) & \text{if } D \equiv 2 \bmod 4 \\ \Psi(D) & \text{if } D \equiv 3 \bmod 4 \\ 2\sigma_{\mathrm{odd}}\left(\frac{D}{4}\right) + 2\Psi\left(\frac{D}{4}\right) & \text{if } D \equiv 4 \bmod 8 \\ 8\sigma\left(\frac{D}{8}\right) & \text{if } D \equiv 8 \bmod 16 \\ 8\sigma_{\mathrm{odd}}\left(\frac{D}{16}\right) + 4\sigma\left(\frac{D}{16}\right) + 4\Psi\left(\frac{D}{16}\right) & \text{if } D \equiv 0 \bmod 16. \end{cases}$$

Now in order to show we indeed recover Kronecker's results, we shall write D in the following ways:

$$D = \begin{cases} m & \text{if } D \equiv 1 \bmod 2 \\ 2m & \text{if } D \equiv 2 \bmod 4 \\ 4n = 2^k m & \text{if } D \equiv 0 \bmod 4. \end{cases}$$

In the last case we refine this to $D = 16q$ when $D \equiv 0 \bmod 16$. Note that in each case m is odd.
We present the derivations below as follows - the top equation is in our notation, while the lower equation is in Kronecker's notation.
Equating with $\overline{\overline{\mathrm{Cl}}}_c(D) = 6 \sum_{-\sqrt{D}<2\tilde{h}<\sqrt{D}} \mathrm{F}\left(D - 4\tilde{h}^2\right)$ yields:

- If $D \equiv 1 \bmod 4$

$$\begin{aligned} \frac{1}{2}\sigma_{\mathrm{odd}}(D) &= \sum_{-\sqrt{D}<2\tilde{h}<\sqrt{D}} \mathrm{F}\left(D - 4\tilde{h}^2\right) \\ \frac{1}{2}\sigma_{\mathrm{odd}}(m) &= \sum_{-\sqrt{m}<2\tilde{h}<\sqrt{m}} \mathrm{F}\left(m - 4\tilde{h}^2\right) \end{aligned} \tag{5.9}$$

- If $D \equiv 2 \bmod 4$

$$\begin{aligned} \sigma_{\mathrm{odd}}(D) &= \sum_{-\sqrt{D}<2\tilde{h}<\sqrt{D}} \mathrm{F}\left(D - 4\tilde{h}^2\right) \\ \sigma_{\mathrm{odd}}(2m) &= \sum_{-\sqrt{2m}<2\tilde{h}<\sqrt{2m}} \mathrm{F}\left(2m - 4\tilde{h}^2\right) \end{aligned} \tag{5.10}$$

- If $D \equiv 3 \bmod 4$

$$\begin{aligned} \frac{1}{2}\Psi(D) &= \sum_{-\sqrt{D}<2\tilde{h}<\sqrt{D}} \mathrm{F}\left(D - 4\tilde{h}^2\right) \\ \frac{1}{2}\Psi(m) &= \sum_{-\sqrt{m}<2\tilde{h}<\sqrt{m}} \mathrm{F}\left(m - 4\tilde{h}^2\right) \end{aligned} \tag{5.11}$$

- If $D \equiv 4 \bmod 8$

$$\begin{aligned} \sigma_{\mathrm{odd}}\left(\frac{D}{4}\right) + \Psi\left(\frac{D}{4}\right) &= \sum_{-\sqrt{D}<2\tilde{h}<\sqrt{D}} \mathrm{F}\left(D - 4\tilde{h}^2\right) \\ \sigma(m) + \Psi(m) &= \sum_{-\sqrt{m}<\tilde{h}<\sqrt{m}} \mathrm{F}\left(4m - 4\tilde{h}^2\right) \end{aligned} \tag{5.12}$$

- If $D \equiv 8 \bmod 16$

$$\begin{aligned} 4\sigma\left(\frac{D}{8}\right) &= \sum_{-\sqrt{D}<2\tilde{h}<\sqrt{D}} \mathrm{F}\left(D - 4\tilde{h}^2\right) \\ 4\sigma(m) &= \sum_{-\sqrt{2m}<\tilde{h}<\sqrt{2m}} \mathrm{F}\left(8m - 4\tilde{h}^2\right) \end{aligned} \tag{5.13}$$

- If $D \equiv 0 \bmod 16$

$$4\sigma_{\text{odd}}\left(\frac{D}{16}\right) + 2\sigma\left(\frac{D}{16}\right) + 2\Psi\left(\frac{D}{16}\right) = \sum_{-\sqrt{D}<2\tilde{h}<\sqrt{D}} \mathrm{F}\left(D - 4\tilde{h}^2\right)$$

$$4\sigma_{\text{odd}}(q) + 2\sigma(q) + 2\Psi(q) = \sum_{-2\sqrt{q}<\tilde{h}<2\sqrt{q}} \mathrm{F}\left(16q - 4\tilde{h}^2\right). \tag{5.14}$$

□

This completes our derivation of Kronecker's equations $(\mathfrak{R})$, $(\mathfrak{R}')$, $(\mathfrak{R}'')$ and $(\mathfrak{R}''')$ on [Kr1897, p. 482].

Theorem 5.1.20.
Let $n \in \mathbb{Z}_{\geqslant 0}$, then $\mathrm{F}(4n) = 2\mathrm{F}(n)$.

Proof.
Recall from Definition 5.1.16 that $\mathrm{F}(0) = 0$ and therefore $0 = \mathrm{F}(4 \cdot 0) = 2 \cdot \mathrm{F}(0)$. Thus we now let $n \in \mathbb{Z}_{>0}$.
Let $n \equiv 1 \bmod 2$ then using Equations 5.6 and 5.12 we have

$$\sum_{-\sqrt{n}<h<\sqrt{n}} \mathrm{F}\left(4\left[n - h^2\right]\right) = \sigma(n) + \Psi(n)$$

$$= 2 \sum_{-\sqrt{n}<h<\sqrt{n}} \mathrm{F}\left(n - h^2\right). \tag{5.15}$$

Similarly, when $2m = n \equiv 2 \bmod 4$, using Equations 5.7 and 5.13we have

$$\sum_{-\sqrt{2m}<h<\sqrt{2m}} \mathrm{F}\left(4\left[2m - h^2\right]\right) = 4\sigma(m)$$

$$= 2 \sum_{-\sqrt{2m}<h<\sqrt{2m}} \mathrm{F}\left(2m - h^2\right). \tag{5.16}$$

Lastly, letting $n \equiv 0 \bmod 4$ and using Equations 5.8 and 5.14 yields

$$\sum_{-2\sqrt{n}<h<2\sqrt{n}} \mathrm{F}\left(4\left[4n - h^2\right]\right) = 4\sigma_{\text{odd}}(n) + 2\sigma(n) + 2\Psi(n)$$

$$= 2 \sum_{-2\sqrt{n}<h<2\sqrt{n}} \mathrm{F}\left(4n - h^2\right). \tag{5.17}$$

We now induct on n.
Base Cases:
$n = 1$: From Equation 5.15 we have

$$\sum_{-1<h<1} \mathrm{F}\left(4[1 - h^2]\right) = 2 \sum_{-1<h<1} \mathrm{F}\left(1 - h^2\right)$$

and therefore $\mathrm{F}(4 \cdot 1) = 2\mathrm{F}(1)$.
$\underline{n = 2:}$ From Equation 5.16 we have

$$\sum_{-\sqrt{2}<h<\sqrt{2}} \mathrm{F}\left(4\left[2 - h^2\right]\right) = 2 \sum_{-\sqrt{2}<h<\sqrt{2}} \mathrm{F}\left(2 - h^2\right).$$

Expanding gives $\mathrm{F}(4 \cdot 1) + \mathrm{F}(4 \cdot 2) + \mathrm{F}(4 \cdot 1) = 2\mathrm{F}(1) + 2\mathrm{F}(2) + 2\mathrm{F}(1)$.
Using our $n = 1$ base case then yields $\mathrm{F}(4 \cdot 2) = 2\mathrm{F}(2)$.
$\underline{n = 3:}$ From Equation 5.15 we have

$$\sum_{-\sqrt{3}<h<\sqrt{3}} \mathrm{F}\left(4\left(3 - h^2\right)\right) = 2 \sum_{-\sqrt{3}<h<\sqrt{3}} \mathrm{F}\left(3 - h^2\right).$$

Expanding gives $\mathrm{F}(4 \cdot 2) + \mathrm{F}(4 \cdot 3) + \mathrm{F}(4 \cdot 2) = 2\mathrm{F}(2) + 2\mathrm{F}(3) + 2\mathrm{F}(2)$.
Using our $n = 2$ base case then yields $\mathrm{F}(4 \cdot 3) = 2\mathrm{F}(3)$.
$\underline{n = 4:}$ From Equation 5.17 we have

$$\sum_{-2<h<2} \mathrm{F}\left(4\left[4 - h^2\right]\right) = 2 \sum_{-2<h<2} \mathrm{F}\left(4 - h^2\right).$$

Expanding gives $\mathrm{F}(4 \cdot 3) + \mathrm{F}(4 \cdot 4) + \mathrm{F}(4 \cdot 3) = 2\mathrm{F}(3) + 2\mathrm{F}(4) + 2\mathrm{F}(3)$.
Using our $n = 3$ base case then yields $\mathrm{F}(4 \cdot 4) = 2\mathrm{F}(4)$.
Thus we have shown $\mathrm{F}(4n) = 2\mathrm{F}(n)$ for $n \leqslant 4$.
$\underline{\text{Inductive Hypothesis:}}$ Suppose $\mathrm{F}(4n) = 2\mathrm{F}(n)$ for $n \leqslant 4k$, $k \in \mathbb{Z}_{>0}$.
$\underline{n = 4k + 1:}$ Applying Equation 5.15 gives

$$\sum_{-\sqrt{4k+1}<h<\sqrt{4k+1}} \mathrm{F}\left(4\left[4k + 1 - h^2\right]\right) = 2 \sum_{-\sqrt{4k+1}<h<\sqrt{4k+1}} \mathrm{F}\left(4k + 1 - h^2\right).$$

We rewrite both sides by moving the $h = 0$ term out of the sum. This expresses the right hand side as:

$$\mathrm{F}(4[4k + 1]) + \sum_{\substack{|h|<\sqrt{4k+1} \\ h \neq 0}} \mathrm{F}\left(4\left[4k + 1 - h^2\right]\right) = 2\mathrm{F}(4k + 1) + 2 \sum_{\substack{|h|<\sqrt{4k+1} \\ h \neq 0}} \mathrm{F}(4k + 1 - h^2).$$

Since $4k+1-h^2 \leqslant 4k$ for $h \in \left(-\sqrt{4k+1}, \sqrt{4k+1}\right) \setminus \{0\}$, we may apply our inductive hypothesis. This gives $\mathrm{F}\left(4\left[4k + 1\right]\right) = 2\mathrm{F}\left(4k + 1\right)$.
$\underline{n = 4k + 2:}$ Applying Equation 5.16 gives

$$\sum_{-\sqrt{4k+2}<h<\sqrt{4k+2}} \mathrm{F}\left(4\left[4k + 2 - h^2\right]\right) = 2 \sum_{-\sqrt{4k+2}<h<\sqrt{4k+2}} \mathrm{F}\left(4k + 2 - h^2\right).$$

Rewriting both sides by moving the $h = 0$ and $h = \pm 1$ terms out of the summation gives

$$\mathrm{F}\left(4\left[4k + 2\right]\right) + 2\mathrm{F}\left(4\left[4k + 1\right]\right) + \sum_{\substack{-\sqrt{4k+2}<h<\sqrt{4k+2} \\ h \neq 0, \pm 1}} \mathrm{F}\left(4\left[4k + 2 - h^2\right]\right) =$$

$$2\mathrm{F}\left(4k+2\right)+4\mathrm{F}\left(4k+1\right)+2\sum_{\substack{-\sqrt{4k+2}<h<\sqrt{4k+2}\\ h\neq 0,\pm 1}}\mathrm{F}\left(4k+2-h^2\right).$$

Since $4k+2-h^2 \leqslant 4k$ for $h \in \left(-\sqrt{4k+2}, \sqrt{4k+2}\right) \setminus \{0, \pm 1\}$ we apply our inductive hypothesis along with the $n = 4k+1$ case. This yields $\mathrm{F}\left(4\left[4k+2\right]\right) = 2\mathrm{F}\left(4k+2\right)$.
n=4k+3: Applying Equation 5.15 gives

$$\sum_{-\sqrt{4k+3}<h<\sqrt{4k+3}}\mathrm{F}\left(4\left[4k+3-h^2\right]\right)=2\sum_{-\sqrt{4k+3}<h<\sqrt{4k+3}}\mathrm{F}\left(4k+3-h^2\right).$$

Rewriting both sides by moving the $h = 0$ and $h = \pm 1$ terms out of the summation gives

$$2\mathrm{F}\left(4\left[4k+2\right]\right)+\mathrm{F}\left(4\left[4k+3\right]\right)+\sum_{\substack{-\sqrt{4k+3}<h<\sqrt{4k+3}\\ h\neq 0,\pm 1}}\mathrm{F}\left(4\left[4k+3-h^2\right]\right)=$$
$$4\mathrm{F}(4k+2)+2\mathrm{F}(4k+3)+2\sum_{\substack{-\sqrt{4k+3}<h<\sqrt{4k+3}\\ h\neq 0,\pm 1}}\mathrm{F}\left(4k+3-h^2\right).$$

Since $4k+3-h^2 \leqslant 4k$ for $h \in \left(-\sqrt{4k+3}, \sqrt{4k+3}\right) \setminus \{0, \pm 1\}$ we apply our inductive hypothesis along with the $n = 4k+2$ case. This yields $\mathrm{F}\left(4\left[4k+3\right]\right) = 2\mathrm{F}\left(4k+3\right)$.
$n = 4(k+1)$: Applying Equation 5.17 gives

$$\sum_{-\sqrt{k+1}<h<\sqrt{k+1}}\mathrm{F}\left(4\left[4(k+1)-h^2\right]\right)=2\sum_{-\sqrt{k+1}<h<\sqrt{k+1}}\mathrm{F}\left(4\left[k+1\right]-h^2\right).$$

Rewriting both sides by moving the $h = 0$ and $h = \pm 1$ terms out of the summation yields

$$2\mathrm{F}\left(4[4k+3]\right)+\mathrm{F}\left(4[4k+4]\right)+\sum_{\substack{-\sqrt{k+1}<h<\sqrt{k+1}\\ h\neq 0,\pm 1}}\mathrm{F}\left(4\left[4(k+1)-h^2\right]\right)=$$
$$4\mathrm{F}\left(4k+3\right)+2\mathrm{F}\left(4k+4\right)+2\sum_{\substack{-\sqrt{k+1}<h<\sqrt{k+1}\\ h\neq 0,\pm 1}}\mathrm{F}\left(4k+4-h^2\right).$$

Since $4k+4-h^2 \leqslant 4k$ for $h \in \left(-\sqrt{4k+4}, \sqrt{4k+4}\right) \setminus \{0, \pm 1\}$ we may apply our inductive hypothesis along with the case $n = 4k+3$. This yields $\mathrm{F}\left(4\left[4k+4\right]\right) = 2\mathrm{F}\left(4k+4\right)$.
Hence we have shown if $\mathrm{F}\left(4n\right) = 2\mathrm{F}\left(n\right)$ for $n \leqslant 4k$ then $\mathrm{F}\left(4q\right) = 2\mathrm{F}\left(q\right)$ for $4k+1 \leqslant q \leqslant 4k+4$. Therefore by induction on $n \in \mathbb{Z}_{>0}$ we have $\mathrm{F}\left(4n\right) = 2\mathrm{F}\left(n\right)$ for all $n \in \mathbb{Z}_{\geqslant 0}$. □

Notes on Section 5.1

We observe the result found in Theorem 5.1.14 differs from Kronecker's claim found at the beginning of Section 21, [Kr1897, p. 481]. The difference is a factor of two and is due to Kronecker implicitly considering definite rather than positive definite forms.

Observation 5.1.21.
The results found in Lemma 5.1.18 match Kronecker's ([Kr1897, p. 482]) exactly. To see this, write $D = m$ when $D \equiv 1 \bmod 2$, $D = 2m$ when $D \equiv 2 \bmod 4$, and $D = 4n$ when $D \equiv 0 \bmod 4$. Then Equations 5.6, 5.7 and 5.8 become:

$$\begin{aligned}
\frac{1}{2}\left(\sigma(m) + \Psi(m)\right) &= \sum_{-2\sqrt{m}<\hat{h}<2\sqrt{m}} \mathrm{F}\left(m - \hat{h}^2\right) \\
2\sigma(m) &= \sum_{-\sqrt{2m}<\hat{h}<\sqrt{2m}} \mathrm{F}\left(2m - \hat{h}^2\right) \\
2\sigma_{\mathrm{odd}}(n) + \sigma(n) + \Psi(n) &= \sum_{-2\sqrt{n}<\hat{h}<2\sqrt{n}} \mathrm{F}\left(4n - \hat{h}^2\right).
\end{aligned}$$

These are (in reverse order) the results given by Kronecker in [Kr1897, p. 482].

Observation 5.1.22.
If by some other method we determine $\mathrm{F}(4n) = 2\mathrm{F}(n)$ for $n \in \mathbb{N}_{\geqslant 0}$ then it is straightforward to recover Equations 5.12, 5.13 and 5.14. This is done by using $\mathrm{F}(4n) = 2\mathrm{F}(n)$ in each of Equations 5.6, 5.7 and 5.8.

We also note that Kronecker's results found on page 444 of [Kr1897] are stated without proof. Kronecker opts to defer the proofs to his earlier paper [Kr1860]. In his earlier paper the details of the proofs are somewhat vague and appear to use non-arithmetic techniques. Consequently we will develop new purely arithmetic proofs in order to fill in the gaps.

5.2 An Arithmetical Deduction for Binary Quadratic Forms with $n = ac - b^2 \equiv 3 \bmod 4$.

In this section we will give an arithmetic derivation of Kronecker's formula $3\mathrm{G}(n) = \left(5 - (-1)^{\frac{n-3}{4}}\right)\mathrm{F}(n)$ when $n \equiv 3 \bmod 4$.

Lemma 5.2.1.
Let $n \in \mathbb{Z}_{>0}$ then the set $\Omega_n = \{(a,b,c) \mid ac - b^2 = n, -\min\{a,c\} < b \leqslant \min\{a,c\}\}$ contains a unique representative for each complete equivalence class of binary quadratic forms $ax^2 + 2bxy + cy^2$ with determinant $ac - b^2 = n$.

Proof.
We first prove the existence of such a binary quadratic form within the complete equivalence class of an arbitrary binary quadratic form with determinant $n = ac - b^2$. We fix a complete equivalence class $[f]_c$ where $f = ax^2 = 2bxy + cy^2$. If f satisfies $-\min\{a,c\} < b \leqslant \min\{a,c\}$ then we are done. Thus we suppose f does not satisfy this. Then we must have either $b = -\min\{a,c\}$ or $|b| > \min\{a,c\}$. If $b = -\min\{a,c\}$ then we apply the transformation $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ if $a \leqslant c$ or apply

$\begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$ if $a > c$. It is straightforward to use Observation 2.4.5 to verify these transformations take f to $\begin{pmatrix} a & a \\ a & c \end{pmatrix}$ or $\begin{pmatrix} a & c \\ c & c \end{pmatrix}$. It is then clear that each of these forms satisfy $-\min\{a,c\} < b \leqslant \min\{a,c\}$. Hence we may now assume $|b| > \min\{a,c\}$.
We may further assume $a \leqslant c$ as if this is not the case then applying the transformation $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ if $b > 0$ or $\begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix}$ if $b < 0$ yields a completely equivalent binary quadratic form with $a \leqslant c$. We note $b \neq 0$ as this would imply we satisfy our criterion.
Thus our goal is to reduce the value of b below a. Observe applying the transformation $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}^k$ yields the form $\begin{pmatrix} a & 2ka+b \\ 2ka+b & 4k^2a+4kb+c \end{pmatrix} = \begin{pmatrix} a' & b' \\ b' & c' \end{pmatrix}$. We may choose $k \in \mathbb{Z}$ so that $-a < 2ka + b \leqslant a$. It then remains to show $-c' < b' \leqslant c'$ also.
If this is already the case then we are done. So suppose it is not the case, thus we have either $b' = -c'$ or we have $c' < |b'| \leqslant a'$. In the first instance we may apply the transformation $\begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$ to get the form $\begin{pmatrix} a' & c' \\ c' & c' \end{pmatrix}$ which satisfies our criterion. Thus we may assume we are in the latter case.
In this case we observe applying the transformation $\begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}^q$ yields the binary quadratic form $\begin{pmatrix} a'+4qb'+4q^2c' & b'+2qc' \\ b'+2qc' & c' \end{pmatrix} = \begin{pmatrix} a'' & b'' \\ b'' & c'' \end{pmatrix}$. We may choose $q \in \mathbb{Z}$ so that $-c' < b' + 2qc' \leqslant c'$.
If we have $-a'' < b'' \leqslant a''$ then we are done. Similarly if $b'' = -a''$ we are done after applying the transformation $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$. If this is not the case then we may repeat this two step process again.
This yields a sequence of integers b, b', b'' where $|b| > |b'| > |b''| > \ldots$. Thus either the process terminates at the desired form or $b = 0$ eventually. However, $b = 0$ results in a form that automatically satisfies our criterion.
Hence every complete equivalence class of binary quadratic forms with determinant $ac - b^2 = n$ contains at least one form f that satisfies $-\min\{a,c\} < b \leqslant \min\{a,c\}$.
We now prove uniqueness. Suppose there exists a complete equivalence class $[f]_c$ containing two binary quadratic forms f, g that satisfy our criterion. We observe that the matrix representations of these binary quadratic forms may instead be viewed as the matrix representations of symmetric bilinear forms. Since $\ker \sigma$ does not change according to whether we are considering binary quadratic or bilinear forms, we apply Theorem 3.1.28 to see we must have $f = g$ unless $|2b| = 2a$ or $|2b| = 2c$. From the proof of Theorem 3.1.28 (special cases 1 and 2) we see when $|2b| = 2a$ or $|2b| = 2c$ then we must have $f = \begin{pmatrix} a & -a \\ -a & c \end{pmatrix}$ and $g = \begin{pmatrix} a & a \\ a & c \end{pmatrix}$ or $f = \begin{pmatrix} a & -c \\ -c & c \end{pmatrix}$ and $g = \begin{pmatrix} a & c \\ c & c \end{pmatrix}$ respectively unless $f = g$. Observe these are matrices that can represent binary quadratic forms and that by the criterion $-\min\{a,c\} < b \leqslant \min\{a,c\}$

only one of these forms is possible in each case. Therefore we must have $f = g$ always. Hence every complete equivalence class of binary quadratic forms with determinant $n = ac - b^2$ contains a unique binary quadratic form satisfying $-\min\{a, c\} < b \leqslant \min\{a, c\}$. □

Our goal now is to prove the first part of Kronecker's claim. We will state the theorem first and then give a series of lemmas that will prove it.

Theorem 5.2.2.
Let $n \in \mathbb{Z}_{>0}$ be such that $n \equiv 3 \bmod 8$. Then $3\mathrm{G}(n) = 4\mathrm{F}(n)$.

In order to prove Theorem 5.2.2 we will use the set Ω_n from Lemma 5.2.1. We shall partition this set into a union of three disjoint sets. Until explicitly stated otherwise, we will assume $n \in \mathbb{Z}$ satisfies $n \equiv 3 \bmod 8$.

Definition 5.2.3.
Let $O, E, W \subseteq \Omega_n$ be defined as follows:

$$\begin{aligned} O &= \{(a, b, c) | a \equiv c \equiv 1 \bmod 2\} \\ E &= \{(a, b, c) | a \equiv c \equiv 0 \bmod 2\} \\ W &= \{(a, b, c) | a \not\equiv c \bmod 2\}. \end{aligned}$$

Observation 5.2.4.
Since the complete equivalence class number is finite we have $|O|$, $|E|$ and $|W| < \infty$. Now observe the binary quadratic form $(1, 0, n) \in O$. This is because $n \equiv 3 \bmod 8$ and it is clear that the determinant is n and the form satisfies $-\min\{a, c, \} < b \leqslant \min\{a, c\}$.
Now observe the binary quadratic form $(2, 1, \frac{n+1}{2}) \in E$. This is because $n \equiv 3 \bmod 8$ implies $2 \mid n + 1$ and $\frac{n+1}{2} \equiv 0 \bmod 2$. It is straightforward to check the determinant is n and that it satisfies $-\min\{a, c\} < b \leqslant \min\{a, c\}$. Thus this form lies in E.
Similarly, we observe $(1, 1, n+1) \in W$. Letting $a = b = 1$ implies $n = ac - b^2 = c - 1$ and so $c = n + 1$. Since $n \equiv 3 \bmod 8$ it follows that c is even. Again it is straightforward to check the determinant is n and that this form satisfies $-\min\{a, c\} < b \leqslant \min\{a, c\}$.
Hence the sets O, E and W are always non-empty when $n \equiv 3 \bmod 8$.

Lemma 5.2.5.
The map

$$\begin{aligned} \pi_1 : W &\longrightarrow W \\ (a, b, c) &\longmapsto (c, b, a) \end{aligned}$$

is a well-defined involution with no fixed points.

Proof.
Well-defined: Let $\pi_1(a, b, c) = (c, b, a) = (a', b', c')$ then since $a \not\equiv c \bmod 2$, $a' \not\equiv c' \bmod 2$ follows. Clearly the determinant is preserved and since (a, b, c) satisfies

$-\min\{a,c\} < b \leqslant \min\{a,c\}$ it follows that (a',b',c') satisfies $-\min\{a',c'\} < b' \leqslant \min\{a',c'\}$. Thus the map π_1 is well-defined.
Injectivity: Suppose $\pi_1(a,b,c) = \pi_1(\hat{a},\hat{b},\hat{c})$ then we have $(c,b,a) = (\hat{c},\hat{b},\hat{a})$ and the map is injective.
Surjectivity: Let $(a,b,c) \in W$ be arbitrary and consider (c,b,a). Then we have $\pi_1(c,b,a) = (a,b,c)$ and by identical reasoning to that found in the well-defined part of the proof, that $(c,b,a) \in W$.
Hence the map π_1 is surjective and hence an involution on the set W.
We observe the map π_1 will have a fixed point $(a,b,c) = (c,b,a)$, that is if $a = c$. However in the set W we have $a \not\equiv c \bmod 2$ so this cannot arise. Therefore π_1 has no fixed points. □

Lemma 5.2.6.
The map π_1 found in Lemma 5.2.5 partitions the set W into a disjoint union of $\hat{W}$ and $\hat{W}^c$ where

$$\hat{W} = \{w \in W | a \equiv 1 \bmod 2, c \equiv 0 \bmod 2\}.$$

Proof.
Let $\hat{W} = \{w \in W | a \equiv 1 \bmod 2, c \equiv 0 \bmod 2\} \subseteq W$. Then we have $\pi_1(\hat{W}) \subseteq \hat{W}^c$ because $\pi_1((a,b,c)) = (c,b,a) = (a',b',c')$ satisfies $a' = c \equiv 0 \bmod 2$, $c' = a \equiv 1 \bmod 2$. Similarly we observe $\pi_1(\hat{W}^c) \subseteq \hat{W}$ by the same logic. Since π_1 is a bijection we have $W = \hat{W} \cup \hat{W}^c$ and $|\hat{W}| = |\hat{W}^c|$ as clearly this is a disjoint union. □

We now prove three quick lemmas to aid the proof of our next map.

Lemma 5.2.7.
Let $n \in \mathbb{Z}_{>0}$ satisfy $n \equiv 3 \bmod 8$ and let (a,b,c) be such that $ac - b^2 = n$ and $a \equiv c \equiv 1 \bmod 2$. Then $a + c \equiv 4 \bmod 8$ if and only if $4 \mid b$, while $a + c \equiv 0 \bmod 8$ if and only if $2 \mid b$ but $4 \nmid b$.

Proof.
Recall $b^2 \equiv 0, 1, 4 \bmod 8$ with $b^2 \equiv 1 \bmod 8$ if and only if $b \equiv 1 \bmod 2$. Thus $n = ac - b^2 \equiv 3 \bmod 8$ implies $ac \equiv 3, 4, 7 \bmod 8$. Since $a \equiv c \equiv 1 \bmod 2$ it follows that $ac \not\equiv 4 \bmod 8$.
Next, observe $ac = (8k + i)(8l + j) \equiv ij \bmod 8$ and so if $i = j$ then $ac \equiv 1 \bmod 8$. Thus we must have $i \neq j$ and both i and j are odd.
We now prove our first claim: $a + c \equiv 4 \bmod 8$ if and only if $4 \mid b$.
($\Rightarrow$) Assume $a + c \equiv 4 \bmod 8$ then $(a + c) = (8k + i) + (8l + j) \equiv i + j \bmod 8$ and thus $(i,j) \in \{(1,3),(3,1),(5,7),(7,5)\}$. Hence we see $ac \equiv 3 \bmod 8$ and therefore $ac - b^2 = n \equiv 3 \bmod 8$ implies $b^2 \equiv 0 \bmod 8$, that is, $4 \mid b$.
($\Leftarrow$) Assume $4 \mid b$ then $ac - b^2 = n \equiv 3 \bmod 8$ implies $ac \equiv 3 \bmod 8$. Since $ac \equiv ij \bmod 8$ we have $(i,j) \in \{(1,3),(3,1),(5,7),(7,5)\}$ and it is straightforward to verify $a + c \equiv 4 \bmod 8$.
We now prove our second claim: $a + c \equiv 0 \bmod 8$ if and only if $2 \mid b$ but $4 \nmid b$.
($\Rightarrow$) Assume $a + c \equiv 0 \bmod 8$ then $(a + c) = (8k + i) + (8l + j) \equiv i + j \bmod 8$ and thus $(i,j) \in \{(1,7),(7,1),(3,5),(5,3)\}$. Hence we see $ac \equiv 7 \bmod 8$ and therefore

$ac - b^2 = n \equiv 3 \bmod 8$ implies $b^2 \equiv 4 \bmod 8$. Hence $2 \mid b$ but $4 \nmid b$.
($\Leftarrow$) Assume $2 \mid b$ but $4 \nmid b$ then $ac - b^2 \equiv 3 \bmod 8$ implies $ac \equiv 7 \bmod 8$ and thus $(i, j) \in \{(1, 7), (7, 1), (3, 5), (5, 3)\}$. It is then straightforward to verify $a + c \equiv 0 \bmod 8$. □

Lemma 5.2.8.
Let $n \equiv 3 \bmod 4$ then within the sets O and E we cannot have equality in the condition $-\min\{a, c\} < b \leqslant \min\{a, c\}$. That is, we have $|b| < \min\{a, c\}$.

Proof.
First consider the set O, where we have $a \equiv c \equiv 1 \bmod 2$. Then $n \equiv 3 \bmod 4$ implies $b \equiv 0 \bmod 2$ and thus $a \neq b$ as well as $c \neq b$. Since we already have $-\min\{a, c\} < b \leqslant \min\{a, c\}$ it follows that we have $|b| < \min\{a, c\}$.
Now consider the set E, where we have $a \equiv c \equiv 0 \bmod 2$. Then $n \equiv 3 \bmod 4$ implies $b^2 \equiv 1 \bmod 4$ and thus $b \equiv 1 \bmod 2$. Again this implies $a \neq b$ and $c \neq b$ and therefore we have $|b| < \min\{a, c\}$. □

Lemma 5.2.9.
Let $n \equiv 3 \bmod 8$ and (a, b, c) be such that $ac - b^2 = n$ with $a \equiv c \equiv 0 \bmod 2$. Then $a \equiv c \equiv 2 \bmod 4$ and $b \equiv 1 \bmod 2$.

Proof.
We have $a \equiv c \equiv 0 \bmod 2$ implies $ac \equiv 0$ or $4 \bmod 8$. Then $ac - b^2 \equiv 3 \bmod 8$ implies $b^2 \equiv 1$ or $5 \bmod 8$. However, $b^2 \equiv 5 \bmod 8$ is impossible and so we must have $ac \equiv 4 \bmod 8$ and $b^2 \equiv 1 \bmod 8$. This then implies $a \equiv c \equiv 2 \bmod 4$ and $b \equiv 1 \bmod 2$. □

Lemma 5.2.10.
The map

$$\begin{aligned} \pi_2 : O &\longrightarrow E \\ (a, b, c) &\longmapsto \left(\frac{a - 2b + c}{2}, \frac{c - a}{2}, \frac{a + 2b + c}{2} \right) \end{aligned}$$

is a well-defined bijection.

Proof.
Well-defined: By Lemma 5.2.7 we have $a+c \equiv 0 \bmod 4$ and $b \equiv 0 \bmod 2$. From this is follows that $\frac{a-2b+c}{2} = \frac{4k-2b}{2} \equiv 0 \bmod 2$. Further, $\frac{c-a}{2} = \frac{(2k+1)-(2m+1)}{2} = k - m \in \mathbb{Z}$ and $\frac{a+2b+c}{2} \equiv 0 \bmod 2$. We also note one can verify $a'c' - b'^2 = \left(\frac{a-2b+c}{2}\right)\left(\frac{a+2b+c}{2}\right) - \left(\frac{c-a}{2}\right) = ac - b^2 = n$ and so π_2 preserves the determinant.
Now let $\pi_2(a, b, c) = \left(\frac{a-2b+c}{2}, \frac{c-a}{2}, \frac{a+2b+c}{2}\right) = (a', b', c')$. We first show a' and $c' > 0$. We have $a' = \frac{a-2b+c}{2}$ and since $a, c > 0$ and $-\min\{a, c\} < b \leqslant \min\{a, c\}$ it follows that $a - 2b + c \geqslant 0$. For it to equal 0 we must have $a = b = c$ and thus $ac - b^2 = 0$, contradicting $n \equiv 3 \bmod 8$. Thus $a' > 0$. A similar argument immediately yields $c' > 0$.

Applying Lemma 5.2.8 we have $-\min\{a,c\} < b < \min\{a,c\}$ which gives the following four chains of inequalities:

$$\begin{aligned}
-a < b \Rightarrow -2a < 2b \qquad & \Rightarrow c-2a < c+2b \Rightarrow c-a < a+2b+c \\
-c < b \Rightarrow -2c < 2b \qquad & \Rightarrow a-2c < a+2b \Rightarrow a-c < a+2b+c \\
b < a \Rightarrow 2b < 2a \qquad & \Rightarrow 2b-c < 2a-c \Rightarrow -a+2b-c < a-c \\
b < c \Rightarrow 2b < 2c \qquad & \Rightarrow 2b-a < 2c-a \Rightarrow -a+2b-c < c-a.
\end{aligned}$$

The first two inequalities combine to yield $-(a+2b+c) < c-a < a+2b+c$ and thus $-2c' < 2b' < 2c'$.
The second pair of inequalities combine to yield $-(a-2b+c) < c-a < a-2b+c$ and thus $-2a' < 2b' < 2a'$.
From these we deduce $-\min\{a',c'\} < b' < \min\{a',c'\}$. Hence we see the map π_2 is well-defined.
Injectivity: Suppose $\pi_2((a,b,c)) = \pi_2((\hat{a},\hat{b},\hat{c}))$ then we have $\left(\frac{a-2b+c}{2}, \frac{c-a}{2}, \frac{a+2b+c}{2}\right) = \left(\frac{\hat{a}-2\hat{b}+\hat{c}}{2}, \frac{\hat{c}-\hat{a}}{2}, \frac{\hat{a}+2\hat{b}+\hat{c}}{2}\right)$. Equating entry-wise we get $a-2b+c = \hat{a}-2\hat{b}+\hat{c}$, $c-a = \hat{c}-\hat{a}$ and $a+2b+c = \hat{a}+2\hat{b}+\hat{c}$. Rearranging the second equation to get $\hat{a} = \hat{c}-c+a$ and substituting this into each of the first and third equations yields

$$\begin{aligned}
c &= \hat{c} + (b-\hat{b}) \\
c &= \hat{c} + (\hat{b}-b).
\end{aligned}$$

Taking the difference of these gives $0 = 2(b-\hat{b})$ and thus $b = \hat{b}$. Using this both the first and third equations become $a+c = \hat{a}+\hat{c}$. Combining with the second then yields $a = \hat{a}$ and $c = \hat{c}$. Hence the map π_2 is injective.
Surjectivity: Let $(a,b,c) \in E$ be arbitrary and let $\left(\frac{a-2b+c}{2}, \frac{c-a}{2}, \frac{a+2b+c}{2}\right) = (a',b',c')$. We first show this lies in the set O. By Lemma 5.2.9 we have $a \equiv c \equiv 2 \bmod 4$ and $b \equiv 1 \bmod 2$. Therefore

$$\begin{aligned}
\frac{a-2b+c}{2} &= \frac{(4k+2)-2b+(4l+2)}{2} \\
&= 2k+1-b+2k+1 \\
&= 2(k+l+1)-b \\
&\equiv b \mod 2 \\
&\equiv 1 \bmod 2.
\end{aligned}$$

In an analogous manner we see $\frac{a+2b+c}{2} \equiv 1 \bmod 2$. Lastly, $\frac{c-a}{2} \in \mathbb{Z}$ as $c-a \equiv 0 \bmod 4$ by Lemma 5.2.9. Thus $\left(\frac{a-2b+c}{2}, \frac{c-a}{2}, \frac{a+2b+c}{2}\right) \in O$.
We now see $\pi_2\left(\left(\frac{a-2b+c}{2}, \frac{c-a}{2}, \frac{a+2b+c}{2}\right)\right)$ has $\frac{\left(\frac{a-2b+c}{2}\right)-2\left(\frac{c-a}{2}\right)+\left(\frac{a+2b+c}{2}\right)}{2} = a$ for its first entry, $\frac{\left(\frac{a+2b+c}{2}\right)-\left(\frac{a-2b+c}{2}\right)}{2} = b$ for its second entry, and $\frac{\left(\frac{a-2b+c}{2}\right)+2\left(\frac{c-a}{2}\right)+\left(\frac{a+2b+c}{2}\right)}{2} = c$ for its last entry. Thus $\pi_2\left(\left(\frac{a-2b+c}{2}, \frac{c-a}{2}, \frac{a+2b+c}{2}\right)\right) = (a,b,c)$ We note the condition $-\min\{a',c'\} < b' \leqslant \min\{a',c'\}$ can be verified directly in the same manner as in the well-defined part of this proof. Hence the map π_2 is surjective and thus is a bijection. An immediate consequence of this is $|E| = |O|$. $\square$

We now partition the sets $\hat{W}$ and O as follows:

$$O = O_b \cup {O_b}^c, \text{ where } O_b = \{(a,b,c) \in O \mid b = 0\}$$
$$\hat{W} = \hat{W}_b \cup \hat{W}_b^c, \text{ where } \hat{W}_b^c = \{(a,b,c) \in \hat{W} \mid a = b\}.$$

Observation 5.2.11.
We observe the sets O_b and O_b^c are disjoint, as are the sets $\hat{W}_b$ and $\hat{W}_b^c$. Next, note that $(1,0,n) \in O_b$ as $n \equiv 3 \bmod 8$ and $(1,1,n+1) \in \hat{W}_b$. It is important to note that the sets O_b^c and $\hat{W}_b^c$ may in fact be empty such as when $n = 3$. Thus in Lemma 5.2.18 it is possible to have a vacuous bijection.

Lemma 5.2.12.
The map

$$\pi_3 : \hat{W}_b \longrightarrow O_b$$
$$(a,a,c) \longmapsto (a,0,c-a)$$

is a well-defined bijection.

Proof.
Well-defined: Let $(a,a,c) \in \hat{W}_b$ be arbitrary and so $a \equiv 1 \bmod 2$ and $c \equiv 0 \bmod 2$. Then $\pi_3(a,a,c) = (a,0,c-a) = (a',b',c')$ satisfies $a'c' - {b'}^2 = a(c-a) - 0^2 = ac - a^2 = \det(a,a,c) = n$. Next we have $a' \equiv c' \equiv 1 \bmod 2$ because $a \equiv 1 \bmod 2$ and thus $c' = c - a \equiv 1 \bmod 2$. Now observe $a' = a > 0$ and observe $c' = c - a > 0$ since we have $a > 0$ and our forms satisfy $-\min\{a,c\} < b \leqslant \min\{a,c\}$, hence $b = a$ implies $a < c$ (Note $a \neq c$ else $n = 0$). Since $b' = 0$ we automatically satisfy $-\min\{a',c'\} < b \leqslant \min\{a',c'\}$ and so we deduce $\pi_3(a,a,c) \subseteq O_b$.
Injectivity: Suppose $\pi_3(a,a,c) = \pi_3(\hat{a},\hat{a},\hat{c})$ then we have $(a,0,c-a) = (\hat{a},0,\hat{c}-\hat{a})$. Hence $a = \hat{a}$, $c = \hat{c}$ and therefore the map π_3 is injective.
Surjectivity: Let $(a,b,c) \in O_b$ be arbitrary and consider $(a,a,c+a) = (a',b',c')$. We will show this lies in $\hat{W}_b$. Since $(a,b,c) \in O_b$ we have $b = 0$ and thus $n = ac - b^2 = ac$. We observe $\det(a,a,c+a) = a(c+a) - a^2 = ac + a^2 - a^2 = ac = n$. Next, $(a,b,c) \in O_b$ implies $a \equiv c \equiv 1 \bmod 2$ and therefore $a' = a \equiv 1 \bmod 2$ and $c' = c + a \equiv 0 \bmod 2$. Further we have $a' = b'$ and it remains to show $-\min\{a',c'\} < b' \leqslant \min\{a',c'\}$.
We see $c' = c + a > a = a'$ as $c > 0$ by positive definiteness. Then since $0 < a' = b'$ we immediately have the above criterion. Thus $(a,a,c+a) \in \hat{W}_b$.
Lastly we see $\pi_3(a,a,c+a) = (a,0,c+a-a) = (a,0,c) = (a,b,c)$. Hence the map π_3 is surjective and therefore is a bijection.
As a consequence we have $|\hat{W}_b| = |O_b|$. □

Our next result is a brief lemma to aid our next map.

Lemma 5.2.13.
Binary quadratic forms in the set $\hat{W}_b^c$ satisfy $b \equiv 1 \bmod 2$ and $-\min\{a,c\} < b < \min\{a,c\}$.

Proof.
Every binary quadratic form in the set $\hat{W}_b^c$ satisfies $a \equiv 1 \bmod 2$, $c \equiv 0 \bmod 2$ and $a \neq b$. Thus $ac \equiv 0 \bmod 2$ and consequently in order to have $ac - b^2 = n \equiv 3 \bmod 8$ we must have $b \equiv 1 \bmod 2$.
Then $-\min\{a,c\} < b \leqslant \min\{a,c\}$ implies either $-a < b < a$ if $a \leqslant c$ as $b \neq a$, or $-c < b < c$ if $c < a$ as $b \equiv \bmod 2$ while $c \equiv 0 \bmod 2$.
Hence we have $-\min\{a,c\} < b < \min\{a,c\}$. □

Lemma 5.2.14.
The map

$$\begin{aligned} \pi_5 : \hat{W}_b^c &\longrightarrow \hat{W}_b^c \\ (a,b,c) &\longmapsto (a,-b,c) = (a',b',c') \end{aligned}$$

is a well-defined involution with no fixed points.

Proof.
Well-defined: Clearly this map preserves the determinant and satisfies $a' > 0$, $c' > 0$. By Lemma 5.2.8 we have $-\min\{a,c\} < b < \min\{a,c\}$ and hence we get $-\min\{a',c'\} < b' < \min\{a',c'\}$. It is evident from this that $b' \neq a'$, and lastly we have $a' = a \equiv 1 \bmod 2$ as well as $c' = c \equiv 0 \bmod 2$. Thus $\pi_5(a,b,c) \subseteq \hat{W}_b^c$.
Injectivity: This is straightforward to verify.
Surjectivity: Let $(a,b,c) \in \hat{W}_b^c$ be arbitrary and consider $(a',b',c') = (a,-b,c)$. This lies in $\hat{W}_b^c$ since it has determinant n, $a' = a \equiv 1 \bmod 2$, $c' = c \equiv 0 \bmod 2$ and by Lemma 5.2.8 satisfies $-\min\{a',c'\} < b' < \min\{a',c'\}$ and thus $b' \neq a'$. Lastly we note $\pi_5(a',b',c') = (a,-(-b),c) = (a,b,c)$ and hence the map π_5 is a surjection and thus an involution.
Now suppose $\pi_5(a,b,c) = (a,b,c)$ then we have $(a,-b,c) = (a,b,c)$ and it is clear this requires $b = 0$. However, by Lemma 5.2.13 we have $b \equiv 1 \bmod 2$ and thus $b = 0$ is impossible.
Hence the map π_5 has no fixed points. □

Corollary 5.2.15.
The set $\hat{W}_b^c$ may be written as the disjoint union of the sets $\hat{W}_{b+}^c$ and $\hat{W}_{b-}^c$, where

$$\begin{aligned} \hat{W}_{b+}^c &= \left\{ (a,b,c) \in \hat{W}_b^c \mid b > 0 \right\} \\ \hat{W}_{b-}^c &= \left\{ (a,b,c) \in \hat{W}_b^c \mid b < 0 \right\}. \end{aligned}$$

Thus $|\hat{W}_b^c| = 2|\hat{W}_{b-}^c|$.

Proof.
With the above definition of the sets $\hat{W}_{b+}^c$ and $\hat{W}_{b-}^c$ it is clear that they are disjoint sets and every element of $\hat{W}_b^c$ lies in one or the other. Thus $\hat{W}_b^c = \hat{W}_{b+}^c \cup \hat{W}_{b-}^c$. Lemma 5.2.14 then provides a bijection such that $\pi_5(\hat{W}_{b+}^c) \subseteq \hat{W}_{b-}^c$ and $\pi_5(\hat{W}_{b-}^c) \subseteq \hat{W}_{b+}^c$.
Consequently we have $|\hat{W}_b^c| = |\hat{W}_{b+}^c| + |\hat{W}_{b-}^c| = 2|\hat{W}_{b-}^c|$. □

Lemma 5.2.16.
The map

$$\begin{aligned}\pi_6 : O_b^c &\longrightarrow O_b^c \\ (a,b,c) &\longmapsto (a,-b,c) = (a',b',c')\end{aligned}$$

is a well-defined involution with no fixed points.

Proof.
Well-defined: Binary quadratic forms in the set O_b^c satisfy $a \equiv c \equiv 1 \bmod 2$, $b \neq 0$ as well as (by Lemma 5.2.8) $-\min\{a,c\} < b < \min\{a,c\}$. We observe $a'c' - b'^2 = ac - (-b)^2 = ac - b^2 = n$ and $b' = -b \neq 0$, $a' = a \equiv 1 \bmod 2$ and $c' = c \equiv 1 \bmod 2$. Since we have $-\min\{a,c\} < b < \min\{a,c\}$ we immediately get $-\min\{a',c'\} < b' < \min\{a',c'\}$. Hence $(a',b',c') \in O_b^c$ and the map π_6 is well-defined.
Injectivity: This is straightforward to verify.
Surjectivity: Let $(a,b,c) \in O_b^c$ and consider $(a,-b,c)$, by the same argument as used to prove π_6 is well-defined, we have $(a,-b,c) \in O_b^c$. Lastly, $\pi_6(a,-b,c) = (a,-(-b),c) = (a,b,c)$ and thus π_6 is surjective and hence is a bijection.
Now suppose $\pi_6(a,b,c) = (a,b,c)$, which implies $(a,b,c) = (a,-b,c)$ and thus $b = 0$. However, in O_b^c we have $b \neq 0$ and therefore we deduce the map π_6 has no fixed points. □

Corollary 5.2.17.
The set O_b^c may be written as the disjoint union of the sets O_{b+}^c and O_{b-}^c, where

$$\begin{aligned}\emptyset_{b+}^c &= \{(a,b,c) \in O_b^c \mid b > 0\} \\ \emptyset_{b-}^c &= \{(a,b,c) \in O_b^c \mid b < 0\}.\end{aligned}$$

Thus $|O_b^c| = 2|O_{b+}^c|$.

Proof.
With the above definition of the sets O_{b+}^c and O_{b-}^c it is clear that they are disjoint sets and every element of O_b^c lies in one or the other. Thus $O_b^c = O_{b+}^c \cup O_{b-}^c$. Lemma 5.2.16 then provides a bijection such that $\pi_6(O_{b+}^c) \subseteq O_{b-}^c$ and $\pi_6(O_{b-}^c) \subseteq O_{b+}^c$.
Consequently we have $|O_b^c| = |0_{b+}^c| + |O_{b-}^c| = 2|O_{b+}^c|$. □

Lemma 5.2.18.
The map

$$\begin{aligned}\pi_4 : \hat{W}_{b-}^c &\longrightarrow O_{b+}^c \\ (a,b,c) &\longmapsto (a,a+b,a+2b+c) = (a',b',c')\end{aligned}$$

is a well-defined bijection.

Proof.
Well-defined: We observe the map π_4 preserves the determinant because

$$a'c' - b'^2 = a(a+2b+c) - (a+b)^2$$

$$\begin{aligned}
&= a^2 + 2ab + ac - a^2 - 2ab - b^2 \\
&= ac - b^2 \\
&= n.
\end{aligned}$$

Since $a, b, c \in \mathbb{Z}$ we have $a', b', c' \in \mathbb{Z}$. Further, $a' > 0$ and $c' > 0$ because $\hat{W}^c_{b-} \subseteq \hat{W}^c_b$, which satisfies $-\min\{a, c\} < b < \min\{a, c\}$ (see Lemma 5.2.13). We also have $a \equiv 1 \bmod 2$ and $c \equiv 0 \bmod 2$ in $\hat{W}^c_{b-}$, thus $a + 2b + c \equiv a \equiv 1 \bmod 2$. Therefore $a' \equiv c' \equiv 1 \bmod 2$.
Now since $b < 0$ in $\hat{W}^c_{b-}$ and using $-\min\{a, c\} < b < \min\{a, c\}$ we see $-a < a+b < a$ (i.e. $-a' < b' < a'$)and $-c < b < c$. The latter inequality implies $b + c > 0$ and so we get $a + b < (a + b) + (b + c) = a + 2b + c$. Further, the minimality criterion implies $-2a - c < 3b$ and so we get $-a - 2b - c < a + b$. Combining these results yields $-(a + 2b + c) < a + b < a + 2b + c$ and so we deduce $-\min\{a', c'\} < b' < \min\{a', c'\}$. Hence the map π_4 is well-defined.
Injectivity: Suppose $\pi_4(a, b, c) = \pi_4(\hat{a}, \hat{b}, \hat{c})$ then we have $(a, a + b, a + 2b + c) = (\hat{a}, \hat{a} + \hat{b}, \hat{a} + 2\hat{b} + \hat{c})$ and it is clear this map is injective.
Surjectivity: Let $(a, b, c) \in O^c_{b+}$ be arbitrary and consider $(a, b - a, a - 2b + c) = (a', b', c')$. We have $a \equiv c \equiv 1 \bmod 2$, $b \equiv 0 \bmod 2$ (Lemma 5.2.7) and $b > 0$ in the set O^c_{b+}.
Therefore we get $a' = a \equiv 1 \bmod 2$ and $c' = a - 2b + c \equiv a + c \equiv 0 \bmod 2$. Further, $b < \min\{a, c\}$ implies $b' = b - a < 0$ and $b' \neq a' = a$. Next,

$$\begin{aligned}
a'c' - b'^2 &= a(a - 2b + c) - (b - a)^2 \\
&= a^2 - 2ab + ac - b^2 + 2ab - a^2 \\
&= ac - b^2 \\
&= n.
\end{aligned}$$

Lastly, we must show $-\min\{a', c'\} < b' \leqslant \min\{a', c'\}$. Since $b > 0$ and $a > 0$ it follows that $-a < b - a < b < a$ and thus $-a' < b' < a'$. Next, $b < \min\{a, c\}$ implies $3b < 2a + c$ and so $b - a < a - 2b + c$. It also implies $b < c$ and thus $b - a < c - a$. This then yields $2b - a < c - a + b$ and so $-a + 2b - c < b - a$ or rather $-(a - 2b + c) < b - a$.
Combining these results yields $-c' < b' < c'$ and so we have $-\min\{a', c'\} < b' < \min\{a', c'\}$. Hence $(a', b', c') \in \hat{W}^c_{b-}$. Lastly, observe $\pi_4(a', b', c') = (a, a + (b - a), a + 2(b - a) + (a - 2b + c)) = (a, b, c)$. Therefore the map π_4 is surjective and hence is a bijection.
An immediate consequence of this map is $|O^c_{b+}| = |\hat{W}^c_{b-}|$. □

We are now in a position to prove Theorem 5.2.2.

Proof of Theorem 5.2.2.
For convenience we shall let $|E| = K$. Then by Lemma 5.2.10 we have $|O| = K$. Next, by Lemma 5.2.12 we have $|\hat{W}_b| = |O_b|$ and by Lemmas 5.2.14, 5.2.16 and 5.2.18 we have $|\hat{W}^c_b| = 2|\hat{W}^c_{b-}| = 2|O^c_{b+}| = |O^c_b|$. Using this we get $|\hat{W}| = |\hat{W}_b| + |\hat{W}^c_b| = |O_b| + |O^c_b| = |O| = K$.

By Lemma 5.2.6 we have $|W| = |\hat{W}| + |\hat{W}^c| = 2K$.
Now by Definition 5.1.4 we have $6\mathrm{G}(n) = |O| + |E| + |W| = 4K$ and $6\mathrm{F}(n) = |O| + |W| = 3K$. From this we deduce $6\mathrm{G}(n) = \frac{4}{3} \cdot 6\mathrm{F}(n)$ and hence $3\mathrm{G}(n) = 4\mathrm{F}(n)$ as desired. □

Our goal now is to prove the second part of Kronecker's claim. Before we begin we prove two lemmas which will aid the proof.

Lemma 5.2.19.
Let $n \in \mathbb{Z}_{>0}$ be such that $n \equiv 7 \bmod 8$. Let (a, b, c) be such that $ac - b^2 = n$ and $a \equiv c \equiv 1 \bmod 2$ then either $a + c \equiv 4 \bmod 8$ and $b \equiv 2 \bmod 4$, or $a + c \equiv 0 \bmod 8$ and $b \equiv 0 \bmod 4$.

Proof.
Observe $a \equiv c \equiv 1 \bmod 2$ and $n \equiv 7 \bmod 8$ implies $b \equiv 0 \bmod 2$. Let $a = 8k + i$ and $c = 8m + j$ $(0 \leqslant i, j \leqslant 7,\ i \equiv j \equiv 1 \bmod 2)$ and observe $ac \equiv ij \bmod 8$. Consequently $i \neq j$ as otherwise we have $n \equiv i^2 - b^2 \bmod 8$. This contradicts $n \equiv 7 \bmod 8$.
Now if $b \equiv 2 \bmod 4$ then $n = ac - b^2 \equiv 7 \bmod 8$ implies $ac \equiv 3 \bmod 8$ and thus $(i, j) \in \{(1, 3), (3, 1), (5, 7), (7, 5)\}$. Whereas if $b \equiv 0 \bmod 4$ then $n = ac - b^2 \equiv 7 \bmod 8$ implies $ac \equiv 7 \bmod 8$ and thus $(i, j) \in \{(1, 7), (7, 1), (3, 5), (5, 3)\}$.
In the first case we have $a + c \equiv 4 \bmod 8$ and $b \equiv 2 \bmod 4$. While in the second case we have $a + c \equiv 0 \bmod 8$ and $b \equiv 0 \bmod 4$. □

Lemma 5.2.20.
Let $n = ac - b^2$ be a positive integer such that $n \equiv 7 \bmod 8$ and let $a \equiv c \equiv 0 \bmod 4$. Then $\frac{a \pm 2b + c}{2} \equiv 1 \bmod 2$.

Proof.
It is sufficient to show $a \pm 2b + c \equiv 2 \bmod 4$. We have $a \equiv c \equiv 0 \bmod 4$ and so $a \pm 2b + c \equiv \pm 2b \bmod 4$. Since $n \equiv 7 \bmod 8$, $b \equiv 1 \bmod 2$ follows and thus $\pm 2b \equiv 2 \bmod 4$. Hence $\frac{a \pm 2b + c}{2} \equiv 1 \bmod 2$. □

We may now state the theorem first before deducing a sequence of lemmas which provide the proof.

Theorem 5.2.21.
Let $n \in \mathbb{Z}_{>0}$ be such that $n \equiv 7 \bmod 8$. Then $3\mathrm{G}(n) = 6\mathrm{F}(n)$.

As in the proof of the 3 mod 8 case we shall begin with the set Ω_n, where $n \in \mathbb{Z}_{>0}$ satisfies $n \equiv 7 \bmod 8$. By Lemma 5.2.1 we know this set contains a unique representative for every complete equivalence class of binary quadratic forms $ax^2 + 2bxy + cy^2$ with determinant $n = ac - b^2$. That is, $|\Omega_n| = 6\mathrm{G}(n)$.

We partition Ω_n into three disjoint sets, O, E and W where

$$O = \{(a, b, c) \in \Omega_n \mid a \equiv c \equiv 1 \bmod 2\}$$
$$E = \{(a, b, c) \in \Omega_n \mid a \equiv c \equiv 0 \bmod 2\}$$

$$W = \{(a, b, c) \in \Omega_n \mid a \not\equiv c \bmod 2\}.$$

Recall $6\mathrm{G}(n) = |W| + |E| + |O|$ and $6\mathrm{F}(n) = |W| + |O|$.

The following illustration gives an excellent overview of our proof.

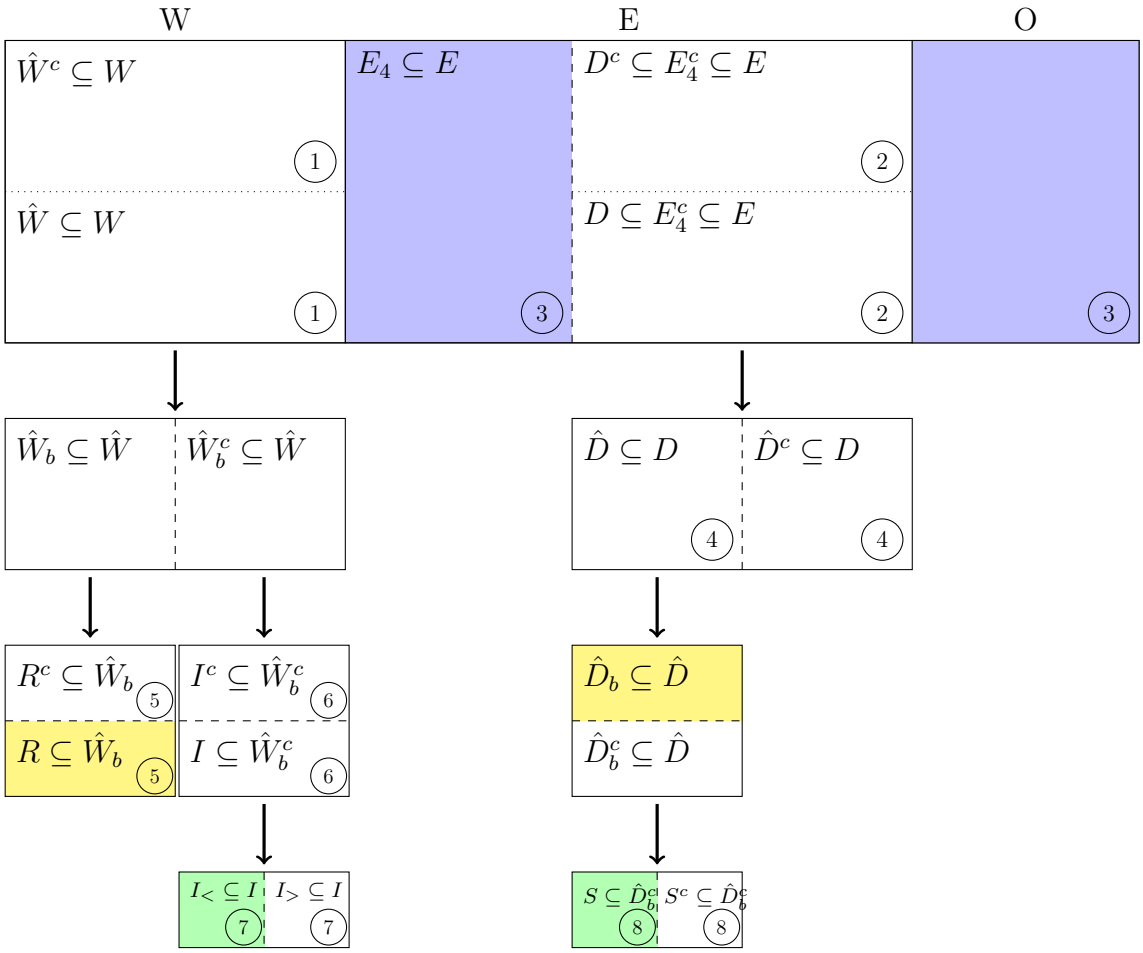


Figure 5.1: The diagram shows $|E| = |O| + |W|$ and thus $6\mathrm{G}(n) = 2\,(|O| + |W|) = 2 \cdot 6\mathrm{F}(n)$.

We begin by partitioning the set E into a disjoint union of the sets E_4 and E_4^c, where

$$E_4 = \{(a, b, c) \in E \mid a \equiv c \equiv 0 \bmod 4\}.$$

Lemma 5.2.22.
The map

$$\begin{aligned} \phi_1 : O &\longrightarrow E_4 \\ (a, b, c) &\longmapsto \left(\frac{a + 2b + c}{2}, \frac{c - a}{2}, \frac{a - 2b + c}{2}\right) \end{aligned}$$

is a well-defined bijection.

Proof.
Well-defined: From the set O we have $a \equiv c \equiv 1 \bmod 2$ and $b \equiv 0 \bmod 2$. By Lemma 5.2.19 we have $a' = \frac{a+2b+c}{2} \equiv 0 \bmod 4$ and $c' = \frac{a-2b+c}{2} \equiv 0 \bmod 4$ as $a + c \equiv \pm 2b \bmod 8$. By Lemma 5.2.8 we have $-\min\{a, c\} < b < \min\{a, c\}$ and this implies $a' > 0$ and $c' > 0$. We now verify the determinant

$$\begin{aligned} a'c' - b'^2 &= \frac{1}{4}\left(\frac{a+2b+c}{2}\right)\left(\frac{a-2b+c}{2}\right) - \frac{1}{4}(c-a)^2 \\ &= \frac{1}{4}\left[4ac - 4b^2\right] \\ &= ac - b^2 \\ &= n. \end{aligned}$$

Next, $c - a \equiv 0 \bmod 2$ and thus $b' \in \mathbb{Z}$. Lastly we have $-\min\{a, c\} < b < \min\{a, c\}$ implies

$$\begin{aligned} b < c \Rightarrow 2b < 2c \Rightarrow 2b - c < c \qquad &\Rightarrow -a + 2b - c < c - a \\ b < a \Rightarrow 2b < 2a \Rightarrow 2b - a < a \qquad &\Rightarrow -a + 2b - c < a - c, \end{aligned}$$

$$\begin{aligned} -c < b \Rightarrow -2c < 2b \Rightarrow a - c < a + 2b + c \\ -a < b \Rightarrow -2a < 2b \Rightarrow c - a < a + 2b + c. \end{aligned}$$

The first pair yield $-c' < b' < c'$, while the second pair yields $-a' < b' < a'$. Therefore we have $-\min\{a', c'\} < b' < \min\{a', c'\}$ and consequently the map ϕ_1 is well-defined.
Injectivity: Suppose $\phi_1((a, b, c)) = \phi_1((\hat{a}, \hat{b}, \hat{c}))$ then we have $\left(\frac{a+2b+c}{2}, \frac{c-a}{2}, \frac{a-2b+c}{2}\right) = \left(\frac{\hat{a}+2\hat{b}+\hat{c}}{2}, \frac{\hat{c}-\hat{a}}{2}, \frac{\hat{a}-2\hat{b}+\hat{c}}{2}\right)$. Equating entry-wise we get $a+2b+c = \hat{a}+2\hat{b}+\hat{c}$, $c-a = \hat{c}-\hat{a}$ and $a - 2b + c = \hat{a} - 2\hat{b} + \hat{c}$. Rearranging the second equation to get $\hat{a} = \hat{c} - c + a$ and substituting this into each of the first and third equations yields

$$\begin{aligned} c &= \hat{c} + (b - \hat{b}) \\ c &= \hat{c} + (\hat{b} - b). \end{aligned}$$

Taking the difference of these gives $0 = 2(b - \hat{b})$ and thus $b = \hat{b}$. Using this both the first and third equations become $a + c = \hat{a} + \hat{c}$. Combining with the second then yields $a = \hat{a}$ and $c = \hat{c}$. Hence the map ϕ_1 is injective.
Surjectivity: Let $(a, b, c) \in E_4$ be arbitrary and consider $\left(\frac{a-2b+c}{2}, \frac{c-a}{2}, \frac{a+2b+c}{2}\right) = (a', b', c')$. We first show this lies in the set O. By Lemma 5.2.20 we have $a' \equiv c' \equiv 1 \bmod 2$. Next, $\frac{c-a}{2} \in \mathbb{Z}$ as $c - a \equiv 0 \bmod 4$ by Lemma 5.2.9. We note the preservation of the determinant and proof of the condition $-\min\{a', c'\} < b' \leqslant \min\{a', c'\}$ proceed in an identical manner to that found in the well-defined part of this proof. Thus $\left(\frac{a+2b+c}{2}, \frac{c-a}{2}, \frac{a-2b+c}{2}\right) \in O$.
We now see $\phi_1\left(\left(\frac{a-2b+c}{2}, \frac{c-a}{2}, \frac{a+2b+c}{2}\right)\right)$ has $\frac{\left(\frac{a-2b+c}{2}\right)-2\left(\frac{c-a}{2}\right)+\left(\frac{a+2b+c}{2}\right)}{2} = a$ for its first entry, $\frac{\left(\frac{a+2b+c}{2}\right)-\left(\frac{a-2b+c}{2}\right)}{2} = b$ for its second entry, and $\frac{\left(\frac{a-2b+c}{2}\right)+2\left(\frac{c-a}{2}\right)+\left(\frac{a+2b+c}{2}\right)}{2} = c$ for its

last entry. Thus $\phi_1\left(\left(\frac{a-2b+c}{2}, \frac{c-a}{2}, \frac{a+2b+c}{2}\right)\right) = (a,b,c)$ We note the condition can be verified directly in the same manner as in the well-defined part of this proof. Hence the map ϕ_1 is surjective and thus is a bijection.
An immediate consequence of this is $|E_4| = |O|$. □

We now consider the set E_4^c and progressively partition it using the following lemmas.

Lemma 5.2.23.
The map

$$\begin{aligned}\phi_2 : E_4^c &\longrightarrow E_4^c \\ (a,b,c) &\longmapsto (c,b,a)\end{aligned}$$

is a well-defined involution with no fixed points.

Proof.
Well-defined: The set E_4^c contains forms (a,b,c) such that $a \equiv c \equiv 0 \bmod 2$ and where we do not have $a \equiv c \equiv 0 \bmod 4$. Since $ac - b^2 = n \equiv 7 \bmod 8$ then implies $b \equiv 1 \bmod 2$, it follows that exactly one of a, c is 0 mod 4, while the other is 2 mod 4. Consequently permuting the a and c entries does not affect this property. Next we note E_4^c is non-empty since $n \equiv 7 \bmod 8$ implies $4 \mid (n+1)$ and therefore $(4, 1, \frac{n+1}{4}) \in E_4^c$.
Lastly, it is clear the determinant and $-\min\{a,c\} < b < \min\{a,c\}$ properties are preserved (strict inequalities by Lemma 5.2.8), thus ϕ_2 is a well-defined map into the set E_4^c.
We now observe $\phi_2^2(a,b,c) = (a,b,c)$ and so by Lemma 3.4.13 the map ϕ_2 is a bijection. Finally, the map ϕ_2 has no fixed points because this would imply $b = 0$, which is impossible when $n \equiv 7 \bmod 8$. □

Corollary 5.2.24.
The set E_4^c may be written as the disjoint union of the sets D and D^c where

$$D = \{(a,b,c) \in E_4^c \mid a \equiv 0 \bmod 4, c \equiv 2 \bmod 4\}$$

and $|D| = |D^c|$.

Proof.
By the proof of Lemma 5.2.23 we know all forms $(a,b,c) \in E_4^c$ satisfy either $a \equiv 0 \bmod 4$ and $c \equiv 2 \bmod 4$ or $a \equiv 2 \bmod 4$ and $c \equiv 0 \bmod 4$, and no form can simultaneously satisfy both conditions. By Lemma 5.2.23, ϕ_2 is a bijection which, permutes the outer coefficients. Thus $\phi_2(D) \subseteq D^c$ and $\phi_2(D^c) \subseteq D$. Hence $E_4^c = D \cup D^c$ and $|D| = |D^c|$. □

Lemma 5.2.25.
The set D may be written as a disjoint union of the sets $\hat{D}$ and $\hat{D}^c$, where

$$\hat{D} = \{(a,b,c) \in D \mid b > 0\}$$

and $|\hat{D}| = |\hat{D}^c|$.

Proof. Observe $b \neq 0$ in the set D because $a \equiv 0 \bmod 4$ and $c \equiv 2 \bmod 4$. Since $D \subseteq E$, Lemma 5.2.8 implies $|b| < \min\{a, c\}$. Therefore for any form $(a, b, c) \in D$ the form $(a, -b, c)$ is distinct and also in D. Thus $D = \hat{D} \cup \hat{D}^c$ and $|\hat{D}| = |\hat{D}^c|$. □

Lemma 5.2.26.
The set $\hat{D}$ may be expressed as a disjoint union of the sets $\hat{D}_b$ and $\hat{D}_b^c$ where

$$\hat{D}_b = \{(a, b, c) \in \hat{D} \mid c = 2b\}.$$

Proof.
Forms in the set $\hat{D}$ satisfy $b > 0$ and $a \equiv c \equiv 0 \bmod 2$. Further, since $\hat{D} \subseteq D \subseteq E_4^c$, we know $a \equiv 0 \bmod 4$, $c \equiv 2 \bmod 4$ and $b \equiv 1 \bmod 2$. This implies we have either $c = 2b$ or $c \neq 2b$, but more importantly, we know $a \neq 2b$. □

Lemma 5.2.27.
The map

$$\begin{aligned} \phi_3 : \hat{D}_b^c &\longrightarrow \hat{D}_b^c \\ (a, b, c) &\longmapsto (a - 2b + c, c - b, c) = (a', b', c') \end{aligned}$$

is a well-defined involution with no fixed points.

Proof.
Well-defined: Recall forms in the set $\hat{D}_b^c$ satisfy $c \neq 2b$, $c \neq 2b$ $b > 0$, $a \equiv 0 \bmod 4$, $c \equiv 2 \bmod 4$ and $-\min\{a, c\} < b < \min\{a, c\}$ as $\hat{D}_b^c \subseteq E$. Therefore we see $b' = c - b > 0$, $a' = a - 2b + c = (\underbrace{a - b}_{>0}) + (\underbrace{c - b}_{>0}) > 0$ and $c' = c > 0$. Next, we note

$$\begin{aligned} a'c' - {b'}^2 &= (a - 2b + c)c - (c - b)^2 \\ &= ac - 2bc + c^2 - c^2 - 2bc - b^2 \\ &= ac - b^2 \\ &= n, \end{aligned}$$

thus the map ϕ_3 preserves the determinant.
Now we note $c \neq 2b$ implies $2c \neq 2b + c$ and thus $2b' = 2(c - b) \neq c = c'$. Further, we have $a' = a - 2b + c \equiv 0 \bmod 4$ because $a \equiv 0 \bmod 4$, $2b \equiv 2 \bmod 4$ and $c \equiv 2 \bmod 4$. Lastly it is clear that $c' = c \equiv 2 \bmod 4$ and thus it remains to show our minimality condition.
We have $b' = c - b > 0$ and so we trivially have $-\min\{a', c'\} < b'$. Also, since $b > 0$ we get $b' = c - b < c = c'$. Lastly, $a' = a - 2b + c = (\underbrace{a - b}_{>0}) + (c - b) > c - b = b'$ and therefore we have $-\min\{a', c'\} < b' < \min\{a', c'\}$.
Finally, we observe $\phi_3^2(a, b, c) = (a - 2b + c - 2[c - b] + c, c - [c - b], c) = (a, b, c)$ and hence by Lemma 3.4.13 we see the map ϕ_3 is an involution on the set $\hat{D}_b^c$.
We now observe the map ϕ_3 has no fixed points as this would imply $c - b = b$ and thus $c = 2b$. This is a contradiction as $\hat{D}_b^c \cap \hat{D}_b = \emptyset$. □

Corollary 5.2.28.
The set $\hat{D}_b^c$ may be partitioned into a disjoint union of the sets S and S^c, where

$$S = \{(a,b,c) \in \hat{D}_b^c \mid 2b < c\}$$
$$S^c = \{(a,b,c) \in \hat{D}_b^c \mid 2b > c\}.$$

Further, we have $|S| = |S^c|$.

Proof.
From the proof of Lemma 5.2.27 we recall forms in $\hat{D}_b^c$ satisfy $2b \neq c$. Therefore we may partition the set $\hat{D}_b^c$ according to whether $2b < c$ or $2b > c$, and we have $\hat{D}_b^c = S \cup S^c$ is a disjoint union. Let $(a,b,c) \in S$ and apply the map ϕ_3 from Lemma 5.2.27. We get $\phi_3(a,b,c) = (a-2b+c, c-b, c)$ satisfies $2b' = 2c - 2b = c + (\underbrace{c-2b}_{>0}) > c = c'$ and thus $\phi_3(S) \subseteq S^c$. Similarly, let $(a,b,c) \in S^c$ then $\phi_3(a,b,c)$ satisfies $2b' = 2(c-b) = c + (\underbrace{c-2b}_{<0}) < c = c'$ and so $\phi_3(S^c) \subseteq S$.
Hence we have $|S| = |S^c|$. □

We now turn our attention to partitioning the set W.

Lemma 5.2.29.
The map

$$\phi_4 : W \longrightarrow W$$
$$(a,b,c) \longmapsto (c,b,a)$$

is a well-defined involution with no fixed points.

Proof.
Well-defined: Forms in the set W satisfy either $a \equiv 1 \bmod 2$ and $c \equiv 0 \bmod 8$ or vice versa. This is because $n = ac - b^2 \equiv 7 \bmod 8$, $a \equiv 1 \bmod 2$ and $c \equiv 0 \bmod 2$ combined with $b^2 \equiv 0, 1, 4 \bmod 8$ implies the even outer coefficient must be divisible by 8 and $b \equiv 1 \bmod 2$. Observe permuting the outer coefficients does not change this property. Next, note the set W is non-empty because $(1,1,n+1) \in W$. Lastly, it is clear the determinant and $-\min\{a,c\} < b \leqslant \min\{a,c\}$ properties are preserved. Thus ϕ_4 is a well-defined map into W.
Note that $\phi_4^2(a,b,c) = (a,b,c)$ and so Lemma 3.4.13 implies the map ϕ_4 is a bijection. Finally, ϕ_4 has no fixed points as this would imply $a \equiv c \bmod 2$, a contradiction to the construction of the set W. □

Corollary 5.2.30.
The set W may be partitioned into a disjoint union of the sets $\hat{W}$ and $\hat{W}^c$, where

$$\hat{W} = \{(a,b,c) \in W \mid a \equiv 1 \bmod 2, c \equiv 0 \bmod 8\}.$$

Further, $|\hat{W}| = |\hat{W}^c|$.

Proof.
From the proof of Lemma 5.2.29 we know either $a \equiv 1 \bmod 2$ and $c \equiv 0 \bmod 8$ or vice versa. Partitioning according to the disjoint sets $\hat{W}$ and $\hat{W}^c$ we see the map ϕ_4 satisfies $\phi_4(\hat{W}) \subseteq \hat{W}^c$ and $\phi_4(\hat{W}^c) \subseteq \hat{W}$. Thus $W = \hat{W} \cup \hat{W}^c$ and $|\hat{W}| = |\hat{W}^c|$. □

Lemma 5.2.31.
The set $\hat{W}$ may be expressed as a disjoint union of the sets $\hat{W}_b$ and $\hat{W}_b^c$ where

$$\hat{W}_b = \{(a, b, c) \in \hat{W} \mid a = b\},$$
$$\hat{W}_b^c = \{(a, b, c) \in \hat{W} \mid a \neq b\}.$$

Proof.
Since forms in the set $\hat{W}$ satisfy $a \equiv b \equiv 1 \bmod 2$ and $c \equiv 0 \bmod 8$ it follows that $a = b$ can occur. Clearly the sets $\hat{W}_b$ and $\hat{W}_b^c$ are disjoint and form a partition of $\hat{W}$. □

Lemma 5.2.32.
The map

$$\phi_5 : \hat{W}_b \longrightarrow \hat{W}_b$$
$$(a, a, c) \longmapsto (c - a, c - a, c)$$

is a well-defined involution with no fixed points.

Proof.
We note the set $\hat{W}_b$ is non-empty because it contains the form $(1, 1, n+1)$ as $n+1 \equiv 0 \bmod 8$.
Well-defined: Since $c \equiv 0 \bmod 8$ and $a \equiv 1 \bmod 2$, it follows that $a' = b' \equiv 1 \bmod 2$. Next, we have

$$\begin{aligned} a'c' - b'^2 &= (c - a)c - (c - a)^2 \\ &= c^2 - ac - c^2 + 2ac - a^2 \\ &= ac - b^2 \text{ as } a = b. \end{aligned}$$

We also note $c' = c \equiv 0 \bmod 8$ and $n = ac - b^2 = a(c - a)$, thus $c > a$ else $n < 0$. It remains to show our minimality condition. Observe $0 < a' = b'$ and so it is sufficient to show $a' < c'$, that is $c - a < c$, but this follows immediately as otherwise $n < 0$. Hence the map ϕ_5 maps into the set $\hat{W}_b$.
We now observe $\phi_5^2(a, b, c) = \phi_5(c - a, c - a, c) = (c - (c - a), c - (c - a), c) = (a, a, c)$. Thus by Lemma 3.4.13 the map ϕ_5 is an involution on the set $\hat{W}_b$. Further, there are no fixed points because this would imply $c - a = a$, thus $c = 2a$. This is a contradiction because $c \equiv 0 \bmod 8$ and $2a \equiv 2 \bmod 4$. □

Corollary 5.2.33.
The set $\hat{W}_b$ may be expressed as the disjoint union of the sets R and R^c where

$$R = \{(a, b, c) \in \hat{W}_b \mid 2b < c\}$$
$$R^c = \{(a, b, c) \in \hat{W}_b \mid c < 2b\}.$$

Further, we have $|R| = |R^c|$.

Proof.
Observe in the set $\hat{W}_b$ we cannot have $c = 2b$ as $a = b \equiv 1 \bmod 2$ and $c \equiv 0 \bmod 8$. Therefore we get $\hat{W}_b = R \cup R^c$. Further, applying Lemma 5.2.32 we see $\phi_5(R) \subseteq R^c$ because if $2a = 2b < c$ then $2b' = 2(c-a) = c + (c-2a) > c = c'$. Similarly, $\phi_4(R^c) \subseteq R$ because if $c < 2b = 2a$ then $2b' = 2(c-a) = c + (c-2a) < c$. Thus we have $|R| = |R^c|$. □

We now develop our second key map for the proof of the 7 mod 8 case.

Lemma 5.2.34.
The map

$$\begin{aligned} \phi_6 : R &\longrightarrow \hat{D}_b \\ (a,b,c) &\longmapsto (\frac{c}{2}, b, 2a) = (a', b', c') \end{aligned}$$

is a well-defined bijection.

Proof.
Well-defined: Recall forms $(a,b,c) \in R$ satisfy $a = b \equiv 1 \bmod 2$, $c \equiv 0 \bmod 8$ and $2b < c$. From this it follows that $a' = \frac{c}{2} \equiv 0 \bmod 4$, $b' = b = a > 0$, and $c' = 2a \equiv 2 \bmod 4$. It is also clear that $a', b', c' > 0$ and that the determinant is preserved under ϕ_6. We also see $c' = 2a = 2 \cdot b = 2b'$. It remains to show we satisfy our minimality condition. Since we have $-\min\{a,c\} < b \leqslant \min\{a,c\}$ we see immediately that $-c' < b' < c'$. We also have $2a = 2b < c$ implies $a < \frac{c}{2}$ and thus $-a < b \leqslant a$ then implies $-a' < b' < a'$. Hence we satisfy $-\min\{a',c'\} < b' \leqslant \min\{a',c'\}$.
Injectivity: This is straightforward to verify directly.
Surjectivity: Let $(a,b,c) \in \hat{D}_b$ be arbitrary and consider the form $(\frac{c}{2}, b, 2a) = (a', b', c')$. We will show this lies in the set R. We recall forms in $\hat{D}_b$ satisfy $c = 2b$, $b > 0$, $b \equiv 1 \bmod 2$, $a \equiv 0 \bmod 4$ and $c \equiv 2 \bmod 4$. We immediate verify $a'c' - {b'}^2 = ac - b^2 = n$. Next, it is clear that a', b' and $c' > 0$. Further, $a' = \frac{c}{2} = \frac{2b}{2} = b$ and thus $a' = b' \equiv 1 \bmod 2$. Since $a \equiv 0 \bmod 4$, it follows that $c' = 2a \equiv 0 \bmod 8$. It remains to show $2b' < c'$ and $-\min\{a',c'\} < b' \leqslant \min\{a',c'\}$. The first of these follows immediately due to $-a < b < a$ ($\hat{D}_b \subseteq E$) as this yields $2b' = 2b < 2a = c'$. It also implies it is sufficient to show $-a' < b' \leqslant a'$. However, we observe $a' = \frac{c}{2} = b = b'$ and thus this is immediately satisfied. Thus $(a', b', c') \in R$. It is then straightforward to check that $\phi_6(\frac{c}{2}, b, 2a) = (a,b,c)$ and therefore the map ϕ_6 is surjective and hence is a bijection. □

Lemma 5.2.35.
The map

$$\begin{aligned} \phi_7 : \hat{W}_b^c &\longrightarrow \hat{W}_b^c \\ (a,b,c) &\longmapsto (a, -b, c) = (a', b', c') \end{aligned}$$

is a well-defined involution with no fixed points. As a consequence the set $\hat{W}_b^c$ may be expressed as a disjoint union of the sets I and I^c where,

$$I = \{(a,b,c) \in \hat{W}_b^c \mid b > 0\},$$

$$I^c = \{(a,b,c) \in \hat{W}_b^c \mid b < 0\}.$$

Further, $|I| = |I^c|$.

Proof.
Well-defined: It is sufficient to show $a' \neq b'$ as only the sign of b has changed and clearly the determinant is preserved. Since forms in $\hat{W}_b^c$ satisfy $-\min\{a,c\} < b \leqslant \min\{a,c\}$ and $a \neq b$, we deduce $-a < b < a$ and thus $-a < -b < a$. Hence $a' \neq b'$. Therefore the map ϕ_7 maps into the set W_b^c. Further, this map has no fixed points because forms in the set $\hat{W}_b^c$ satisfy $a \equiv b \equiv 1 \bmod 2$ and $c \equiv 0 \bmod 8$. Thus $b \neq 0$ and there are no fixed points.
Lastly, we observe $\phi_7^2(a,b,c) = (a,b,c)$ and thus by Lemma 3.4.13 we see see the map ϕ_7 is an involution with no fixed points.
As a consequence we may partition $\hat{W}_b^c$ into $I \cup I^c$ and we observe $\phi_7(I) \subseteq I^c$ as well as $\phi_7(I^c) \subseteq I$ because the map ϕ_7 changes the sign on the b term. Since ϕ_7 has no fixed points, we deduce $|I| = |I^c|$. □

Lemma 5.2.36.
The map

$$\begin{aligned} \phi_8 : I &\longrightarrow I \\ (a,b,c) &\longmapsto (a-2b+c, c-b, c) = (a',b',c') \end{aligned}$$

is a well-defined involution with no fixed points.

Proof.
Well-defined: Recall forms in the set I satisfy $b > 0$, $a \neq b$, $a \equiv 1 \bmod 2$ and $c \equiv 0 \bmod 8$. These forms also satisfy $-\min\{a,c\} < b \leqslant \min\{a,c\}$. If $c = b$ then $n = ac - b^2 = c(a-c) \equiv 0 \bmod 8$ which is a contradiction. Hence we deduce $b' = c - b > 0$ and thus $a' = a - 2b + c > 0$. Clearly, we have $c' = c > 0$. Next, observe

$$\begin{aligned} a'c' - b'^2 &= (a-2b+c)c - (c-b)^2 \\ &= ac - 2bc + c^2 - c^2 + 2bc - b^2 \\ &= ac - b^2 \\ &= n \end{aligned}$$

thus the determinant is preserved under the map ϕ_8.
We also note $a' = a - 2b + c = \underbrace{(a-b)}_{>0} + (c-b) \neq c - b = b'$ because $I \subseteq \hat{W}_b^c$ whose forms satisfy $a \neq b$. Further, $a' = a - 2b + c \equiv 1 \bmod 2$ since $a \equiv 1 \bmod 2$, $2b \equiv 0 \bmod 2$ and $c \equiv 0 \bmod 8$. We trivially have $c' = c \equiv 0 \bmod 8$. Thus it now remains to show our minimality condition.
We have $b' = c - b > 0$ and thus $-\min\{a',c'\} < b'$ is straightforward. Also, since $b > 0$, we have $b' < c'$. Lastly, $a \neq b$ and $-\min\{a,c\} < b \leqslant \min\{a,c\}$ imply $a' = a - 2b + c = \underbrace{(a-b)}_{>0} + (c-b) > c - b = b'$. Hence we have $-\min\{a',c'\} < b' <$

$\min\{a', c'\}$. Therefore ϕ_8 maps into the set I.
We now observe $\phi_8^2(a, b, c) = (a - 2b + c - 2[c - b] + c, c - [c - b], c) = (a, b, c)$ and so by Lemma 3.4.13 we see the map ϕ_8 gives an involution on the set I.
Finally, we note the map ϕ_8 has no fixed points because this would imply $b = c - b$, that is $2b = c$. This is a contradiction because $a \equiv 1 \bmod 2$ and $c \equiv 0 \bmod 8$ along with $n \equiv 7 \bmod 8$ imply $b \equiv 1 \bmod 2$ and hence $2b \equiv 2 \bmod 4 \not\equiv c \equiv 0 \bmod 8$. □

Corollary 5.2.37.
The set I may be partitioned into a disjoint union of the sets $I_<$ and $I_>$, where

$$I_< = \{(a, b, c) \in I \mid 2b < c\},$$
$$I_> = \{(a, b, c) \in I \mid 2b > c\}$$

and they satisfy $|I_<| = |I_>|$.

Proof.
From the proof of Lemma 5.2.36 we know forms in the set I do not satisfy $2b = c$. Therefore we may partition the set I according to whether $2b < c$ or $2b > c$ and then $I = I_< \cup I_>$ is a disjoint union. Now let $(a, b, c) \in I_<$ and apply the map ϕ_8 from Lemma 5.2.36. We get $\phi_8(a, b, c) = (a - 2b + c, c - b, c)$, which satisfies $2b' = 2c - 2b = c + (\underbrace{c - 2b}_{>0}) > c = c'$. Thus $\phi_8(I_<) \subseteq I_>$. Similarly, let $(a, b, c) \in I_>$ then we have $\phi_8(a, b, c)$ satisfies $2b' = 2c - 2b = c + (\underbrace{c - b}_{<0}) < c = c'$ and thus $\phi_8(I_>) \subseteq I_<$.
Hence we have $|I_<| = |I_>|$. □

The following lemma provides the final map needed to prove the 7 mod 8 result.

Lemma 5.2.38.
The map

$$\phi_9 : I_< \longrightarrow S$$
$$(a, b, c) \longmapsto \left(\frac{c}{2}, b, 2a\right) = (a', b', c')$$

is a well-defined bijection and consequently $|I_<| = |S|$.

Proof.
Well-defined: It is straightforward to verify the map ϕ_9 preserves the determinant and satisfies a', b' and $c' > 0$. Next, we have $c' = 2a \neq 2b = 2b'$ because $I_< \subseteq I \subseteq \hat{W}_b^c$, where $a \neq b$. Further, $I_< \subseteq \hat{W}$ implies $a' = \frac{c}{2} \equiv 0 \bmod 4$ and $c' = 2a \equiv 2 \bmod 4$ because $a \equiv 1 \bmod 2$ and $c \equiv 0 \bmod 8$. We also have $2b' = 2b < 2a = c'$ because forms in $I_<$ satisfy $-\min\{a, c\} < b \leqslant \min\{a, c\}$ and $a \neq b$. It remains to show our minimality criterion holds. Since forms in $I_<$ satisfy $b > 0$ and also $-a < b < a$ it follows that $-\min\{a', c'\} < b'$. We also immediately get $b < a < 2a = c'$. Further, since forms in $I_<$ satisfy $2b < c$ it follows that $b' = b < \frac{c}{2} = a'$ and thus we have $-\min\{a', c'\} < b' < \min\{a', c'\}$. Hence $(a', b', c') \in S$.

Injectivity: This is straightforward to verify.
Surjectivity: Let $(a,b,c) \in S$ be arbitrary and consider $(a',b',c') = (\frac{c}{2}, b, 2a)$, we will show this lies in $I_<$. It is clear determinant is preserved and that a', b' and $c' > 0$ as $S \subseteq \hat{D}$. Next, forms in S satisfy $a \equiv 0 \bmod 4$ and $c \equiv 2 \bmod 4$ and so we have $a' = \frac{c}{2} \equiv 1 \bmod 2$ and $c' = 2a \equiv 0 \bmod 8$. Further observe $a' = \frac{c}{2} \neq \frac{2b}{2} = b = b'$ as forms in S satisfy $c \neq 2b$. We also have $2b' = 2b < 2a = c'$ as $S \subseteq E$ implies the minimality criterion has strict inequalities (Lemma 5.2.8). It remains to show (a',b',c') satisfies the minimality criterion.
We have $b' = b > 0$ and so we automatically get $-\min\{a',c'\} < b'$. Next, forms in S satisfy $2b < c$ and thus $b' = b < \frac{c}{2} = a'$. Further, forms in S satisfy $b < a$ (as $S \subseteq E$) and thus we have $b' = b < a < 2a = c'$. Hence we have $-\min\{a',c'\} < b' < \min\{a',c'\}$ and therefore $(a',b',c') \in I_<$.
Since $\phi_9(a',b',c') = (a,b,c)$, we see the map ϕ_9 is surjective and therefore is a bijection. An immediate consequence is then $|I_<| = |S|$. □

We now prove Theorem 5.2.21.

Proof of Theorem 5.2.21.
Let n be a positive integer such that $n \equiv 7 \bmod 8$. Recall from Definition 5.1.4 that $6\mathrm{G}(n) = |O| + |E| + |W|$ and $6\mathrm{F}(n) = |O| + |W|$. Since our theorem is $3\mathrm{G}(n) = 6\mathrm{F}(n)$ it is sufficient to show $|E| = |O| + |W|$.
We have

$$\begin{aligned}
|E| &= |E_4| + |E_4^c| \\
&= |O| + |E_4^c| \text{ by Lemma 5.2.22} \\
&= |O| + 2|D| \text{ by Corollary 5.2.24} \\
&= |O| + 4|\hat{D}| \text{ by Lemma 5.2.25} \\
&= |O| + 4|\hat{D}_b| + 4|\hat{D}_b^c| \text{ by Lemma 5.2.26} \\
&= |O| + 4|\hat{D}_b| + 8|S| \text{ by Corollary 5.2.28} \\
&= |O| + 4|\hat{D}_b| + 8|I_<| \text{ by Lemma 5.2.38} \\
&= |O| + 4|\hat{D}_b| + 4|I| \text{ by Corollary 5.2.37} \\
&= |O| + 4|\hat{D}_b| + 2|\hat{W}_b^c| \text{ by Lemma 5.2.35} \\
&= |O| + 4|R| + 2|\hat{W}_b^c| \text{ by Lemma 5.2.34} \\
&= |O| + 2|\hat{W}_b| + 2|\hat{W}_b^c| \text{ by Corollary 5.2.33} \\
&= |O| + 2|\hat{W}| \text{ by Lemma 5.2.31} \\
&= |O| + |W| \text{ by Corollary 5.2.29.}
\end{aligned}$$

Hence we have $6\mathrm{G}(n) = |O| + |E| + |W| = |O| + |O| + |W| + |W| = 2(|O| + |W|) = 2 \cdot 6\mathrm{F}(n)$ and consequently upon division by 2 we get Kronecker's result, $3\mathrm{G}(n) = 6\mathrm{F}(n)$. □

Corollary 5.2.39.
Let n be a positive integer such that $n \equiv 3 \bmod 4$, then $3\mathrm{G}(n) = \left(5 - (-1)^{\frac{n-3}{4}}\right)\mathrm{F}(n)$.

Proof.
Let n be a positive integer such that $n \equiv 3 \bmod 4$. From Theorems 5.2.2 and 5.2.21 we have $3\mathrm{G}(n) = 4\mathrm{F}(n)$ when $n \equiv 3 \bmod 8$ and $3\mathrm{G}(n) = 6\mathrm{F}(n)$ when $n \equiv 7 \bmod 8$. Observe when $n = 8k+3$ we have $5-(-1)^{\frac{n-3}{4}} = 5-(-1)^{\frac{8k}{4}} = 5-(-1)^2 k = 5-1 = 4$, and when $n = 8k+7$ we have $5-(-1)^{\frac{n-3}{4}} = 5-(-1)^{\frac{8k+4}{4}} = 5-(-1)^{2k+1} = 5+1 = 6$. Hence we have

$$\begin{aligned} 3\mathrm{G}(n) &= \begin{cases} 4\mathrm{F}(n) & n \equiv 3 \bmod 8 \\ 6\mathrm{F}(n) & n \equiv 7 \bmod 8 \end{cases} \\ &= \begin{cases} 5-(-1)^{\frac{n-3}{4}} & n \equiv 3 \bmod 8 \\ 5-(-1)^{\frac{n-3}{4}} & n \equiv 7 \bmod 8 \end{cases} \\ &= \left(5-(-1)^{\frac{n-3}{4}}\right)\mathrm{F}(n). \end{aligned}$$

□

5.3 Representations of an Integer as a Sum of Three Squares

In this section we derive Kronecker's expression for the number of representations of a positive integer as a sum of three squares.

Let $n \in \mathbb{Z}_{\geqslant 0}$, from Lemma 5.1.17 we have

$$\sum_{-2\sqrt{n} \leqslant h \leqslant 2\sqrt{n}} \left(\mathrm{G}\left(4n-h^2\right) - \mathrm{F}\left(4n-h^2\right)\right) = \sigma(n) + \Psi(n).$$

Also, using $D = 4n$ in Equation 5.8 we have

$$\sum_{-2\sqrt{n} \leqslant h \leqslant 2\sqrt{n}} \mathrm{F}\left(4n-h^2\right) = 2\sigma_{\mathrm{odd}}(n) + \sigma(n) + \Psi(n).$$

It is important to note we have used $\mathrm{F}(0) = 0$ to extend this summation to include equality without changing the equation.

Subtracting the first equation above from the latter then yields

$$\sum_{-2\sqrt{n} \leqslant h \leqslant 2\sqrt{n}} \left(2\mathrm{F}\left(4n-h^2\right) - \mathrm{G}\left(4n-h^2\right)\right) = 2\sigma_{\mathrm{odd}}(n). \tag{5.18}$$

Definition 5.3.1.
For $n \in \mathbb{Z}_{\geqslant 0}$ define $\mathrm{E}(n) = 2\mathrm{F}(n) - \mathrm{G}(n)$.

Using our newly defined function, Equation 5.18 may be rewritten as:

$$\sum_{-2\sqrt{n} \leqslant h \leqslant 2\sqrt{n}} \mathrm{E}\left(4n-h^2\right) = 2\sigma_{\mathrm{odd}}(n). \tag{5.19}$$

We now prove some properties of $\mathrm{E}(n)$. It is useful to recall for all $n \in \mathbb{Z}_{\geqslant 0}$ the following hold true.

$$\begin{aligned}
\mathrm{F}(4n) &= 2\mathrm{F}(n), \text{ see Theorem 5.1.20,}\\
\mathrm{G}(4n) &= \mathrm{F}(4n) + \mathrm{G}(n), \text{ see Lemma 5.1.7,}\\
\mathrm{G}(n) &= \mathrm{F}(n) \text{ when } n \equiv 1, 2 \bmod 4, \text{ see Lemma 5.1.8,}\\
3\mathrm{G}(n) &= \left(5 - (-1)^{\frac{n-3}{4}}\right)\mathrm{F}(n) \text{ when } n \equiv 3 \bmod 4, \text{ see Corollary 5.2.39.}
\end{aligned}$$

Lemma 5.3.2.
For all $n \in \mathbb{Z}_{\geqslant 0}$ we have $\mathrm{E}(4n) = \mathrm{E}(n)$.

Proof.
First note $\mathrm{E}(4 \cdot 0) = \mathrm{E}(0) = 2\mathrm{F}(0) - \mathrm{G}(0) = -\left(-\frac{1}{6}\right) = \frac{1}{6}$.
Now let $n \in \mathbb{Z}_{>0}$, then we have

$$\begin{aligned}
\mathrm{E}(4n) &= 2\mathrm{F}(4n) - \mathrm{G}(4n)\\
&= 2\mathrm{F}(4n) - (\mathrm{F}(4n) + \mathrm{G}(n)) \text{ by Lemma 5.1.7}\\
&= \mathrm{F}(4n) - \mathrm{G}(n)\\
&= 2\mathrm{F}(n) - \mathrm{G}(n) \text{ by Theorem 5.1.20}\\
&= \mathrm{E}(n).
\end{aligned}$$

□

Lemma 5.3.3.
Let $n \in \mathbb{Z}_{>0}$ satisfy $n \equiv 1$ or $2 \bmod 4$, then we have $\mathrm{E}(n) = \mathrm{F}(n)$.

Proof.
Let $n \equiv 1$ or $2 \bmod 4$ then we have

$$\begin{aligned}
\mathrm{E}(n) &= 2\mathrm{F}(n) - \mathrm{G}(n)\\
&= 2\mathrm{F}(n) - \mathrm{F}(n) \text{ by Lemma 5.1.8}\\
&= \mathrm{F}(n).
\end{aligned}$$

□

Lemma 5.3.4.
Let $n \in \mathbb{Z}_{>0}$ satisfy $n \equiv 3 \bmod 8$ then we have $\mathrm{E}(n) = \frac{2}{3}\mathrm{F}(n)$.

Proof.
Let $n \in \mathbb{Z}_{>0}$ satisfy $n \equiv 3 \bmod 8$ then we have

$$\begin{aligned}
\mathrm{E}(n) &= 2\mathrm{F}(n) - \mathrm{G}(n) \text{ and so}\\
3\mathrm{E}(n) &= 6\mathrm{F}(n) - 3\mathrm{G}(n)\\
&= 6\mathrm{F}(n) - 4\mathrm{F}(n) \text{ by Theorem 5.2.2}\\
&= 2\mathrm{F}(n).
\end{aligned}$$

Hence $\mathrm{E}(n) = \frac{2}{3}\mathrm{F}(n)$ when $n \equiv 3 \bmod 8$. □

Lemma 5.3.5.
Let $n \in \mathbb{Z}_{>0}$ satisfy $n \equiv 7 \bmod 8$ then we have $\mathrm{E}(n) = 0$.

Proof.
Let $n \in \mathbb{Z}_{>0}$ satisfy $n \equiv 7 \bmod 8$ then we have

$$\begin{aligned} \mathrm{E}(n) &= 2\mathrm{F}(n) - \mathrm{G}(n) \text{ and so} \\ 3\mathrm{E}(n) &= 6\mathrm{F}(n) - 3\mathrm{G}(n) \\ &= 6\mathrm{F}(n) - 6\mathrm{F}(n) \text{ by Theorem 5.2.21} \\ &= 0. \end{aligned}$$

Hence $\mathrm{E}(n) = 0$ when $n \equiv 7 \bmod 8$. □

Summary 5.3.6.
Combining Lemmas 5.3.3, 5.3.4 and 5.3.5 we get

$$\mathrm{E}(n) = \begin{cases} \mathrm{F}(n) & \text{if } n \equiv 1, 2 \bmod 4 \\ \frac{2}{3}\mathrm{F}(n) & \text{if } n \equiv 3 \bmod 8 \\ 0 & \text{if } n \equiv 7 \bmod 8. \end{cases}$$

Our goal now is to split up the summation in Equation 5.19. The following observations will help.

Observation 5.3.7.
Note $\displaystyle\sum_{-\sqrt{n} \leqslant h \leqslant \sqrt{n}} \mathrm{E}\left(n - h^2\right) = \sum_{-\sqrt{n} \leqslant h \leqslant \sqrt{n}} \mathrm{E}\left(4n - 4h^2\right)$ for all $n \in \mathbb{Z}_{\geqslant 0}$.

Observation 5.3.8.
If $n \in \mathbb{Z}_{\geqslant 0}$ is even then $4n - k^2 \equiv 7 \bmod 8$ for all odd integers k. From Lemma 5.3.5 it follows that $\displaystyle\sum_{\substack{k \text{ odd} \\ -2\sqrt{n} < k < 2\sqrt{n}}} \mathrm{E}\left(4n - k^2\right) = 0$.
Note equality holds in the summation index without changing the result. This is because k is odd and thus we never take $k = \pm 2\sqrt{n}$.

Observation 5.3.9.
If $n \in \mathbb{Z}_{>0}$ is odd then $4n \equiv 4 \bmod 8$ and $4n - k^2 \equiv 3 \bmod 8$ for all odd integers k. Applying Lemma 5.3.4 yields $\displaystyle\sum_{\substack{k \text{ odd} \\ -2\sqrt{n} \leqslant 2\sqrt{n}}} \mathrm{E}\left(4n - k^2\right) = \sum_{\substack{k \text{ odd} \\ -2\sqrt{n} \leqslant k \leqslant 2\sqrt{n}}} \frac{2}{3}\mathrm{F}\left(4n - k^2\right)$.

Now consider Equation 5.19. We split the left hand side into two summations, one for when h is odd and the other for when h is even.

$$\begin{aligned} 2\sigma_{\text{odd}} &= \sum_{-2\sqrt{n} \leqslant h \leqslant 2\sqrt{n}} \mathrm{E}\left(4n - h^2\right) \\ &= \sum_{\substack{h \text{ even} \\ -2\sqrt{n} \leqslant h \leqslant 2\sqrt{n}}} \mathrm{E}\left(4n - h^2\right) + \sum_{\substack{h \text{ odd} \\ -2\sqrt{n} \leqslant h \leqslant 2\sqrt{n}}} \mathrm{E}\left(4n - h^2\right) \end{aligned}$$

$$= \sum_{-\sqrt{n}\leqslant\tilde{h}\leqslant\sqrt{n}} \mathrm{E}\left(4n-4\tilde{h}^2\right) + \sum_{\substack{h \text{ odd}\\ -2\sqrt{n}\leqslant h\leqslant 2\sqrt{n}}} \mathrm{E}\left(4n-h^2\right). \tag{5.20}$$

If n is even then the second summation in Equation 5.20 is 0 by Observation 5.3.8. Therefore Equation 5.20 becomes

$$\begin{aligned} 2\sigma_{\text{odd}} &= \sum_{-\sqrt{n}\leqslant\tilde{h}\leqslant\sqrt{n}} \mathrm{E}\left(4\left[n-\tilde{h}^2\right]\right) \\ &= \sum_{-\sqrt{n}\leqslant\tilde{h}\leqslant\sqrt{n}} \mathrm{E}\left(n-\tilde{h}^2\right). \end{aligned} \tag{5.21}$$

Whereas if n is odd then the second summation in Equation 5.20 may be replaced with $\sum_{-2\sqrt{n}\leqslant h\leqslant 2\sqrt{n}} \frac{2}{3}\mathrm{F}\left(4n-h^2\right)$. Therefore when n is odd we get

$$\begin{aligned} 2\sigma_{\text{odd}} &= \sum_{-\sqrt{n}\leqslant\tilde{h}\leqslant\sqrt{n}} \mathrm{E}\left(4\left[n-h^2\right]\right) + \sum_{\substack{h \text{ odd}\\ -2\sqrt{n}\leqslant h\leqslant 2\sqrt{n}}} \frac{2}{3}\mathrm{F}\left(4n-h^2\right) \\ &= \sum_{-\sqrt{n}\leqslant\tilde{h}\leqslant\sqrt{n}} \mathrm{E}\left(n-\tilde{h}^2\right) + \sum_{\substack{h \text{ odd}\\ -2\sqrt{n}\leqslant h\leqslant 2\sqrt{n}}} \frac{2}{3}\mathrm{F}\left(4n-h^2\right). \end{aligned}$$

This rearranges to give

$$\sum_{-\sqrt{n}\leqslant\tilde{h}\leqslant\sqrt{n}} \mathrm{E}\left(n-\tilde{h}^2\right) = 2\sigma_{\text{odd}} - \sum_{\substack{h \text{ odd}\\ -2\sqrt{n}\leqslant h\leqslant 2\sqrt{n}}} \frac{2}{3}\mathrm{F}\left(4n-h^2\right). \tag{5.22}$$

These two results match those of Kronecker's, found at the top of page 484, [Kr1897]. Our aim now is to derive a unified expression for $\sum_{-\sqrt{n}\leqslant\tilde{h}\leqslant\sqrt{n}} \mathrm{E}\left(n-\tilde{h}^2\right)$.

Lemma 5.3.10.
Let n be a positive integer. Then $\sum_{\substack{h \text{ odd}\\ -2\sqrt{n}\leqslant h\leqslant 2\sqrt{n}}} \mathrm{F}\left(4n-h^2\right) = 2\sigma_{\text{odd}}$.

Proof.
We have

$$\begin{aligned} \sum_{\substack{h \text{ odd}\\ -2\sqrt{n}\leqslant h\leqslant 2\sqrt{n}}} \mathrm{F}\left(4n-h^2\right) &= \sum_{-2\sqrt{n}\leqslant h\leqslant 2\sqrt{n}} \mathrm{F}\left(4n-h^2\right) - \sum_{\substack{h \text{ even}\\ -2\sqrt{n}\leqslant h\leqslant 2\sqrt{n}}} \mathrm{F}\left(4n-h^2\right) \\ &= \sum_{-2\sqrt{n}\leqslant h\leqslant 2\sqrt{n}} \mathrm{F}\left(4n-h^2\right) - \sum_{-\sqrt{n}\leqslant\tilde{h}\leqslant\sqrt{n}} \mathrm{F}\left(4\left[n-\tilde{h}^2\right]\right) \\ &\overset{\text{Theorem 5.1.20}}{=} \sum_{-2\sqrt{n}\leqslant h\leqslant 2\sqrt{n}} \mathrm{F}\left(4n-h^2\right) - 2\sum_{-\sqrt{n}\leqslant\tilde{h}\leqslant\sqrt{n}} \mathrm{F}\left(n-\tilde{h}^2\right). \end{aligned}$$

Applying Equations 5.6 and 5.8 we get

$$\sum_{\substack{h \text{ odd} \\ -2\sqrt{n}\leqslant h\leqslant 2\sqrt{n}}} \mathrm{F}\left(4n-h^2\right) = \left(2\sigma_{\text{odd}}(n)+\sigma(n)+\Psi(n)\right) - 2\left(\frac{1}{2}\left[\sigma(n)+\Psi(n)\right]\right)$$
$$= 2\sigma_{\text{odd}}(n). \tag{5.23}$$

□

Lemma 5.3.11.
Let n be a positive integer then

$$\sum_{-\sqrt{n}\leqslant \tilde{h}\leqslant\sqrt{n}} \mathrm{E}\left(n-\tilde{h}^2\right) = \begin{cases} 2\sigma_{\text{odd}}(n) & \text{if } n\equiv 0 \bmod 2 \\ \frac{2}{3}\sigma_{\text{odd}}(n) & \text{if } n\equiv 1 \bmod 2. \end{cases}$$

Proof.
Let n be a positive integer. From Equations 5.21 and 5.22 we have

$$\sum_{-\sqrt{n}\leqslant \tilde{h}\leqslant\sqrt{n}} \mathrm{E}\left(n-\tilde{h}^2\right) = \begin{cases} 2\sigma_{\text{odd}} & \text{if } n\equiv 0 \bmod 2 \\ 2\sigma_{\text{odd}} - \displaystyle\sum_{\substack{h \text{ odd} \\ -2\sqrt{n}\leqslant h\leqslant 2\sqrt{n}}} \frac{2}{3}\mathrm{F}\left(4n-h^2\right) & \text{if } n\equiv 1 \bmod 2 \end{cases}$$
$$= \begin{cases} 2\sigma_{\text{odd}} & \text{if } n\equiv 0 \bmod 2 \\ 2\sigma_{\text{odd}} - \frac{2}{3}\cdot 2\sigma_{\text{odd}} & \text{if } n\equiv 1 \bmod 2, \text{ by Lemma 5.3.10} \end{cases}$$
$$= \begin{cases} 2\sigma_{\text{odd}}(n) & \text{if } n\equiv 0 \bmod 2 \\ \frac{2}{3}\sigma_{\text{odd}}(n) & \text{if } n\equiv 1 \bmod 2. \end{cases}$$

□

The following theorem repackages the above result in a tidy manner and gives the pivotal result for Kronecker to determine the number of representations of a positive integer as a sum of three squares.

Theorem 5.3.12.
Let n be a positive non-zero integer. Then

$$12\sum_{-\sqrt{n}\leqslant h\leqslant\sqrt{n}} \mathrm{E}\left(n-h^2\right) = 8\left(2+(-1)^n\right)\sigma_{\text{odd}}(n).$$

Proof.
Let n be a positive non-zero integer. Using the result found in Lemma 5.3.11 and multiplying by 3 yields

$$3\sum_{-\sqrt{n}\leqslant h\leqslant\sqrt{n}} \mathrm{E}\left(n-h^2\right) = \begin{cases} 2\cdot 3\sigma_{\text{odd}}(n) & \text{if } n\equiv 0 \bmod 2 \\ 2\cdot 1\sigma_{\text{odd}}(n) & \text{if } n\equiv 1 \bmod 2. \end{cases}$$

Now observe $1 = 2 + (-1)^1$ and $3 = 2 + (-1)^2$, thus we have

$$2 + (-1)^n = \begin{cases} 3 & \text{if } n \equiv 0 \bmod 2 \\ 1 & \text{if } n \equiv 1 \bmod 2. \end{cases}$$

Applying this and multiplying the result by 4 then gives

$$\begin{aligned} 12 \sum_{-\sqrt{n} \leqslant h \leqslant \sqrt{n}} \mathrm{E}\left(n - h^2\right) &= 4 \cdot 2 \left(2 + (-1)^n\right) \sigma_{\mathrm{odd}}(n) \\ &= 8 \left(2 + (-1)^n\right) \sigma_{\mathrm{odd}}(n). \end{aligned}$$

□

Corollary 5.3.13.
From Appendix A.2 Corollary A.2.19, the right hand side of Theorem 5.3.12 is $r_4(n)$. That is, the number of ways to represent a positive integer n as a sum of four squares. Consequently, we have $12 \sum_{-\sqrt{n} \leqslant h \leqslant \sqrt{n}} \mathrm{E}\left(n - h^2\right)$ is the number of ways to write n as a sum of four squares.

Theorem 5.3.14.
Let n be a positive non-zero integer and let h satisfy $-\sqrt{n} \leqslant h \leqslant \sqrt{n}$. Then $12\mathrm{E}\left(n - h^2\right)$ is the number of ways to represent the positive non-zero integer $n - h^2$ as a sum of three squares.

Proof.
Fix $n \in \mathbb{Z}_{\geqslant 0}$ and $h \in \mathbb{Z}$ such that $-\sqrt{n} \leqslant h \leqslant \sqrt{n}$. Define the following three sets

$$\begin{aligned} \chi_n &= \left\{(d_1, d_2, d_3, d_4) \mid d_1^2 + d_2^2 + d_3^2 + d_4^2 = n, d_i \in \mathbb{Z}, i \in \{1, 2, 3, 4\}\right\} \\ \chi_h &= \left\{(d_1, d_2, d_3, h) \mid d_1^2 + d_2^2 + d_3^2 + h^2 = n, d_i \in \mathbb{Z}, i \in \{1, 2, 3\}\right\} \subseteq \chi_n \\ \chi_{2,h} &= \left\{(r_1, r_2, r_3) \mid r_1^2 + r_2^2 + r_3^2 = n - h^2, r_i \in \mathbb{Z}, i \in \{1, 2, 3\}\right\}. \end{aligned}$$

We will show the map

$$\begin{aligned} J : \chi_h &\longrightarrow \chi_{2,h} \\ (d_1, d_2, d_3, h) &\longmapsto (d_1, d_2, d_3) \end{aligned}$$

is a well-defined bijection.
Well-defined:
It is sufficient to show $r_1^2 + r_2^2 + r_3^2 = d_1^2 + d_2^2 + d_3^2 = d_1^2 + d_2^2 + d_3^2 + h^2 - h^2 = n - h^2$.
Injectivity: This is straightforward to verify.
Surjectivity: Let $(r_1, r_2, r_3) \in \chi_{2,h}$ be arbitrary and consider (r_1, r_2, r_3, h). This satisfies $r_1^2 + r_2^2 + r_3^2 + h^2 = n - h^2 + h^2 = n$ and clearly each element lies in $\mathbb{Z}$ thus $(r_1, r_2, r_3, h) \in \chi_h$. Since $J(r_1, r_2, r_3, h) = (r_1, r_2, r_3)$ we have a bijection.
Consequently we have a one-to-one correspondence between representations of $n - h^2$ as a sum of three squares and representations of n as a sum of four squares, where the last term to be squared is h.

Observe that in the set χ_n the largest any d_i may be is $\sqrt{n}$ and this may only occur when all other d_j are zero. Using this we may write as the following disjoint union

$$\chi_n = \bigcup_{-\sqrt{n}\leqslant h\leqslant\sqrt{n}} \chi_h.$$

This is because $\chi_{h_1} \cap \chi_{h_2} = \emptyset$ unless $h_1 = h_2$.

Thus $r_4(n) = \sum_{-\sqrt{n}\leqslant h\leqslant\sqrt{n}} |\chi_h|$. Applying the bijection given by the map J to the right hand side yields $r_4(n) = \sum_{-\sqrt{n}\leqslant h\leqslant\sqrt{n}} |\chi_{2,h}|$.
Combining this with Theorem 5.3.12 yields

$$\sum_{-\sqrt{n}\leqslant h\leqslant\sqrt{n}} 12\mathrm{E}(n-h^2) = \sum_{-\sqrt{n}\leqslant h\leqslant\sqrt{n}} |\chi_{2,h}|\,.$$

Since $|\chi_{2,h}|$ is the number of representations of the positive non-zero integer $n-h^2$ as a sum of three squares, this implies $12\mathrm{E}\left(n-h^2\right)$ is the number of representations of $n-h^2$ as a sum of three squares. □

The last observation Kronecker makes in his section 22 connects sums of three squares to sums of three triangle numbers. The following lemma makes this connection.

Lemma 5.3.15.
Every positive integer n may be written as a sum of three triangle numbers if and only if every number of the form $8n+3$ is a sum of three squares.

Proof.

Recall a positive integer ∇ is called a triangle number if $\nabla = \sum_{i=1}^{m} i$ for some positive integer m.
Let $n \in \mathbb{Z}_{\geqslant 0}$ and suppose $n = \nabla_1 + \nabla_2 + \nabla_3$, where ∇_i is a triangle number for $i \in \{1,2,3\}$. Then we have

$$\begin{aligned} n &= \nabla_1 + \nabla_2 + \nabla_3 \\ &= \sum_{i=1}^{N_1} i + \sum_{i=1}^{N_2} i + \sum_{i=1}^{N_3} i \\ &= \frac{N_1\left(N_1+1\right)}{2} + \frac{N_2\left(N_2+1\right)}{2} + \frac{N_3\left(N_3+1\right)}{2} \\ &= \frac{1}{2}\left(N_1^2+N_2^2+N_3^2+N_1+N_2+N_3\right). \end{aligned}$$

Using this it follows that

$$8n+3 = 8\left(\frac{1}{2}\left[N_1^2+N_2^2+N_3^2+N_1+N_2+N_3\right]\right)+3$$

$$= 4N_1^2 + 4N_2^2 + 4N_3^2 + 4N_1 + 1 + 4N_2 + 1 + 4N_3 + 1$$
$$= (2N_1 + 1)^2 + (2N_2 + 1)^2 + (2N_3 + 1)^2 .$$

Thus $8n + 3$ is a sum of three squares. Reversing this argument yields the converse statement. □

Finally, we prove a small observation due to Kronecker about the number of representations of a positive integer n as a sum of three triangle numbers.

Lemma 5.3.16.
The number of ways a positive integer n may be expressed as a sum of three triangle numbers is $\mathrm{F}(8n + 3)$.

Proof.
From Lemma 5.3.15 we know a positive integer n maybe expressed as a sum of three triangle numbers if and only if $8n + 3$ may be written as a sum of three squares. Since the squares mod 8 are $0, 1, 4$ we must have three odd squares. From this it follows that none of the squares are 0. Consequently, given a 3-tuple (a, b, c) such that $8n + 3 = a^2 + b^2 + c^2$, there are $2^3 = 8$ ways to generate another distinct 3-tuple with the same property by choosing where to place negative signs. Of these eight, only one will have the property that a, b and c are all positive.
Since $A(8n + 3) = 12\mathrm{E}(8n + 3)$ is the number of representations of $8n + 3$ as a sum of three squares, we may apply Lemma 5.3.4 to get $12\mathrm{E}(8n + 3) = 12\frac{2}{3}\mathrm{F}(8n + 3) = 8\mathrm{F}(8n + 3)$.
From the definition of a triangle number, the number of terms in the summation must be positive and so in the proof of Lemma 5.3.15 for the reverse direction we must consider N_1, N_2 and N_3 to be all positive. By our above remark, there is only one way for this out of a possible eight.
Therefore we have the number of ways to write n as a sum of three triangle numbers is $\frac{1}{8} \cdot 12\mathrm{E}(8n + 3) = \mathrm{F}(8n + 3)$. □

Notes on Section 5.3

Observation 5.3.17.
In order to have consistency between Kronecker's paper [Kr1897] and Weil's paper [We1974] we make the following remark. Observe the number of representations of a positive integer n as a sum of three squares is denoted by $\mathrm{A}(n)$ in Kronecker's work; whereas Weil uses $R_3(n)$, which we have written as $r_3(n)$ in order to avoid confusion with the next section.

5.4 Deriving Gauss' Theorem

In this section we prove the connection between Kronecker's sums of three squares work and the following classical result due to Gauss.

Theorem 5.4.1 (Gauss' Theorem)**.**
Let $R_3(n)$ denote the number of ***primitive*** *solutions to the equation $x^2+y^2+z^2=n$. Let $h(-n)$ be the number of proper equivalence classes of* ***primitive*** *binary quadratic forms $Ax^2+Bxy+Cy^2$ where*

$$B^2-4AC=\begin{cases} -4n & \text{if } n\equiv 1,2,5 \text{ or } 6 \bmod 8. \\ -n & \text{if } n\equiv 3 \bmod 8. \end{cases}$$

Let $\delta_n=1$ except for $\delta_1=\frac{1}{2}$ and $\delta_3=\frac{1}{3}$. Then

$$R_3(n)=\begin{cases} 12\delta_n h(-4n) & \text{if } n\equiv 1,2,5 \text{ or } 6 \bmod 8 \\ 24\delta_n h(-n) & \text{if } n\equiv 3 \bmod 8. \end{cases}$$

The statement of Gauss' Theorem and a small treatment of it may be found in Grosswald, [Gr1985, p. 51]. We shall derive a new proof of Theorem 5.4.1 by utilising our knowledge of Kronecker.

Our proof requires a series of intermediate results and so we begin by examining the effect of requiring our binary quadratic forms to be primitive.

Lemma 5.4.2.
Let $\mathcal{A}$ be a bilinear form with matrix representation $A=\begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix}$ that satisfies $\gcd(A_{11},A_{12},A_{21},A_{22}=1$ and let $M\in \mathrm{GL}_2(\mathbb{Z})$. Then every bilinear form $\mathcal{B}$ in the equivalence class of $\mathcal{A}$ satisfies $\gcd(B_{11},B_{12},B_{21},B_{22})=1$.

Proof.
Let $B=M^tAM=\begin{pmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{pmatrix}$ and $d=\gcd(B_{11},B_{12},B_{21},B_{22})$.
Then $B=\begin{pmatrix} d & 0 \\ 0 & d \end{pmatrix}\begin{pmatrix} B'_{11} & B'_{12} \\ B'_{21} & B'_{22} \end{pmatrix}$.
Consequently we have

$$\begin{aligned} A &= (M^{-1})^tM^tAMM^{-1} \\ &= (M^{-1})^tBM^{-1} \\ &= (M^{-1})^t\begin{pmatrix} d & 0 \\ 0 & d \end{pmatrix}\begin{pmatrix} B'_{11} & B'_{12} \\ B'_{21} & B'_{22} \end{pmatrix}M^{-1} \\ &= \begin{pmatrix} d & 0 \\ 0 & d \end{pmatrix}(M^{-1})^tB'M^{-1}. \end{aligned}$$

That is, each element of A is divisible by d. However, $\gcd(A_{11},A_{12},A_{21},A_{22})=1$ and thus we deduce $d=1$.
Since $M\in \mathrm{GL}_2(\mathbb{Z})$ it follows that every bilinear form which is equivalent to the primitive bilinear form $\mathcal{A}$ is primitive. □

Corollary 5.4.3.
If the equivalence class of a binary quadratic form $Ax^2+Bxy+Cy^2$ contains a primitive form ($\gcd(A,B,C)=1$) then every binary quadratic form in the equivalence class is primitive.

Proof.
We may view the binary quadratic form $Ax^2 + Bxy + Cy^2$ as the bilinear form with $A_{11} = A$, $A_{12} = A_{21} = \frac{B}{2}$ and $A_{22} = C$. Thus $\gcd(A, B, C) = 1$ is the same as $\gcd(A_{11}, A_{12}, A_{21}, A_{22}) = \gcd(A_{11}, A_{12}, A_{22}) = 1$. Lemma 5.4.2 then yields the result. □

Lemma 5.4.4.
Let n be a positive non-zero integer then

$$r_3(n) = \begin{cases} 2 \cdot \sum\limits_{\substack{d=1 \\ d^2|n}}^{n} 6\mathrm{F}_p\left(\frac{n}{d^2}\right) & \text{if } n \equiv 1, 2 \bmod 4 \\ \frac{4}{3} \cdot \sum\limits_{\substack{d=1 \\ d^2|n}}^{n} 6\mathrm{F}_p\left(\frac{n}{d^2}\right) & \text{if } n \equiv 3 \bmod 8 \\ 0 & \text{if } n \equiv 7 \bmod 8, \end{cases}$$

where $6\mathrm{F}_p(k)$ is the number of complete equivalence classes of positive definite binary quadratic forms $ax^2 + 2bxy + cy^2$ satisfying $ac - b^2 = k$, $\gcd(a, b, c) = 1$ and at least one of a, c is odd.

Proof.
From Theorem 5.3.14 $12\mathrm{E}(n)$ is the number of representations (primitive and imprimitive) of the integer n as a sum of three integer squares. Thus $r_3(n) = 12\mathrm{E}(n)$. By Definition 5.3.1 and Lemma 5.3.2 we have $\mathrm{E}(n) = 2\mathrm{F}(n) - \mathrm{G}(n)$ and $\mathrm{E}(4n) = \mathrm{E}(n)$ for all positive integers n.
Further, by Summary 5.3.6 we have

$$\mathrm{E}(n) = \begin{cases} \mathrm{F}(n) & \text{if } n \equiv 1, 2 \bmod 4 \\ \frac{2}{3}\mathrm{F}(n) & \text{if } n \equiv 3 \bmod 8 \\ 0 & \text{if } n \equiv 7 \bmod 8. \end{cases}$$

Consequently we have

$$12\mathrm{E}(n) = \begin{cases} 12\mathrm{F}(n) & \text{if } n \equiv 1, 2 \bmod 4 \\ 8\mathrm{F}(n) & \text{if } n \equiv 3 \bmod 8 \\ 0 & \text{if } n \equiv 7 \bmod 8 \end{cases} = \begin{cases} 2 \cdot 6\mathrm{F}(n) & \text{if } n \equiv 1, 2 \bmod 4 \\ \frac{4}{3} \cdot 6\mathrm{F}(n) & \text{if } n \equiv 3 \bmod 8 \\ 0 & \text{if } n \equiv 7 \bmod 8. \end{cases} \tag{5.24}$$

Recall in Kronecker's notation $6\mathrm{F}(n)$ is the number of complete equivalence classes of positive definite binary quadratic forms with $ac - b^2 = n$ and at least one of a, c is odd. There is no mention of primitivity and thus we now express this quantity as a sum over primitive sets.
Let $V\{[(a, b, c)]_c \mid ac - b^2 = n, \text{at least one of } a, c \text{ is odd}\}$, thus $|V| = 6\mathrm{F}(n)$. By Lemma 5.2.1 the set $\Omega_n = \{(a, b, c) \mid ac - b^2 = n, -\min\{a, c\} < b \leqslant \min\{a, c\}\}$ contains a unique representative for every complete equivalence class of binary quadratic forms with $ac - b^2 = n$. We recall (see Observation 2.4.5 the property "at least one of a, c is odd" is invariant under transformation by $M \in \ker \sigma$, hence we have

$|V| = 6\mathrm{F}(n) = |\hat{\Omega}_n|$, where $\hat{\Omega}_n = \{(a,b,c) \in \Omega_n \mid \text{at least one of } a, c \text{ is odd}\}$.
We now partition $\hat{\Omega}_n$ into a finite disjoint union of the sets $\hat{\Omega}_n^d$, where

$$\hat{\Omega}_n^d = \left\{(a,b,c) \in \hat{\Omega} \mid \gcd(a,b,c) = d\right\}.$$

We note $d \neq 2k$ for any $k \in \mathbb{Z}$ because at least one of a, c is odd. Next we define the set L_n^d as follows:

$$L_n^d = \{(x,y,z) \mid xz - y^2 = \frac{n}{d^2}, -\min\{x,z\} < y \leqslant \min\{x,z\}, \gcd(x,y,z) = 1, \\ \text{at least one of } x, z \text{ is odd}\}.$$

Now we show the following map η is a well-defined bijection.

$$\eta : \hat{\Omega}_n^d \longrightarrow L_n^d$$
$$(a,b,c) \longmapsto \left(\frac{a}{d}, \frac{b}{d}, \frac{c}{d}\right) = (x,y,z).$$

Well-defined: We have $d = \gcd(a,b,c)$ and so $(x,y,z) \in \mathbb{Z}^3$. Next, $n = ac - b^2 = d^2\left(\frac{a}{d} \cdot \frac{c}{d} - \left(\frac{b}{d}\right)^2\right) = d^2(xz - y^2)$ thus $xz - y^2 = \frac{n}{d^2}$. Now suppose $x \equiv z \equiv 0 \bmod 2$, then $a = dx$ and $c = dz$ are both even, a contradiction and thus at least one of x, z is odd. Clearly we also have $\gcd(x,y,z) = 1$. Lastly, we observe $-\min\{a,c\} < b \leqslant \min\{a,c\}$ is equivalent to $-\min\{dx,dz\} < dy \leqslant \min\{dx,dz\}$ and so since $d > 0$ it follows that $-\min\{x,z\} < y \leqslant \min\{x,z\}$. Hence the map η is well-defined.
Injectivity: This is straightforward to verify.
Surjectivity: We repeat the argument given in the well-defined section, but this time in the opposite direction.
Hence the map η is a bijection.
Thus using Lemma 5.2.1 we have shown $6\mathrm{F}(n) = |V| = |\hat{\Omega}_n| = \sum_{\substack{d=1 \\ d^2|n}}^{n} 6\mathrm{F}_p\left(\frac{n}{d^2}\right)$, where $6\mathrm{F}_p(k)$ is the number of complete equivalence classes of positive definite binary quadratic forms $ax^2 + 2bxy + cy^2$ such that $ac - b^2 = q$, $\gcd(a,b,c) = 1$ and at least one of a, c is odd.
Substituting this result into Equation 5.24 then yields

$$r_3(n) = \begin{cases} 2 \cdot \sum_{\substack{d=1 \\ d^2|n}}^{n} 6\mathrm{F}_p\left(\frac{n}{d^2}\right) & \text{if } n \equiv 1, 2 \bmod 4 \\ \frac{4}{3} \cdot \sum_{\substack{d=1 \\ d^2|n}}^{n} 6\mathrm{F}_p\left(\frac{n}{d^2}\right) & \text{if } n \equiv 3 \bmod 8 \\ 0 & \text{if } n \equiv 7 \bmod 8. \end{cases}$$

□

We now establish a similar result for the relationship between $r_3(n)$ and $R_3(n)$.

Lemma 5.4.5.
Let n be a positive integer then

$$r_3(n) = \sum_{\substack{d=1 \\ d^2|n}}^{n} R_3\left(\frac{n}{d^2}\right).$$

Proof.
Let $A^n = \{(x_1, x_2, x_3) \mid x_1^2 + x_2^2 + x_3^2 = n, \gcd(x_1, x_2, x_3) \geqslant 1\}$. Thus $|A^n| = r_3(n)$. We partition the set A^n into a disjoint union of the sets
$A_d^n = \{(x_1, x_2, x_3) \mid x_1^2 + x_2^2 + x_3^2 = n, \gcd(x_1, x_2, x_3) = d\}$, so $A^n = \bigcup_{d=1}^{n} A_d^n$. We note $A_d^n = \emptyset$ if $d^2 \nmid n$.

Consequently we have $r_3(n) = |A^n| = \sum_{\substack{d=1 \\ d^2|n}}^{n} |A_d^n|$.

Now let $B_d^n = \left\{(y_1, y_2, y_3) \mid y_1^2 + y_2^2 + y_3^2 = \frac{n}{d^2}, \gcd(y_1, y_2, y_3) = 1\right\}$. It is straightforward to verify the map $\eta : A_d^n \longrightarrow B_d^n$ given by $(x_1, x_2, x_3) \longmapsto \left(\frac{x_1}{d}, \frac{x_2}{d}, \frac{x_3}{d}\right)$ is a well-defined bijection. The proof is very similar to that found in the proof of Lemma 5.4.4.

We observe $|B_d^n|$ is the number of primitive solutions to the equation $y_1^2 + y_2^2 + y_3^2 = \frac{n}{d^2}$ and hence $|B_d^n| = R_3\left(\frac{n}{d^2}\right)$.

Thus we deduce $r_3(n) = |A^n| = \sum_{\substack{d=1 \\ d^2|n}}^{n} |A_d^n| = \sum_{\substack{d=1 \\ d^2|n}}^{n} |B_d^n| = \sum_{\substack{d=1 \\ d^2|n}}^{n} R_3\left(\frac{n}{d^2}\right)$. □

Lemma 5.4.6.
Let n and d be positive integers such that $d^2 \mid n$. If $n \equiv 1, 2 \bmod 4$ then $\frac{n}{d^2} \equiv 1, 2 \bmod 4$ respectively. Further, if $n \equiv 3 \bmod 4$ then $\frac{n}{d^2} \equiv n \bmod 8$.

Proof.
First suppose $n \equiv 1$ or $2 \bmod 4$. Since $d^2 \equiv 0, 1 \bmod 4$ depending on whether d is even or odd, we cannot have $d \equiv 0 \bmod 2$ else $n = \hat{n}d^2 \equiv 0 \bmod 4$. Thus $\hat{n} \equiv \hat{n}d^2 = n \equiv 1, 2 \bmod 4$ respectively.
Now suppose $n \equiv 3 \bmod 4$ and write

$$n = \prod p_i^{e_i} \prod q_j^{f_j} \prod s_k^{g_k} \prod t_l^{h_l}, \text{ where}$$

p_i, q_j, s_k, t_l are primes such that $p_i \equiv 1 \bmod 8$, $q_j \equiv 3 \bmod 8$, $s_k \equiv 5 \bmod 8$ and $t_l \equiv 7 \bmod 8$. Observe any divisor d such that $d^2 \mid n$ is necessarily odd and that dividing by d^2 results in decreasing each of the e_i, f_j, g_k and h_l by a multiple of 2. Consequently, writing

$$\frac{n}{d^2} = \prod p_i^{e_i'} \prod q_j^{f_j'} \prod s_k^{g_k'} \prod t_l^{h_l'}$$

we observe $e_i + f_j + g_k + h_l \equiv e_i' + f_j' + g_k' + h_l'$ and thus $\frac{n}{d^2} \equiv n \bmod 8$ when $n \equiv 3 \bmod 4$. This is because $d \equiv 1 \bmod 2$ implies $d^2 \equiv 1 \bmod 8$. □

Lemma 5.4.7.
Let n be a positive integer then $R_3(n) = \begin{cases} 2 \cdot 6\mathrm{F}_p(n) & \text{if } n \equiv 1, 2 \bmod 4 \\ \frac{4}{3} \cdot 6\mathrm{F}_p(n) & \text{if } n \equiv 3 \bmod 8 \\ 0 & \text{if } n \equiv 7 \bmod 8. \end{cases}$

Proof.
Combining the results of Lemmas 5.4.4 and 5.4.5 yields

$$\sum_{\substack{d=1 \\ d^2|n}}^{n} R_3\left(\frac{n}{d^2}\right) = \begin{cases} 2 \cdot \displaystyle\sum_{\substack{d=1 \\ d^2|n}}^{n} 6\mathrm{F}_p\left(\frac{n}{d^2}\right) & \text{if } n \equiv 1, 2 \bmod 4 \\ \frac{4}{3} \cdot \displaystyle\sum_{\substack{d=1 \\ d^2|n}}^{n} 6\mathrm{F}_p\left(\frac{n}{d^2}\right) & \text{if } n \equiv 3 \bmod 8 \\ 0 & \text{if } n \equiv 7 \bmod 8. \end{cases}$$

By Lemma 5.4.6 we know dividing by d^2 leaves us in the same category. Hence we apply an inductive argument. The base case is when n is square free. In this case the summations consist of a single term and we clearly get our result.
Now suppose our claim holds for all numbers less than K. We consider each of the cases in turn and note that dividing by a square (if possible) gives a number smaller than K. Thus expanding both summations and applying the inductive hypothesis leads to cancellation of all terms except the term on each side corresponding to $d = 1$.
Hence we deduce $R_3(n) = \begin{cases} 2 \cdot 6\mathrm{F}_p(n) & \text{if } n \equiv 1, 2 \bmod 4 \\ \frac{4}{3} \cdot 6\mathrm{F}_p(n) & \text{if } n \equiv 3 \bmod 8 \\ 0 & \text{if } n \equiv 7 \bmod 8. \end{cases}$
Hence by induction we have our result. □

In order to prove Theorem 5.4.1 it will be necessary to consider three cases. The following observation explains why.

Observation 5.4.8.
Recall $6\mathrm{F}_p(n)$ is the number of complete equivalence classes of primitive binary quadratic forms $ax^2 + 2bxy + cy^2$ with $\gcd(a, b, c) = 1$, $ac - b^2 = n$ and at least one of a, c is odd. Using the fact that these binary quadratic forms may be viewed as bilinear forms, and applying our bilinear automorph results found in Table 2.3, we know the only reduced binary quadratic forms with non-trivial proper automorphs are $(a, 0, a)$ and $(2b, b, 2b)$. Since these are imprimitive for $a \neq 1$ ($n = 1$)and $b \neq 1$ ($n = 3$) respectively, we conclude for $n \neq 1, 3$ there are no non-trivial proper automorphs and thus $6 \mid 6\mathrm{F}_p(n)$. Therefore it is sufficient to consider the proper equivalence classes of reduced binary quadratic forms when $n \neq 1, 3$. Thus we have three cases to consider, namely: $n = 1$, $n \equiv 1, 2 \bmod 4$ ($n \neq 1$), and $n \equiv 3 \bmod 8$. The last case will require careful consideration when $n = 3$.

Lemma 5.4.9.
Let $n = 1$, then $2\mathrm{F}_p(n) = h(-4)$.

Proof.
We know $6\mathrm{F}_p(1)$ is the number of complete equivalence classes of primitive binary quadratic forms $ax^2+2bxy+cy^2=1$ with $ac-b^2=1$. To count these we look at the reduced forms, of which there is precisely one, namely $(1,0,1)$. By our automorph theory the proper equivalence class of this form contains exactly 3 complete equivalence classes, all of which have at least one odd outer coefficient and are primitive. Hence $6\mathrm{F}_p(1)=3$.
Thus $2\mathrm{F}_p(1)=1$ and this is the number of primitive proper equivalence classes of such binary quadratic forms. However, $(1,0,1)$ may also be thought of as the form $Ax^2+Bxy+Cy^2$ where $A=C=1$ and $B=0$. This satisfies $B^2-4AC=-4$ and $\gcd(A,B,C)=1$, thus we deduce $2\mathrm{F}_p(1)\leqslant h(-4)$.
Now suppose we have a form $Ax^2+Bxy+Cy^2$ where $\gcd(A,B,C)=1$ and $B^2-4AC=-4$. Then we must have $2\mid B$ which implies $1=AC-b^2$, where $2B=b$. Further, it is clear if $d=\gcd(A,b,C)$ then $d\mid A$, $d\mid 2b$ and $d\mid C$. Since $2b=B$, $d\mid\gcd(A,B,C)=1$ follows. Hence the our form $Ax^2+Bxy+Cy^2$ is also of the form $ax^2+2bxy+cy^2$ with $\gcd(a,b,c)=1$ and $ac-b^2=1$. Since every binary quadratic form is properly equivalent to a unique reduced binary quadratic form of the same determinant, we deduce $h(-4)\leqslant 2\mathrm{F}_p(1)$.
Hence $2\mathrm{F}_p(1)=h(-4)$. □

Corollary 5.4.10.
We have $R_3(1)=6h(-4)$.

Proof.
Combining Lemmas 5.4.7 and 5.4.9 we get

$$\begin{aligned} R_3(1) &= 2\cdot 6\mathrm{F}_p(1)\\ &= 2\cdot 3\cdot 2\mathrm{F}_p(1)\\ &= 6h(-4). \end{aligned}$$

□

Lemma 5.4.11.
Let n be a positive integer strictly greater than 1 that satisfies $n\equiv 1$ or $2 \bmod 4$. Then $\mathrm{F}_p(n)=h(-4n)$.

Proof.
Let n be a positive integer strictly greater than 1 that satisfies $n\equiv 1$ or $2 \bmod 4$. Recall $6\mathrm{F}_p(n)$ is the number of complete equivalence classes of binary quadratic forms $ax^2+2bxy+cy^2$ where $ac-b^2=n$, $\gcd(a,b,c)=1$ and at least one of a, c is odd. From our theory of automorphs, the only such binary quadratic forms with a non-trivial proper automorph are $(a,0,a)$ and $(2b,b,2b)$ and since $n\equiv 1,2 \bmod 4$, $n\neq 1$ it follows these cases do not arise when we consider $6\mathrm{F}_p(n)$. Hence every proper equivalence class contains exactly 6 complete equivalence classes and therefore $\mathrm{F}_p(n)$ is the number of proper equivalence classes of binary quadratic forms $ax^2+2bxy+cy^2$ where $ac-b^2=n$, $\gcd(a,b,c)=1$ and at least one of a, c is odd.

Now observe we may view these binary quadratic forms as $Ax^2+Bxy+Cy^2$ where $A = a$, $B = 2b$ and $C = c$. Since at least one of a, c is odd it follows that $\gcd(A, B, C) = \gcd(a, 2b, c) = \gcd(a, b, c) = 1$. Further, note that $B^2 - 4AC = 4b^2 - 4ac = -4(ac - b^2) = -4n$. Thus we deduce $\mathrm{F}_p(n) \leqslant h(-4n)$.
Now let $Ax^2+Bxy+Cy^2$ be a reduced binary quadratic form such that $\gcd(A, B, C) = 1$ and $B^2-4AC = -4n$. Thus it is necessarily true that $B \equiv 0 \bmod 2$ and hence every such form may be expressed as $ax^2 + 2bxy + cy^2$ by letting $a = A$, $b = \frac{B}{2}$ and $c = C$. We note $4(ac - b^2) = 4\left(AC - \left(\frac{B}{2}\right)^2\right) = 4n$ and so $ac - b^2 = n$. Thus every such reduced form is in fact a reduced form counted by $\mathrm{F}_p(n)$. Hence $h(-4n) \leqslant \mathrm{F}_p(n)$. Therefore we have $\mathrm{F}_p(n) = h(-4n)$ when $n \equiv 1$ or $2 \bmod 4$, $n \neq 1$. □

Corollary 5.4.12.
Let n be a positive integer such that $n \equiv 1$ or $2 \bmod 4$, $n \neq 1$.
Then $R_3(n) = 12h(-4n)$.

Proof.
Let n be a positive integer such that $n \equiv 1$ or $2 \bmod 4$, $n \neq 1$. By combining Lemmas 5.4.7 and 5.4.12 we deduce

$$\begin{aligned} R_3(n) &= 2 \cdot 6\mathrm{F}_p(n) \\ &= 2 \cdot 6h(-4n) \\ &= 12h(-4n). \end{aligned}$$

□

We now develop some results which will permit us to deal with the $n \equiv 3 \bmod 8$ case.

Lemma 5.4.13.
Let n be a positive integer such that $n \equiv 3 \bmod 8$ and define the sets H_n and K_n as follows:

$$\begin{aligned} H_n &= \left\{[(A, B, C)]_+ \mid B^2 - 4AC = -n, \gcd(A, B, C) = 1\right\} \\ K_n &= \left\{[(a, b, c)]_+ \mid ac - b^2 = n, \gcd(a, b, c) = 1, a \equiv c \equiv 0 \bmod 2\right\}. \end{aligned}$$

Then the map

$$\begin{aligned} \zeta : H_n &\longrightarrow K_n \\ (A, B, C) &\longmapsto (2A, B, 2C) = (a, b, c) \end{aligned}$$

is a well-defined bijection.
Note: Binary quadratic forms in H_n are of the form $Ax^2 + Bxy + Cy^2$ [shorthand (A, B, C)], while those in K_n are of the form $ax^2 + 2bxy + cy^2$ [shorthand (a, b, c)].

Proof.
First note the sets H_n and K_n are well-defined. This is because primitivity is preserved under equivalence and the property of having at least one outer coefficient odd is

preserved under proper equivalence.
Well-defined: Clearly we have $a = 2A \equiv 2C = c \equiv 0 \bmod 2$. Next, we see $ac - b^2 = (2A)(2C) - B^2 = 4AC - B^2 = n$. Now let $d = \gcd(a, b, c)$, then $d|2A$, $d|2C$ and $d|B$. Since $4AC - B^2 \equiv 3 \bmod 8$ it follows that $A \equiv B \equiv C \equiv 1 \bmod 2$ and thus $d \equiv 1 \bmod 2$. Hence $d|A$ and $d|C$ and therefore $d|\gcd(A, B, C) = 1$, so $d = 1$.
Lastly, we show the map ζ respects proper equivalence classes. Suppose $f, g \in H_n$, $f \sim_+ g$ and they have matrix representations A and B respectively. Then there exists a matrix $M \in \mathrm{SL}_2(\mathbb{Z})$ such that $M^t AM = B$. Then

$$\begin{aligned}\zeta(g) = B' &= 2I_2 B \\ &= 2I_2 M^t AM \\ &= M^t(2I_2 A)M \\ &= M^t A' M = M^t \zeta(f) M.\end{aligned}$$

Thus $\zeta(f) \sim_+ \zeta(g)$ and hence the map ζ respects proper equivalence classes.
Injectivity:
Suppose $\zeta([(A, B, C)]_+) = \zeta([(A', B', C')]_+)$ then $[(2A, B, 2C)]_+ = [(2A', B', 2C')]_+$. Thus there exists $M \in \mathrm{SL}_2(\mathbb{Z})$ such that

$$\begin{aligned}\begin{pmatrix} 2A' & B' \\ B' & 2C' \end{pmatrix} &= M^t \begin{pmatrix} 2A & B \\ B & 2C \end{pmatrix} M \\ &= M^t 2I_2 \begin{pmatrix} A & \frac{B}{2} \\ \frac{B}{2} & C \end{pmatrix} M \\ &= 2I_2 M^t \begin{pmatrix} A & \frac{B}{2} \\ \frac{B}{2} & C \end{pmatrix} M.\end{aligned}$$

Since $\begin{pmatrix} 2A'B' & \\ B' & 2C' \end{pmatrix} = 2I_2 \begin{pmatrix} A' & \frac{B'}{2} \\ \frac{B'}{2} & C' \end{pmatrix}$ and $2I_2$ is invertible, it follows that $[(A, B, C)]_+ = [(A', B', C')]_+$.
Surjectivity: Let $[(a, b, c)]_+ \in K_n$ and consider $[(A, B, C)]_+ = [(\frac{a}{2}, b, \frac{c}{2})]_+$, we will show this lies in the set H_n. Since $[(a, b, c)]_+ \in K_n$ we have $a \equiv c \equiv 0 \bmod 2$ and thus $[(A, B, C)]_+$ has integer entries. Since we are dealing with positive definite forms we recall A and C are still positive. Next, $ac - b^2 \equiv 3 \bmod 8$ implies $c \equiv a \equiv 2 \bmod 4$ and $b \equiv 1 \bmod 2$ thus $A \equiv C \equiv B \equiv 1 \bmod 2$. Further, we have $B^2 - 4AC = -\left(4\left(\frac{a}{2}\right)\left(\frac{c}{2}\right) - b^2\right) = -n$. Now let $d = \gcd(A, B, C)$ then in particular $d|B = b$ and so $d \equiv 1 \bmod 2$. then $d|A = \frac{a}{2}$, $d|C = \frac{c}{2}$ with $d \equiv 1 \bmod 2$ implies $d|a$ and $d|c$, thus $d|\gcd(a, b, c) = 1$. Hence $d = 1$.
Lastly, we observe the same argument as given in the well-defined part of the proof works for showing proper equivalence classes are respected. The caveat being we use $\frac{1}{2}I_2$ instead of $2I_2$.
Thus the map ζ is surjective and hence is a well-defined bijection. □

Corollary 5.4.14.
Let $n \equiv 3 \bmod 8$ then

$$h(-n) = \begin{cases} 3\mathrm{G}_p(n) - 3\mathrm{F}_p(n) & \text{if } n = 3 \\ \mathrm{G}_p(n) - \mathrm{F}_p(n) & \text{otherwise.} \end{cases}$$

Proof.
Let n be a positive integer such that $n \equiv 3 \bmod 8$. From Lemma 5.4.13 we have $h(-n) = |H_n|$ and $|K_n|$ is the number of proper equivalence classes of primitive binary quadratic forms $ax^2 + 2bxy + cy^2$ such that $ac - b^2 = n$ and $a \equiv c \equiv 0 \bmod 2$. From our automorph theory (see Table 2.3) we see when $n \neq 3$ there are no primitive reduced binary quadratic forms with a non-trivial proper automorph. Thus every proper equivalence class must contain exactly 6 complete equivalence classes. Thus $6|6\mathrm{G}_p(n)$ and therefore $\mathrm{G}_p(n)$ is the number of proper equivalence classes of primitive binary quadratic forms $ax^2 + 2bxy + cy^2$. Further, since the property of having at least one of a, c odd is preserved under $\mathrm{GL}_2(\mathbb{Z})$ it follows that $|K_n| = \mathrm{G}_p(n) - \mathrm{F}_p(n)$. Now assume $n = 3$ then the reduced form $(2, 1, 2) \in K_n$ and it is primitive. This has 2 complete equivalence classes within its proper equivalence class. The only other reduced form with $ac - b^2 = 3$ is $(1, 0, 3)$ which is clearly primitive, satisfied $a \equiv c \equiv 1 \bmod 2$ and has no non-trivial proper automorphs. Thus we deduce $6\mathrm{G}_p(n) = 8$ and $6\mathrm{F}_p(n) = 6$, therefore $3\mathrm{G}_p(n) = 4$ and $3\mathrm{F}_p(n) = 3$. Consequently $|K_n| = 1 = 3\mathrm{G}_p(n) - 3\mathrm{F}_p(n)$ when $n = 3$.
Since Lemma 5.4.13 shows the map ζ is a bijection between the sets H_n and K_n when $n \equiv 3 \bmod 8$, our claim follows immediately. □

Note: Lemma 5.4.13 is essentially the same as Lemma 5.1.5 but with the added condition that primitivity is required in both $\mathcal{Q}_n$ and $\mathcal{R}_n$.

Lemma 5.4.15.
Let n be a positive integer such that $n \equiv 3 \bmod 8$ then $3\mathrm{G}_p(n) = 4\mathrm{F}_p(n)$.

Proof.
From Theorem 5.2.2 we have $3\mathrm{G}(n) = 4\mathrm{F}(n)$ for all positive integers n such that $n \equiv 3 \bmod 8$. We split the proof into two cases, namely when n is square-free and otherwise.
Case I: n is square-free, that is $n \neq kq^2$ for some $q \neq \pm 1$.
Let $ax^2 + 2bxy + cy^2$ be an arbitrary binary quadratic form satisfying $ac - b^2 = n$ and let $d = \gcd(a, b, c)$. Then $n = d^2(\hat{a}\hat{c} - \hat{b}^2)$. Since n is square-free it follows that $d = 1$ and hence our initial form is primitive.
Therefore when $n \equiv 3 \bmod 8$ and n is square-free we have $3\mathrm{G}_p(n) = 3\mathrm{G}(n) = 4\mathrm{F}(n) = 4\mathrm{F}_p(n)$.
Case II: $n = kq^2$.
Observe $n \equiv 3 \bmod 8$ implies $q \equiv 1 \bmod 2$ and $k \equiv 3 \bmod 8$. From our theory of automorphs (see Table 2.3) the only non-trivial proper automorphs are $(a, 0, a)$ and $(2b, b, 2b)$. Since $a^2 \not\equiv 3 \bmod 8$ the former cannot occur, whilst the latter may only arise when $k = 3$. Consequently, when $k \neq 3$ we know every proper equivalence class contains exactly six complete equivalence classes and thus $6|\mathrm{G}(n)$ and $6|\mathrm{F}(n)$. Now suppose $k = 3$ then the only proper equivalence class with a non-trivial proper automorph is that of $(2q, q, 2q)$ and it contains two complete equivalence classes. All of the remaining proper equivalence classes contain 6 complete equivalence classes. Thus $6 \nmid 6\mathrm{G}(n)$. However, $2|6\mathrm{G}(n)$ is $2 = \gcd(2, 6)$. Also, since $(2q, q, 2q)$ clearly has both outer coefficients even, we see that $6|\mathrm{F}(n)$.

From this we deduce $2|6\mathrm{G}(n)$ and $6|6\mathrm{F}(n)$ whenever $n = kq^2 \equiv 3 \bmod 8$. We now finish our claim by inducting on the number of (positive) divisors of q.
Base case: q is prime.
Then we have

$$\begin{aligned} 3\mathrm{G}(kq^2) &= 3\mathrm{G}_p(kq^2) + 3\mathrm{G}_p(k) \\ &= 3\mathrm{G}_p(kq^2) + 4\mathrm{F}_p(k). \end{aligned}$$

Here the last line follows from Case I because k is square free.
Similarly, we have $4\mathrm{F}(kq^2) = 4\mathrm{F}_p(kq^2) + 4\mathrm{F}_p(k)$. Applying Theorem 5.2.2 then yields $3\mathrm{G}_p(kq^2) = 4\mathrm{F}_p(kq^2)$ and our base case is complete.
Inductive Hypothesis:
Let $n = kq^2$ have M distinct divisors of q and assume $3\mathrm{G}_p(kd^2) = 4\mathrm{F}_p(kd^2)$ for all divisors d q.
Now suppose $n = kq^2$ is such that q has $M + 1$ distinct divisors.
Then $\frac{kq^2}{d^2}$ has less than or equal to M distinct divisors provided $d \neq 1$.
Thus we have

$$\begin{aligned} 3\mathrm{G}(kq^2) &= 3\mathrm{G}_p(kq^2) + \sum_{\substack{d|q \\ d\neq 1}} 3\mathrm{G}_p\left(\frac{kq^2}{d^2}\right) \\ &= 3\mathrm{G}(kq^2) + \sum_{\substack{d|q \\ d\neq 1}} 4\mathrm{F}_p\left(\frac{kq^2}{d^2}\right) \text{ by our inductive hypothesis.} \end{aligned}$$

Similarly, we have $4\mathrm{F}(kq^2) = 4\mathrm{F}_p(kq^2) + \sum_{\substack{d|q \\ d\neq 1}} 4\mathrm{F}_p\left(\frac{kq^2}{d^2}\right)$.
Then applying Theorem 5.2.2 we get $3\mathrm{G}_p(kq^2) = 4\mathrm{F}_p(kq^2)$.
Hence by induction on the number of divisors of q we have $3\mathrm{G}_p(kq^2) = 4\mathrm{F}_p(kq^2)$, where $n = kq^2 \equiv 3 \bmod 8$.
Consequently, combining the results of Cases I and II we have $3\mathrm{G}_p(n) = 4\mathrm{F}_p(n)$ when $n \equiv 3 \bmod 8$. □

Corollary 5.4.16.
Let n be a positive integer such that $n \equiv 3 \bmod 8$, then

$$3h(-n) = \begin{cases} 3\mathrm{F}_p(n) & \text{if } n = 3 \\ \mathrm{F}_p(n) & \text{otherwise.} \end{cases}$$

Proof.
Let n be a positive integer such that $n \equiv 3 \bmod 8$ then we have

$$\begin{aligned} 3h(-n) &= \begin{cases} 9\mathrm{G}_p(n) - 9\mathrm{F}_p(n) & \text{if } n = 3 \\ 3\mathrm{G}_p(n) - 3\mathrm{F}_p(n) & \text{otherwise} \end{cases} \quad \text{by Corollary 5.4.14} \\ &= \begin{cases} 12\mathrm{F}_p(n) - 9\mathrm{F}_p(n) & \text{if } n = 3 \\ 4\mathrm{F}_p(n) - 3\mathrm{F}_p(n) & \text{otherwise} \end{cases} \quad \text{by Lemma 5.4.15} \end{aligned}$$

$$= \begin{cases} 3\mathrm{F}_p(n) & \text{if } n = 3 \\ \mathrm{F}_p(n) & \text{otherwise.} \end{cases}$$

□

Corollary 5.4.17.
Let n be a positive integer such that $n \equiv 3 \bmod 8$, then

$$R_3(n) = \begin{cases} 8h(-n) & \textit{if } n = 3 \\ 24h(-n) & \textit{otherwise.} \end{cases}$$

Proof.
Let $n \equiv 3 \bmod 8$ and apply Lemma 5.4.7 and Corollary 5.4.16 to get:

$$\begin{aligned} R_3(n) &= \frac{4}{3} \cdot 6\mathrm{F}_p(n) \\ &= \begin{cases} \frac{4}{3} \cdot 2 \cdot 3\mathrm{F}_p(n) & \text{if } n = 3 \\ \frac{4}{3} \cdot 6 \cdot \mathrm{F}_p(n) & \text{otherwise} \end{cases} \\ &= \begin{cases} \frac{4}{3} \cdot 2 \cdot 3h(-n) & \text{if } n = 3 \\ \frac{4}{3} \cdot 6 \cdot 3h(-n) & \text{otherwise} \end{cases} \\ &= \begin{cases} 8h(-n) & \text{if } n = 3 \\ 24h(-n) & \text{otherwise.} \end{cases} \end{aligned}$$

□

We now provide the proof of Gauss' Theorem (Theorem 5.4.1).

Proof. Let n be a positive integer such that $4 \nmid n$, then applying Lemma 5.4.7 in conjunction with Corollaries 5.4.10, 5.4.12 and 5.4.17 yields:

$$R_3(n) = \begin{cases} 6h(-4 \cdot n) & \text{if } n = 1 \\ 12h(-4 \cdot n) & \text{if } n \equiv 1, 2 \bmod 4, n \neq 1 \\ 8h(-n) & \text{if } n = 3 \\ 24h(-n) & \text{if } n \equiv 3 \bmod 8, n \neq 3 \\ 0 & \text{if } n \equiv 7 \bmod 8. \end{cases}$$

Letting $\delta_n = 1$ for all positive integers n except for $n = 1, 3$, where $\delta_1 = \frac{1}{2}$ and $\delta_3 = \frac{1}{3}$ then yields

$$\begin{aligned} R_3(n) &= \begin{cases} 12 \cdot \delta_1 h(-4 \cdot n) & \text{if } n = 1 \\ 12\delta_n h(-4 \cdot n) & \text{if } n \equiv 1, 2 \bmod 4, n \neq 1 \\ 24 \cdot \delta_3 h(-n) & \text{if } n = 3 \\ 24\delta_n h(-n) & \text{if } n \equiv 3 \bmod 8, n \neq 3 \\ 0 & \text{if } n \equiv 7 \bmod 8. \end{cases} \\ &= \begin{cases} 12\delta_n h(-4n) & \text{if } n \equiv 1, 2, 5 \text{ or } 6 \bmod 8 \\ 24\delta_n h(-n) & \text{if } n \equiv 3 \bmod 8. \end{cases} \end{aligned}$$

□

It remains for completeness to discuss the situation when $n \equiv 7 \bmod 8$ or $4 \mid n$.

Lemma 5.4.18.
Let n be a positive integer such that $4 \mid n$. Then there are no primitive representations of n as a sum of three squares, that is, $R_3(n) = 0$.

Proof.
Let n be a positive integer such that $4 \mid n$ and write n as a sum of three squares. Thus $x^2 + y^2 + z^2 = n \equiv 0 \bmod 4$.
Since the squares mod4 are $0, 1$, it is straightforward to verify that we must have $x^2 \equiv y^2 \equiv z^2 \equiv 0 \bmod 4$. Consequently, we have $x \equiv y \equiv z \equiv 0 \bmod 2$ and thus $\gcd(x, y, z) > 1$ so the representation cannot be primitive.
Hence $R_3(n) = 0$ when $4|n$. □

Corollary 5.4.19.
Let n and k be positive integers such that $4^k \mid n$ but $4^{k+1} \nmid n$. Then $r_3(n) = r_3\left(\frac{n}{4^k}\right)$.

Proof.
Let n and k be as above and let $x^2 + y^2 + z^2 = \frac{n}{4^k}$. Then $(2^k x)^2 + (2^k y)^2 + (2^k z)^2 = n$ is a representation of n as a sum of three integer squares. Thus $r_3(n) \geqslant r_3\left(\frac{n}{4^k}\right)$.
Now let $a^2 + b^2 + c^2 = n \equiv 0 \bmod 4^k$. In particular, $4 \mid n$ and so by Lemma 5.4.18 we know $2|a$, $2|b$ and $2|c$. Thus $\left(\frac{a}{2}\right)^2 + \left(\frac{b}{2}\right)^2 + \left(\frac{c}{2}\right)^2 = \frac{n}{4}$ is a representation of the positive integer $\frac{n}{4}$ as a sum of three integer squares. Repeating this process a total of k times yields
$\left(\frac{a}{2^k}\right)^2 + \left(\frac{b}{2^k}\right)^2 + \left(\frac{c}{2^k}\right)^2 = \frac{n}{4^k}$ and thus $r_3\left(\frac{n}{4^k}\right) \geqslant r_3(n)$.
Hence $r_3(n) = r_3\left(\frac{n}{4^k}\right)$. □

Lemma 5.4.20.
Let n be a positive integer such that $n \equiv 7 \bmod 8$. Then $r_3(n) = R_3(n) = 0$.

Proof.
Since the squares mod8 are $0, 1, 4$, it is straightforward to verify that $x^2 + y^2 + z^2 \equiv 0, 1, 2, 3, 4, 5\text{or}6 \bmod 8$.
Thus there are no representations of n as a sum of three squares and thus $r_3(n) = R_3(n) = 0$. □

An interesting lemma follows immediately from Gauss' Theorem (5.4.1)

Lemma 5.4.21.
Let n be a positive integer such that $4 \nmid n$ and $n \not\equiv 7 \bmod 8$. Then $R_3(n) \geqslant 1$.

Proof.
Let n be as stated and observe the proper class number, $h(-n)$, satisfies $h(-n) \geqslant 1$. This is because the binary quadratic form $x^2 + ny^2$ always exists. Then applying Gauss' Theorem (5.4.1) immediately yields $R_3(n) \geqslant 1$. □

In other words for any positive integer n such that $4 \nmid n$ and $n \not\equiv 7 \bmod 8$, there is always a way to write $n = x^2 + y^2 + z^2$ where $\gcd(x, y, z) = 1$.
We note that our results do not present a way for finding this representation though. Our next lemma is a stepping stone result to deriving another well-known result due to Gauss.

Lemma 5.4.22.
Let $n > 3$ be a positive integer such that $n \equiv 3 \bmod 8$. Then $\mathrm{F}_p(n) = h(-4n)$.

Proof.
Let n be as above and consider the set counted by $\mathrm{F}_p(n)$. This set consists of a unique representative for every proper equivalence class of primitive ($\gcd(a, b, c) = 1$) binary quadratic forms $ax^2 + 2bxy + cy^2$ where $n = ac - b^2$. We may choose to view these as primitive binary quadratic forms $Ax^2 + Bxy + Cy^2$ with $4AC - B^2 = 4n$. This is done by letting $A = a$, $B = 2b$ and $C = c$. Thus $4AC - B^2 = 4ac - (2b)^2 = 4(ac - b^2) = 4n$. Since $\gcd(a, b, c) = 1$ it is clear that $\gcd(A, B, C) = 1$. Thus $|\mathrm{F}_p(n)| \leqslant h(-4n)$.
Now let (A, B, C) be any primitive binary quadratic form that is counted by $h(-4n)$. We will show its proper equivalence class is in fact counted by $\mathrm{F}_p(n)$. We have $4AC - B^2 = 4n$ and thus $B^2 = 4(AC - n)$, implying $2 \mid B$. We write $B = 2b$ and thus we have the binary quadratic form $Ax^2 + 2bxy + Cy^2$. This satisfies $ac - b^2 = AC - \left(\frac{B}{2}\right)^2 = \frac{1}{4}(4AC - B^2) = \frac{1}{4}4n = n$. Thus the proper equivalence class of this binary quadratic form is a candidate to be counted by $\mathrm{F}_p(n)$. To do so, it remains to show at least one of A, C is odd and $\gcd(A, b, C) = 1$.
We know $\gcd(A, B, C) = 1$ and $B = 2b$, thus $\gcd(A, 2b, C) = 1$ and so at least one of A, C must be odd. Further, let $d = \gcd(A, b, C)$ then $d \mid \gcd(A, 2b, C) = 1$ and therefore $d = 1$.
Hence the proper equivalence class of the binary quadratic form $Ax^2 + Bxy + Cy^2$ is counted by $\mathrm{F}_p(n)$ and so $h(-4n) \leqslant \mathrm{F}_p(n)$.
Consequently we have $\mathrm{F}_p(n) = h(-4n)$. □

The following corollary is mentioned in a paragraph at the bottom of page 42 in [Gr1985] as being known to Gauss.

Corollary 5.4.23.
Let n be a positive integer such that $n \equiv 3 \bmod 8$. Then $h(-4n) = h(-n)$ if $n = 3$, otherwise $h(-4n) = 3h(-n)$.

Proof.
We first deal with the case $n = 3$. It is straightforward to verify the only primitive reduced binary quadratic form which satisfies $b^2 - 4ac = -3$ is the form $x^2 + xy + y^2$. Thus $h(-3) = 1$.
Similarly, we may verify the only primitive reduced binary quadratic form satisfying $b^2 - 4ac = -12$ is the form $x^2 + 3y^2$. Thus $h(-12) = 1 = h(-3)$.
Now let $n > 3$ be such that $n \equiv 3 \bmod 8$. By Lemma 5.4.22 we have $\mathrm{F}_p(n) = h(-4n)$ and by Corollary 5.4.16 we have $\mathrm{F}_p(n) = 3h(-n)$. Hence $h(-4n) = 3h(-n)$ when $n > 3$, $n \equiv 3 \bmod 8$. □

Notes on Section 5.4

In his book, [Gr1985], Grosswald leaves the reader an exercise (problem 6, [Gr1985, p. 65]) to show Gauss' Theorem may be stated as $R_3(n) = 24\mathrm{F}(n) - 12\mathrm{G}(n)$, and thus prove Kronecker's result. It is clear Grosswald was aware of Kronecker's work, however he failed to note Kronecker did not require primitivity in his work. Whereas Grosswald requires primitivity in his book. This is why we introduced the subscripts F_p and G_p before deriving the connection between Gauss' Theorem and Kronecker's result.
Further, one should note Grosswald cites Kronecker's earlier paper [Kr1860], which contained an error that was later stated correctly in [Kr1897]. This error claimed $3\mathrm{G}(n) = 4\mathrm{F}(n)$ if $n \equiv 3 \bmod 8$, except if $n = 3(2m+1)^2$ when $3\mathrm{G}(n) = 4\mathrm{F}(n) + 2$. The correct statement of the result is given in Theorem 5.2.2. Consequently, the hint Grosswald gives the reader is incorrect.

Lastly, one should note Grosswald acknowledged the level of difficulty required to prove some of Kronecker's stated relationships. It is unclear whether Grosswald supplied any proofs himself.

Appendices

Here we present several appendices that provide a connection between Kronecker's method for determining the number of representations of an integer as a sum of three squares (see [Kr1897]), and the method given by Weil for the same problem in the 3 mod 8 case (see [We1974]).

A.1 Ireland & Rosen Representations as Sums of Two Squares

In this appendix we give a method to calculate the number of representations of a positive integer as a sum of two squares. This argument is an expanded version of the exposition given in Chapter 17, §6 [IR1990, p. 278-280].

We begin with an important definition, which shall be repeatedly used within Appendices A.1, A.2, A.3, A.4 and A.5. The notation introduced here is due to Weil [We1974, p. 216]

Definition A.1.1.
Let $i \in \{2, 3, 4\}$, $m \in \mathbb{Z}_{>0}$ and consider the equation:

$$x_1^2 + x_2^2 + \ldots + x_i^2 = m, \tag{A.1}$$

where $x_h \in \mathbb{Z}_{>0}$, $x_h \equiv 1 \bmod 2$ and $1 \leqslant h \leqslant i$.
Define $N_i(m)$ to be the number of solutions $(x_1, x_2, \ldots, x_i)$ to this equation under these assumptions.

Observation A.1.2.
Clearly, $N_i(m) = 0$ if $m = 0$. Recall that any odd integer k satisfies $k^2 \equiv 1 \bmod 8$. Thus we require $m \equiv i \bmod 8$ also for a solution to exist.

Definition A.1.3.
Define $r_i(m)$ to be the number of solutions to the equation $m = x_1^2 + \cdots + x_i^2$, where $m \in \mathbb{Z}_{>0}$, $x_h \in \mathbb{Z}$ for $1 \leqslant h \leqslant i$.

Definition A.1.4.
An arithmetic function is a real or complex valued function that is defined on the positive integers.

Definition A.1.5.
The formal Dirichlet series is defined as $\sum_{n=1}^{\infty} \frac{a_n}{n^s}$, where $s > 1$. This is an example of an arithmetic function.

Definition A.1.6.
Let f and g be arithmetic functions. Define their Dirichlet product (or Dirichlet convolution) to be $\sum_{d|n} f(d) g\left(\frac{n}{d}\right)$.

Definition A.1.7.
Define $\chi(n) = \begin{cases} 1, & \text{if } n \equiv 1 \bmod 4 \\ -1, & \text{if } n \equiv 3 \bmod 4 \\ 0, & \text{if } n \equiv 0 \bmod 2. \end{cases}$

Definition A.1.8.
Define the zeta function as $\zeta(s) = \prod_p \frac{1}{1-\frac{1}{p^s}} = \sum_{n=1}^{\infty} \frac{1}{n^s}$.

Theorem A.1.9.
Let $m \in \mathbb{Z}_{>0}$. The number of integral solutions (x_1, x_2) to the equation $x_1^2 + x_2^2 = m$ such that $x_1 > 0$, $x_2 \geqslant 0$, is given by $\sum_{d|m} \chi(d)$.

The proof presented here appears in Ireland & Rosen, [IR1990, p. 279].

Proof.
Consider the ring of Gaussian integers, $\mathbb{Z}[i]$. Since the units of this ring are $\pm 1, \pm i$, each non-zero $\alpha \in \mathbb{Z}[i]$ has a unique associate $x + iy$, $x > 0$, $y \geqslant 0$. Recalling that $\mathbb{Z}[i]$ is a principal ideal domain and we have a norm $N(x+iy) = x^2 + y^2$, implies that the number of solutions is the number of ideals (α) where $N(\alpha) = m$.
Denote this number by a_m
Lastly, recall that every such α may be decomposed into a product of irreducibles, which are given by $1+i$, π and q. Here π satisfies $N(\pi) = p \equiv 1 \bmod 4$, p prime, and q is any rational prime congruent to 3 modulo 4. Now we use the formal Dirichlet series defined by $\{a_m\}$ to get $\sum_{m=1}^{\infty} \frac{a_m}{m^s} = \prod_{(\gamma)} \left(\frac{1}{1-\frac{1}{N(\gamma)^s}} \right)$.
Here the product is over all unassociated irreducibles in $\mathbb{Z}[i]$.
This product may then be expressed in terms of three products, one for each type of irreducible in $\mathbb{Z}[i]$. Since $N(1+i) = 2$ and $N(\pi) = N(\bar{\pi}) = p$, we get the right hand side equals

$$\left(\frac{1}{1-\frac{1}{2^s}} \right) \prod_{p \equiv 1 \bmod 4} \left(\frac{1}{1-\frac{1}{p^s}} \right)^2 \prod_{q \equiv 3 \bmod 4} \left(\frac{1}{1-\frac{1}{q^{2s}}} \right).$$

Now notice $1 - \frac{1}{q^{2s}} = (1-\frac{1}{q^s})(1+\frac{1}{q^s})$. Then applying the definition of the zeta function (Definition A.1.8), we see the right hand side equals:

$$\zeta(s) \prod_{p \equiv 1 \bmod 4} \left(\frac{1}{1-\frac{1}{p^s}} \right) \prod_{q \equiv 3 \bmod 4} \left(\frac{1}{1+\frac{1}{q^s}} \right).$$

Applying Definition A.1.7 to this yields:

$$\zeta(s) \prod_p \frac{1}{1-\frac{\chi(p)}{p^s}}.$$

Since χ is multiplicative, it follows that this may be rewritten as

$$\zeta(s)\sum_{m=1}^{\infty}\frac{\chi(m)}{m^s}.$$

Hence we have $\displaystyle\sum_{m=1}^{\infty}\frac{a_m}{m^s}=\left(\sum_{m=1}^{\infty}\frac{1}{m^s}\right)\left(\sum_{m=1}^{\infty}\frac{\chi(m)}{m^s}\right)$.
Thus to complete the proof we need to calculate the coefficient of $\frac{1}{m^s}$ on the right hand side. Since each of the sums in the product is an arithmetic function, we may apply Dirichlet convolution (see Definition A.1.6) with $f(m)=\frac{1}{m^s}$ and $g(m)=\frac{\chi(m)}{m^s}$ to get

$$\sum_{m=1}^{\infty}\frac{a_m}{m^s}=\sum_{m=1}^{\infty}\sum_{d|m}\frac{\chi\left(\frac{m}{d}\right)}{m^s}.$$

Hence $a_m=\displaystyle\sum_{d|m}\chi\left(\frac{m}{d}\right)=\sum_{d|m}\chi(d)$ which completes the proof. □

Corollary A.1.10.
The number of solutions $(x_1,x_2)\in\mathbb{Z}\times\mathbb{Z}$ *to* $x_1^2+x_2^2=m$ *is given by* $r_2(m)=4\displaystyle\sum_{d|m}\chi(d)$.

Proof.
Observe each term in Equation (A.1) is squared and we may partition $(\mathbb{Z}\times\mathbb{Z})\setminus(0,0)$ into a disjoint union of the following four sets:

$$\{(x_1,x_2):x_1>0,x_2\geqslant 0\},$$
$$\{(x_1,x_2):x_1\leqslant 0,x_2>0\},$$
$$\{(x_1,x_2):x_1<0,x_2\leqslant 0\},$$
$$\{(x_1,x_2):x_1\geqslant 0,x_2<0\}.$$

Hence by the symmetry between x_1 and x_2 the result follows from Theorem A.1.9. □

Corollary A.1.11. *Let* m *be a positive odd integer. The number of integral solutions* (x_1,x_2), $x_1>0$, $x_2>0$ *to* $x_1^2+x_2^2=2m$ *is* $\displaystyle\sum_{d|m}\chi(d)$.

Proof.
Since m is odd, $2m\equiv 2 \bmod 4$ which, implies that x_2 cannot equal zero. By Theorem A.1.9, the number of solutions is given by $\displaystyle\sum_{d|2m}\chi(d)$. However, the divisors of $2m$ are the divisors $\hat{d}$ of m and $2\hat{d}$. Since $\chi(2\hat{d})=0$, it follows that the number of integral solutions is given by $\displaystyle\sum_{d|m}\chi(d)$. □

We now show that it is sufficient to know $N_2(m)$ in order to know $r_2(m)$ for all values of m.

Observation A.1.12.
Recall any odd number when squared is congruent to 1 mod. 8. Also, any even number when squared is congruent to either 0 or 4 mod. 8. It follows that any sum of 2 squares is necessarily congruent to one of $0, 1, 2, 4$ or 5 mod. 8.

To prove our claim, we will need the following two lemmas.

Lemma A.1.13.
Let $k \in \mathbb{Z}_{>0}$ then $r_2(k) = r_2(4k)$.

Proof.
Assume $k = x^2 + y^2$, then $4k = 4(x^2 + y^2) = (2x)^2 + (2y)^2$. Define the map

$$\begin{aligned} \phi : \{\text{solutions to } x^2 + y^2 = k\} &\longrightarrow \{\text{solutions to } x^2 + y^2 = 4k\} \\ (x, y) &\longmapsto (2x, 2y). \end{aligned}$$

We will show ϕ is a bijection. Assume $\phi(x, y) = \phi(u, v)$, then $(2x, 2y) = (2u, 2v)$. Hence $x = u$ and $y = v$, so ϕ is injective.
Let $(\hat{x}, \hat{y})$ be a solution to $x^2 + y^2 = 4k$ for some $k \in \mathbb{Z}_{>0}$. Then the left hand side is divisible by four and so we have $\left(\frac{\hat{x}}{2}\right)^2 + \left(\frac{\hat{y}}{2}\right)^2 = k$. Letting $\hat{x} = 2\bar{x}$ and $\hat{y} = 2\bar{y}$. That is, $\bar{x}^2 + \bar{y}^2 = k$, $\bar{x}, \bar{y} \in \mathbb{Z}_{>0}$. Hence ϕ is a surjection and thus a bijection.
Thus $r_2(k) = r_2(4k)$. □

Lemma A.1.14.
Let $k \in \mathbb{Z}_{>0}$ then $r_2(4k + 1) = r_2(8k + 2)$.

Proof.
Suppose that $4k+1 = x^2+y^2$, then $8k+2 = 2(4k+1) = 2(x^2+y^2) = (x+y)^2+(x-y)^2$. Define the map

$$\begin{aligned} \pi : A = \{\text{solutions to } x^2 + y^2 = 4k + 1\} &\longrightarrow \{\text{solutions to } x^2 + y^2 = 8k + 2\} \\ (x, y) &\longmapsto (x + y, x - y). \end{aligned}$$

We shall show this is a bijection.
Suppose $\pi(x, y) = \phi(u, v)$, then $(x+y, x-y) = (u+v, u-v)$. Thus $x+y = u+v$ and $x - y = u - v$. Adding these two equations yields $2x = 2u$, i.e. $x = u$. Subtracting them yields $2y = 2v$, i.e. $y = v$. Hence π is injective.
Next, assume $x^2 + y^2 = 8k + 2$. Consider the equations $\hat{x} + \hat{y} = x$ and $\hat{x} - \hat{y} = y$, where $\hat{x}, \hat{y} \in \mathbb{Z}$. Then $2\hat{x} = x+y$ and $2\hat{y} = x-y$, it follows that $\hat{x} = \frac{x+y}{2}$ and $\hat{y} = \frac{x-y}{2}$. Therefore we have:

$$\hat{x}^2 + \hat{y}^2 = \left(\frac{x + y}{2}\right)^2 + \left(\frac{x - y}{2}\right)^2$$

$$= \frac{1}{4}2(x^2 + y^2)$$
$$= \frac{1}{2}(8k + 2)$$
$$= 4k + 1.$$

Therefore $(\hat{x}, \hat{y}) \in A$ is such that $\pi(\hat{x}, \hat{y}) = (x, y)$. Thus, π is a surjection and hence π is a bijection.
Thus, $r_2(4k + 1) = r_2(8k + 2)$. □

Lemma A.1.15.
Let $m \in \mathbb{Z}_{>0}$, then $r_2(m)$ is completely determined once we know $N_2(m)$.

Proof.
Let $m \in \mathbb{Z}_{>0}$ be arbitrary. By Lemma A.1.13 we may divide m by 4 as many times as possible without changing the result. Hence we may assume m is not divisible by 4. Now consider $m \bmod 8$. By Observation A.1.12 it follows that $r_2(m) = 0$ if m is congruent to 3, 6 or 7 modulo 8. Further, observe that m cannot be congruent to 0 or 4 modulo 8 as we assumed m is not divisible by 4. Hence we may apply Lemma A.1.14 and Corollary A.1.10 to see that $r_2(m)$ is completely determined by $N_2(m)$. □

Lemma A.1.16.
If $m \in \mathbb{Z}_{>0}$ and $m \equiv 2 \bmod 4$ then $N_2(m) = \sum_{a|\frac{m}{2}} \chi(a)$.

Proof.
Observe $m \equiv 2 \bmod 4$ implies that $x_2^2 > 0$. Recalling Definition A.1 and using Theorem A.1.9 we have $N_2(m) = \sum_{d|m} \chi(d)$. Now write $m = 2\hat{d}$ since m is divisible by two.
Thus, $N_2(m) = \sum_{d|2\hat{d}} \chi(d) = \sum_{d|\hat{d}} \chi(d)$, as $\chi(2d) = 0$ for all d.
But this is equivalent to $N_2(m) = \sum_{a|\frac{m}{2}} \chi(a)$. □

Observation A.1.17.
In Observation A.1.2 we deduced $m \equiv i \bmod 8$ in order for $N_i(m) > 0$. However, in Lemma A.1.16 we assume $m \equiv 2 \bmod 4$. This does not give a contradiction for the following reason. If $m \equiv 2 \bmod 4$ and $m \not\equiv 2 \bmod 8$, then $m \equiv 6 \bmod 8$. Thus $m = 2\hat{m} = 2(4k + 3)$ for some $k \in \mathbb{Z}_{>0}$. Hence $\hat{m}$ is odd and so all divisors of $\hat{m}$ are odd. Recall that if $l|\hat{m}$ and $l \equiv 3 \bmod 4$ then the complementary divisor to l is of the form $4p + 1$. Consequently for every divisor l of $\frac{m}{2}$ such that $l \equiv 3 \bmod 4$ there exists a unique divisor q of $\frac{m}{2}$ such that $q \equiv 1 \bmod 4$. Since $\chi(l) = -1$ and $\chi(q) = 1$, we see that $\sum_{a|\frac{m}{2}} \chi(a) = 0$ when $m \equiv 6 \bmod 8$.

Lemma A.1.18.
If $n \equiv 1 \bmod 2$ *then* $\chi(n) = (-1)^{\frac{n-1}{2}}$.

Proof.
Since $n \equiv 1 \bmod 2$, $\frac{n-1}{2}$ is an integer.
If $n \equiv 1 \bmod 4$ then $\frac{n-1}{2} \equiv 0 \bmod 2$ and so $\chi(n) = 1 = (-1)^{\frac{n-1}{2}}$.
If $n \equiv 3 \bmod 4$ then $\frac{n-1}{2} \equiv 1 \bmod 2$ and so $\chi(n) = -1 = (-1)^{\frac{n-1}{2}}$. □

The following lemma will prove useful later on.

Lemma A.1.19. $\chi(n)\chi(n') = (-1)^{\frac{n-n'}{2}}$ *whenever* $n \equiv n' \equiv 1 \bmod 2$, $n > 0$, $n' > 0$.

Proof.
Let $n > 0$, $n' > 0$ and $n \equiv n' \equiv 1 \bmod 2$. Applying Lemma A.1.18 gives:

$$\begin{aligned}
\chi(n)\chi(n') &= (-1)^{\frac{n-1}{2}+\frac{n'-1}{2}} \\
&= (-1)^{\frac{n+n'-2}{2}} \\
&= (-1)^{\frac{n+n'}{2}-1} \\
&= (-1)^{\frac{n-n'}{2}+1-1} \text{ as } \tfrac{n-n'}{2} \not\equiv \tfrac{n+n'}{2} \text{ as they differ by } n' \text{ which is odd} \\
&= (-1)^{\frac{n-n'}{2}}.
\end{aligned}$$

□

A.2 Ireland & Rosen Representations as Sums of Four Squares

In this appendix we give an argument for determining the number of representations of an integer as a sum of four squares. This argument is based upon [IR1990, p. 282-284] and exercises 16-22 [IR1990, p. 295-296].

The reader will find it useful to recall Lemma 3.4.13 before proceeding.

Proposition A.2.1.
Let n *be a positive integer such that* $n \equiv 4 \bmod 8$. *The number of integral solutions* (x, y, z, w), $x, y, z, w > 0$ *and all odd, to the equation* $n = x^2 + y^2 + z^2 + w^2$ *is*

$$\sum_{\substack{d|n \\ d \text{ odd} \\ d>0}} d.$$

An immediate corollary of this is the following:

Corollary A.2.2.
Let n *be a positive integer,* $n \equiv 4 \bmod 8$. *The number of integral solutions* (x, y, z, w), $x, y, z, w \in \mathbb{Z}$ *and all odd, to the equation* $x^2 + y^2 + z^2 + w^2 = n$ *is given by*

$$16 \sum_{d|n} d.$$

Proof.
Since each of x, y, z, w is odd, we may get a new distinct solution by changing the sign of each coordinate independently. Thus there are 2^4 solutions obtainable from a single solution (x, y, z, w).
Hence there are $16 \sum_{d|n} d$ solutions in this case. □

In order to prove Proposition A.2.1 we will need several lemmas.

Observation A.2.3.
Using Definition A.1.1, observe $N_4(n)$ denotes the number of integral solutions to the problem given in Proposition A.2.1.

Lemma A.2.4.
Let n be a positive integer such that $n \equiv 4 \bmod 8$. Write $n = 2m$ and observe $m \equiv 2 \bmod 4$. Then $N_4(n)$ is the number of solutions (x, y, z, w, u, v), where x, y, z, w, u, v are all odd and positive, to the system of Diophantine equations:

$$\begin{aligned} x^2 + y^2 &= 2u \\ z^2 + w^2 &= 2v \\ u + v &= m \end{aligned}$$

Proof.
Let $n \equiv 4 \bmod 8$ and write $n = 2m$ where $m \equiv 2 \bmod 4$.
Let $S = \left\{ (x, y, z, w) \;\middle|\; \begin{array}{l} x^2 + y^2 + z^2 + w^2 = n, \quad x, y, z, w \equiv 1 \bmod 2 \\ x, y, z, w \in \mathbb{Z}_{>0} \end{array} \right\}$ and
$T = \left\{ (x, y, z, w, u, v) \;\middle|\; \begin{array}{ll} x^2 + y^2 = 2u, & z^2 + w^2 = 2v, u + v = m \\ x, y, z, w \in \mathbb{Z}_{>0}, & x \equiv y \equiv z \equiv w \equiv u \equiv v \equiv 1 \bmod 2 \end{array} \right\}$.
By definition we have $N_4(n) = |S|$. We will show the following map, ϕ, is a bijection. Define

$$\begin{aligned} \phi : S &\longrightarrow T \\ (x, y, z, w) &\longmapsto (x, y, z, w, \frac{x^2 + y^2}{2}, \frac{z^2 + w^2}{2}) = (x, y, z, w, u, v). \end{aligned}$$

Well-defined: It is sufficient to show $u + v = m$ and $x^2 + y^2 = 2u$. Let $(x, y, z, w) \in S$ then we have $n = x^2 + y^2 + z^2 + w^2 = 2u + 2v = 2(u + v)$ and so $u + v = m$. Further, $x \equiv y \equiv 1 \bmod 2$ implies $x^2 \equiv y^2 \equiv 1 \bmod 4$ and thus $x^2 + y^2 \equiv 2 \bmod 4$. Thus $u = \frac{x^2+y^2}{2} \equiv 1 \bmod 2$. A similar calculation shows $v \equiv 1 \bmod 2$. Hence the map ϕ is well-defined.
Injectivity: Assume $\phi(x, y, z, w) = \phi(a, b, c, d)$ then we have
$(x, y, z, w, u, v) = (a, b, c, d, \hat{u}, \hat{v})$. From this we have $x = a, y = b, z = c$ and $w = d$, as well as $2u = x^2 + y^2 = a^2 + b^2 = 2\hat{u}$, $2v = z^2 + w^2 = c^2 + d^2 = 2\hat{v}$, thus $u = \hat{u}$ and $v = \hat{v}$. Therefore the map ϕ is injective.
Surjectivity: Let $(x, y, z, w, u, v) \in T$ be arbitrary, then $x^2 + y^2 + z^2 + w^2 = 2u + 2v = 2(u + v) = 2m = n$ and the remaining properties are straightforward to verify. Hence

(x, y, z, w) lies in S and maps onto (x, y, z, w, u, v). So ϕ is a bijection and we have the desired result. □

Lemma A.2.5.
$N_4(n) = \sum \chi(de) = \sum (-1)^{\frac{de-1}{2}}$, where the sum is over all solutions (d, e, s, t) (all positive odd integers) such that $m = ds + et$.

Proof.
By the previous lemma we will look at counting over all $u + v = m$, u, v odd. Note that $m \equiv 2 \bmod 4$ implies both u and v are odd. By Corollary A.1.11, we have the number of solutions to $x^2 + y^2 = 2u$ (x, y both odd and positive) is equal to the number of solutions to $x^2 + y^2 = u$. A similar statement holds for $z^2 + w^2 = 2v$.
By Lemma A.1.9 the equation $x^2 + y^2 = u$ has $\displaystyle\sum_{d|u} \chi(d)$ solutions and likewise there are $\displaystyle\sum_{e|v} \chi(e)$ solutions to $z^2 + w^2 = v$.
Further these solution pairs are independent, so by fixing a solution to $x^2 + y^2 = u$, we get a new solution to the problem posed in Proposition A.2.1 each time as we run through all the solutions to $z^2 + w^2 = v$.
So in total there are $\chi(d_1) \left(\displaystyle\sum_{e|v} \chi(e) \right) + \chi(d_2) \left(\sum_{e|v} \chi(e) \right) + \cdots + \chi(d_n) \left(\sum_{e|v} \chi(e) \right)$, where $d_1, \cdots, d_n$ are all the divisors of u.
Hence we have $\left(\sum_{e|v} \chi(e) \right) \left(\sum_{d|u} \chi(d) \right)$ solutions to the problem for fixed u and v.
We may rewrite this product of summations as $\displaystyle\sum_{\substack{d|u \\ e|v}} \chi(d)\chi(e)$.

Thus we see that

$$N_4(n) = \sum_{\substack{u,v \\ u+v=m}} \left(\sum_{\substack{d|u \\ e|v}} \chi(d)\chi(e) \right). \tag{A.2}$$

Since $d \mid u$ and $e \mid v$ we may write $u = ds$, and $v = et$. Further because each associated divisor to d and e is unique, it follows that there is a one-to-one correspondence between (d, e, t, s), d, e, t, s positive and odd, $ds + et = m$ and the terms in Equation (A.2).

Since χ is multiplicative, it follows that $N_4(n) = \displaystyle\sum_{\substack{u,v \\ u+v=m}} \left(\sum_{\substack{d|u \\ e|v}} \chi(de) \right) =$

$\sum \chi(de)$, where the last sum is over d, e, t, s positive and odd such that $ds + et = m$. This proves the first equality.
Since $d \equiv e \equiv 1 \bmod 2$ we have $de \equiv 1 \bmod 2$ and so we apply Lemma A.1.18to see $\chi(de) = (-1)^{\frac{de-1}{2}}$. This supplies the second equality. □

We now consider $\sum \chi(de)$, where the sum is over all (d, e, t, s) positive and odd. First focus on the terms where $d = e$, so $m = d(s+t)$ and therefore d is necessarily an odd divisor of m. Now consider $s + t = \frac{m}{d} \in \mathbb{Z}_{>0}$. If we run through s from 1 to $\frac{m}{d}$ then t is uniquely determined in each case. Note that $\frac{m}{d}$ is even and so either both s and t are both odd or both even. Hence there are $\frac{m}{2d}$ pairs (s, t) that satisfy $s + t = \frac{m}{d}$, s, t positive and odd. Each such solution contributes 1 as $\chi(d^2) = 1$ because d is odd. Thus we get $\frac{m}{2d}$ solutions for each positive odd divisor d of m.

Hence there are $\sum_{d|m} \frac{m}{2d}$ solutions in total. Recall that $m \equiv 2 \bmod 4$ and write $m = 2q$, where $q \equiv 1 \bmod 2$. Then since d is odd, $d|m$ implies $d|q$ and so $q = dr$ for some $r \in \mathbb{N}$.
So our sum becomes $\sum_{d|m} \frac{2q}{2d} = \sum_{d|m} r$, where $m = 2dr$. But it is then clear this is equivalent to $\sum_{d|m} d$.

The proof of Proposition A.2.1 will be complete once we show $\sum \chi(de) = 0$ for (d, e, t, s) positive, odd and $d \neq e$. We observe we may pair (d, e, t, s) with (e, d, s, t) to see that it is sufficient to show $\sum \chi(de) = 0$ for $d > e$.

Lemma A.2.6.
Consider the set

$$J = \{(d, e, t, s) \in \mathbb{Z}^4_{>0} \,|\, m = ds + et,\ d \equiv e \equiv t \equiv s \equiv 1 \bmod 2, m \equiv 2 \bmod 4\}$$

and define the map

$$\begin{aligned} \phi : J &\longrightarrow J \\ (d, e, t, s) &\longmapsto (e, d, s, t). \end{aligned}$$

Then the map ϕ is a bijection.

Proof.
The map ϕ is well-defined since we re-ordered the pairs (d, e) and (s, t) in a manner which preserves $et + ds = m$. Observe that $\phi^2(d, e, t, s) = \phi(e, d, s, t) = (d, e, t, s)$. Hence by Observation 3.4.13 the map ϕ is a bijection. □

Next, we partition the set J into the following disjoint union: $J = J_0 \cup J_+ \cup J_-$, where

$$\begin{aligned} J_0 &= \{(d, e, t, s) \,|\, (d, e, t, s) \in J \text{ and } d = e\} \\ J_+ &= \{(d, e, t, s) \,|\, (d, e, t, s) \in J \text{ and } d > e\} \\ J_- &= \{(d, e, t, s) \,|\, (d, e, t, s) \in J \text{ and } d < e\}. \end{aligned}$$

Lemma A.2.7.
The map ϕ from Lemma A.2.6 is such that $\phi(J_+) \subseteq J_-$ and $\phi(J_-) \subseteq J_+$. As a consequence we have $|J_+| = |J_-|$.

Proof.
Let $(d,e,t,s) \in J_+$ be arbitrary and observe $\phi(d,e,t,s) = (e,d,s,t) \in J_-$. This is because $(d,e,t,s) \in J_+$ implies $d > e$. Thus $\phi(J_+) \subseteq J_-$.
Next, let $(x,y,z,w) \in J_-$ and therefore $x < y$. Then we see $\phi(x,y,z,w) = (y,x,w,z)$, thus $\phi(J_-) \subseteq J_+$.
Since the map ϕ is a bijection, it follows that $|J_+| = |(J_-)|$. □

Next, define $A_n = \begin{pmatrix} n+1 & n+2 \\ n & n+1 \end{pmatrix}$, $n \in \mathbb{Z}_{\geqslant}0$. Note $\det(A_n) = 1$ for all n, so A_n is invertible. Then define (d',e',t',s') by $A_n \begin{pmatrix} t \\ s \end{pmatrix} = \begin{pmatrix} d' \\ e' \end{pmatrix} = \begin{pmatrix} t(n+1)+s(n+2) \\ nt+s(n+1) \end{pmatrix}$ and $A_n^{-1} \begin{pmatrix} d \\ e \end{pmatrix} = \begin{pmatrix} t' \\ s' \end{pmatrix} = \begin{pmatrix} d(n+1)-e(n+2) \\ -dn+e(n+1) \end{pmatrix}$. It is then straightforward to check $A_n \begin{pmatrix} t & d \\ s & -e \end{pmatrix} = \begin{pmatrix} d' & t' \\ e' & -s' \end{pmatrix}$.
Since $\det(A_n) = 1$ we see that $ds+et = d's'+e't'$ and so A_n gives a map $\psi_n : \mathbb{Z}^4 \to \mathbb{Z}^4$ that preserves m.

Observe that d', e', t' and s' are all odd since one of $\{n, n+1\}$ and one of $\{n+1, n+2\}$ will always be odd. Also, $d' > 0$ and $e' > 0$ as $t, s > 0$.

Also observe

$$d' = t(n+1)+s(n+2) = \underbrace{[tn+s(n+1)]}_{e'} + \underbrace{(s+t)}_{>0} > e' \tag{A.3}$$

Lemma A.2.8.
Given $(d,e,t,s) \in J_+$ there is a unique $n \in \mathbb{Z}_{\geqslant 0}$ such that $\psi_n(d,e,t,s) \in J_+$.

Proof.
By the above comments we know that d', e', t' and s' are all odd and $d' > 0, e' > 0$. So we want to have $t' > 0$ and $s' > 0$. For $t' > 0$ we require $d(n+1) - e(n+2) > 0$ which, rearranges to $n > \frac{e}{d-e} - 1$. Similarly, for $s' > 0$ we require $-dn + e(n+1) > 0$ which, rearranges to $n < \frac{e}{d-e}$.
Combining these two conditions yields $\frac{e}{d-e} - 1 < n < \frac{e}{d-e}$. Note that $d-e$ is positive and even, $e > 0$ and is odd, thus $\frac{e}{d-e} \notin \mathbb{Z}$. Hence we see there is a unique $n \in \mathbb{Z}_{\geqslant 0}$ that satisfies this condition.
Hence there exists a unique $n \in \mathbb{Z}_{\geqslant 0}$ such that $\psi_n(d,e,t,s) \in J_+$. □

We may quantify the map $\psi_n : \mathbb{Z}_4 \longrightarrow \mathbb{Z}_4$ in the following manner.

Observation A.2.9.
Define the block matrix representation of ψ_n by $\bar{A}_n = \left(\begin{array}{c|c} 0 & A_n \\ \hline A_n^{-1} & 0 \end{array}\right)$. Then

$$\begin{aligned}
\bar{A}_n \begin{pmatrix} d \\ e \\ t \\ s \end{pmatrix} &= \left(\begin{array}{cc|cc} 0 & 0 & n+1 & n+2 \\ 0 & 0 & n & n+1 \\ \hline n+1 & -n-2 & 0 & 0 \\ -n & n+1 & 0 & 0 \end{array}\right) \begin{pmatrix} d \\ e \\ t \\ s \end{pmatrix} \\
&= \begin{pmatrix} (n+1)t + (n+2)s \\ nt + (n+1)s \\ (n+1)d - (n+2)e \\ -nd + (n+1) \end{pmatrix} \\
&= \begin{pmatrix} d' \\ e' \\ t' \\ s' \end{pmatrix}.
\end{aligned}$$

We see that $\left(\begin{array}{c|c} 0 & A_n \\ \hline A_n^{-1} & 0 \end{array}\right)\left(\begin{array}{c|c} 0 & A_n \\ \hline A_n^{-1} & 0 \end{array}\right) = \begin{pmatrix} A_n A_n^{-1} & 0 \\ 0 & A_n^{-1} A_n \end{pmatrix} = \begin{pmatrix} I_2 & 0 \\ 0 & I_2 \end{pmatrix}$.
Hence $\psi_n^2 = \mathrm{id}$ and by Lemma 3.4.13 the map ψ_n is a bijection.

Now define $\Phi : J_+ \to J_+$ by $\Phi(d, e, t, s) = \psi_n(d, e, t, s)$.

Lemma A.2.10.
The map

$$\begin{aligned}
\Phi : J_+ &\longrightarrow J_+ \\
(d, e, t, s) &\longmapsto \psi_n(d, e, t, s)
\end{aligned}$$

is a well-defined bijection.

Proof.
First note this map is well-defined since each (d, e, t, s) has a unique A_n associated to it by Lemma A.2.8. We show that Φ^2 is the identity map.
Let $(d, e, t, s) \in J_+$ be arbitrary. Then

$$\begin{aligned}
\phi^2(d, e, t, s) &= \phi(\psi_n(d, e, t, s)) \\
&= \psi_n^2(d, e, t, s) \\
&= (d, e, t, s) \text{ as } \psi^2 = \mathrm{id}
\end{aligned}$$

Hence $\phi^2 = \mathrm{id}$ so by Lemma 3.4.13 ϕ is a bijection. □

Lemma A.2.11.
Assume m is a positive integer such that $m \equiv 2 \bmod 4$, $m = ds + et$ where d, e, t, s are all positive odd integers. Then $\frac{d-e}{2}$ is odd if and only if $\frac{s+t}{2}$ is even.

Proof.
Observe $m = ds+et \equiv 2 \bmod 4$, thus $ds+1+et+1 \equiv 0 \bmod 4$. Factoring then yields $(d-1)(s-1)+(e-1)(t-1)+s+d+e+t \equiv 0 \bmod 4$. Since d, s, e and t are all odd, we see that $4|(d-1)(s-1)$ and $4|(e-1)(t-1)$. Consequently $s+d+e+t \equiv 0 \bmod 4$. Recalling that e odd implies $2e \equiv 2 \bmod 4$. Thus, $s+d+e+t-2e \equiv -2 \bmod 4$. Hence $d-e+s+t \equiv 2 \bmod 4$. Dividing by 2 yields $\frac{d-e}{2} + \frac{s+t}{2}$ is odd.
The proof is then complete since this means precisely one of $\frac{d-e}{2}$, $\frac{s+t}{2}$ must be odd and the other even. □

We now finish the proof of Proposition A.2.1 by showing $\sum_{J_+} \chi(de) = 0$.

Proof.
From Equation A.3 we have $d'-e' = s+t$. From Lemma A.2.5 we know $\chi(de) = (-1)^{\frac{d-e}{2}}$. Recalling that $m \equiv 2 \bmod 4$ and applying Lemma A.2.11 gives $\frac{d-e}{2}$ is even if and only if $\frac{s+t}{2}$ is odd. Thus:

$$\chi(de) = (-1)^{\frac{d-e}{2}} = (-1)(-1)^{\frac{s+t}{2}} = (-1)(-1)^{\frac{d'-e'}{2}} = -\chi(d'e').$$

Hence $M = \sum_S \chi(de) = -\sum_S \chi(d'e') = -M$. Therefore $M = 0$ and the proof is complete. □

We now determine $r_4(m)$ for arbitrary $m \in \mathbb{Z}_{>0}$ by following exercises (16)-(22) in [IR1990, p. 295] although we will use notation that is consistent with that found in [We1974].

Lemma A.2.12.
Let $n \in \mathbb{Z}_{>0}$ be arbitrary. Then $r_4(2n) = r_4(4n)$.

Proof.
Let n be a positive non-zero integer and consider the sets

$$\begin{aligned}\mathcal{T}_{4n} =& \{(x_1,x_2,x_3,x_4) | x_1^2+x_2^2+x_3^2+x_4^2 = 4n\} \text{ and} \\ \mathcal{T}_{2n} =& \{(x_1,x_2,x_3,x_4) | x_1^2+x_2^2+x_3^2+x_4^2 = 2n\}.\end{aligned}$$

We will show the map

$$\begin{aligned}\phi : \mathcal{T}_{4n} &\longrightarrow \mathcal{T}_{2n} \\ (x_1,x_2,x_3,x_4) &\longmapsto \left(\frac{x_1+x_2}{2}, \frac{x_1-x_2}{2}, \frac{x_3+x_4}{2}, \frac{x_3-x_4}{2}\right)\end{aligned}$$

is a well-defined bijection.
Well-defined: We have $x_1^2+x_2^2+x_3^2+x_4^2 = 4n$, thus the left hand side is divisible by four. Recall the squares mod4 are either 0 or 1, so it follows that either all $x_i \equiv 1 \bmod 2$ or all $x_i \equiv 0 \bmod 2$. In both situations, x_i+x_j and x_i-x_j ($i,j \in \{1,2,3,4\}$) are even, thus ϕ produces integer values. Further, $(\frac{x_1+x_2}{2})^2 + (\frac{x_1-x_2}{2})^2 + (\frac{x_3+x_4}{2})^2 + (\frac{x_3-x_4}{2})^2 =$

$\frac{(x_1^2+x_2^2+x_3^2+x_4^2)}{2} = 2n$. Hence ϕ is well-defined.
Injectivity: Suppose $\phi(x_1, x_2, x_3, x_4) = \phi(\hat{x_1}, \hat{x_2}, \hat{x_3}, \hat{x_4})$. Then we have $\frac{x_1+x_2}{2} = \frac{\hat{x_1}+\hat{x_2}}{2}$, thus $x_1 + x_2 = \hat{x_1} + \hat{x_2}$. Also $\frac{x_1-x_2}{2} = \frac{\hat{x_1}-\hat{x_2}}{2}$ and so $x_1 - x_2 = \hat{x_1} - \hat{x_2}$. Adding these two results yields $x_1 = \hat{x_1}$, while subtracting yields $x_2 = \hat{x_2}$.
In a similar manner we see that $x_3 = \hat{x_3}$ and $x_4 = \hat{x_4}$. Thus ϕ is injective.
Surjectivity: Let ${\hat{x_1}}^2 + {\hat{x_2}}^2 + {\hat{x_3}}^2 + {\hat{x_4}}^2 = 2n$. Take $x_1 = \hat{x_1} + \hat{x_2}$, $x_2 = \hat{x_1} - \hat{x_2}$, $x_3 = \hat{x_3} + \hat{x_4}$ and $x_4 = \hat{x_3} - \hat{x_4}$. Then

$$\begin{aligned} x_1^2 + x_2^2 + x_3^2 + x_4^2 &= (\hat{x_1} + \hat{x_2})^2 + (\hat{x_1} - \hat{x_2})^2 + (\hat{x_3} + \hat{x_4})^2 + (\hat{x_3} - \hat{x_4})^2 \\ &= 2(2n) \\ &= 4n. \end{aligned}$$

It is then straightforward to see $\phi(x_1, x_2, x_3, x_4) = (\hat{x_1}, \hat{x_2}, \hat{x_3}, \hat{x_4})$, thus ϕ is surjective. Hence ϕ is a bijection and so $r_4(2n) = r_4(4n)$ for any $n \in \mathbb{Z}_{>0}$. □

Lemma A.2.13.

Let $n \in \mathbb{Z}_{>0}$ be odd. Then $16\left(\sum_{d|n} d\right) + r_4(n) = r_4(4n)$.

Proof.
Observe $n \equiv 1 \bmod 2$ implies $4n \equiv 4 \bmod 8$. Thus $x_1^2+x_2^2+x_3^2+x_4^2 \equiv 4 \bmod 8$ implies that either all x_i are odd or they are all even. We will show the map

$$\begin{gathered} \phi : \{(x_1, x_2, x_3, x_4) \mid \sum_{i=1}^{4} x_i^2 = n\} \to \{(x_1, x_2, x_3, x_4) \mid \sum_{i=1}^{4} x_i^2 = 4n, x_i \equiv 0 \bmod 2\} \\ (x_1, x_2, x_3, x_4) \mapsto (2x_1, 2x_2, 2x_3, 2x_4) \end{gathered}$$

is a well-defined bijection.
Observe ϕ is well-defined because $2x_i$ is always even and $\sum(2x_i)^2 = 4\sum x_i^2 = 4n$.
Now suppose that $\phi(x_1, x_2, x_3, x_4) = \phi(y_1, y_2, y_3, y_4)$. Then $(2x_1, 2x_2, 2x_3, 2x_4) = (2y_1, 2y_2, 2y_3, 2y_4)$ and so $x_i = y_i$ for $i \in \{1, 2, 3, 4\}$. Thus ϕ is injective.
Lastly let (x_1, x_2, x_3, x_4) be such that $\sum_{i=1}^{4} x_i^2 = 4n$, x_i all even. Then $(\frac{x_1}{2}, \frac{x_2}{2}, \frac{x_3}{2}, \frac{x_4}{2})$ is well defined and satisfies $\sum \left(\frac{x_i}{2}\right)^2 = n$. Thus $\phi(\frac{x_1}{2}, \frac{x_2}{2}, \frac{x_3}{2}, \frac{x_4}{2}) = (x_1, x_2, x_3, x_4)$. So ϕ is surjective and hence the map ϕ is a bijection.
From this claim it follows that $r_4(n) = |\{(x_1, x_2, x_3, x_4) \mid \sum x_i^2 = 4n, x_i \equiv 0 \bmod 2\}|$.
By Corollary A.2.2 we have

$$r_4(4n) = 16\left(\sum_{d|4n} d\right) + \{\text{number of solutions for which } x_i \equiv 0 \bmod 2 \,\forall i\}.$$

Thus, $r_4(4n) = 16\left(\sum_{d|4n} d\right) + r_4(n)$.
Now observe the positive odd divisors of $4n$ are exactly the positive odd divisors of

n, hence we get our result.

$$r_4(4n) = 16\left(\sum_{d|n} d\right) + r_4(n). \qquad \square$$

Lemma A.2.14.
Let n be an odd integer and $|S|$ be the number of solutions to $x_1^2 + x_2^2 + x_3^2 + x_4^2 = 2n$ with $x_1 \equiv x_2 \equiv 1 \bmod 2$ and $x_3 \equiv x_4 \equiv 0 \bmod 2$. Then $|S| = \frac{1}{6} r_4(2n)$.

Proof.
Observe n is odd and so $2n \equiv 2 \bmod 4$. The squares modulo 4 are 0 and 1 so we have exactly two of the x_i are odd and the other two are both even in any solution in $r_4(2n)$.
There are $\binom{4}{2} = 6$ ways to select two of the x_i to be congruent to 1 mod2. This determines all of the x_i as the others must be congruent to 0 mod2.
Hence $|S| = \frac{1}{6} r_4(2n)$. $\square$

Lemma A.2.15.
If $n \equiv 1 \bmod 4$ and $|S|$ is as in Lemma A.2.14 then $|S| = \frac{1}{2} r_4(n)$. Further it follows that $r_4(2n) = 3r_4(n)$.

Proof.
Since $n \equiv 1 \bmod 4$, $x_1^2 + x_2^2 + x_3^2 + x_4^2 = n$ must have exactly one $x_i \equiv 1 \bmod 2$, while the rest are congruent to 0 modulo 2. So we may partition the set with cardinality $r_4(n)$ into four disjoint sets: $R_4^1(n), R_4^2(n), R_4^3(n)$ and $R_4^4(n)$, where the superscript i denotes that x_i is odd.
It follows that there is a one-to-one correspondence between elements of $R_4^i(n)$ and $R_4^j(n)$ $(i, j \in \{1, 2, 3, 4\})$ via interchanging the x_i with x_j. Hence $|R_4^i(n)| = |R_4^j(n)|$ for all i, j as above.
Without loss of generality, consider half of $r_4(n)$ via the set $R_4^1(n) \cup R_4^2(n)$. This has cardinality $\frac{r_4(n)}{2}$.
We will show the following map is a well-defined bijection. Define

$$\phi : \{\ (x_1, x_2, x_3, x_4) | \sum_{i=1}^{4} x_i^2 = n,\ x_1 \text{ or } x_2 \equiv 1 \bmod 2,\ \text{all other } x_i \equiv 0 \bmod 2\ \} \to S$$
$$(x_1, x_2, x_3, x_4) \mapsto (x_1 + x_2, x_1 - x_2, x_3 + x_4, x_3 - x_4).$$

Well-defined: The map ϕ is well-defined since $x_1 \pm x_2 \equiv 1 \bmod 2$. This is because only one of x_1, x_2 may be congruent to 1 modulo 2 at anytime. Further $x_3 \pm x_4 \equiv 0 \bmod 2$ always.
Injectivity: Suppose $\phi(x_1, x_2, x_3, x_4) = \phi(y_1, y_2, y_3, y_4)$. Then the equations $x_1 + x_2 = y_1 + y_2$ and $x_1 - x_2 = y_1 - y_2$ add to give $2x_1 = 2y_1$ and subtract to give $2x_2 = 2y_2$. Similarly, the equations $x_3 + x_4 = y_3 + y_4$ and $x_3 - x_4 = y_3 - y_4$ give $2x_3 = 2y_3$ and $2x_4 = 2y_4$. Hence ϕ is injective.
Surjectivity: Let $(\hat{x_1}, \hat{x_2}, \hat{x_3}, \hat{x_4}) \in S$. Then define $x_1 = \frac{\hat{x_1} + \hat{x_2}}{2}$, $x_2 = \frac{\hat{x_1} - \hat{x_2}}{2}$, $x_3 = \frac{\hat{x_3} + \hat{x_4}}{2}$

and $x_4 = \frac{\hat{x_3} - \hat{x_4}}{2}$.
This is well-defined since $\hat{x_1}$, $\hat{x_2}$ are both odd, so their sum and difference is divisible by 2. Further the difference between their sum and difference is $\hat{x_2}$ which, is odd, so either x_1 or x_2 but not both must be odd. Similarly, $\hat{x_3}$, $\hat{x_4}$ are both even, so their sum and difference is divisible by 2. Further the difference between their sum and difference is $\hat{x_4}$, which, is even. Hence x_3 and x_4 are both odd or both even.

Now observe $x_1^2 + x_2^2 + x_3^2 + x_4^2 = \frac{1}{4}\left(2\hat{x_1}^2 + 2\hat{x_2}^2 + 2\hat{x_3}^2 + 2\hat{x_4}^2\right) = \frac{2(2n)}{4} = n$, thus we see that since exactly one of the x_i must be odd and we know exactly one of x_1, x_2 is already odd, we get $x_3 \equiv x_4 \equiv 0 \bmod 2$.
Thus the map ϕ is surjective. Hence ϕ is a bijection and we have $|S| = \frac{r_4(n)}{2}$.

By Lemma A.2.14 we know for n odd, $|S| = \frac{1}{6}r_4(2n)$ and so $\frac{1}{2}r_4(n) = \frac{1}{6}r_4(2n)$. Thus $3r_4(n) = r_4(2n)$. □

Lemma A.2.16.
If $n \equiv 3 \bmod 4$ *then* $r_4(2n) = 3r_4(n)$.

Proof.
Assume $n \equiv 3 \bmod 4$, then $\sum_{i=1}^{4} x_i^2 = n$ implies there is exactly one even x_i and all of the rest are odd. We partition the set with cardinality $r_4(n)$ in a similar manner to that found in Lemma A.2.15, $R_4^i(n)$ has solutions for which, the i^{th} entry is even. It follows that there is a one-to-one correspondence between the elements of $R_4^i(n)$ and $R_4^j(n)$ and so these sets have the same cardinality.

Without loss of generality consider $R_4^1(n) \cup R_4^2(n)$ which, has cardinality $\frac{r_4(n)}{2}$.

Define the map

$$\psi : \{\ (x_1, x_2, x_3, x_4) \mid \sum x_i^2 = n,\ x_1 \text{ or } x_2 \equiv 0 \bmod 2,\ \text{all other } x_i \equiv 1 \bmod 2\ \} \to S$$
$$(x_1, x_2, x_3, x_4) \longmapsto (x_1 + x_2, x_1 - x_2, x_3 + x_4, x_3 - x_4).$$

We will show this a well-defined bijection.
The map ψ is well-defined as only one of x_1, x_2 may be odd, so $x_1 \pm x_2 \equiv 1 \bmod 2$, $x_3 \pm x_4 \equiv 0 \bmod 2$ as both x_3 and x_4 are odd. Observe that $(x_1 + x_2)^2 + (x_1 - x_2)^2 + (x_3 + x_4)^2 + (x_3 - x_4)^2 = 2\sum x_i^2 = 2n$.
Next, the proof that ψ is injective is identical to that of the map ϕ found in Lemma A.2.15.
We now show the map ψ is surjective. Let $(\hat{x_1}, \hat{x_2}, \hat{x_3}, \hat{x_4}) \in S$ be arbitrary. Let $x_1 = \frac{\hat{x_1} + \hat{x_2}}{2}$, $x_2 = \frac{\hat{x_1} - \hat{x_2}}{2}$, $x_3 = \frac{\hat{x_3} + \hat{x_4}}{2}$ and $x_4 = \frac{\hat{x_3} - \hat{x_4}}{2}$. Then $\hat{x_1} \pm \hat{x_2} \equiv 0 \bmod 2$ and $\hat{x_3} \pm \hat{x_4} \equiv 0 \bmod 2$, so $x_1, x_2, x_3, x_4 \in \mathbb{Z}$. Further, x_1 and x_2 differ by $\hat{x_2}$ which is odd, so exactly one of x_1, x_2 is odd and the other is even. Also, x_3 and x_4 differ by $\hat{x_4}$ which, is even and so x_3 and x_4 are both odd or both even. However, $\sum x_i^2 = n \equiv 3 \bmod 4$ implies that there may only be one x_i even and we know that exactly one of x_1, x_2 is already even. Hence both x_3 and x_4 must be odd.

Hence $\psi(x_1, x_2, x_3, x_4) = (\hat{x_1}, \hat{x_2}, \hat{x_3}, \hat{x_4})$ and ψ is surjective. Thus the map ψ is a bijection.

Hence $|S| = \frac{r_4(n)}{2}$. It follows in the same manner as Lemma A.2.15 that $3r_4(n) = r_4(2n)$. □

Lemma A.2.17.
If n is odd then $r_4(n) = 8\sum_{d|n} d$ and $r_4(2n) = 24\sum_{d|n} d$.

Proof.
Since n is odd, by Lemmas A.2.15, A.2.16 and A.2.13 we have

$$3r_4(n) = r_4(2n) = r_4(4n) = 16\left(\sum_{d|n} d\right) + r_4(n).$$

Thus, $2r_4(n) = 16\sum_{d|n} d$ and hence $r_4(n) = 8\sum_{d|n} d$ if n is odd. □

Lemma A.2.18.
If n is even, $n = 2^s m$, $s \geqslant 1$ and m odd, then $r_4(n) = 24\sum_{d|m} d$.

Proof.
We apply Lemma A.2.12 repeatedly to reduce to the case where $\hat{n} = 2m$, m odd. Then applying Lemma A.2.17 yields $r_4(2m) = 24\sum_{d|m} d$. □

Corollary A.2.19.
Let n be a positive integer, then the number of representations of n as a sum of four squares is given by

$$r_4(n) = 8\left(2 + (-1)^n\right)\sigma_{odd}(n).$$

Proof.
Let n be a positive integer and write $n = 2^s m$ where $m \equiv 1 \bmod 2$ and s is the greatest non-negative integer such that 2^s divides n but 2^{s+1} does not divide n. Recall from Definition 4.6.5 the meaning of $\sigma_{\text{odd}}(n)$. We recall if $n \equiv 1 \bmod 2$ then $s = 0$ and $\sigma(n) = \sigma_{\text{odd}}(n) = \sigma_{\text{odd}}(m) = \sigma(m)$; whilst if $n \equiv 0 \bmod 2$ then $\sigma(n) \neq \sigma_{\text{odd}}(n) = \sigma_{\text{odd}}(m) = \sigma(m)$.
Combining the results of Lemmas A.2.17 and A.2.18 we get

$$\begin{aligned} r_4(n) &= \begin{cases} 24\sum_{d|m} d & n \equiv 0 \bmod 2 \\ 8\sum_{d|m} d & n \equiv 1 \bmod 2 \end{cases} \\ &= \begin{cases} 24\sigma_{\text{odd}}(n) & n \equiv 0 \bmod 2 \\ 8\sigma_{\text{odd}}(n) & n \equiv 1 \bmod 2. \end{cases} \end{aligned}$$

Observing $(2 + (-1)^n) = \begin{cases} 3 & \text{if } n \equiv 0 \bmod 2 \\ 1 & \text{if } n \equiv 1 \bmod 2 \end{cases}$ and factoring out an 8 then yields

$$r_4(n) = 8\left(2 + (-1)^n\right)\sigma_{\text{odd}}(n).$$

□

Observation A.2.20.
Lemmas A.2.12 through A.2.18 prove Weil's claim that $r_4(m)$ is known for all $m > 0$ once you know $N_4(m)$.

A.3 Weil's First Four Squares Proof

In this appendix we give in detail Andrë Weil's first proof for $N_4(m)$ which, by Observation A.2.20, is sufficient to calculate the number of representations of a positive integer as a sum of four squares. A concise version is found in [We1974, p. 217].

Lemma A.3.1.
Let m be a positive integer such that $m \equiv 4 \bmod 8$. Then $N_4(m) = \sum_{m=r+s} N_2(r)N_2(s)$, $r \equiv s \equiv 2 \bmod 4$, $r > 0$, $s > 0$.

Proof.
In the definition of $N_4(m)$, all x_i are odd, therefore if we let $r = x_1^2+x_2^2$ and $s = x_3^2+x_4^2$, we see that $r \equiv s \equiv 2 \bmod 4$. This is because all odd numbers when squared are equivalent to 1 modulo 4. Note that r and s are necessarily in $\mathbb{N}$ by the definition of $N_4(m)$.
Further if we run through all such r, then s is automatically defined, so we get the number of all solutions by

$$N_4(m) = \sum_{\substack{r,s \\ r+s=m}} N_2(r)N_2(s).$$

This is because each solution to $x_1^2 + x_2^2 = r$ is independent of the solution to $x_3^2 + x_4^2$. □

Lemma A.3.2.
$N_4(m) = \sum(-1)^{\frac{a-c}{2}}$, *where* $m = 2ab+2cd$, $a \equiv b \equiv c \equiv d \equiv 1 \bmod 2$ *and* $a, b, c, d > 0$.

Proof.
We apply the result found in Lemma A.3.1 and get:

$$\begin{aligned}
N_4(m) &= \sum N_2(r)N_2(s) \text{ by Lemma A.3.1} \\
&= \sum_{r+s=m} \left[\left(\sum_{a|\frac{r}{2}} \chi(a) \right) \left(\sum_{c|\frac{s}{2}} \chi(c) \right) \right] \text{ by Lemma A.1.16} \\
&= \sum_{r+s=m} \left[\chi(a_1) \sum_{c|\frac{s}{2}} \chi(c) + \cdots + \chi(a_n) \sum_{c|\frac{s}{2}} \chi(c) \right] \\
&= \sum_{r+s=m} \left[\sum_{c|\frac{s}{2}} \chi(a_1)\chi(c) + \cdots + \sum_{c|\frac{s}{2}} \chi(a_n)\chi(c) \right]
\end{aligned}$$

$$= \sum_{r+s=m} \left[\sum_{c|\frac{s}{2}} (-1)^{\frac{a_1-c}{2}} + \cdots + \sum_{c|\frac{s}{2}} (-1)^{\frac{a_n-c}{2}} \right] \text{ by Lemma A.1.19}$$
$$= \sum_{r+s=m} \left[\sum (-1)^{\frac{a-c}{2}} \right]$$
$$= \sum (-1)^{\frac{a-c}{2}}.$$

Note that in the second to last equality, the inner sum is over all $a|\frac{r}{2}$ and all $c|\frac{s}{2}$ where r and s are fixed. In the last line, the sum is over all r, s such that $r+s=m$, $r \equiv s \equiv 2 \bmod 4$ and all a, c such that $a|\frac{r}{2}$ and $c|\frac{s}{2}$.
By denoting the complementary divisors of a and c by b and d respectively, we see that $m = 2ab + 2cd$. Since $2ab \equiv 2 \bmod 4$ it follows that $a \equiv b \equiv 1 \bmod 2$. Similarly, we obtain $c \equiv d \equiv 1 \bmod 2$. □

Now we may define a change of variables as follows:
Let $x = \frac{a+c}{2}$, $y = \frac{a-c}{2}$, $z = \frac{b+d}{2}$ and $t = \frac{d-b}{2}$. This is a well-defined change of variables because $a \equiv b \equiv c \equiv d \equiv 1 \bmod 2$. The associated change of basis matrix is given by

$$\begin{pmatrix} \frac{1}{2} & 0 & \frac{1}{2} & 0 \\ \frac{1}{2} & 0 & -\frac{1}{2} & 0 \\ 0 & \frac{1}{2} & 0 & \frac{1}{2} \\ 0 & -\frac{1}{2} & 0 & \frac{1}{2} \end{pmatrix}.$$

This has determinant $\frac{1}{4}$ and hence the change of variables is invertible.
It remains to determine the conditions that apply to these new variables.

Observe $a \equiv c \equiv 1 \bmod 2$ implies $x \not\equiv y \bmod 2$. Similarly, $b \equiv d \equiv 1 \bmod 2$ implies $z \not\equiv t \bmod 2$.
Since $a, b, c, d > 0$, we have $x, z > 0$ and observe that $|y| = \begin{cases} \frac{a-c}{2} \text{ if } c \leqslant a \\ \frac{c-a}{2} \text{ if } a < c \end{cases}$, hence $x > |y|$. In a similar manner we see $z > |t|$.

Observe that $m = r + s = 2(x+y)(z-t) + 2(x-y)(z+t) = 4(xz - yt)$.
Since $m \equiv 4 \bmod 8$, this implies $xz - yt \equiv 1 \bmod 2$ and so $x \not\equiv y \bmod 2$, $z \not\equiv t \bmod 2$ implies $y \equiv t \bmod 2$ and $z \equiv x \bmod 2$. Observing that $y = \frac{a-c}{2}$ yields $y \equiv t \equiv \frac{a-c}{2} \bmod 2$.

Lemma A.3.2 then says

$$N_4(m) = \sum_{(x,y,z,t)} (-1)^y. \tag{A.4}$$

Here the sum is over all y satisfying the above relations on x, y, z and t.

We now extend this notation to allow us to consider when y is positive, negative or zero.

Definition A.3.3.
Let $N_0 = \sum(-1)^y$, $N_+ = \sum(-1)^y$ and $N_- = \sum(-1)^y$ where the summation is restricted to the values of x, y, z, t that satisfy Equation A.4 and where $y = 0$, $y > 0$ and $y < 0$ respectively.

We first calculate N_0.

Lemma A.3.4.
$N_0 = \sum d$ where $d > 0$ is an odd divisor of m.

Proof.
Here, $y = 0$ and so $m = 4xz$, then $m \equiv 4 \bmod 8$ implies $\frac{m}{4} = xz$. It follows that $\frac{m}{4}$ is not divisible by 2 else m would be congruent to $0 \bmod 8$, a contradiction. Thus $x \equiv z \equiv 1 \bmod 2$. The conditions on Equation A.4 then state $t \equiv 0 \bmod 2$.
So if d is an odd divisor of $\frac{m}{4}$ and hence an odd divisor of m it follows that there are d solutions to the set of conditions on Equation A.4. This is because the solutions are given by $y = 0, z = d, x = \frac{m}{4d}$ and $t = t$, where $|t| < z = d$. So there are exactly d possible choices for t. This is because there are $2d$ possible choices for t but $t \not\equiv z = d$. Hence, we calculate N_0 by summing over all such positive odd divisors of m. This gives

$$N_0 = \sum_{\substack{d|m \\ d \text{ odd}}} d.$$

□

It is important to note that the d used to denote a positive odd divisor of m in the above proof is different to the d used in the proof of Lemma A.3.2.
Note that in the conditions placed on x, y, z, t in Equation A.4, we may replace both y and t by their negatives and still have a solution. This gives a bijection as we see in the next Lemma.

Lemma A.3.5.
Let

$$S = \{(x, y, z, t) \,|\, xz - yt \equiv 1 \bmod 2,\ x \not\equiv y \bmod 2,\ z \not\equiv t \bmod 2,\ x > |y|,\ z > |t|, y \equiv t \bmod 2\ \}$$

and define the map

$$\begin{aligned} \phi : S &\longrightarrow S \\ (x, y, z, t) &\longmapsto (x, -y, z, -t). \end{aligned}$$

We will show this is a bijection. Further, define $S_0 \subseteq S$ to be those (x, y, z, t) for which $y = 0$, $S_+ \subseteq S$ those where $y > 0$ and $S_- \subseteq S$ those where $y < 0$. Then $|S_+| = |S_-|$ and consequently $N_+ = N_-$ (see Definition A.3.3).

Proof.
First observe $xz - (-y)(-t) = xz - yt \equiv 1 \bmod 2$. Next, $-y \equiv y \not\equiv x \bmod 2$ and $-t \equiv t \not\equiv z \bmod 2$. Also, $-y \equiv y \equiv t \equiv -t \bmod 2$. Lastly, $|-y| = |y| < x$ and $|-t| = |t| < z$, hence ϕ maps into S.
Further, $\phi^2(x, y, z, t) = \phi(x, -y, z, -t) = (x, y, z, t)$, so by Lemma 3.4.13 we have a bijection.
Note that if $y = 0$ then $\phi(x, 0, z, t) = (x, 0, z, -t)$ and so $\phi(S_0) = S_0$. Thus let $(x, y, z, t) \in S$ be such that $y > 0$. Then $\phi(x, y, z, t)$ has $-y < 0$ and so $\phi(S_+) \subseteq S_-$. Similarly, $\phi(S_-) = S_+$ and so $|S_+| = |S_-|$. Finally, recall that $-1^y = -1^{-y}$ and so each element of S_+ contributes the same term to N_+ as its image under ϕ in S_- contributes to N_-. Hence $N_+ = N_-$. □

Thus, we only need to calculate N_+.

Lemma A.3.6.
$N_+ = 0$.

Proof.
Assume $y > 0$ and (x, y, z, t) is a solution to the set of conditions for Equation A.4. Then $y < x$ implies $\frac{x}{y} > 1$ and since $x \not\equiv y \bmod 2$, either $\frac{x}{y}$ is not an integer (as the denominator is divisible by 2 while the numerator isn't) or it must be an even integer. Therefore, $\frac{x}{y}$ is definitely not an odd integer and so there exists a unique $u \in \mathbb{N}$ such that $2u - 1 < \frac{x}{y} < 2u + 1$.

Next define $x' = 2uz - t$, $y' = z$, $z' = y$ and $t' = 2uy - x$.
We observe that $4(x'z' - y't') = 4((2uz - t)y - z(2uy - x)) = 4(xz - yt) = m$.
Also, observe that $x' > 0$ and so we have

$$\begin{aligned} x' &= 2uz - t \\ &> z + (uz - t) \text{ as } u \text{ is positive and even} \\ &> z + 2z - t \\ &> z \text{ as } |t| < z \Rightarrow 0 < t < 2z \text{ and so } 2z - t > 0 \\ &= y'. \end{aligned}$$

Multiplying both sides by -1 yields $-x' < -y' \leqslant |y'|$ and thus $|y'| < x'$.

Similarly we have $|t'| = |2uy - x| = \begin{cases} 2uy - x & \text{if } 2uy - x \geqslant 0 \\ x - 2uy & \text{if } 2uy - x < 0. \end{cases}$
We observe that for $y > 0$, $2u - 1 < \frac{x}{y}$ implies $2uy < x + y$ and so $2uy - x < y$. Likewise, $\frac{x}{y} < 2u + 1$ implies $x - 2uy < y$ for $y > 0$. Hence we see that $|t'| < y = z'$.

Then note that $2uz \equiv 0 \bmod 2$ and $-t \equiv t \bmod 2$. We therefore have $x' \equiv t \not\equiv z \equiv y' \bmod 2$. Similarly, $2uy \equiv 0 \bmod 2$ and we get $t' \equiv x \not\equiv y \equiv z' \bmod 2$.

By definition of $z = \frac{b+d}{2}$, $b, d > 0$, we see that $y' > 0$ and further because $y \equiv t \bmod 2$, we have $y \equiv t \not\equiv z \equiv y'$.

To summarise, (x', y', z', t') is a solution to the set of conditions placed of Equation A.4 and $y' > 0$, $y' \not\equiv y \bmod 2$.

By the remark at the beginning of this proof, given (x', y', z', t') a solution to the conditions placed on Equation A.4, there is a unique value of u such that $2u - 1 < \frac{x'}{y'} = \frac{2uz-t}{z} = 2u - \frac{t}{z} < 2u + 1$. Note that $\frac{t}{z} < 1$ and so we recover the value of u used in the substitution, hence we recover (x, y, z, t). So we have a bijection and thus a permutation of the elements that contribute to N_+.
Since each pairing maps an odd y to an even y' (and vice versa), we see that each pair of solutions contributes 0 to N_+. Hence $N_+ = -N_+$ and so $N_+ = 0$. □

Recalling that $N_+ = N_-$, from this claim it follows that

$$N_4(m) = N_0 + N_+ + N_- = N_0 = \sum_{\substack{d|m \\ d \text{ odd}}} d.$$

This completes the proof of Proposition A.2.1. By Observation A.2.20 it follows we can calculate $r_4(m)$ for any $m > 0$.

A.4 Weil's Second Four Squares Proof

In this section we give the second of Weil's proofs for $N_4(m)$.

Lemma A.4.1.
Let a, b and $n \in \mathbb{Z}_{>0}$. Let $f(a, b, n)$ be the number of integer solutions to $aX + bY = n$, where $0 < X < b$, $a < Y$ and $Y \not\equiv 0 \bmod a$. Then $f(a, b, n) = f(b, a, n)$.

Proof.
Let (X, Y) be a solution to the problem posed in Lemma A.4.1. Then since $a < Y$ and $Y \not\equiv 0 \bmod a$ it follows that $1 < \frac{Y}{a}$ and $\frac{Y}{a}$ is not an integer. Hence there exists a unique $u \in \mathbb{Z}_{>0}$ such that $u < \frac{Y}{a} < u + 1$.
Now define $X' = Y - ua$ and $Y' = X + ub$.
Claim: (X', Y') is a solution to $bX' + aY' = n$ where $0 < X' < a$, $b < Y'$ and $Y' \not\equiv 0 \bmod b$.
We have

$$\begin{aligned} bX' + aY' &= b(Y - ua) + a(X + ub) \\ &= aX + bY + aub - aub \\ &= n. \end{aligned}$$

Further, $u < \frac{Y}{a} < u + 1$ implies $0 < \frac{Y}{a} - u < 1$, so $\frac{X'}{a} = \frac{Y}{a} - u$ satisfies $0 < \frac{X'}{a} < 1$ and hence $0 < X' < a$.
Also, we know $u \geqslant 1$ and $X \geqslant 1$, hence $Y' = X + ub > ub \geqslant b$. Thus $b < Y'$.

Lastly, $Y' = X + ub$ yields $Y' - ub = X$ and so since $0 < X < b$, $b \nmid Y' - ub$. Thus $b \nmid Y'$, that is, $Y' \not\equiv 0 \bmod b$.
This completes the proof of the claim, so (X', Y') is a solution to the problem. We note this means (X', Y') is a solution to the initial problem with the roles of a and b interchanged.

Now observe $b < Y'$, $b > 0$ and $Y' \not\equiv 0 \bmod b$ imply there exists a unique $v \in \mathbb{Z}_{>0}$ such that $v < \frac{Y'}{b} < v + 1$.
Then we have $\frac{Y'}{b} = \frac{X}{b} + u$ and note that $0 < \frac{X}{b} < 1$ because $0 < X < b$. So we have $u < \frac{Y'}{b} = \frac{X}{b} + u < u + 1$.
Thus it follows that $v = u$.

Hence given (X', Y') we may recover (X, Y) uniquely via $X = Y' - ub$ and $Y = X' + ua$.

So for any solution to $aX + bY = n$ under the conditions given in the Lemma, there is a unique corresponding solution to $bX' + aY' = n$ with the appropriately modified conditions.
Hence we have a bijection between the two sets of solutions and so $f(a, b, n) = f(b, a, n)$. □

Proposition A.4.2.
With the hypotheses of Lemma A.4.1 we have $f(a, b, n) = 0$ unless $n \geqslant ab + a + b$ and n is a multiple of $\gcd(a, b)$.

Proof.
Assume $aX + bY = n$, where $0 < X < b$, $a < Y$ and $Y \not\equiv 0 \bmod a$. Observe $X \geqslant 1$ and $Y \geqslant a + 1$. Thus $n \geqslant a + b(a + 1) = ab + a + b$. Further, it is clear that $\gcd(a, b)$ must divide n, i.e. n is a multiple of $\gcd(a, b)$. □

We now state and prove Weil's Lemma 2, which plays a pivotal role in his calculation of $N_3(m)$.

Lemma A.4.3.
Let $a, b \in \mathbb{Z}_{>0}$, let $m \in \mathbb{Z}$ and let $\alpha, \beta \in \{0, 1\}$. Let $\phi(a, b, \alpha, \beta, m)$ denote the number of solutions to:

$$aX + bY = m,\ |X| < b,\ a < Y,\ X \equiv \alpha \bmod 2,\ Y \equiv \beta \bmod 2,\ Y \not\equiv a \bmod 2a. \quad \text{(A.5)}$$

Then $\phi(a, b, \alpha, \beta, m) = \phi(b, a, \beta, \alpha, m)$.

Before we give the proof, we will prove the following useful proposition.

Proposition A.4.4. *Let (X, Y) be a solution to Equation A.5. Then there exists a unique $u \in \mathbb{Z}_{>0}$ such that $|Y - 2ua| < a$.*

Proof.
Given $Y \in \mathbb{Z}$, the division algorithm tells us there exists a unique $u \in \mathbb{Z}$ such that $Y = u \cdot 2a + r$ where $-a < r \leqslant a$. Since (X, Y) is a solution to Equation A.5 we have $Y \not\equiv a \bmod 2a$ and so it follows that r cannot equal a. Since $0 < a < Y$ it follows that $u \in \mathbb{Z}_{>0}$. Hence we have $|Y - 2ua| < a$. □

We now give a proof of Lemma A.4.3.

Proof of Lemma A.4.3.
Let (X, Y) be a solution to the problem given in Lemma A.4.3. Let u be the unique positive integer such that $|Y - 2ua| < a$ as in Lemma A.4.4.
Apply the change of variables $X' = Y - 2ua$ and $Y' = X + 2ub$.
Claim: (X', Y') is a solution to

$$bX' + aY' = m \text{ where } |X'| < a,\ b < Y',\ X' \equiv \beta \bmod 2,\ Y' \equiv \alpha \bmod 2 \text{ and } Y' \not\equiv\ b \bmod 2b. \tag{A.6}$$

Proof: We have

$$\begin{aligned} bX' + aY' &= b(Y - 2ua) + a(X + 2ub) \\ &= aX + bY - 2uab + 2uab \\ &= m. \end{aligned}$$

Further, $|X'| = |Y - 2ua| < a$ by our choice of u using Lemma A.4.4. We also have

$$\begin{aligned} Y' &= X + 2ub \\ &> -b + 2ub \text{ as } |X| < b \text{ and } b \in \mathbb{Z}_{>0} \\ &= b(2u - 1) \\ &> b \text{ as } u \text{ is at least 1.} \end{aligned}$$

Also, $X' = Y - 2ua \equiv Y \bmod 2$ and we recall $Y \equiv \beta \bmod 2$, so $X' \equiv \beta \bmod 2$.
Similarly, $Y' = X + 2ub \equiv X \bmod 2$ but $X \equiv \alpha \bmod 2$ and thus $Y' \equiv \alpha \bmod 2$.
So (X', Y') is a solution to Equation A.6. This completes the proof of the claim.

Now by Lemma A.4.4 there exists a unique $v \in \mathbb{Z}_{>0}$ such that $|Y' - 2vb| < b$.

Claim: $v = u$.
Proof: We have

$$\begin{aligned} b &> |Y' - 2vb| \\ &= |X + 2ub - 2vb| \\ &= |X + 2b(u - v)|. \end{aligned}$$

Recalling that $|X| < b$, we see that as $u - v \in \mathbb{Z}$, we will have $|X + 2b(u - v)| > b$ unless $u - v = 0$, that is $v = u$. This completes the proof of the claim.

Now define $S = \{(X, Y) \mid (X, Y) \text{ satisfies Equation A.5}\}$ and
$T = \{(X', Y') \mid (X', Y') \text{ satisfies Equation A.6}\}$.
It is straightforward to see $|S|$ is finite because X is bounded and integer, and so the equation $aX + bY = m$ implies Y takes only finitely many values. A similar argument yields $|T|$ is finite.

Define a map $f : S \longrightarrow T$ by $f(X, Y) = (Y - 2ua, X + 2ub)$ where u is the unique positive integer such that $|Y - 2ua| < a$ by Lemma A.4.4. By the previous part of this proof, f is well-defined.

We now show f is injective.
Suppose $f(X, Y) = f(\hat{X}, \hat{Y}) = (X', Y')$ for some $(X, Y), (\hat{X}, \hat{Y}) \in S$ and $(X', Y' \in T)$. Then by Lemma A.4.4 there exist unique positive integers $u, \hat{u}$ such that $|Y - 2ua| < a$ and $|\hat{Y} - 2\hat{u}a| < a$ respectively. We get two equations, $Y - 2ua = \hat{Y} - 2\hat{u}a$ and $X + 2ub = \hat{X} + 2\hat{u}b$, which yield $\frac{Y-\hat{Y}}{2a} = u - \hat{u}$ and $\frac{\hat{X}-X}{2b} = u - \hat{u}$ respectively.
Since $(X', Y') = f(X, Y) \in T$ there exists a unique positive integer v such that $|Y' - 2vb| < b$ and applying the above claim, we see that $v = u$. But also, $(X', Y') = f(\hat{X}, \hat{Y}) \in T$ and so applying the claim again yields $v = \hat{u}$.
Hence $u = \hat{u}$ and it follows that $X = \hat{X}$ and $Y = \hat{Y}$. So f is injective.
Define $g : T \longrightarrow S$ by $g(X', Y') = (Y' - 2ub, X' + 2ua)$ where u is the unique positive integer such that $|Y' - 2ub| < b$. It follows that g is injective because of the symmetry between the functions f and g.

Hence we have an injection in each direction between two finite sets and so $|S| = |T|$ and we have a bijection between them. So we have $\phi(a, b, \alpha, \beta, m) = |S| = |T| = \phi(b, a, \beta, \alpha, m)$. This completes the proof of Lemma A.4.3. □

Lemma A.4.5.
$\phi(a, b, \alpha, \beta, m) = 0$ *unless* m *is a multiple of* $\gcd(a, b)$ *and* $m \geqslant a + b$ *and* $m \equiv \alpha a + \beta b \bmod 2$.

Proof.
As in the proof of Lemma A.4.1 it is clear that m must be a multiple of $\gcd(a, b)$. Recall that both a and b are positive integers.
We know $a < Y$, so $a + 1 \leqslant Y$. Also $|X| < b$, so $X \geqslant -b + 1$, thus the smallest X can be is $-b + 1$. So

$$\begin{aligned} aX + bY &\geqslant aX + b(a + 1) \\ &\geqslant a(-b + 1) + ab + b \\ &= a + b. \end{aligned}$$

Lastly, we see $m = aX + bY \equiv a\alpha + b\beta \bmod 2$ because $X \equiv \alpha \bmod 2$ and $Y \equiv \beta \bmod 2$. □

Lemma A.4.6.
$Y \not\equiv a \bmod 2a$ *follows naturally if* $Y \equiv \beta \bmod 2$ *and* $a \not\equiv \beta \bmod 2$.

Proof.
Assume $Y > a > 0$, $Y \equiv \beta \bmod 2$ and $a \not\equiv \beta \bmod 2$.
Then $Y > a > 0$ implies $Y = a + k$ for some $k \in \mathbb{Z}_{>0}$. Working modulo 2 gives $a + k \equiv \beta \bmod 2$ and $a \not\equiv \beta \bmod 2$ implies $k \equiv 1 \bmod 2$. Thus $Y = a + 2q + 1$ for some $q \in \mathbb{Z}_{\geqslant 0}$ and so $Y - a$ is odd, so $2a \nmid (Y - a)$, that is $Y \not\equiv a \bmod 2a$. □

We now give Weil's second proof of Proposition A.2.1. We begin part way through his first proof, having already determined N_0 and wishing to calculate N_+. From Equation A.4 we have

$$\frac{m}{4} = xz - yt,\ |y| < x,\ |t| < z,\ y \not\equiv x \bmod 2,\ t \not\equiv z \bmod 2,\ m \equiv 4 \bmod 8 \tag{A.7}$$

We will show $N_+ = 0$. From the above we have $N_+ = \sum(-1)^y$ where the sum is over all x, y, z and t satisfying Equation A.7 and $y, z \in \mathbb{Z}_{>0}$.

We see Equation A.7 implies $y \not\equiv z \bmod 2$ due to the comment following Lemma A.3.2.

Next, identify $aX + bY = m$ with the equation $y(-t) + z(x) = \frac{m}{4}$. That is, for the quadtuple (a, b, X, Y) take $(y, z, -t, x)$.

Now we may apply Lemma A.4.3 for fixed y and z values. We can do this because for N_+ we have $y > 0$ and $z > 0$ by assumption. We also have $|y| < x$ implies $y < x$ as $y > 0$. Further, $|-t| = |t| < z$ and $-t \equiv t \equiv y \equiv \bar{y} \bmod 2$ and $x \equiv z \equiv \bar{z} \bmod 2$. Note that $\bar{y} \equiv t \not\equiv z \equiv x \equiv \bar{z} \bmod 2$ and so by Lemma A.4.6 it follows that $x \not\equiv y \bmod 2y$.

Applying Lemma A.4.3 gives $\phi(y, z, \bar{y}, \bar{z}, \frac{m}{4})$ solutions for each pair $(y, z) \in \mathbb{Z}_{>0} \times \mathbb{Z}_{>0}$ where $y \not\equiv z \bmod 2$. We denote this condition by $(\star)$.

So we get

$$N_+ = \sum_{(y,z)} (-1)^y \phi(y, z, \bar{y}, \bar{z}, \frac{m}{4}). \tag{A.8}$$

Here the sum is over all (y, z) satisfying $(\star)$ and we note that we have removed the dependence of the sum on x and t.

Claim A.4.7.
The summation in Equation A.8 is a finite sum.

Proof.
Recall Lemma A.4.5 says $\phi(y, z, \bar{y}, \bar{z}, \frac{m}{4}) = 0$ for $y + z > \frac{m}{4}$. Since y and z are integers, there are only finitely many such y, z so that $y + z < \frac{m}{4}$. Hence the summation is a finite sum. □

Now let $S = \{(y, z, \bar{y}, \bar{z}, \frac{m}{4}) \mid y \not\equiv z \bmod 2\, y, z \in \mathbb{Z}_{>0},\ \frac{m}{4} \equiv \bar{y}y + \bar{z}z \bmod 2\}$.

Define $\psi : S \to S$ by $\psi(y, z, \bar{y}, \bar{z}, \frac{m}{4}) = (z, y, \bar{z}, \bar{y}, \frac{m}{4})$. The map ψ is well-defined and such that $\psi^2 = \text{id}$. Hence we have

$$\begin{aligned} N_+ = & \sum_{(y,z)} (-1)^y \phi(y, z, \bar{y}, \bar{z}, \frac{m}{4}) \\ = & \sum (-1)^y \phi(z, y, \bar{z}, \bar{y}, \frac{m}{4}) \text{ by Lemma A.4.3} \\ = & \sum (-1)^{z+1} \phi(z, y, \bar{z}, \bar{y}, \frac{m}{4}) \text{ as } y \not\equiv z \bmod 2 \\ = & -\sum (-1)^z \phi(z, y, \bar{z}, \bar{y}, \frac{m}{4}) \\ = & -N_+ \text{ as } \psi \text{ is a bijection.} \end{aligned}$$

Thus $N_+ = 0$ and the proof is complete using the result in the first proof that $N_+ = N_-$.

A.5 Weil's Three Squares Proof for $m \equiv 3 \bmod 8$

In this appendix we give a detailed examination of Andrë Weil's method for determining the number of representations of an integer m as a sum of three squares in the special case where $m \equiv 3 \bmod 8$.

Henceforth unless explicitly stated, in this section m shall refer to a positive integer such that $m \equiv 3 \bmod 8$.

Recall from Definition A.1.1 Weil defines $N_3(m)$ to be the number of representations of an integer m as $m = x_1^2 + x_2^2 + x_3^2$, where $x_i \equiv 1 \bmod 2$ and $x_i > 0$, $1 \leqslant i \leqslant 3$.

Lemma A.5.1.
$r_3(m) = 8N_3(m)$.

Proof.
Since $m \equiv 3 \bmod 8$ and for any integer we have $y^2 \equiv 0, 1, 4 \bmod 8$, it follows that any integer solution (y_1, y_2, y_3) to $m = y_1^2 + y_2^2 + y_3^2$ must satisfy $y_i \equiv 1 \bmod 2$ $(1 \leqslant i \leqslant 3)$. Thus no y_i is zero and consequently it is sufficient to find solutions for which all $y_i > 0$. This is denoted by $N_3(m)$ and it follows that there are 8 ways to assign signs to (y_1, y_2, y_3). Thus $r_3(m) = 8N_3(m)$. □

Hence it is sufficient for us to focus upon determining the value of $N_3(m)$.

Definition A.5.2.
Let $k \in \mathbb{Z}$ and let $H(k)$ denote the number of solutions (a, b, c), $a, b, c \in \mathbb{N}$ to

$$k = 4ac - b^2,\ b > 0,\ b < 2a,\ b < 2c,\ b \equiv 1 \bmod 2. \tag{A.9}$$

Observation A.5.3.
We observe $H(k) = 0$ unless $k > 0$ and $k \equiv 3 \bmod 4$. This is because $b^2 < (2a)(2c) =$

$4ac$ and $l^2 \equiv 1 \bmod 4$ for any odd integer l.
We also observe if $a \leqslant c$ then we have $0 < b \leqslant 2a \leqslant 2c$. Since $b \equiv 1 \bmod 2$ it follows that $0 < b \leqslant 2a - 1$. Consequently $k = 4ac - b^2$ implies:

$$\begin{aligned} k+1 &= 4ac - b^2 + 1 \\ &\geqslant 4ac - (4a^2 - 4a + 1) + 1, \text{ as } b^2 \leqslant (2a-1)^2 = 4a^2 - 4a + 1 \\ &= 4ac - 4a^2 + 4a \\ &= 4a(c - a + 1). \text{ Therefore } a \leqslant \frac{k+1}{4}. \end{aligned}$$

By the symmetry of the initial conditions, if $c \leqslant a$ then we get $k + 1 \geqslant 4c(a - c + 1)$ and so $c \leqslant \frac{k+1}{4}$.
In each case, we see that b is bounded and we conclude that c or a respectively is uniquely determined. So $H(k)$ is finite.

Observation A.5.4.
Assume $a \leqslant c$ and that an integer solution to $k = 4ac - b^2$ exists. Then we may write $a \leqslant c = \frac{k+b^2}{4a}$ and observe that for any fixed (positive) value of a, c is largest when b is largest. By Observation A.5.3 b is at most $2a - 1$, thus $c \leqslant \frac{k+(2a-1)^2}{4a} = \frac{k+4a^2-4a+1}{4a} = \frac{k+1}{4a} + a - 1$. This is a continuous function on the interval $[1, \frac{k+1}{4}]$ so we may apply the extreme value theorem. Both endpoints have the same value, $\frac{k+1}{4}$ and taking a derivative with respect to a yields $-\frac{(k+1)}{4a^2} + 1$. This is zero in our interval at $a = \frac{\sqrt{k+1}}{2}$. Applying the second derivative test shows this is a local minimum. Hence we see $c \leqslant \frac{k+1}{4}$ also. Similarly, if $c \leqslant a$ then we see that $a \leqslant \frac{k+1}{4}$. Thus any solution (a, b, c) that contributes to $H(k)$ must satisfy $a \leqslant \frac{k+1}{4}$, $b \leqslant \min\{2a-1, 2c-1\}$, $c \leqslant \frac{k+1}{4}$. This will be useful for any algorithm for determining the number of elements in $H(k)$.

Observation A.5.5.
Assume $k \equiv 3 \bmod 8$, $k = 4ac - b^2$ and $b \equiv 1 \bmod 2$. Then it follows that $4ac \equiv 4 \bmod 8$ since $l^2 \equiv 1 \bmod 8$ for any odd integer l. Hence ac must be odd and so both a and c are odd.

The crux of Weil's paper [We1974] is the connection between $N_3(m)$ and the cardinality of the set $H(m)$ when m is a positive integer such that $m \equiv 3 \bmod 8$. We give Weil's theorem below and devote the remainder of this appendix to proving it.

Theorem A.5.6 (Weil)**.**
Let m be a positive integer such that $m \equiv 3 \bmod 8$ then $N_3(m) = H(m)$.

The proof of Theorem A.5.6 requires several stages.

Lemma A.5.7.
Assume $l \equiv 4 \bmod 8$. Then $N_4(l) = \sum_{\substack{t>0 \\ t \equiv 1 \bmod 2}} N_3\left(l - t^2\right)$.

Proof.
Assume $l \equiv 4 \bmod 8$ and define
$S = \{(x,y,z,t) \,|\, x^2+y^2+z^2+t^2 = l,\ x,y,z,t \equiv 1 \bmod 2,\ x,y,z,t > 0\}$. Then clearly $N_4(l) = |S|$.
For each odd integer $t > 0$, let $S_t = \{(x,y,z,t) \,|\, x^2+y^2+z^2+t^2 = l\} \subseteq S$. If $t_i \neq t_j$ then $S_{t_i} \cap S_{t_j} = \emptyset$ because if $(x,y,z,t) \in S_{t_i} \cap S_{t_j}$ then $x^2+y^2+z^2+t_i^2 = l = x^2+y^2+z^2+t_j^2$ and since $t_i,\ t_j > 0$ it follows that $t_i = t_j$. Note that there are finitely many non-empty sets S_t since $t > 0$ and $t \leqslant \sqrt{l}$. Thus, $S = \bigcup_{\substack{t>0 \\ t \text{ odd}}} S_t$ and this is a disjoint union by the above.
Now observe that $|S_t| = N_3(l-t^2)$ as $x^2+y^2+z^2 = l-t^2$ and $t > 0$ is fixed, plus $t \equiv 1 \bmod 2$ implies $l - t^2 \equiv 3 \bmod 8$.
Hence we have

$$N_4(l) = \sum_{\substack{t>0 \\ t \equiv 1 \bmod 2}} |S_t| = \sum_{\substack{t>0 \\ t \equiv 1 \bmod 2}} N_3\left(l-t^2\right). \tag{A.10}$$

□

Our next lemma is pivotal in the proof of Theorem A.5.6. We will give its statement below and leave its proof until after we have proved Theorem A.5.6.

Lemma A.5.8.
Assume $l \equiv 4 \bmod 8$. *Then* $N_4(l) = \sum_{\substack{x>0 \\ x \equiv 1 \bmod 2}} H\left(l-x^2\right)$.

We now prove Theorem A.5.6 assuming the truth of Lemma A.5.8.

Proof of Theorem A.5.6.
Assume Lemma A.5.8 has been proved. We will use induction on m where m is a positive integer such that $m \equiv 3 \bmod 8$.
Base Step: $m = 3$, so $4 = m+1 \equiv 4 \bmod 8$
From Lemma A.5.7 we have $N_4(4) = \sum_{\substack{t \text{ odd} \\ t>0}} N_3\left(4-t^2\right) = N_3(3)$.
By the result in Lemma A.5.8 we also have $N_4(4) = \sum_{\substack{x \text{ odd} \\ x>0}} H\left(4-x^2\right) = H(3)$.
Hence $N_3(3) = H(3)$.

Inductive Step: Suppose that for some $k \equiv 3 \bmod 8$ we know $N_3(m) = H(m)$ for all $m \leqslant k$, where $m \equiv 3 \bmod 8$. We want to show this implies $N_3(k+8) = H(k+8)$.
We first note that for any odd positive integer t we have $k+1-(t^2-8) \equiv 3 \bmod 8$ as $t^2 \equiv 1 \bmod 8$. We also note that for $t \geqslant 3$, and odd, we have $t^2-8 \geqslant 1$ and so $k+1-(t^2-8) \leqslant k+1-1 = k$. Then applying Lemma A.5.7 yields:

$$N_4\left((k+8)+1\right) = \sum_{\substack{t \text{ odd} \\ t>0}} N_3\left((k+8)+1-t^2\right)$$

$$= N_3(k+8) + \sum_{\substack{t \text{ odd} \\ t>1}} N_3\left(k+1-(t^2-8)\right)$$
$$= N_3(k+8) + \sum_{\substack{t \text{ odd} \\ t>1}} H\left(k+1-(t^2-8)\right) \text{ by the inductive hypothesis.}$$

By Lemma A.5.8 we also know

$$N_4\left((k+8)+1\right) = \sum_{\substack{x \text{ odd} \\ x>0}} H\left((k+8)+1-x^2\right)$$
$$= H(k+8) + \sum_{\substack{x \text{ odd} \\ x>1}} H\left(k+1-(x^2-8)\right).$$

So substituting yields $N_3(k+8) = H(k+8)$.
Hence Theorem A.5.6 is true under the assumption that Lemma A.5.8 has been proved. □

We now proceed to prove Lemma A.5.8.

Notation A.5.9.
To simplify notation write $l = 4n$ where $n \equiv 1 \bmod 2$.
Also, write $X_n = \frac{1}{2} \sum_{\substack{x\in\mathbb{Z} \\ x\equiv 1 \bmod 2}} H\left(4n-x^2\right)$. Notice that the terms in this summation are symmetric with respect to x. Thus each $H(k)$ is counted twice. Hence X_n is the right hand side of the equation given in the statement of Lemma A.5.8.

Notation A.5.10.
We use a modified version of the notation used in [We1974, p. 220]. Let $\{R\}$ denote the set of relations that specify a system of equations that we wish to solve. $\{R\}$ may include equalities, inequalities and congruences as well as variables. We shall denote the number of integer solutions to the system $\{R\}$ by $|R|$.

Now fix $n \in \mathbb{Z}_{>0}$ and odd.
Using the notation already developed we may write

$$X_n = \frac{1}{2}\left|\left\{n = ac + \frac{x^2-b^2}{4},\ b>0,\ b<2a,\ b<2c,\ b \equiv x \equiv 1 \bmod 2\right\}\right|.$$

This is because $l \equiv 4 \bmod 8$, $l = 4n$ where n is odd, $X_n = \frac{1}{2}\sum H\left(4n-x^2\right)$ where the sum is over all odd integers, x, and $H\left(4n-x^2\right)$ is the number of solutions to $4n - x^2 = 4ac - b^2$, which rearranges to $n = ac + \dfrac{x^2-b^2}{4}$. Now $x^2 - b^2 \equiv 0 \bmod 4$ since $b, x \equiv 1 \bmod 2$ implies $b^2, x^2 \equiv 1 \bmod 4$. The rest of the relations follow from the previous conditions on $H(l-x^2)$.

Next observe that $b \equiv x \bmod 2$ implies $b + x = 2y$ for some $y \in \mathbb{Z}$. Similarly we may write $b - x = 2z$ for some $z \in \mathbb{Z}$. Observe that $x^2 - b^2 = (x - b)(x + b) = -4yz$, and that b odd and $b = y + z$ imply $y \not\equiv z \bmod 2$. Thus we get

$$X_n = \frac{1}{2} \left| \{ n = ac - yz,\ y + z > 0,\ y + z < 2a,\ y + z < 2c,\ y \not\equiv z \bmod 2 \} \right|.$$

Observe $b = y + z$ and $x = y - z$ imply there is a bijection between the two formulations for X_n. Notice $y \not\equiv z \bmod 2$ implies $yz \equiv 0 \bmod 2$. Then since $n \equiv 1 \bmod 2$ it follows that $ac \equiv 1 \bmod 2$ and so again we see that both a and c are odd.

Notice that the conditions for calculating X_n are symmetric in a and c and also in y and z. Since a and c are both odd, we have $a \equiv c \equiv 1 \bmod 2$. Then $y \not\equiv z \bmod 2$ implies that $a - y \not\equiv c - z \bmod 2$ and so $a - y \neq c - z$. Thus we may partition the solution set into those solutions that satisfy $a - y < c - z$ and those that satisfy $a - y > c - z$. Further, since a and c are positive integers (see Definition A.5.2), the conditions $y + z < 2a$ and $y + z < 2c$ imply $y + z < a + c$ and so $y - a < c - z$.

We define the sets S and T as follows:

$$\begin{aligned} S = \{ (a, c, y, z) \,|\, & n = ac - yz,\ y + z > 0,\ y + z < 2a,\ y + z < 2c, \\ & y \not\equiv z \bmod 2, a - y < c - z \} \\ T = \{ (a, c, y, z) \,|\, & n = ac - yz,\ y + z > 0,\ y + z < 2a,\ y + z < 2c, \\ & y \not\equiv z \bmod 2, c - z < a - y \}. \end{aligned}$$

We note that elements of S and elements of T satisfy $y - a < c - z$, while elements of S also satisfy $a - y < c - z$. Thus we may replace the condition $a - y < c - z$ in S by $|a - y| < c - z$. We denote this condition by (†).

Define $\tau : S \longrightarrow T$ by $\tau(a, c, y, z) = (c, a, z, y)$ and define $\sigma : T \longrightarrow S$ by $\sigma(a, c, y, z) = (c, a, z, y)$. We now show $\sigma \circ \tau = \mathrm{id}_S$ and $\tau \circ \sigma = \mathrm{id}_T$.

We note the map τ is well-defined since $a - y < c - z$ in S and $c - z$ is the new "$a - y$" in (c, a, z, y). Thus (c, a, z, y) is a valid solution in T. Similarly, σ is well-defined since $a - y > c - z$ in T and $c - z$ is the new "$a - y$" in (c, a, z, y). Thus (c, a, z, y) is a valid solution in S.
Now observe $\sigma \circ \tau(a, c, y, z) = \sigma(c, a, z, y) = (a, c, y, z)$ for any $(a, c, y, z) \in S$ and likewise $\tau \circ \sigma(a, c, y, z) = (a, c, y, z)$ for any $(a, c, y, z) \in T$. It follows that $\sigma \circ \tau = \mathrm{id}_S$ and $\tau \circ \sigma = \mathrm{id}_T$. Therefore we have a bijection between S and T, and so $|S| = |T|$.

Hence we observe adding the condition $a - y < c - z$ to the conditions in (X_n) leaves only half of the solutions. Thus

$$\begin{aligned} X_n &= \frac{1}{2} \left| \{ n = ac - yz,\ y + z > 0,\ y + z < 2a,\ y + z < 2c,\ y \not\equiv z \bmod 2 \} \right| \\ &= \left| \{ n = ac - yz,\ y + z > 0,\ y + z < 2a,\ y + z < 2c,\ y \not\equiv z \bmod 2, a - y < c - z \} \right| \end{aligned}$$

$$= |\{n = ac - yz,\, y + z > 0,\, y + z < 2a,\, y + z < 2c, y \not\equiv z \bmod 2, |a - y| < c - z\}| \,.$$

The last line here is due to (†).

Now define the sets A and B by

$$\begin{aligned} A &= \{(a, c, y, z) \,|\, n = ac - yz,\, 0 < y + z < 2a,\, y + z < 2c,\, y \not\equiv z \bmod 2, \\ &\quad |a - y| < c - z\} \,, \\ B &= \{(a, c, y, z) \,|\, n = ac - yz,\, 0 < y + z < 2a,\, y \not\equiv z \bmod 2,\, |a - y| < c - z\} \,. \end{aligned}$$

Then $A \subseteq B$ since $(a, c, y, z) \in A$ satisfies all the relations in B plus $y + z < 2c$. That is, the set of conditions for B is less restrictive than those for A.

Next define $C = B \setminus A$, that is

$$\begin{aligned} C = \{(a, c, y, z) \mid n = ac - yz, 0 < y + z < 2a,\, y + z > 2c, \\ |a - y| < c - z, y \not\equiv z \bmod 2\} \,. \end{aligned}$$

This is because $y \not\equiv z \bmod 2$ implies $y + z$ is not even, so $y + z \neq 2c$ and if $y + z < 2c$ then $(a, c, y, z) \in A$.
Observe that the condition $y + z < 2a$ in C is actually a consequence of the others. This is due to the following reasoning. Recall that a is a positive integer because $0 < y + z < 2a$. Further, $c - z > |a - y| \geqslant y - a$ implies $c - \underbrace{(y + z)}_{>0} > -a$ and so $c > -a$, that is $-c < a$. But we also have $c - z > y - a$ implies $c + a > y + z > 2c$, so $a > c$ and it follows that $a > |c|$. Thus $y + z < 2a$.

This is an important result because by going from the conditions in A to those in B, we have removed the condition that $0 < y + z < 2c$ and so in B we now have the possibility that c is negative.

Further, we note the condition $y \not\equiv z \bmod 2$ in $\{B\}$ implies yz is even; then $n = ac - yz$ implies both a and c are still odd.
Now we make the following change of variables on the set B. Let

$$\begin{aligned} a &= a \\ u &= a \quad - y \\ v &= \quad c \quad - z \\ w &= -a \quad + y - z \end{aligned}$$

This change of variables has matrix representation (with respect to the above ordering)

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \\ -1 & 0 & 1 & 1 \end{pmatrix} .$$

This matrix has determinant 1 and so the change of variables is a bijection.
The set B is mapped bijectively onto the set D where

$$D = \left\{(a,u,v,w) \,|\, n = u^2 + av + uw,\ |w| < a,\ |u| < v,\ a \not\equiv w \bmod 2\right\}.$$

This is because $n = ac - yz = a(u+v+w) - (a-u)(u+w) = u^2 + av + uw$ and $0 < y + z < 2a$ becomes $0 < a + w < 2a$, that is $|w| < a$. Similarly, $c - z > |a - y|$ becomes $u + v + w - (u + w) > |a - (a - u)|$, that is $v > |u|$. Lastly, $y \not\equiv z \bmod 2$ becomes $a - u \not\equiv u + w \bmod 2$ thus $a \not\equiv w \bmod 2$.

Note that a remained unchanged, so in D we have $a \equiv 1 \bmod 2$, then $a \not\equiv w \bmod 2$ implies $w \equiv 0 \bmod 2$.

We now consider solutions to $\{D\}$ for which $u = 0$. So $n = av$, $|w| < a$, $v > 0$ and $a \not\equiv w \bmod 2$. So we get at least one solution for every positive odd divisor a of n because $a \equiv 1 \bmod 2$. Now observe that we have $|w| < a$ and w is even, plus the value of w has no impact on the solution when $u = 0$. So since there are a even numbers w such that $-a < w < a$ (including $w = 0$), we get for each positive odd divisor a of n there are a solutions to $\{D\}$ when $u = 0$. Thus the total number of solutions to $\{D\}$ when $u = 0$ is $\sum_{\substack{a \text{ odd} \\ a|n}} a$ since $n \equiv 1 \bmod 4$ implies $4n \equiv 4 \bmod 8$.
By Proposition A.2.1 and Notation A.5.9 this is just $N_4(4n) = N_4(m)$.

Now partition the set of solutions (a,u,v,w) to $\{D\}$ as follows:

$$\begin{aligned} D_0 &= \{(a,u,v,w) \,|\, (a,u,v,w) \in D \text{ and } u = 0\}, \\ D_+ &= \{(a,u,v,w) \,|\, (a,u,v,w) \in D \text{ and } u > 0\}, \\ D_- &= \{(a,u,v,w) \,|\, (a,u,v,w) \in D \text{ and } u < 0\}. \end{aligned}$$

Clearly these sets are disjoint.

We now construct a bijection $\tau : D \longrightarrow D$ given by $\tau(a,u,v,w) = (a,-u,v,-w)$.
We see the map τ is well-defined because (a,u,v,w) satisfies $n = u^2 + av + uw = (-u)^2 + av + (-u)(-w)$, $|-w| = |w| < a$, $|-u| = |u| < v$ and $-w \equiv w \not\equiv a \bmod 2$. So τ maps D to D.
Now observe $\tau^2(a,u,v,w) = \tau(a,-u,v,-w) = (a,-(-u),v,-(-w)) = (a,u,v,w)$. Thus $\tau^2 = \mathrm{id}$ and so by Lemma 3.4.13, τ is a bijection.

Now observe if $(a,0,v,w) \in D_0$ then $\tau(a,0,v,w) = (a,0,v,-w) \in D_0$. Further, if $(a,u,v,w) \in D_+$ then $\tau(a,u,v,w) = (a,-u,v,-w) \in D_-$ as $u > 0$ implies $-u < 0$. Thus $\tau(D_+) \subseteq D_-$. It follows similarly that $\tau(D_-) \subseteq D_+$. Since τ is a bijection it follows that $|D_+| = |D_-|$.

Now consider the subset
$D_+ = \{(a,u,v,w) | n = u^2 + av + uw,\ |w| < a,\ v > u > 0, a \equiv 1 \bmod 2, w \equiv 0 \bmod 2\}$

and let $Y = |D_+|$. Since $|D_+| = |D_-|$ it follows upon recalling that the set B is in bijection with the set D that $|B| = |D_0| + 2|D_+| = N_4(m) + 2Y$.

Our goal remains to show B is a finite set and $|C| = 2Y$. This will complete the proof of Lemma A.5.8 because

$$\sum_{\substack{x \text{ odd} \\ x>0}} H\left(m - x^2\right) = X_n = |A| = |B| - |C| = (N_4(m) + 2Y) - (2Y) = N_4(m).$$

Resuming our consideration of D_+, we may write $n - u^2 = av + uw$. Recalling that n is odd, we note that if $u \equiv 0 \bmod 2$ then $n - u^2 \equiv 1 \bmod 2$, $uw \equiv 0 \bmod 2$, so we require $av \equiv 1 \bmod 2$. Noting $a \equiv 1 \bmod 2$ implies $v \equiv 1 \bmod 2$. Similarly if $u \equiv 1 \bmod 2$ then $n - u^2 \equiv - \bmod 2$, $uw \equiv 0 \bmod 2$ as $w \equiv 0 \bmod 2$. Thus we require $av \equiv 0 \bmod 2$. But $a \equiv 1 \bmod 2$ and so $v \equiv 0 \bmod 2$. Hence we see that $u \not\equiv v \bmod 2$.

We now note $n - u^2 = av + uw$ may be identified as a candidate for applying Lemma A.4.3. This is because we may think of "a" $= u$, "b" $= a$, "X" $= w$ and "Y" $= v$. The conditions in $\{D_+\}$ translate to $\underbrace{|X| < b}_{|w|<a}$, $\underbrace{a < Y}_{u<v}$, $\underbrace{x \equiv 0 \bmod 2}_{w \equiv 0 \bmod 2}$, $\underbrace{Y \equiv a + 1 \bmod 2}_{v \equiv u+1 \bmod 2}$ and $\underbrace{Y \not\equiv a \bmod 2a}_{v \not\equiv u \bmod 2u}$. We observe the last two conditions follow from $u \not\equiv v \bmod 2$, $v \equiv u + 1 \bmod 2$ and an application of Lemma A.4.6.

Hence we meet all of the conditions for Lemma A.4.3 and so the number of solutions to $\{D_+\}$ is

$$Y = \sum_{(u,a)} \phi(u, a, 0, \overline{u+1}, n - u^2) \tag{A.11}$$

where $u > 0$, $a > 0$ and $a \equiv 1 \bmod 2$.

By the proof of Lemma A.4.3, $\phi(u, a, 0, \overline{u+1}, n - u^2) = 0$ unless $n - u^2 \geqslant u + a$. Since n is fixed and both u and a are positive, it follows that for each u there are only finitely many values for a and since $n - u^2$ must be positive, there are only finitely many values for u. Hence Y is finite and so $|B| = N_4(m) + 2Y$ is finite.

We now turn our considerations to the set C. As discussed earlier here, we may omit the condition $0 < y + z < 2a$ so

$$C = \{n = ac - yz,\, y + z > 0,\, y + z > 2c,\, |a - y| < c - z,\, y \not\equiv z \bmod 2\}$$

We apply the following change of variables:

$$\begin{aligned} a &= u + v + w \\ y &= u + w \\ z &= -u + c \end{aligned}$$

$$c = \qquad\qquad\qquad c.$$

The associated matrix representation (with respect to this ordering) is

$$\begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ -1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

The determinant of this matrix is -1 and so the change of variables is invertible. Thus under this change of variables, the set C is mapped bijectively onto the set E, where

$$E = \left\{(u, v, w, c) \,|\, n = u^2 + cv + uw,\ w > |c|,\ u > |v|,\ w \not\equiv c \bmod 2\right\}.$$

This is because $n = ac - yz = (u+v+w)c - (u+w)(c-u) = u^2 + vc + uw$, $y + z > 0$ implies $w > -c$, $y + z > 2c$ implies $w > c$ and so $w > |c|$, $c - z > |a - y|$ implies $u > |v|$ and $y \not\equiv z \bmod 2$ implies $w \not\equiv c \bmod 2$.
Now recalling that in C we showed both a and c to be odd. Since we have constructed a bijection between the sets C and E via our change of variables, and c has not changed, we see $c \equiv 1 \bmod 2$ and consequently $w \equiv 0 \bmod 2$. It follows that $c \neq 0$.

Define $\tau' : E \longrightarrow E$ by $\tau'(u, v, w, c) = (u, -v, w, -c)$. We show the map τ' is a bijection.

Proof: τ' is well-defined since $n = u^2 + uw + vc = u^2 + uw + (-v)(-c)$, $|-c| = |c| < w$, $|-v| = |v| < u$ and $-c \equiv c \not\equiv w \bmod 2$.
Next, observe that $\tau'^2 = \tau'(u, -v, w, -c) = (u, -(-v), w, -(-c)) = (u, v, w, c)$. Hence $\tau'^2 = \mathrm{id}$ and so by Lemma 3.4.13, τ' is a bijection.

□

In a similar manner to earlier, we partition the set E according to whether c is positive or negative :

$$E_+ = \{(u, v, w, c) \mid n = u^2 + cv + uw, w > c > 0, u > |v|, c \equiv 1 \bmod 2, w \equiv 0 \bmod 2\}$$
$$E_- = \{(u, v, w, c) \mid n = u^2 + cv + uw, c < 0, w > |c|, u > |v|, c \equiv 1 \bmod 2, w \equiv 0 \bmod 2\}.$$

Note for any $(u, v, w, c) \in E_+$, we have $\tau'(u, v, w, c) = (u, -v, w, -c) \in E_-$. This is because $-c < 0$. So we have $\tau'(E_+) \subseteq E_-$ and a similar argument shows $\tau'(E_-) \subseteq E_+$. Since τ' is a bijection and we have shown that $c \neq 0$, it follows that $|E_+| = |E_-|$. Since there exists a bijection between the sets E and C, we have $|C| = |E| = 2|E_+|$.

Letting $Y' = |E_+|$, we see that $|C| = 2Y'$. Now we observe $n = u^2 + uw + vc$ may be rewritten as $n - u^2 = uw + vc$ and again we have a candidate for Lemma A.4.3.
We first show a result which is needed to verify we satisfy all of the conditions for Lemma A.4.3. Recall $n - u^2 = cv + uw$, $w \equiv 0 \bmod 2$ and $c \equiv 1 \bmod 2$. Then if

$u \equiv 0 \bmod 2$ it follows that $cv + uw \equiv 1 \bmod 2$ and so since $uw \equiv 0 \bmod 2$ we must have $v \equiv 1 \bmod 2$. Similarly, if $u \equiv 1 \bmod 2$ then it follows that $cv + uw \equiv 0 \bmod 2$ and so $cv \equiv 0 \bmod 2$ implies $v \equiv 0 \bmod 2$. Hence we have $u \not\equiv v \bmod 2$.

Now we may think of "a" $= c$, "b" $= u$, "X" $= v$ and "Y" $= w$. Then we have $\underbrace{|X| < b}_{|v|<u}$, $\underbrace{a < Y}_{c<w}$, $\underbrace{X \equiv \overline{b+1} \bmod 2}_{v \equiv \overline{u+1} \bmod 2}$, $\underbrace{Y \equiv 0 \bmod 2}_{w \equiv 0 \bmod 2}$ and $\underbrace{Y \not\equiv a \bmod 2a}_{w \not\equiv c \bmod 2c}$. Here the last relation follows from Lemma A.4.6 because $c \not\equiv w \bmod 2$ and $w \equiv 0 \bmod 2$.

Hence we may follow Lemma A.4.3 and define the number of solutions to (E_+) as

$$Y' = \sum_{(c,u)} \phi\left(c, u, \overline{u+1}, 0, n - u^2\right)$$

where the sum is over all (c, u) such that $c > 0$, $u > 0$ and $c \equiv 1 \bmod 2$. This sum is finite because there exists a bijection between the sets E and C, which is a subset of B, which we have shown is a finite set.

Now applying the result of Lemma A.4.3, we see that

$$Y' = \sum_{(c,u)} \phi\left(u, c, 0, \overline{u+1}, n - u^2\right)$$

and this is the same as Y in Equation A.11 where c plays the role of a.

Hence $Y' = Y$ and so $|A| = |B| - |C| = N_4(l) + 2Y - 2Y = N_4(l)$.

Thus $\sum_{\substack{x>0 \\ x \equiv 1 \bmod 2}} H\left(l - x^2\right) = N_4(l)$. This completes the proof of Lemma A.5.8.

Hence Theorem A.5.6 is proven.

Bibliography

[Fl1989] Daniel E. Flath. *Introduction to Number Theory.* John Wiley & Sons, 1989.

[Gr1985] Emil Grossward. *Representations of Integers as Sums of Squares.* Springer-Verlag, 1985.

[IR1990] Kenneth Ireland and Michael Rosen. *A Classical Introduction to Modern Number Theory*. Springer, 2nd edition, 1990.

[Kr1860] Leopold Kronecker. Über die Anzahl der verschiedenen Classen quadratischer Formen von negativer Determinante. *Journal für die Reine und Angewandte Mathematik*, 57:248-255, 1860.

[Kr1897] Leopold Kronecker. Über Bilineare Formen mit Vier Variabeln, (1883). In Kurt Hensel, editor, *Leopold Kronecker's Werke*, volume 2, pages 425-495. Königlich Preussischen Akademie der Wissenschaften, 1897.

[LeV1956] William Judson LeVeque. *Topics In Number Theory*, volume 2. Addison-Wesley, 1956.

[NZM1991] Ivan Niven, Herbert Zuckerman, and Hugh Montgomery. *An Introduction to the Theory of Numbers*. John Wiley & Sons, 1991.

[Ro2002] Joseph J. Rotman. *Advanced Modern Algebra*. Springer-Verlag, 2002.

[We1974] André Weil. Sur les sommes de trois et quatre carrés. *L'Enseignement Mathématique*, 20:215-222, 1974.

[Za1990] Don Zagier. A one-sentence proof that every prime $p \equiv 1 \bmod 4$ is a sum of two squares. *The American Mathematical Monthly*, 97(2):144-144, 1990.

Vita

Jonathan Angus Constable

Education

Advisor: Dr David Leep

- M.A., Mathematics, University of Kentucky, 2013.
- M.Math, Mathematics, 1st Class (Honours), University of St Andrews, Scotland, 2010.

Awards

- *College of Arts & Sciences Certificate for Outstanding Teaching*, University of Kentucky, 2014.