5-1-2014

Pre-computation in Width-w τ-adic NAF Implementations on Koblitz Curves

William Robert Trost
University of Wisconsin-Milwaukee

PRE-COMPUTATION IN WIDTH-W τ-ADIC NAF IMPLEMENTATIONS ON KOBLITZ CURVES

by

William R. Trost

A Thesis Submitted in
Partial Fulfillment of the
Requirements for the Degree of

Master of Science
in Computer Science

at

The University of Wisconsin - Milwaukee
May 2014

ABSTRACT

PRE-COMPUTATION IN WIDTH-W τ-ADIC NAF IMPLEMENTATIONS ON KOBLITZ CURVES

by
William R. Trost

The University of Wisconsin - Milwaukee, 2014
Under the Supervision of Professor Guangwu Xu

This paper examines scalar multiplication on Koblitz curves employing the Frobenius endomorphism. We examine simple binary scalar multiplication, binary Non Adjacent Formats or NAF's, followed by τ-NAF methods. We pay particular attention to *width-w* τ-NAF where we focus on pre-computation. We present alternative pre-computation arrangements for α_u for width sizes of 5 and 6 which are better than any previously published results since they: involve a single power of τ; are based on least norms; and have a maximum of $2^{w-2} - 1$ elliptic curve operations. We then study widths of 7 and 8 producing efficient arrangements. Arrangements for width sizes of 7 and 8 have never before appeared in the literature.

Furthermore, we introduce a simplified rounding technique for reduction modulo $\dfrac{\tau^m - 1}{\tau - 1}$ relaxing the requirement of least norms. Lastly, we discuss an $O(n)$ technique for finding arbitrary powers of τ in software.

To
my wife, Sharon, my son, Nathan
and
my daughter, Sammi

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

TABLE OF ALGORITHMS

LIST OF SYMBOLS

G	group
R	ring
I	ideal
F	field
$\mathbb{Z}$	the set of integers
$\mathbb{R}$	the set of real numbers
$\mathbb{C}$	the set of complex numbers
F_{2^m}	an extension field of characteristic 2 (binary field)
$\langle P \rangle$	the cyclic group generated by the point P
$R[x]$	a polynomial over the ring R
$\|G\|$	the order of the group G
E	elliptic curve
E_0	Koblitz curve where $a = 0$
E_1	Koblitz curve where $a = 1$
μ	$(-1)^{1-a}$ where $a = 0, 1$ from the Koblitz Curve
$\mathrm{E}(F)$	elliptic curve defined over a finite field F
∞	the identity element in the additive group $(\mathrm{E}(F), +)$
kP	the scalar multiple of the point P by the integer k
NAF	Nonadjacent Format
τ	the complex number $\dfrac{\mu + \sqrt{-7}}{2}$
$\mathbb{Z}[\tau]$	the ring of polynomials in τ with integer coefficients
τ-NAF	tau-addic NAF
$N(...)$	the norm
δ	$\dfrac{\tau^m - 1}{\tau - 1}$
$\overline{\delta}$	the conjugate of δ

ACKNOWLEDGEMENTS

First and foremost, I wish to express my sincere thanks to my thesis advisor and mentor Professor Guangwu Xu. This was a journey for me which proved to be difficult, surprising at times, but extremely rewarding. I will never forget reading the first few papers he suggested and thinking to myself, "how will I ever do this"? The mathematics was daunting for me but he was so willing to teach and encourage. There are no words to express my gratitude for all the time spent with me above and beyond a typical student/advisor relationship, and for answering every single one of my questions! His patience with me was unyielding. Somehow a sincere thank you just doesn't seem enough. I walk away with a tremendous amount of knowledge gained, not only in elliptic curve cryptography, but in mathematics as well. Well done Professor!

I also need to thank my family. My wife Sharon and my children Nathan and Samantha. I know I spent many hours away from them pursuing my master's degree as well as writing this thesis paper. I could not have done this without their encouragement, support, and understanding. I most certainly have been blessed with a wonderful family!

My heartfelt thanks to Professor Christine Cheng who was my first instructor upon starting my pursuit of a master's degree in computer science. She truly inspires her students! Most of all, however, I appreciated her "pearls of wisdom"- one of which was a personal mantra for my thesis project.

I thank my friend and colleague Ross Ellison. He allowed me to ramble on continuously about my thesis work and listened to every word I said. I also thank him for producing the "$\mathcal{U}$ Tiling" figure, 3.1 which I know took a lot of time. I appreciated his sound advice and feedback but, most of all, I appreciated his friendship.

I acknowledge the help and support from my peers and associates at AT&T- particularly Brian Rexroad, who suggested study in elliptic curve cryptography, Mark Regas, Craig Harvey, and Garry Hodgson. Without their support I would not have been able to complete this work. My deepest thanks!

Last, but certainly not least, my friend Homer Eshbaugh for spending many hours proofreading my thesis paper and correcting my grammar and punctuation. His wisdom has made this thesis substantially more readable for which I am very grateful.

Chapter 1

Introduction

Elliptic Curve Cryptography is an approach to data encryption proposed independently by Neal Koblitz [10] and Victor Miller [16] in 1985. It is based on the intractability of certain mathematical equations which, in this case, is the problem of discrete logarithms.

> Given an elliptic curve E defined over a finite field F_q, a point $P \in E(F_q)$ of order n, and a point $Q \in \langle P \rangle$, find the integer $k \in [0, n-1]$ such that $Q = kP$. The integer k is called the discrete logarithm or ECDLP of Q to the base P and denoted as $k = \log_P Q$ [8].

Such problems are also known as *one way functions* since it easy to compute the value of a function $y = f(x)$, given x, but very difficult to compute its inverse $x = f^{-1}(y)$ given y.

The goal of elliptic curve cryptography is to provide the same level of security as other well known asymmetric key encryption techniques, e.g. RSA, ElGamal and Rabin, but with a much smaller key size [6]. Table 1.1 provides a survey of key sizes.

The advantage of smaller keys sizes is that it takes less computational time to encrypt/decrypt information. Although symmetric key ciphers offer more security for smaller key sizes it requires that two parties share a key or “secret”. One of the disadvantages

Symmetric Key Size	RSA and Diffie-Hellman Key Size	Elliptic Curve Key Size
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	521

TABLE 1.1: Key Size Comparison (in bits) [14]

of symmetric key ciphers is the inability to scale. For example, if n parties wish to share secrets amongst themselves then this would require $\binom{n}{2} = \frac{n!}{(n-2)!2!}$ symmetric keys! Additionally, according to *Kerckhoff's Principle*, one should always assume that an adversary knows the encryption/decryption algorithm, and resistance to cipher attacks should be based solely on the inability to guess the key[6]. The key size should be large enough to make it extremely difficult to guess the key and impossible, or very nearly impossible, to enumerate all the possible key values. It should also be small enough that it can encrypt/decrypt information.

Although elliptic curve cryptography can utilize smaller key sizes, it relies heavily on scalar multiplication of kP where k is an integer (very large) and P is a point on the elliptic curve. As we will elaborate upon later in this thesis, we can form an algebraic group from a finite set of points on the elliptic curve under the binary operation of addition so that the meaning of kP is one of multiples, i.e. $P + P + \cdots + P$ up to k times. As we will discover, this is not your typical cartesian point addition, where we simply add points, but an addition that follows a *chord-tangent* rule.

Since scalar multiplication is a major operation in elliptic curve cryptography, a vast amount of research has been focused on improving scalar multiplication. This research ranges from improvements in the algorithms used to perform basic mathematical operations, such as multiplication and division (multiplication by inverse and exponentiation), to improvements in the implementation of scalar multiplication. This thesis mainly focuses on improvements in implementation, specifically pre-computation in *width-w* τ-NAF, but we also offer an improvement in the basic mathematical operation of power of squares needed in τ-adic methods.

One immediate improvement in calculating kP, over simply taking multiples of P, is to convert k to its binary representation taking advantage of the fact that *on average* 50% of the binary terms will be 0. Moreover, since computing "$-P$" is trivial, past researchers extended binary methods to *nonadjacent formats* or NAF's, capitalizing further on the sparseness. Further improvements were discovered by taking *width-w* NAF's where we pre-compute multiples of P in sizes up to w.

Koblitz [11] introduced a class of elliptic curves over a field of characteristic 2 taking advantage of the Frobenius mapping

$$\tau(\infty) = \infty, \qquad \tau(x, y) = (x^2, y^2)$$

whose characteristic equation is of the form

$$\tau^2 = \mu\tau - 2$$

where μ is a parameter derived from the elliptic curve. Koblitz called these curves *Anomalous Binary Curves*, but today they are labeled Koblitz curves in honor of their discoverer. These curves are recognized as some of the standard curves used for data encryption by the National Institute of Standards and Technology or NIST [12]. It is important to note that solving this characteristic equation for τ results in a complex number.

Since scalar multiplication is computationally expensive but squaring is relatively inexpensive, Koblitz showed that point doubling, $2P$, could be replaced by the much more efficient power series in τ by diligent use of the Frobenius characteristic equation. τP is substantially easier to compute then $2P$. This opened the door to a whole new methodology for scalar multiplication.

Jerome Solinas [19] took advantage of this fact and introduced a τ-adic NAF method which offered a 50% time improvement over any previously known methods for operating on nonsupersingular elliptic curves. Furthermore, Solinas demonstrated that any signed binary representation of an integer can be replaced by an equivalent (and unique) signed τ-adic expansion, in terms of sums and differences of distinct powers of τ, maintaining the nonadjacency property. Analogously following *width-w* binary NAF methods, Solinas extended his τ-adic NAF method to a window *width-w* τ-adic method utilizing pre-computation which offers dramatic savings in computational time.

Ian F. Blake, Kumar Murty, and Guangwu Xu in [2] proved the existence of a window τ-NAF using a more flexible approach which they called a *general window* τ*-adic form.* They further expanded this idea to characteristic 3 elliptic curves [1] and then on to all general quadratic Euclidean imaginary fields [3].

Pre-computation involves computing all multiples of P for a width size of w. It is, therefore, advantageous to streamline pre-computation, especially in larger width sizes of w, where pre-computation begins to dominate the total calculation time. Solinas offered a set of equation or arrangements for pre-computation using least norms but they were suboptimal.

Blake, Murty, and Xu [2] later provided a more optimal set of arrangements for a width size $w = 6$. They were able to do this by proving that other congruence class representatives, which were not of least norm, but, satisfying the condition that the norm of the representative is less than τ^w, could be used. This arrangement was more optimal but contained a τ^2 term.

We expanded upon this work in pre-computation and now offer better arrangements than any previously published results. These arrangements involve just a single power of τ, use least norms, and employ no more than $2^{w-2} - 1$ elliptic curve additions. We not only provide efficient arrangements for current width sizes, which have been published up to width size of 6, but expand this to width sizes of 7 and 8. Width sizes of 7 and 8 have never before been presented in the literature. This work is the result of tireless analysis and observation, first expanding on the smaller width arrangements, and then moving to the larger width 7 and 8 arrangements. We present our results for width sizes from 5 to 8 and conjecture that such efficient arrangements exist for even larger widths.

This thesis is organized into 5 chapters and several appendices. Chapter 2 covers background information with a brief study in abstract algebra for concepts needed in later chapters, as well as a thorough discussion on elliptic curve mathematics and scalar multiplication. Chapter 3 is an extensive survey of scalar multiplication techniques culminating in our work on pre-computation in *width-w* τ-adic NAF's. Our contribution begins at the end of chapter 3 and continues through chapter 4. Chapter 4 is our pinnacle chapter where we discuss how we derived our efficient arrangements based on observation, as well as a complete listing of these efficient arrangements for width size of 5 through 8. Chapter 5 offers a brief summary as well as possible future work. Appendices A: and B: provide a complete listing of τ-NAF's for all equivalence class representatives such that the norm of the representative is less than τ^w. These tables were used extensively in our search for efficient arrangements.

Chapter 2

Background and Preparation

2.1 Weierstrass Equations

An elliptic curve E over a field F is the graph of an equation of the form

$$\mathrm{E} : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{2.1}$$

where $a_1, a_2, a_3, a_4, a_6 \in F$ and $\triangle \neq 0$. $\triangle$ is the discriminant of E and is defined as follows:

$$\begin{cases} \triangle = -{d_2}^2 d_8 - 8{d_4}^3 - 27{d_6}^2 + 9d_2d_4d_6 \\ d_2 = {a_1}^2 + 4a_2 \\ d_4 = 2a_4 + a_1a_3 \\ d_6 = {a_3}^2 + 4a_6 \\ d_8 = {a_1}^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2{a_3}^2 - {a_4}^2 \end{cases}$$

If K is any extension field of F then the set of K rational points on E is given by

$$\mathrm{E}(K) = \{\infty\} \cup \{(x, y) \in K \times K \mid y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0\}$$

The ∞ element acts as the identity element and is justified by extending the affine plane over K to the projective plane, P^2_K, where the affine plane is defined as:

$$A^2_K = \{(x, y) \in K \times K\}$$

such that

$$A^2_K \hookrightarrow P^2_K.$$

All vertical lines in the x-y plane intersect at the point of ∞ in the projective plane. Additionally, $\infty = -\infty$*. In practical applications, such as computer programs, it is enough to treat the point at ∞ as a special case and assign a sentinel value consisting of any point not on E.

*For a further discussion of the projective plane and the point at ∞ see [20].

It is not possible to draw meaningful graphs of elliptic curves over most finite fields; however, to get an idea what an elliptic curve looks like, we can draw them over the real numbers as can be seen in figures 2.1 and 2.2. for the equation $y^2 = x^3 + ax + b$[*]

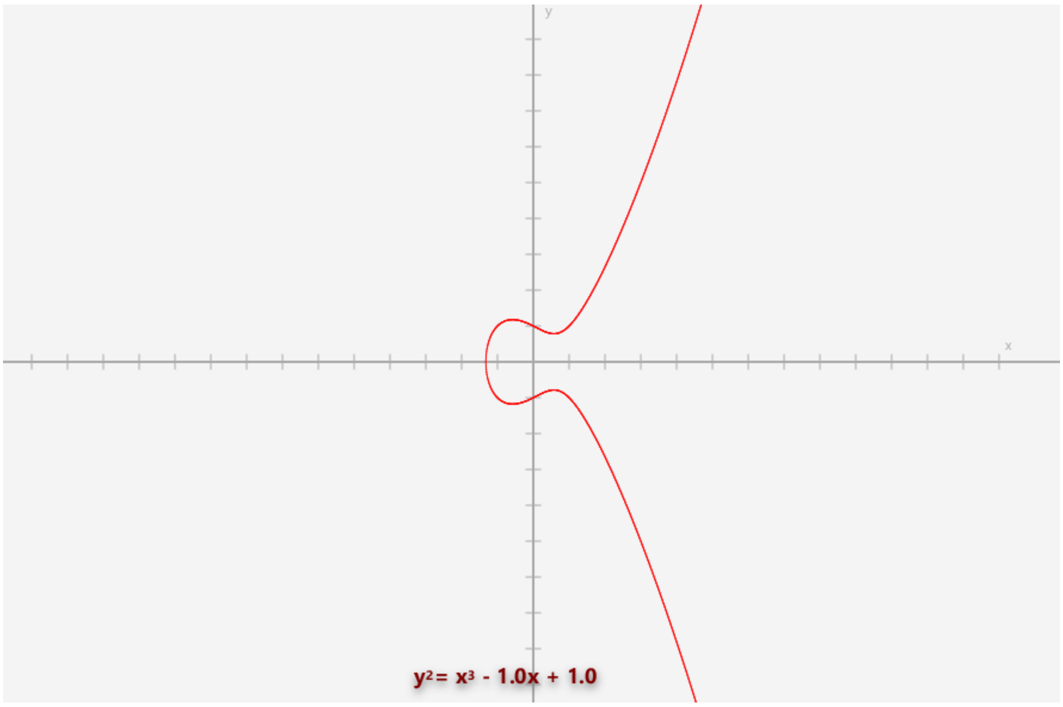

FIGURE 2.1: Elliptic Curve a = -1 and b = 1 with $F = \mathbb{R}$

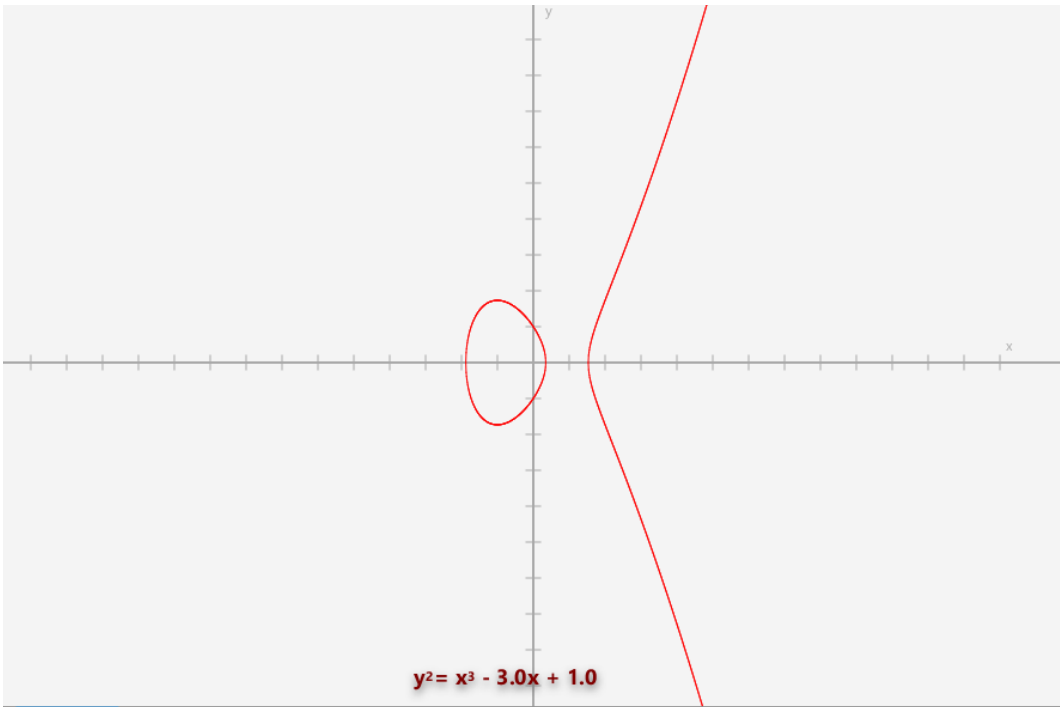

FIGURE 2.2: Elliptic Curve a = -3 and b = 1 with $F = \mathbb{R}$

[*] For a general in depth treatment of Weierstrass equations and elliptic curves in general see [8] [20] [18].

2.2 Review of Groups, Rings, and Fields

The purpose of this section is to provide a basic understanding of the mathematics required in Elliptic Curve Cryptography. We define the mathematical (abstract) structures of Groups, Rings, and Fields. This is not intended to be a panoptic treatment of this topic but a short review of this subject as it applies to the mathematics needed for later discussion. For a comprehensive treatise, we refer the reader to the many excellent resources that can be found in the bibliography. See [17] [7] [5] [9].

2.2.1 Groups

2.2.1.1 Group Definition

A **Group** is one of the most basic algebraic structures consisting of a set with a single binary operation designated as $*$. A binary operator $*$ on a nonempty set G is a rule which assigns to each ordered pair (a, b), $a, b \in G$, exactly *one* element a $*$ b in G, $a, b \in G \times G$. In symbolic form $* : G \times G \to G$ on a nonempty set G. A set G along with this binary operator $*$, denoted as $(G, *)$, satisfies the following axioms:

1. $*$ is associative. For all, $x, y, z \in G, x * (y * z) = (x * y) * z$.
2. There is an identity element e in G such that $a * e = a$ and $e * a = a$ for every element a in G.
3. For every element a in G, there is an element a^{-1} in G such that $a * a^{-1} = e$ and $a^{-1} * a = e$. That is, every element has an inverse.

Further, G is called an abelian group or commutative group, if for all $x, y \in G, x * y = y * x$. Note that this is not a requirement in order for the set G to be a group under $*$.

2.2.1.2 Order of a Group

If G is a finite group then the number of elements in G is called the *order of* G and is customarily denoted by the symbol $|G|$.

2.2.1.3 Subgroups

Among the nonempty subsets of a group G some subsets may themselves be groups with respect to the binary operator $*$. Such a subset is called a *subgroup* of G. Formally, if a subset $H \subseteq G$ forms a group with respect to $*$ then the subset H is called a subgroup of G.

If the order of a group G is finite then, by Lagrange's Theorem, the order of any subgroup of G divides the order of G. More precisely, if H is a subgroup of G, then $|G| \;/\; |H| =$ [G : H], an integer value, where [G : H] is called the index of H in G.

2.2.1.4 Cyclic Subgroups

If H is a group generated by a single element $a \in G$, we call H a *cyclic* subgroup generated by a which is denoted by $\langle a \rangle$.

More definitively, let G be a group. For any $a \in G$, the subgroup

$$H = \langle a \rangle = \{x \in G \,|\, x = a^n \text{ for some } n \in \mathbb{Z}\}$$

is the subgroup generated by a. That is, a is a generator of G and forms a cyclic group. The order of an element a is defined to be the least positive integer n such that $a^n = e$[*][†]. If there does not exist such a nonzero integer n then we say that a has order infinity.

2.2.2 Rings

Next in complexity is the algebraic structure termed a **Ring** which involves two binary operations, traditionally called addition and multiplication, and commonly denoted as $+$ and $\cdot$. One must caution that the definition of addition and multiplication in this case extends beyond the conventional meaning of addition and multiplication of numbers.

2.2.2.1 Definition of Rings

By a ring, then, we mean a set R with operations called addition and multiplication satisfying the following axioms:

1. R under the operation of addition alone forms an abelian group.
2. R is closed under multiplication. That is, $x, y \in R$ implies that $x \cdot y \in R$.[‡]
3. Multiplication is associative.

[*] If the operation on the group is multiplication then we speak in terms of powers of a, i.e. $a^0, a^1, a^2, \ldots, a^{n-1}$. When working with additive groups we speak of multiples of a, i.e. $\ldots, (-a) + (-a) + (-a), (-a) + (-a), -a, a, a + a, a + a + a$.

[†] The order of an element a is also defined as $| < a > |$.

[‡] In practice it is common to see $x \cdot y$ abbreviated as xy.

4. Two distributive laws hold on R, for all $x, y, z \in R$:
   (a) $x \cdot (y + z) = x \cdot y + x \cdot z$.
   (b) $(x + y) \cdot z = x \cdot z + y \cdot z$.

Since R under the operation of addition alone is an abelian group, there is an additive *identity* called the zero element written as 0. Additionally, every element has an additive *inverse*, called its negative, which is denoted by $-a$. Subtraction is then defined as:

$$a - b = a + (-b).$$

2.2.2.2 Commutative Ring

By definition, addition is commutative but there is *no* such requirement for multiplication. If multiplication is also commutative then we call this ring a commutative ring. In addition, there is no requisite that a ring have a multiplicative identity, i.e. an element $e \in R$, such that $xe = ex = x$ for all $x \in R$. If there is an identity under the operation of multiplication then it is called the unity of R and is denoted by the symbol 1. If R has a unity then we call R a *ring with unity.* Note that $1 \neq 0$. If $1 = 0$ and $x \in R$ then $x = x1 = x0 = 0$ and, hence, 0 must necessarily be the only element in the ring, i.e. we would have a trivial ring.

2.2.2.3 Ring with Unity

If R is a *ring with unity* e and there is an element x in R such that $ax = xa = e$ then x is a multiplicative inverse of a and a is called a *unit*[*]. The multiplicative inverse of a is denoted as a^{-1}.

The ring that we use later in this thesis will be a commutative ring with unity.

2.2.2.4 Zero Divisors

Let R be a ring and given $a \in R$ such that $a \neq 0$. If there exists another element $b \in R$ and $b \neq 0$ such that either $ab = 0$ or $ba = 0$ then a is called a *zero divisor.* For example, in the ring $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$, $2 \cdot 3 = 0$ even though the factors 2 and 3 are both nonzero[†].

[*] a is also said to be invertible.

[†] Notice, 3 and 4 are also zero divisors since $3 \cdot 4 = 0$.

2.2.2.5 Integral Domain

So far we have defined the terms *commutative ring, ring with unity,* and *zero divisors*, all of which are important concepts leading to the definition of an *integral domain.*

Let D be a ring. Then D is an Integral Domain provided:

1. D is a commutative ring.
2. D has a unity e and $e \neq 0$. The fact that $e \neq 0$ means that D must have at least two elements.
3. D has no zero divisors.

2.2.2.6 Ideals

A subset I is called an *ideal* of a ring R if I satisfies the following conditions:

1. I is nonempty.
2. $x \in I$ and $y \in I$ implies that $x + y \in I$. That is, I is closed under addition
3. $x \in I$ implies $-x \in I$. That is, I is closed under negatives.
4. $x \in I$ and $r \in R$ implies that xr and rx are in I. That is, I absorbs products in R.

More succinctly, a nonempty subset of I of a ring R is called an *ideal* of R if I is closed with respect to addition and negatives, and I absorbs products in R.

2.2.2.7 Cosets

Let R be a ring and I an ideal of R. For any element $r \in R$ the symbol $I + r$ denotes the set of all sums $i + r$ as r remains fixed and i ranges over I. Symbolically,

$$I + r = \{i + r \,|\, i \in I\}$$

$I + r$ is called the coset of I in R.

Notice that a ring R is an abelian group under addition and any ideal I of R is a normal subgroup of this additive group. Let R/I represent the additive group that consists of all the cosets

$$r + I = I + r = \{r + i \,|\, i \in I\}$$

of I in R. Further it can be shown that if $a \in R$ and $b \in R$ then

$$(a + I) + (b + I) = (a + b) + I$$

and hence, R/I is an abelian group with respect to this operation of addition, called coset addition, i.e. $(R/I, +)$

Additionally, we can form a ring from the cosets in R/I if we consider the multiplication defined by

$$(a + I)(b + I) = ab + I.$$

It can be shown that under this operation of multiplication, called coset multiplication, and the operation of coset addition defined above $(R/I, +, \cdot)$ forms a ring. This ring is called a quotient ring of R by I. Moreover, the quotient ring construction is a methodology for producing homomorphic images of any ring R. Matter of fact, it is a way of producing *all* of the homomorphic images of R. Homomorphism is discussed in detail in the next section.

2.2.2.8 Homomorphism

A ring homomorphism is a function or mapping between two rings which respects the operations of addition and multiplication.

More precisely, a homomorphism from a ring R to a ring S is a function $f : R \to S$ such that

1. $f(a + b) = f(a) + f(b)$ for all a and b in R.
2. $f(ab) = f(a)f(b)$ for all a and b in R.

If f is a homomorphism from a ring R to a ring S, the *kernel* of f is the set of all elements of R which are mapped by f onto the zero element of S. Thus, the kernel of f is the set

$$K = \{x \in R \,|\, f(x) = 0\}.$$

It is a very important fact that the kernel of f is an *ideal* of R.

An isomorphism from a ring R to a ring S is a homomorphism which has both a *one-to-one* (injective mapping) correspondence and *onto* (surjective mapping) correspondence. This is written symbolically as

$$R \cong S.$$

By the *Fundamental Theorem of Ring Homomorphisms* we have

Theorem 2.1. *If f is an onto mapping from a ring R to a ring S then S is isomorphic to R/K where K is the kernel of f.*

2.2.2.9 Characteristic of a Ring

If there are positive integers n such that $nr = 0$ for *all* r in the ring R then the smallest such *positive* integer is called the characteristic of R. If no such positive integer exists then R is said to have characteristic zero.

For example, the ring of integers, $\mathbb{Z}$, has characteristic zero since $nr = 0$ for all $r \in R$ requires that $n = 0$; whereas, the finite ring $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ has characteristic 6 since $6r = 0$ for all $r \in \mathbb{Z}_6$.

2.2.3 Field

If R is a *commutative ring with unity in which every nonzero element is invertible* then R is called a **field**. In other words, a ring R, $(R, +, \cdot)$, is a field if $(R\backslash\{0\}^*, \cdot)$ is also an abelian group.

Some important properties of fields are[†]:

1. Every field is an integral domain.
2. Every *finite* integral domain is a field.
3. $\mathbb{Z}_n$ is a field if and only if n is prime.

Fields are of considerable importance in mathematics since they possess many beautiful properties and have many fascinating applications. Some important fields are: the field of rational numbers, $\mathbb{Q}$; the field of real numbers, $\mathbb{R}$; and the field of complex numbers, $\mathbb{C}$. All of these will be exploited later in this thesis.

2.2.3.1 Polynomials over a Ring

Let R be a commutative ring with unity 1, and let x be an indeterminant[‡]. A polynomial in x with coefficients in R is an expression of the form:

$$a_0x^0 + a_1x^1 + a_2x^2 + \ldots + a_nx^n$$

where n is a nonnegative integer and each $a_i \in R$. The set of all polynomials in x over R is denoted by the symbol $R[x]$.

In order to specify the ring of polynomial, we need to define two binary operators, viz. addition and multiplication. Let $f(x) = \sum_{i=0}^{n} a_ix^i$ and $g(x) = \sum_{i=0}^{m} a_ix^i$ in $R[x]$. Define

[*] The set of elements in R less the zero element.

[†] See [17] [7] [5] [9] for proofs of these properties.

[‡] x is nothing but a formal symbol used as a placeholder here.

addition as:

$$f(x) + g(x) = \sum_{i=0}^{k} (a_i + b_i)x^i$$

where k is the larger of n or m[*]. Additionally, define multiplication as:

$$f(x)g(x) = \sum_{i=0}^{n+m} c_i x^i$$

where

$$c_i = \sum_{j=0}^{i} a_j b_{i-j}.$$

It can be shown[†] that, under the operations of addition and multiplication defined above, $R[x]$ is, indeed, a ring.

Because of the possible presence of zero divisors, synonymous with our earlier discussion on rings, and, in order to obtain the results we need on the division of polynomials required later in this paper, the ring of coefficients must actually be a field. This assures that every nonzero element of F has a multiplicative inverse. The polynomial whose coefficients come from a field will be denoted as $F[x]$.

2.2.3.2 Irreducible Polynomial

A polynomial of positive degree n over the field F has at most n distinct zeros in F. A polynomial $p(x)$ in $F[x]$ is *irreducible* if $p(x)$ cannot be expressed as a product $p(x) = f(x)g(x)$ with both $f(x)$ and $g(x)$ of positive degree. $p(x)$ is said to be reducible if it is not irreducible.

2.2.3.3 Polynomial Quotient Ring

If $p(x)$ is a polynomial with positive degree over the field F then $F[x]/(p(x))$ along with coset addition defined as

$$[f(x) + (p(x))] + [g(x) + (p(x))] = (f(x) + g(x)) + (p(x)),$$

and coset multiplication defined as

$$[f(x) + (p(x))][g(x) + (p(x))] = f(x)g(x) + (p(x))$$

forms a quotient ring. It can be further shown that this is a commutative ring with unity.

If $p(x)$ is an irreducible polynomial then the ring $F[x]/(p(x))$ is a field.

2.2.3.4 Extension Field

If F and K are fields such that $K \subseteq F$ then F is called an extension field of K

[*] We extend the smaller polynomial with leading zero terms.

[†] Again, we point the reader to the excellent resources in the bibliography for proofs.

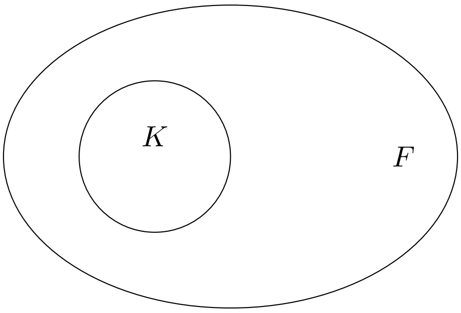

Figure 2.3: Showing F as an extension field of K

Extension fields are important since it can be proved that if a polynomial over F has no roots in F then there exists a suitable extension field of F which does contain roots. A perfect example of this is the polynomial $x^2 + 1 = 0$ which has no roots in $\mathbb{R}$. It does, however, have roots (solution) in $\mathbb{C}$. In fact, if we let F be a field and $p(x)$ a nonconstant polynomial in $F[x]$ then there exists an extension field K of F and an element c in K such that c is a root of $p(x)$.

2.3 Mathematics of Elliptic Curves

2.3.1 Elliptic Curve as an Additive Group

If E is an elliptic curve defined over the *field* F (or an extension field of F), then there is a tangent-chord rule for adding two points in E(F) to give a third point in E(F). Under the binary operation of addition, and, setting the identity element as ∞, the set of E(F) forms an abelian group, (E(F), +). That is to say, it forms an additive group such that:

1. $P + Q = Q + P$ for all P, Q on E (Commutativity).
2. $P + \infty = P$ for all points P on E. (Existence of Identity Element).
3. Given P on the curve E there exist a Q such that $P + Q = \infty$. The point Q will usually be expressed as $-P$ (Additive Inverse).
4. $(P + Q) + R = P + (Q + R)$ for all P, Q, R on E (Associativity).

Again, it is not possible to draw meaningful graphs over the finite field F, since we have a discrete number of points, but we can get a "flavor" for how the tangent-chord rule behaves on the field $\mathbb{R}$. Figures 2.3 and 2.4 depict point addition and figure 2.5 demonstrates point doubling.

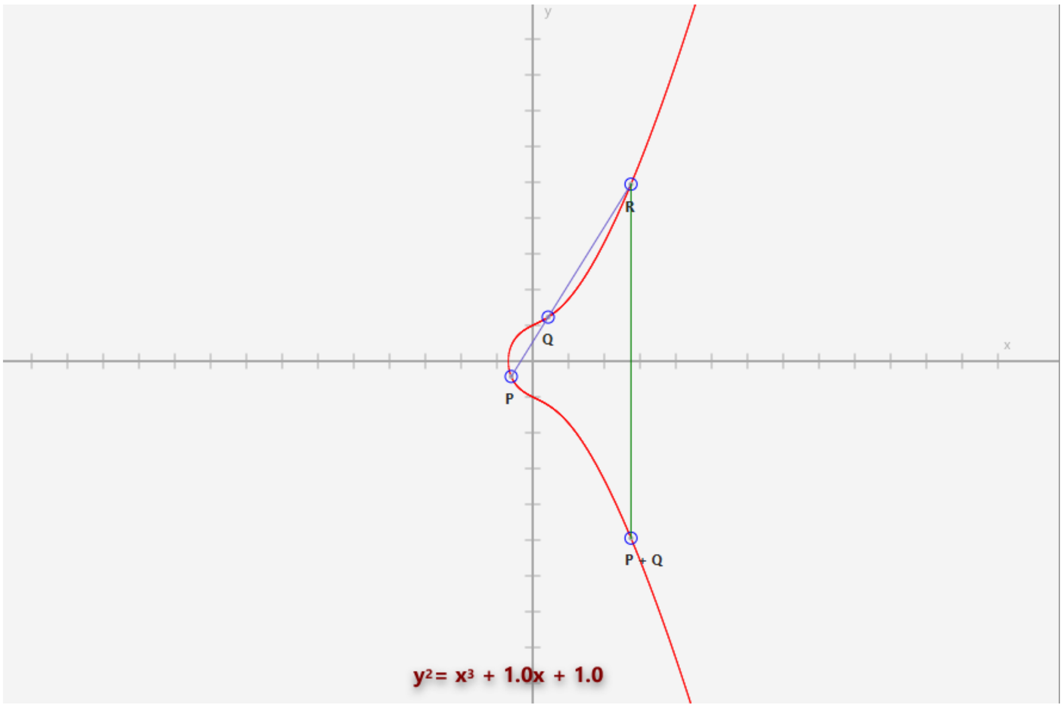

FIGURE 2.4: Elliptic Curve $y^2 = x^3 + x + 1$ demonstrating point addition

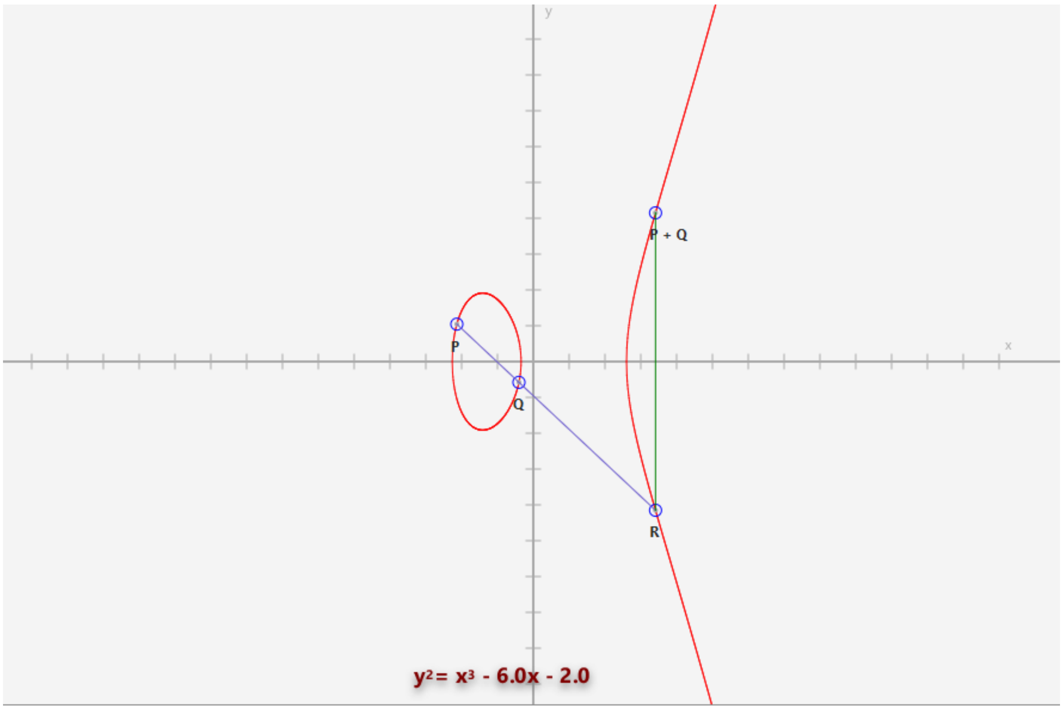

FIGURE 2.5: Elliptic Curve $y^2 = x^3 - 6x - 2$ demonstrating point addition

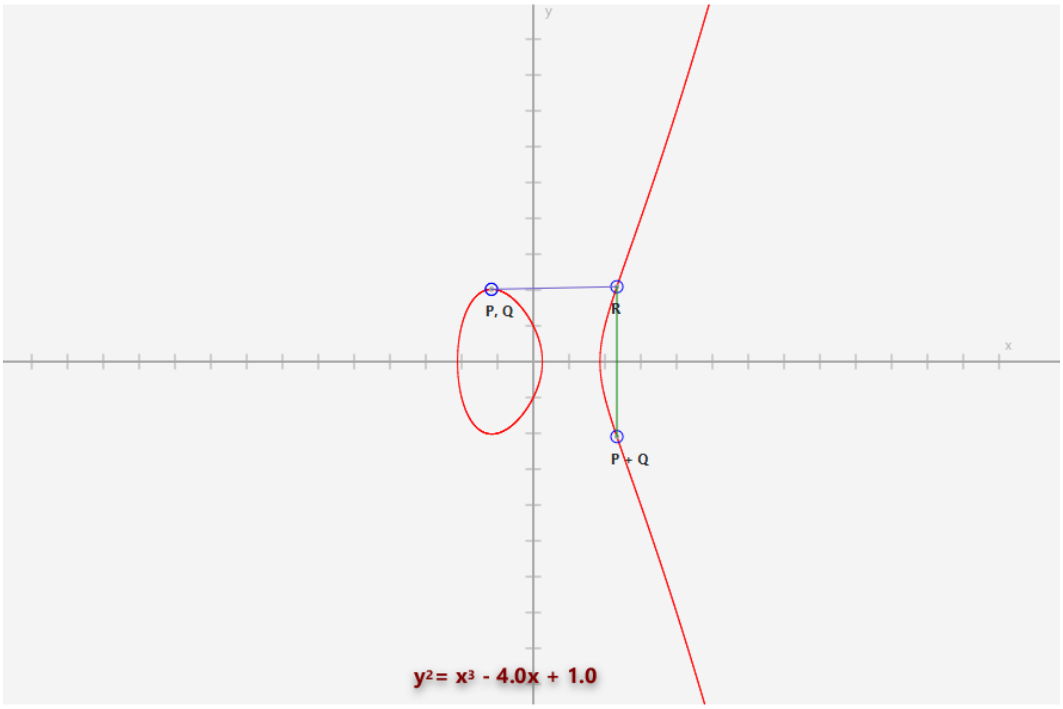

FIGURE 2.6: Elliptic Curve $y^2 = x^3 - 4x$ demonstrating point doubling when $P = Q$

2.3.2 Elliptic Curves over F_{2^m}

For the purpose of our research, we work with a specific class of elliptic curves over the finite field F_{2^m} where m is prime and the characteristic is 2. By making an appropriate change of variable, this results in a simplified version of the Weierstrass equation. Given a field with characteristic 2, there are two cases to consider, viz. $a_1 = 0$ and $a_1 \neq 0$.

If $a_1 = 0$ then the permissable change of variables is defined as:

$$(x, y) \to (x + a_2, y) \tag{2.2}$$

which transforms the elliptic curve (2.1) into

$$y^2 + cy = x^3 + ax + b \tag{2.3}$$

where $a, b, c \in K$ with discriminant $\triangle = c^4$.

If $a_1 \neq 0$ then we can apply the following change of variables

$$(x, y) \to \left(a_1^2 x + \frac{a_3}{a_1}, a_1^3 y + \frac{a_1^2 a_4 + a_3^2}{a_1^3} \right) \tag{2.4}$$

which transforms the elliptic curve (2.1) into

$$y^2 + xy = x^3 + ax^2 + b \tag{2.5}$$

where $a, b \in K$ with discriminant $\triangle = b$. [8][20].

We are mostly interested in the latter for the case where $a = 0$ or 1 since such curves are nonsingular, i.e. there is a tangent line at each point*, and they have interesting properties which we can exploit to substantially improve scalar multiplication. Such curves are called *anomalous binary curves*. See section 3.2.

2.3.3 Group Law for E/F_{2^m} : $y^2 + xy = x^3 + ax^2 + b$

1. Identity: $P + \infty = \infty + P = P$ for all $P \in \text{E}(F_{2^m})$.

2. Negatives: if $P = (x, y) \in \text{E}(F_{2^m})$ then $(x, y)+(x, x+y) = \infty$. Since $P+(-P) = \infty$ then $-P = (x, x + y)$.

3. Point Addition: Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ such that $P, Q \in \text{E}(F_{2^m})$ and $P \neq \pm Q$ then $P + Q = (x_3, y_3)$ where:

   $$x_3 = \lambda^2 + \lambda + x_1 + x_2 + a$$

   and

   $$y_3 = \lambda(x_1 + x_3) + x_3 + y_1,$$

   and $\lambda = \dfrac{y_1 + y_2}{x_1 + x_2}$.

4. Point Doubling: Let $P = (x_1, y_1) \in \text{E}(F_{2^m})$ such that $P \neq -P$. Then $2P = (x_3, y_3)$ where

   $$x_3 = \lambda^2 + \lambda + a = x_1^2 + \frac{b}{x_1^2}$$

   and

   $$y_3 = x_1^2 + \lambda x_3 + x_3$$

   with

   $$\lambda = x_1 + \frac{y_1}{x_1}.$$

*The first derivative does not vanish at any points.

2.3.4 Group Law for $\mathbf{E}/F_{2^m} : y^2 + cy = x^3 + ax + b$

Although we will not be considering this class of binary elliptic curves I present the group law for completeness:

1. Identity: $P + \infty = \infty + P = P$ for all $P \in \mathrm{E}(F_{2^m})$.

2. Negatives: if $P = (x, y) \in \mathrm{E}(F_{2^m})$ then $(x, y)+(x, y+c) = \infty$. Since $P+(-P) = \infty$ then $-P = (x, y + c)$.

3. Point Addition: Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ such that $P, Q \in \mathrm{E}(F_{2^m})$ and $P \neq \pm Q$ Then $P + Q = (x_3, y_3)$ where:

   $$x_3 = \lambda^2 + x_1 + x_2$$

   and

   $$y_3 = \lambda(x_1 + x_3) + y_1 + c,$$

   and $\lambda = \dfrac{y_1 + y_2}{x_1 + x_2}$.

4. Point Doubling: Let $P = (x_1, y_1) \in \mathrm{E}(F_{2^m})$ such that $P \neq -P$. Then $2P = (x_3, y_3)$ where:

   $$x_3 = \left(\frac{x_1^2 + a}{c}\right)^2$$

   and

   $$y_3 = \left(\frac{x_1^2 + a}{c}\right)(x_1 + x_3) + y_1 + c.$$

We present algorithm 1 for an implementation of point addition, and algorithm 2 for a naive approach to scaler multiplication on elliptic curves. Algorithm 2 is particularly naive since it is infeasible to calculate large values of k and is synonymous with computing exponentiation over a large group.

Algorithm 1: Basic Elliptic Curve Point Addition for $y^2 + xy = x^3 + ax^2 + b$

```
Input: Points $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ on E
Output: The sum $R := P + Q$
if $P = \infty$[a] then
    output $R \leftarrow Q$ and stop
if $Q = \infty$ then
    output $R \leftarrow P$ and stop
if $x_1 = x_2$ then
    if $y_1 + y_2 = x_2$ then
        output $\infty$ and stop
    else
        $\lambda \leftarrow x_2 + y_2/x_2$
        $x_3 \leftarrow \lambda^2 + \lambda + a$
        $y_3 \leftarrow x_2^2 + (\lambda + 1)x_3$
else
    $\lambda \leftarrow (y_1 + y_2)/(x_1 + x_2)$
    $x_3 \leftarrow \lambda^2 + \lambda + x_1 + x_2 + a$
    $y_3 \leftarrow (x_2 + x_3)\lambda + x_3 + y_2$
Output $R \leftarrow (x_3, y_3)$
```

[a] The point at infinity. Sometime written as $\mathcal{O}$ in the literature. In software, this is typically implemented as any point **not** on the curve- typically (0, 0) if this point is not on the curve.

Algorithm 2: Computing kP (Naive)

```
Input:
        A positive integer $k$
        A point $P$ on the elliptic curve
Output: $kP$
$Q \leftarrow \infty$
for $i = 0; i < k; i++$ do
    $Q \leftarrow Q + P$      // using a point addition algorithm
return Q      // $kP$
```

Chapter 3

Methods

3.1 Elliptic Curve Scalar Multiplication

Since we are working with points on an elliptic curve, a majority of the computational time is spent performing point addition and subtraction in the abelian group, $(E(F), +)$. Specifically, when dealing with elliptic curve cryptography, a majority of the protocols are based on scalar multiplication where a point P is added to itself k times, denoted as kP, and, hence, the computational time depends mostly on the complexity of scalar multiplication.

This section discusses techniques that offer improvements in performing scalar multiplication, culminating in our research on *width-w* $\tau - adic$ NAF's as applied to a specific class of elliptic curves known as Anomalous Binary Curves (ABC's) or Koblitz curves. This class of curves has some very interesting mathematical properties which, particularly, lend themselves to substantially improved scalar multiplication techniques.

We also propose a simplified rounding technique as well as a method for efficiently computing higher powers of the τ endomorphism in software. Finally, we examine the *width-w* equivalence class tables and provide, what we believe, are optimal arrangements of these tables in α_u.

3.1.1 Binary Method

A simple approach but an improvement over algorithm 2 is to convert the integer k to its binary format and only consider *nonzero* bits. Note that every integer has a unique binary representation.

Algorithm 3: Binary Method for Computing kP

```
Input:
        A positive integer $k$ in the binary format $(b_0 b_1 \cdots b_{t-1})$
        A point $P$ on the elliptic curve
Output: $kP$
$Q \leftarrow P$
for $i = t - 2; i \geq 0; i--$ do
    $Q \leftarrow 2Q$
    if $b_i = 1$ then
        $Q = Q + P$        // using a point addition algorithm
return Q        // $kP$
```

The complexity of this algorithm is[*]

$$mD + \frac{m}{2}A$$

where m = $\lceil log_2 k \rceil$, D is the number of point doublings, and A is the number of point additions [8].[†]

3.1.2 Non Adjacent Format (NAF)

As a further improvement, we can reduce the number of point additions by converting the scalar multiplier k to its nonadjacent format, NAF, representation. Just as every integer has a unique binary representation, every integer also has a unique NAF.

More formally, a NAF for an integer $k > 0$ has the following representation:

$$k = c_0 + c_1 2 + c_2 2^2 + \ldots + c_{t-1} 2^{t-1}$$

such that

1. $c_i \in \{0, 1, -1\}$.
2. $c_i c_{i+1} = 0$.

When computing the binary representation of a positive integer, we repeatedly divide by 2 and store off the remainder until one can no longer divide by 2. To compute the NAF, we follow the same process but, instead, allowing a remainder of -1, 0, or 1 and choosing the remainder which makes the quotient even. This can be implemented in software by algorithm 4.

[*] $t - 1 \backsim log_2 n$.

[†] You would expect, on average, that $b_i = 1$ half of the time, and hence, we reduce the number of additions by one half.

Algorithm 4: Computing NAF(k)

```
Input: A positive integer $k$
Output: NAF(k)
$i \leftarrow 0$
while $k \geq 1$ do
    if $k$ mod $2 \neq 0$ then
        $c_i \leftarrow 2 - (k \bmod 4)$
        $k \leftarrow k - c_i$
    else
        $c_i \leftarrow 0$
    $k \leftarrow k/2$
    $i++$
return $c_0, c_1, \ldots, c_{t-1}$
```

Example 3.1. *As an example, we compute the* NAF *of* $k = 107$

$$\mathrm{NAF}(107) = \{1, 0, 0, -1, 0, -1, 0, -1\} = 128 - 16 - 4 - 1 = 107.$$

The scalar multiplication k of a point P, kP, on an elliptic curve, can be computed as follows by algorithm 5.

Algorithm 5: Computing kP using NAF(k)

```
Input:
        The NAF of a positive integer $k$
        A point $P$ on the elliptic curve
Output: The point $kP$
$Q \leftarrow P$
for $i = t - 2; i \geq 0; i --$ do
    $Q \leftarrow 2Q$        // Point Doubling
    if $c_i = 1$ then
        $Q \leftarrow Q + P$        // Point Addition
    else if $c_i = -1$ then
        $Q \leftarrow Q - P$        // Point Addition
return $Q$
```

The complexity of this algorithm is approximately

$$mD + \frac{m}{3}A$$

due to that fact that the *average* density of nonzero digits is close to 1/3 [8].

It should be noted that this is not the most efficient implementation since it requires the computation of NAF(k) up front (called a left-to-right method) requiring more storage space. It is possible to use a right-to-left method which builds up the NAF starting at the least significant bit and ending at the most significant bit. Although this does not change the complexity of the algorithm, it does offer an improvement in storage and overall running time.

3.1.3 Non Adjacent Format (NAF) - Window Method

A more efficient NAF algorithm can be devised with the use of additional memory and performing some precalculation. This method is called the *width-w window method* and will be denoted as $\text{NAF}_w(k)$. It can be shown that given $w > 1$ then each positive integer k has a unique *width-w* τ-NAF of the form:

$$k = \sum_{i=0}^{l-1} u_i 2^i$$

where

1. each nonzero u_i is odd and $|u_i| < 2^{w-1}$.
2. among any w consecutive coefficients, at most only one is nonzero.

Additionally, $\text{NAF}_w(k)$ have the following properties [8]:

1. $\text{NAF}_2(k) = \text{NAF}(k)$.
2. The length of $\text{NAF}_w(k)$ is at most one more digit (binary) in length when compared to the corresponding binary representation.
3. The *average* density of nonzero digits among all $\text{NAF}_w(k)$ of the same length for a given w is approximately $1/(w+1)$.

The $\text{NAF}_w(k)$ can be efficiently computed using algorithm 6.

Algorithm 6: Computing $\text{NAF}_w(k)$

```
Input:
        A positive integer $k$
        $w > 1$
Output: $\text{NAF}_w(k) = \langle u_{l-1}, u_{l-2}, \ldots, u_1, u_0 \rangle$
$c \leftarrow k$
$NAF \leftarrow \langle\rangle$
while $c > 0$ do
    if $c$ is odd then
        $u = c \text{ mods}^a\ 2^w$
        $c \leftarrow c - u$
    else
        $u \leftarrow 0$
    Prepend $u$ to $NAF$
    $c \leftarrow c/2$
return $NAF$
```

[a] mods means that the remainder u satisfies $-2^{w-1} \leq u < 2^{w-1}$.

Notice that when $w = 2$, this reduces to the case of the ordinary NAF.

Example 3.2. *As an example, we compute the* NAF *of* $k = 107$ *for window sizes* $2 \leq w \leq 6$. *Notice that* $\text{NAF}_2(107)$ *furnishes the same representation as that of the ordinary* NAF

- $\text{NAF}_2(107) = \langle 1, 0, 0, -1, 0, -1, 0, -1 \rangle = 1 \cdot 2^7 - 1 \cdot 2^4 - 1 \cdot 2^0 = 128 - 16 - 4 - 1 = 107$
- $\text{NAF}_3(107) = \langle 1, 0, 0, 0, -3, 0, 0, 3 \rangle = 1 \cdot 2^7 - 3 \cdot 2^3 + 3 \cdot 2^0 = 128 - 24 + 3 = 107$
- $\text{NAF}_4(107) = \langle 7, 0, 0, 0, -5 \rangle = 7 \cdot 2^4 - 5 \cdot 2^0 = 112 - 5 = 107$
- $\text{NAF}_5(107) = \langle 3, 0, 0, 0, 0, 11 \rangle = 3 \cdot 2^5 + 11 \cdot 2^0 = 96 + 11 = 107$
- $\text{NAF}_6(107) = \langle 1, 0, 0, 0, 0, 0, 0, -21 \rangle = 1 \cdot 2^7 - 21 \cdot 2^0 = 96 + 11 = 107.$

The scalar multiplication k of a point P on an elliptic, kP, can be computed using algorithm 7 using the $\text{NAF}_w(k)$ algorithm 6.

Algorithm 7: Computing kP using $\text{NAF}_w(k)$

```
Input:
        The $NAF_w$ of a positive integer $k$
        A point $P$ on the elliptic curve
Output: The point $kP$
$P_0 \leftarrow P$
$P_{2^{w-2}-1} \leftarrow 2P_0$
for $i = 1; i < 2^{w-2} - 1; i++$ do
    $P_i \leftarrow P_{i-1} + P_{2^{w-2}-1}$
$Q \leftarrow \infty$
for $i = l - 1; i \geq 0; i--$ do
    $Q \leftarrow 2Q$
    if $u_i \neq 0$ then
        $j \leftarrow (|u_i| - 1)/2$
        if $u_i > 0$ then
            $Q \leftarrow Q + P_j$
        else
            $Q \leftarrow Q - P_j$
    return $Q$
```

According to [8], the complexity of this algorithm is approximately

$$[D + (2^{w-2} - 1)A] + \left[\frac{m}{w+1} A + mD \right]$$

3.2 Koblitz Curves

We now turn our attention to a specific class of elliptic curves which are particulary well suited for scalar multiplication. A method using τ-NAF's, which boasts a 50% improvement in computation time over any previously known methods, was first presented by Solinas in [19] for such a class of elliptic curves. We review this class of curves along with the τ-NAF method and present some improvements.

Anomalous binary curves[*] or ABC's for short were first proposed by Neal Koblitz in his seminal paper on utilizing elliptic curves in cryptography [10]. ABC's are more commonly called Koblitz curves and contain properties which provide for efficient scalar multiplication. These curves are defined over F_2 as follows:

1. $\mathrm{E}_0 : y^2 + xy = x^3 + 1$.
2. $\mathrm{E}_1 : y^2 + xy = x^3 + x^2 + 1$.

or more compactly

$$\mathrm{E}_a : y^2 + xy = x^3 + ax^2 + 1$$

where $a = 0$ or 1.

3.2.1 Main Subgroup

Let $\mathrm{E}_a(F_{2^m})$ denote the group of F_{2^m} rational points on the elliptic curve E_a. This group should be chosen such that it is difficult to compute the discrete logarithms of its elements. It is desirable that the group order of $\mathrm{E}_a(F_{2^m})$, $|E_a(F_{2^m})|$, should be divisible by a large prime [15]. Notice that any group that one works with is an extension of the group $\mathrm{E}_a(F_2)$, and thus, by Lagrange's theorem, the order of this group will be divisible by the order of the subgroup $\mathrm{E}_a(F_2)$. For the elliptic curve E_a, we have

$$f = |\mathrm{E}_a(F_2)|^{\dagger} = \begin{cases} 4 & \text{for a} = 0 \\ 2 & \text{for a} = 1 \end{cases} \tag{3.1}$$

The Koblitz curves over F_2 are

$$\mathrm{E}_0(F_2) = \{\infty, (0,1), (1,0), (1,1)\},$$
$$\mathrm{E}_1(F_2) = \{\infty, (0,1)\}.$$

[*] An elliptic curve $\mathrm{E}_a(F_{2^m})$ of p elements will be called anomalous if the trace of the Frobenius map (the map $(x, y) \mapsto (x^q, y^q)$) is equal to 1. Equivalently, an anomalous curve over F, is one for which the number of F_q-points is equal to q. [11].

[†] This is also written as $\#\mathrm{E}_a(F_2)$.

The order of $\mathrm{E}_a(F_{2^m})$ will never be prime, but we can choose our groups such that they are very nearly prime. That is, we choose groups $\mathrm{E}_a(F_{2^m})$ such that the order is divisible by f and a large prime number so that

$$|\mathrm{E}_a(F_{2^m})| = \begin{cases} 4 \cdot r & \text{for a} = 0 \\ 2 \cdot r & \text{for a} = 1 \end{cases} \tag{3.2}$$

where $r > 2$ and r is prime*. It is the subgroup of order r which is of main interest for cryptographic purposes. This subgroup is termed the *the main subgroup.*

3.2.2 Frobenius Mapping (Endomorphism)

An important property of a Koblitz curve is that if $P = (x, y)$ is a point on E_a then the point $Q = (x^2, y^2)$ is also on E_a. This forms an endomorphism† known as the Frobenius map

$$\tau : \mathrm{E}_a(F_{2^m}) \rightarrow \mathrm{E}_a(F_{2^m})$$

where

$$\tau(\infty) = \infty \text{ and } \tau(x, y) = (x^2, y^2).$$

As will be shown later, squaring can be efficiently computed.

It can also be shown that the following relationship holds

$$(x^4, y^4) + 2(x, y) = \mu \cdot (x^2, y^2) \tag{3.3}$$

where

$$\mu = (-1)^{1-a}$$

for every (x, y) on E_a. Given that $\tau(x, y) = (x^2, y^2)$, equation (3.3) can be written symbolically as

$$\tau^2 P + 2P = \mu\tau P \tag{3.4}$$

or

$$(\tau^2 + 2)P = \mu\tau P \tag{3.5}$$

for all $P \in \mathrm{E}_a(F_{2^m})$. Therefore, on an anomalous elliptic curve $\mathrm{E}_a(F_{2^m})$ the Frobenius map satisfies the characteristic equation

$$\tau^2 - \mu\tau + 2 = 0. \tag{3.6}$$

*This can only happen if m is prime. If m is not prime then any subgroups will have an order that divides m which will not be prime by Lagrange's theorem. If m is prime then the only subgroups will be $\mathrm{E}_a(F_2)$ and that arising from the subgroup of order r.

†A morphism which maps an object to itself, i.e. if a group G is a group homomorphism, $f : G \rightarrow G'$ then $G = G'$.

Solving 3.6 for τ we get

$$\tau = \frac{\mu + \sqrt{-7}}{2}. \tag{3.7}$$

Let $\mathbb{Z}[\tau]$ denote the ring of polynomials in τ with integer coefficients. We can now multiply points on E_a by any element in the ring $\mathbb{Z}[\tau]$ such that if

$$\alpha = u_{k-1}\tau^{k-1} + \cdots + u_1\tau + u_0 \in \mathbb{Z}[\tau] \tag{3.8}$$

and $P \in \mathrm{E}_a(F_{2^m})$ then

$$(u_{k-1}\tau^{k-1} + \cdots + u_1\tau + u_0)P = u_{k-1}\tau^{k-1}P + \cdots + u_1\tau P + u_0P. \tag{3.9}$$

However, since $\tau^2 = \mu\tau - 2$ then every $\alpha \in \mathbb{Z}[\tau]$ can be expressed in the canonical form $\alpha = a_0 + a_1\tau$ where $a_0, a_1 \in \mathbb{Z}$.

3.2.3 The Norm of a $\mathbb{Z}[\tau]$ and Associated Properties

The complex numbers are not well ordered*, but we can impose an ordering by taking the norm. The norm of $\alpha = a_0+a_1\tau \in \mathbb{Z}[\tau]$ is the product of α and its complex conjugate so that the norm is

$$N(a_0 + a_1\tau) = a_0^2 + \mu a_0 a_1 + 2a_1^2.^{\dagger} \tag{3.10}$$

We have the following properties for the norm function from [8][19]:

1. $N(\alpha) \geq 0$ for all $\alpha \in \mathbb{Z}[\tau]$ with equality if and only if $\alpha = 0$.
2. 1 and -1 are the only elements of $\mathbb{Z}[\tau]$ having a norm of 1.
3. $N(\tau) = 2$.
4. $N(\tau - 1) = f = |\mathrm{E}_a(F_2)|$.
5. $N(\tau^m - 1) = |\mathrm{E}_a(F_{2^m})|$.
6. $N((\tau^m - 1)/(\tau - 1)) = \dfrac{|\mathrm{E}_a(F_{2^m})|}{|\mathrm{E}_a(F_2)|} = \dfrac{|\mathrm{E}_a(F_{2^m})|}{f} = r.$
7. The norm function is multiplicative so that it satisfies $N(\alpha\beta) = N(\alpha)N(\beta)$ for all $\alpha, \beta \in \mathbb{Z}[\tau]$.
8. The distance (Euclidean) from 0 to α in the complex plane is given by $\sqrt{N(\alpha)}$ so that the *Triangle Inequality* has the form $\sqrt{N(\alpha)N(\beta)} \leq \sqrt{N(\alpha)} + \sqrt{N(\beta)}$.

*You cannot order the complex numbers due to the presence of $i^2 = -1$.

†One must be careful when deriving this equation. τ must be separated into its real and imaginary parts before taking the conjugate.

9. The ring $\mathbb{Z}[\tau]$ is a Euclidean domain with respect to the norm function. That is, for any $\alpha, \beta \in \mathbb{Z}[\tau]$ with $\beta \neq 0$, there exists $\kappa, \rho \in \mathbb{Z}[\tau]$, not necessarily unique, such that $\alpha = \kappa\beta + \rho$ and $N(\rho) < N(\beta)$. As a result, the ring $\mathbb{Z}[\tau]$ has a unique factorization and the element τ, having a prime norm, is a prime element.

3.2.4 Group Order

The size of the group is very important in the determination of the cryptographic strength of an elliptic curve. It is easy to see that the larger the group size the more difficult it is to solve the discrete logarithm problem, thus providing greater cryptographic strength. It is elementary to determine the group size of a Koblitz curves given the following information.

3.2.4.1 Lucas Sequence

The Lucas sequences[*] are defined as follows:

$$U_0 = 0, U_1 = 1 \quad and \quad U_{k+1} = \mu U_k - 2U_{k-1} \; for \; k \geq 1. \tag{3.11}$$

$$V_0 = 2, V_1 = \mu \quad and \quad V_{k+1} = \mu V_k - 2V_{k-1} \; for \; k \geq 1. \tag{3.12}$$

3.2.4.2 τ identity

It can be proved by induction that

$$\tau^k = U_k\tau - 2U_{k-1} \; for \; k \geq 1. \tag{3.13}$$

3.2.4.3 Group Order of Koblitz Elliptic Curve

We can now compute the group order for a Koblitz curve from the property

$$N(\tau^m - 1) = |\mathrm{E}_a(F_{2^m})| \tag{3.14}$$

using the norm function given in section 3.2.3 and the identity given in equation (3.13).

In later sections we will be focusing on the main subgroup, so its order will also be important. Of course, if one knows the order of the group $\mathrm{E}_a(F_{2^m})$, one can find the

[*] Lucas sequences $L_n(P, Q)$ are a certain integer sequence that satisfy the recursion relation $X_n = PX_{n-1} - QX_{n-2}$ where P and Q are fixed integers. The Fibonacci sequence and the Mersenne primes are examples.

order of the main subgroup by dividing by the value given in equation (3.1). The order of the main subgroup can also be calculated by the equation:

$$|\mathrm{E}_a(F_{2^m})| = 2^m + 1 - V_m. \tag{3.15}$$

3.3 $\tau - NAF$

Most of the work in this section is a recapitulation of the work done by [19] as well as information from [8]. It is important to review this work, since the details will be needed later to increase the understanding of the *window-w* τ-NAF method, where we exploit this information in order to improve on this methodology. In addition, we have tried to expound on the information where necessary in order to increase clarity.

Koblitz [11] demonstrated that it was possible to convert an integer $n \in \mathbb{Z}$ into an equivalent τ-adic expression by representing n "to the base τ", i.e. a power series in τ. Koblitz also proved that n has a unique representation in the form

$$\sum u_i \tau^i$$

where $u_i \in \{0, 1\}$. However, this representation does not exhibit the nonadjacency property. It was Solinas [19] who proved that it was feasible to create a τ-adic expansion such that no two consecutive terms were nonzero, i.e. exhibits the nonadjacency property. This is called a τ-NAF or TNAF. A τ-NAF is defined as:

Definition 3.1. A τ-NAF of a nonzero element $k \in \mathbb{Z}[\tau]$ is an expression

$$\alpha = \sum_{i=0}^{l-1} u_i \tau^i$$

where $u_i \in \{0, \pm 1\}, u_{l-1} \neq 0$, and no two consecutive digits, u_i, are nonzero.

Example 3.3. *For example, with $a = 1$, we have*[*]

$$9 = \tau^5 - \tau^3 + 1$$

so that if $P = (x, y)$ is a point on E_1, then

$$9P = (x^{32}, y^{32}) - (x^8, y^8) + (x, y)$$

Before presenting the algorithm for the τ-NAF, we need the following theorem for the division of $\alpha \in \mathbb{Z}[\tau]$ by τ and τ^2.

Theorem 3.2. *Let $\alpha = r_0 + r_1\tau \in \mathbb{Z}[\tau]$*[†]

(i) α is divisible by τ if and only if r_0 is even. If r_0 is even then

$$\alpha/\tau = (r_1 + \mu r_0/2) - (r_0/2)\tau.$$

[*] To see this, resolve terms by powers of τ^2 and substitute the identity $\tau^2 = \tau - 2$.

[†] Recall from the norm properties 3.2.3 property 4 that the norm of τ is 2, and hence, the possible remainders upon division by τ are {1, -1}.

(ii) α *is divisible by* τ^2 *if and only if* $r_0 \equiv 2r_1$ *(mod 4).*

Solinas also proved

Theorem 3.3. *Every element of the ring* $\mathbb{Z}[\tau]$ *has a unique* τ*-adic NAF.*

He also showed by proposition

Proposition 3.4. *The average density among* τ*-adic NAF's of length* ℓ *is asymptotically 1/3.*

We now present algorithm 8 for the computation of a τ-NAF.

Algorithm 8: Computing TNAF

```
Input: Integers $r_0, r_1$ representing $\kappa = r_0 + r_1\tau \in \mathbb{Z}[\tau]$
Output: $\tau - NAF(\kappa)$
$i \leftarrow 0$
while $r_0 \neq 0$ or $r_1 \neq 0$ do
    if $r_0$ is odd then
        $u_i \leftarrow 2 - (r_0 - 2r_1 \bmod 4)$
        $r_0 \leftarrow r_0 - u_i$
    else
        $u_i \leftarrow 0$
    $t \leftarrow r_0$
    $r_0 \leftarrow r_1 + \mu r_0/2$
    $r_1 \leftarrow -t/2$
    $i \leftarrow i + 1$
return $(u_{i-1}, u_{i-2}, \ldots, u_1, u_0)$
```

Example 3.4. *Following example 3.1 for the ordinary* NAF(107)*, we calculate the* $\tau-$NAF*(107) for* $a = 1$

$$\begin{aligned}\tau\text{−NAF}(107) &= \langle -1, 0, 0, 0, 0, -1, 0, 0, 0, 1, 0, -1, 0, -1 \rangle \\ &= -1 \cdot \tau^{13} - 1 \cdot \tau^{8} + 1 \cdot \tau^{4} - 1 \cdot \tau^{2} - 1 \cdot \tau^{0}.\end{aligned}$$

From the Lucas sequence, equation 3.11, we have

$$\begin{aligned}\tau^2 &= \tau - 2, \\ \tau^4 &= -3\tau + 2, \\ \tau^8 &= -3\tau - 14, \\ \tau^{13} &= -\tau - 90,\end{aligned}$$

so that

$$\begin{aligned}\tau\text{−NAF}(107) &= -\tau^{13} - \tau^{8} + \tau^{4} - \tau^{2} - 1\\ &= -(-\tau - 90) - (-3\tau - 14) + (-3\tau + 2) - (\tau - 2) - 1\\ &= 107.\end{aligned}$$

The length of the τ-NAF(k) is approximately $\log_2(N(k)) = 2\log_2 k$ [8] which is twice the length of the NAF(k). This virtually eliminates the advantage of the τ-adic NAF. Fortunately, this situation can be rectified by replacing the τ-adic NAF with an equivalent expression called the *reduced τ-adic NAF*, which is only half as long [19].

3.3.1 Reduced τ-NAF or RTNAF

In order to find the reduced τ-NAF or RTNAF, we need the following proposition and theorem.

Proposition 3.5. *If $\gamma, \rho \in \mathbb{Z}[\tau]$ with*

$$\gamma \equiv \rho \ mod \ (\tau^m - 1)$$

then

$$\gamma P = \rho P$$

for all $P \in \mathrm{E}_a(F_{2^m})$.[*]

For cryptographic purposes, we can further refine proposition 3.5 by narrowing our focus to the main subgroup[†]. From the norm properties 4, 5, and 6 given in section 3.2.3, it can be shown that

Theorem 3.6. *Given $\delta = (\tau^m - 1)/(\tau - 1)$ with*

$$\gamma \equiv \rho (mod \ \delta)$$

then

$$\gamma P = \rho P.$$

It follows from Theorem 3.6 that the

$$reduced \quad \tau\text{−NAF(n)} = \tau\text{−NAF}(\rho) \tag{3.16}$$

where

$$\rho = n \ mod \ \delta \tag{3.17}$$

[*] This follows from the fact that $\tau^m(P) = P$ and $\delta(P) = P$ so that $(\tau^m - 1)P = \tau^m P - P = P - P = \infty$. But $\gamma \equiv \rho(mod \ \tau^m - 1) \Rightarrow \gamma = \kappa(\tau^m - 1) + \rho$ for some $\kappa \in \mathbb{Z}[\tau]$ by the division theorem. Hence $\gamma P = \kappa(\tau^m - 1)P + \rho P = \kappa\infty + \rho P = \infty + \rho P = \rho P$.

[†] as opposed to the entire group $\mathrm{E}_a(F_{2^m})$.

with respect to the main subgroup. Solinas proved that the length of the reduced τ-NAF (RTNAF), ℓ_{RTNAF}, is bounded above [19]

$$\ell_{RTNAF} \leq m + a.$$

Thus, the weight of the RTNAF(k) is about equal to the weight of NAF(k), but RTNAF eliminates the elliptic point doubling using the more efficient τ mapping[*] with roughly the same number of point additions. However, to exploit the RTNAF, we need an algorithm to reduce an integer n modulo δ.

3.3.2 Division and Modular Reduction in $\mathbb{Z}[\tau]$

By property 9 of the norm properties 3.2.3, $\mathbb{Z}[\tau]$ is an euclidean domain, and, hence, we can utilize the division theorem[†]. From the division theorem and analogous to integer division, we wish to find a quotient $\kappa = q_0 + q_1\tau$ and a remainder $\rho = r_0 + r_1\tau$ where ρ has the smallest norm possible (a condition we will later relax) such that

$$\gamma = \kappa\delta + \rho$$

where $\gamma = c_0 + c_1\tau$ and $\delta = d_0 + d_1\tau$. In order to do this, you obtain κ by rounding off γ/δ and then find ρ, the remainder, by subtracting this result from γ. That is

$$\rho = \gamma - \kappa\delta.$$

To obtain κ by rounding off γ/δ, we let

$$\frac{\gamma}{\delta} = \frac{\gamma\overline{\delta}}{\delta\overline{\delta}} = \frac{\gamma\overline{\delta}}{N(\delta)} = \frac{g_0 + g_1\tau}{N}.$$

In order to find $\gamma\overline{\delta}$, we need the complex conjugate of $\delta = d_0 + d_1\tau$, i.e. $\overline{\delta}$. To find $\overline{\delta}$, we need to split δ into its real and imaginary parts. Hence,

$$\delta = \left(\left(d_0 + \frac{d_1\mu}{2}\right) + \frac{d_1\sqrt{-7}}{2}\right)$$

so that

[*] Although [19] recommends converting to a normal basis since squaring can be implemented by a register shift in computer hardware, we show that computing powers of τ can be implemented efficiently in software as well.

[†] $a = qn + r \Rightarrow q = \lfloor a/n \rfloor$ and r = a - qn where a is a positive integer. See [13].

$$\overline{\delta} = \left(\left(d_0 + \frac{d_1\mu}{2}\right) - \frac{d_1\sqrt{-7}}{2}\right).$$

Thus

$$\begin{aligned}
\gamma\overline{\delta} &= \left(\left(c_0 + \frac{c_1\mu}{2}\right) + \frac{c_1\sqrt{-7}}{2}\right)\left(\left(d_0 + \frac{d_1\mu}{2}\right) - \frac{d_1\sqrt{-7}}{2}\right) \\
&= c_0d_0 + \frac{c_0d_1\mu}{2} + \frac{c_1d_0\mu}{2} + \frac{c_1d_1\mu^2}{4} + \frac{c_1d_0\sqrt{-7}}{2} \\
&+ \frac{c_1d_1\mu\sqrt{-7}}{4} - \frac{c_0d_1\sqrt{-7}}{2} - \frac{c_1d_1\mu\sqrt{-7}}{4} + \frac{7c_1d_1}{4}.
\end{aligned}$$

Simplifying and given that $\mu^2 = 1$, we have

$$\begin{aligned}
&= c_0d_0 + \frac{c_0d_1\mu}{2} + \frac{c_1d_0\mu}{2} + \frac{c_1d_0\sqrt{-7}}{2} - \frac{c_0d_1\sqrt{-7}}{2} + 2c_1d_1 \\
&= c_0d_0 + c_1d_0\left[\frac{\mu + \sqrt{-7}}{2}\right] - c_0d_1\left[\frac{-\mu + \sqrt{-7}}{2}\right] + 2c_1d_1 \\
&= c_0d_0 + c_1d_0\tau - c_0d_1\left[\frac{\mu + \sqrt{-7}}{2} - \mu\right] + 2c_1d_1 \\
&= c_0d_0 + c_1d_0\tau - c_0d_1\tau + c_0d_1\mu + 2c_1d_1 \\
&= [c_0d_0 + c_0d_1\mu + 2c_1d_1] + [c_1d_0 - c_0d_1]\tau \\
&= g_0 + g_1\tau. \qquad (3.18)
\end{aligned}$$

so that

$$g_0 = c_0d_0 + c_0d_1\mu + 2c_1d_1 \quad \mathit{and} \quad g_1 = c_1d_0 - c_0d_1. \qquad (3.19)$$

We find κ by rounding

$$\kappa = \mathit{round}\left(\frac{g_0 + g_1\tau}{N}\right)$$

and the remainder ρ by

$$\rho = \gamma - \kappa\delta.$$

This now makes it easy to write the following algorithm 9 for division in $\mathbb{Z}[\tau]$.

```
Algorithm 9: Division in $\mathbb{Z}[\tau]$
Input:
        The dividend $\gamma = c_0 + c_1\tau$
        The divisor $\delta = d_0 + d_1\tau$
Output:
        The quotient $\kappa = q_0 + q_1\tau$
        The remainder $\rho = r_0 + r_1\tau$
$g_0 \leftarrow c_0d_0 + c_0d_1\mu + 2c_1d_1$
$g_1 \leftarrow c_1d_0 - c_0d_1$
$N \leftarrow d_0^2 + d_0d_1\mu + 2d_1^2$
$\lambda_0 = g_0/N$
$\lambda_1 = g_1/N$
$(q_0, q_1) \leftarrow round(\lambda_0, \lambda_1)$
$r_0 \leftarrow c_0 - d_0q_0 + 2d_1q_1$
$r_1 \leftarrow c_1 - d_1q_0 - d_0q_1 - d_1q_1\mu$
return $q_0, q_1, r_0, r_1$
```

The rounding function in algorithm 9 is compulsory since $\lambda_0, \lambda_1 \in \mathbb{Q}$, and we require all coefficients to be elements of $\mathbb{Z}$. The rounding function must "pick" an element of $\mathbb{Z}[\tau]$ that is close to the complex number $\lambda_0 + \lambda_1\tau$. In the ring of integers, the division algorithm always produces a remainder of least value; however, this may not necessarily be the case in the complex numbering system since the complex numbering system is not well ordered*.

Solinas [19] took great care in presenting a methodology in which the norm of this remainder was of least value. As a result, Solinas determined that an arbitrary point $\lambda_0 + \lambda_1\tau$ lies in the interior of a region $\mathcal{U}$ if it satisfies the following set of inequalities (see figure 3.1):

1. $-2 \leq \lambda_0 - 3\mu\lambda_1 < 2$ represented by the labels "a" and "b" in figure 3.1.
2. $-1 \leq 2\lambda_0 + \mu\lambda_1 < 1$ represented by the labels "c" and "d" in figure 3.1.
3. $-2 \leq \lambda_0 + 4\mu\lambda_1 < 2$ represented by the labels "e" and "f" in figure 3.1.

This set of inequalities tiles the τ plane as shown in figure 3.1.

*Again, we impose an ordering by taking norms.

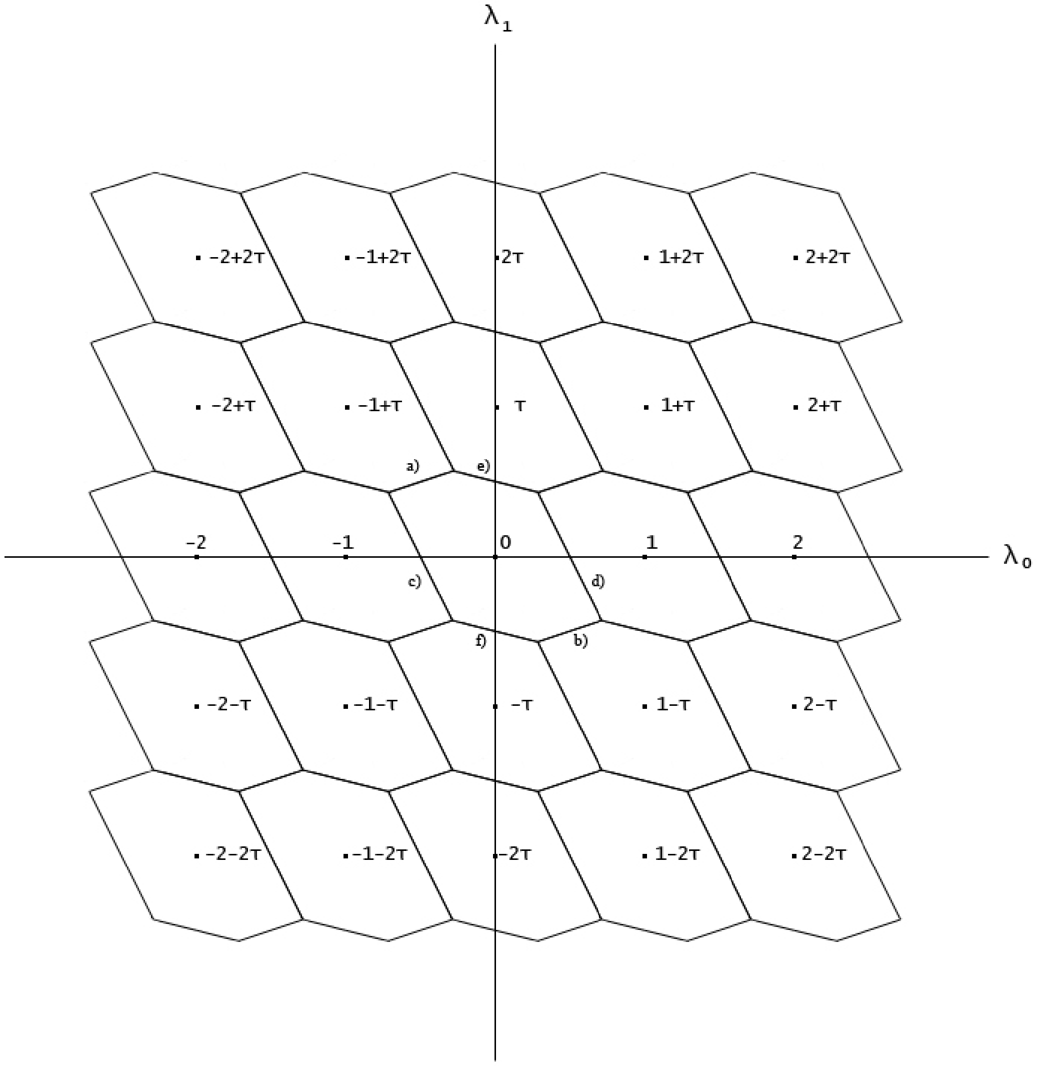

FIGURE 3.1: $\mathcal{U}$ tiling for a = 1

Solinas presented algorithm 10 for rounding λ based on this set of inequalities.

Algorithm 10: Rounding(λ)

```
Input: Real numbers $\lambda_0, \lambda_1$ where $\lambda = \lambda_0 + \lambda_1\tau$
Output: Integer numbers $q_0, q_1$ where $\kappa = q_0 + q_1\tau = round(\lambda)$
$f_0 \leftarrow round(\lambda_0)^a$
$f_1 \leftarrow round(\lambda_1)$
$r_0 \leftarrow \lambda_0 - f_0$
$r_1 \leftarrow \lambda_1 - f_1$
$h_0 \leftarrow 0$
$h_1 \leftarrow 0$
$r = 2r_0 + \mu r_1$
if $r \geq 1$ then
    if $r_0 - 3\mu r_1 < -1$ then
        $h_1 \leftarrow \mu$
    else
        $h_0 \leftarrow 1$
else
    if $r_0 + 4\mu r_1 \geq 2$ then
        $h_1 \leftarrow \mu$
if $r < -1$ then
    if $r_0 - 3\mu r_1 \geq 1$ then
        $h_1 \leftarrow -\mu$
    else
        $h_0 \leftarrow -1$
else
    if $r_0 + 4\mu r_1 < -2$ then
        $h_1 \leftarrow -\mu$
$q_0 \leftarrow f_0 + h_0$
$q_1 \leftarrow f_1 + h_1$
return $q_0, q_1$
```

[a] Rounding here is the standard rounding algorithm applied to floating point numbers.

If we ignore the quotient κ in algorithm 9 and output the remainder ρ, then this algorithm can be regarded as a modular reduction algorithm. We can further simplify this algorithm by making the following alterations.

From equation (3.19)

$$\begin{aligned} g_0 &= c_0d_0 + \mu c_0d_1 + 2c_1d_1, \\ g_1 &= c_1d_0 - c_0d_1. \end{aligned} \tag{3.20}$$

Let $\gamma = n$ then

$$\gamma = c_0 + c_1\tau = n \Rightarrow c_0 = n \quad \text{and} \quad c_1 = 0 \tag{3.21}$$

so that the integers appearing in 3.19 are

$$\begin{aligned} g_0 &= (d_0 + \mu d_1)n, \\ g_1 &= (-d_1)n. \end{aligned} \tag{3.22}$$

Let

$$\begin{aligned} s_0 &= (d_0 + \mu d_1), \\ s_1 &= -d_1. \end{aligned} \tag{3.23}$$

We now present algorithm 11 for reducing an integer n modulo δ.

Algorithm 11: Reduction Modulo $(\tau^m - 1)/(\tau - 1)$

```
Input:
        $m$ from the field characteristic $F_{2^m}$
        $a$ the elliptic curve parameter
        $s_0, s_1$ as defined in equation (3.23)
        $r$ the order of the main subgroup[a]
        $n$ the scalar multiple
Output: Integer numbers $r_0, r_1$ where $r_0 + r_1\tau = n\ mod(\tau^m - 1)/(\tau - 1)$
$d_0 \leftarrow s_0 + \mu s_1$
$\lambda_0 \leftarrow s_0 n/r$
$\lambda_1 \leftarrow s_1 n/r$
$(q_0, q_1) = round(\lambda_0, \lambda_1)$[b]
$r_0 \leftarrow n - d_0 q_0 - 2 s_1 q_1$
$r_1 \leftarrow s_1 q_0 - s_0 q_1$
return $r_0, r_1$
```

[a] See equation 3.15.

[b] via algorithm 10.

3.3.2.1 A Simplified Rounding Technique in Modular Reduction

As mentioned earlier, we claim that we can relax the requirement that the remainder ρ be of least norm, and develop a rounding algorithm leading to a simplified modular reduction technique. This is accomplished by truncating the values of λ_0 and λ_1 such that

$$\begin{aligned} q_0 &= \left\lfloor \lambda_0 \right\rfloor = \left\lfloor \frac{(d_0 + \mu d_1)n}{N(\delta)} \right\rfloor, \\ q_1 &= \left\lfloor \lambda_1 \right\rfloor = \left\lfloor \frac{-\,d_1 n}{N(\delta)} \right\rfloor. \end{aligned} \tag{3.24}$$

Effectively, this can be seen as a square tiling of the τ plane represented by the following set of inequalities:

1. $-1/2 \leq \lambda_0 < 1/2$.

2. $-1/2 \leq \lambda_1 < 1/2$.

This slightly changes the representatives of the equivalence classes used in τ-*NAF* methods since part of the $\mathcal{U}$ tiles will lay outside the square tiles. In practice, there is no guarantee that least norms are more efficient in τ-NAF methods. The fact that this is an equally valid representation can be seen by the fact that, given $nP = (r_0 + r_1\tau)P$ (*modulo* δ), then, by the division theorem, we have

$$n = (q_0 + q_1\tau)\delta + (r_0 + r_1\tau) \tag{3.25}$$

where q_0 and q_1 are given by 3.24 so that

$$r_0 + r_1\tau = n - (q_0 + q_1\tau)\delta. \tag{3.26}$$

Since any multiple of δ is 0, we have that $n = (r_0 + r_1\tau)$ modulo δ. We now present the following reduction algorithm, algorithm 12, using this simplified rounding technique.

Algorithm 12: Simplified Reduction Modulo $(\tau^m - 1)/(\tau - 1)$

```
Input:
        $m$ from the field characteristic $F_{2^m}$
        $a$ the elliptic curve parameter
        $s_0, s_1$ as defined in equation (3.23)
        $r$ the order of the main subgroup
        $n$ the scalar multiple
Output: Integer numbers $r_0, r_1$ where $r_0 + r_1\tau = n\ mod(\tau^m - 1)/(\tau - 1)$
$d_0 \leftarrow s_0 + \mu s_1$
$\lambda_0 \leftarrow s_0 n/r$
$\lambda_1 \leftarrow s_1 n/r$
$q_0 = \lfloor \lambda_0 \rceil$
$q_1 = \lfloor \lambda_1 \rceil$
$r_0 \leftarrow n - d_0 q_0 - 2 s_1 q_1$
$r_1 \leftarrow s_1 q_0 - s_0 q_1$
return $r_0, r_1$
```

We now have the necessary components to compute the reduced τ-NAF which is accomplished by algorithm 13.

Algorithm 13: Reduced τ-NAF

```
Input:
    $m$ from the field characteristic $F_{2^m}$
    $a$ the elliptic curve parameter
    $s_0, s_1$ as defined in equation (3.23)
    $r$ the order of the main subgroup
    $n$ the scalar multiple
Output: $RTNAF(n)$
$(r_0, r_1) \leftarrow n \ mod \ \delta$ via algorithm 11 or 12[a]
$(u_{i-1}, u_{i-2}, \ldots, u_1, u_0) = TNAF(r_0, r_1)$ via algorithm 8
return $(u_{i-1}, u_{i-2}, \ldots, u_1, u_0)$
```

[a] $\rho = r_0 + r_1\tau$.

3.3.2.2 Scalar Multiplication using Reduced $\tau - NAF$

The following is the scalar multiplication algorithm using the reduced τ-NAF.

Algorithm 14: Scalar Multiplication on Koblitz Curves

```
Input:
    $m$ from the field characteristic $F_{2^m}$
    $a$ the elliptic curve parameter
    $s_0, s_1$ as defined in equation (3.23)
    $r$ the order of the main subgroup.
    $n < r/2$ the scalar multiple
    $P$ a point on the elliptic curve within the main subgroup
Output: $nP$
$(r_0, r_1) \leftarrow n \ mod \ \delta$ via algorithm 11[a]
$Q \leftarrow \infty$
$P_0 \leftarrow P$
while $r_0 \neq 0$ or $r_1 \neq 0$ do
    if $r_0$ is odd then
        $u \leftarrow 2 - (r_0 - 2r_1 \ mod \ 4)$
        $r_0 \leftarrow r_0 - u$
        if $u = 1$ then
            $Q \leftarrow Q + P_0$
        else if $u = -1$ then
            $Q \leftarrow Q - P_0$
    $P_0 \leftarrow \tau P_0$    // using the $\tau$ mapping
    $(r_0, r_1) \leftarrow (r_1 + \mu r_0/2, -r_0/2)$
return $Q$
```

[a] $\rho = r_0 + r_1\tau$.

Solinas showed in [19] this algorithm has only $m/3$ point additions and no point doublings!

3.3.2.3 Efficient Squaring

In algorithm 14, step 12 can be efficiently implemented in hardware when working with a normal basis. It is well known that there exists an element $\beta \in F_{2^m}$ such that the set $\{\beta, \beta^2, \beta^{2^2}, \ldots, \beta^{2^{m-1}}\}$ is a basis of F_{2^m} over F_2 known as a normal basis. The binary vector associated with $a = \sum_{i=0}^{m-1} a_i \beta^{2^i}$ is $A = (a_{m-1} \ldots a_1 a_0)$, and, hence, squaring is a simple right cyclic shift in this representation. [4]

It is also possible to implement squaring efficiently in software when working with binary fields. Recall from chapter 2, subsection 2.2.3.1, the discussion on *Polynomials over a Ring*

$$R[x] = a_0 + a_1 x + a_2 x^2 + \ldots + a_{m-1} x^{m-1}. \tag{3.27}$$

Here x serves merely as a positional place holder. If we square this polynomial, we obtain

$$R^2[x] = a_0 + a_1 x^2 + a_2 x^4 + \ldots + a_{m-1} x^{2m-2}. \tag{3.28}$$

This is equivalent to placing a zero term between each term of the original representation. This is easily accomplished in software by simply reading each of the binary bits of the base and transferring them to every other bit location in the receiving target[*].

We can expand on this notion by noting that continually squaring $R[x]$ results in

$$\begin{aligned}
R^4[x] &= a_0 + a_1 x^4 + a_2 x^8 + \ldots + a_{m-1} x^{4(m-1)} &&\Rightarrow \quad 3 \textit{ zeros between terms} \\
R^8[x] &= a_0 + a_1 x^8 + a_2 x^{16} + \ldots + a_{m-1} x^{8(m-1)} &&\Rightarrow \quad 7 \textit{ zeros between terms} \\
R^{16}[x] &= a_0 + a_1 x^{16} + a_2 x^{32} + \ldots + a_{m-1} x^{16(m-1)} &&\Rightarrow \quad 15 \textit{ zeros between terms} \\
&\vdots \\
R^m[x] &= a_0 + a_1 x^m + a_2 x^{2m} + \ldots + a_{m-1} x^{m(m-1)} &&\Rightarrow \quad (m-1) \textit{ zeros between terms.}
\end{aligned}$$

This can be used when calculating powers of τ since

$$\begin{aligned}
\tau P(x,y) &\mapsto P(x^2, y^2) \\
\tau^2 P(x,y) &\mapsto P(x^4, y^4) \\
\tau^3 P(x,y) &\mapsto P(x^8, y^8) \\
&\vdots \\
\tau^m P(x,y) &\mapsto P(x^{2^m}, y^{2^m}).
\end{aligned}$$

[*] See the square method in appendix C: for an implementation in Java.

3.4 Width-w τ-NAF

We now wish to elucidate a *width-w τ-adic NAF* method following the same strategy as the ordinary *width-w NAF* described in section 3.1.3 and specified in [19]. As with the *width-w* NAF, we pre-compute and store the points in the corresponding odd congruence class ($mod\ \tau^w$). Recall from theorem 3.2 that an element $r_0 + r_1\tau$ is divisible by τ if and only if r_0 is even. By odd, then, it is meant that r_0 is odd. Thus, when an odd element $r_0 + r_1\tau$ is encountered, then the odd congruence class $r_0 + r_1\tau$, *modulo* τ^w in which it belongs must be determined, and the congruence class representative must be subtracted off producing a new element divisible by τ^w. Analogous with the *width-w* NAF, we can determine the congruence class by examining the w least significant bits.

From 3.13, we know that

$$\tau^k = U_k\tau - 2U_{k-1}\ for\ k \geq 1. \tag{3.29}$$

Multiplying this equation by its conjugate, i.e. taking the norm, we get[*]

$$U_k^2 - \mu U_k U_{k-1} + 2U_{k-1}^2 = 2^{k-1},\ for\ all\ k \geq 1. \tag{3.30}$$

Let

$$t_k = 2U_{k-1}U_k^{-1}(mod\ 2^k). \tag{3.31}$$

Now U_k is odd since $U_0 = 0, U_1 = 1 \Rightarrow U_2 = 1$ so succeeding terms will consist of an odd term, minus an even term, which will always be odd. In addition, U_k^{-1} will also be odd since $U_k\ odd \Rightarrow gcd(U_k, 2^k) = 1$. Then, by the extended Euclidean Algorithm,

$$sU_k + t2^k = 1.$$

Now $t2^k$ is even so sU_k must be odd. But U_k odd $\Rightarrow s$ must also be odd. Further, s is the inverse of U_k modulo $2^k \Rightarrow U_k^{-1}(mod\ 2^k)$ is odd. Therefore t_k is a well defined integer modulo 2^k that is even but not divisible by 4[†].

Therefore, by 3.30 and 3.31,

$$t_k^2 - \mu t_k + 2 \equiv 0\ (mod\ 2^k),\ for\ all\ k \geq 1.^{\ddagger} \tag{3.32}$$

Hence, t_k satisfies the same polynomial equation over $\mathbb{Z}/2^k\mathbb{Z}$ that τ satisfies over the complex numbers, viz. $\tau^2 - \mu\tau + 2$. [19] showed that the correspondence $\tau \mapsto t_w$ induces

[*] Recall $N(d_0 + d_1\tau) = d_0^2 - \mu d_0 d_1 + 2d_1^2$. Let $d_0 = -2U_{k-1}$ and $d_1 = U_k$. Further $N(\tau) = 2$ so that $N(\tau^k) = 2^k$. Hence $2^k = 4U_{k-1}^2 - 2\mu U_k U_{k-1} + 2U_k^2 \Rightarrow 2^{k-1} = u_k^2 - \mu U_k U_{k-1} + 2U_{k-1}^2$.

[†] Since we multiply two odd numbers by 2. The result is not divisible by 4 since neither U_{k-1} or U_k^{-1} is divisible by 2 both being odd numbers.

[‡] or $t_k^2 + 2 \equiv \mu t^k\ (mod\ 2^k)$.

a ring homomorphism (surjective) via the mapping

$$\phi_w : \mathbb{Z}[\tau] \rightarrow \mathbb{Z}/2^w\mathbb{Z} \tag{3.33}$$

with kernal

$$\{\alpha \in \mathbb{Z}[\tau] \,|\, \alpha \; is \; divisible \; by \; \tau^k\}. \tag{3.34}$$

This asserts that the odd equivalence classes in $\mathbb{Z}[\tau]$ are incongruent modulo τ^w so that an even value for α has a 0 residual, and an odd value for α will have a residual (mod τ^w) falling into one of the equivalence classes $\pm 1, \pm 3, \ldots, \pm(2^{w-1} - 1)$. Furthermore, under the mapping ϕ_w, the odd congruence classes in $\mathbb{Z}[\tau]$ (mod τ^w) equate with the odd elements in $\mathbb{Z}/2^w\mathbb{Z}$. Hence, [2]

$$r_0 + r_1\tau \equiv 0 \; (mod \; \tau^k) \Leftrightarrow r_0 + r_1 t_k \equiv 0 \; (mod \; 2^k). \tag{3.35}$$

Therefore, if we let $\alpha_u = u \; mod \; \tau^w$ then the numbers $\pm\alpha_1, \pm\alpha_3, \ldots, \pm\alpha_{(2^{w-1}-1)}$ will also have an odd residual (mod τ^w).

We are now in a position to write down Solinas's *width-w* τ-adic NAF algorithm (algorithm 15).

Algorithm 15: *width-w* τ-adic NAF Method

```
Input:
        $m$ from the field characteristic $F_{2^m}$
        $a$ the elliptic curve parameter
        $s_0, s_1$ as defined in equation (3.23)
        $r$ the order of the main subgroup
        $w$ the window width
        $t_w (= 2U_{w-1}U_w^{-1})$
        $\alpha_u (= \beta_u + \gamma_u \tau$ for $u = 1, 3, \ldots, 2^{w-1} - 1)$
        A positive integer $n$
        An elliptic point $P$

        Precompute:
        $P_u = \alpha_u P$ for $u = 1, 3, \ldots, 2^{w-1} - 1$
Output: The point $nP$
$j \leftarrow 0$
$(r_0, r_1) \leftarrow n \; mod \; \delta$        // from algorithm 11
$Q \leftarrow \infty$
while $r_0 \neq 0$ or $r_1 \neq 0$ do
    if $r_0$ is odd then
        $u \leftarrow (r_0 + r_1 t_w)$ mods$^a$ $2^w$
        if $u > 0$ then
            $\xi \leftarrow 1$
        else
            $\xi \leftarrow -1$
            $u \leftarrow -u$
        $Q \leftarrow Q + \xi P_u$
    $j \leftarrow j + 1$
    $Q \leftarrow \tau^{-1} Q$
    $r_0 \leftarrow r_1 + \mu r_0 / 2$
    $r_1 \leftarrow -r_0 / 2$
$Q \leftarrow \tau^j Q$
return $Q$
```

[a] mods means that the remainder u satisfies $-2^{w-1} \leq u < 2^{w-1}$.

This algorithm has an approximate running time of:

$$\left(2^{w-2} - 1 + \frac{m}{w+1}\right) A$$

with no point doublings [8].

3.4.1 Precomputation Width-w τ-NAF

We now turn our attention to pre-computation in the *width-w* τ-adic NAF algorithm 15. In table 2 of [19], and, as stated in [2], pre-computation costs 39% of the point multiplication for a width size of $w = 6$, but 60% for a width size of $w = 7$. We explore various width sizes and offer improvements in pre-computation over current published results. In addition, we explore width sizes of $w = 7$ and $w = 8$, since widths of these sizes have not been produced in any literature to date, and offer efficient tables for these widths as well.

Again, the *mods* used in algorithm 15 means that the remainder u satisfies $-2^{w-1} \leq u < 2^{w-1}$ implying that α is an element with the smallest norm. [2] demonstrated and provided a proof of termination that this condition can be relaxed provided that $N(\alpha_u) < 2^w$ for $u = 3, 5, \ldots, 2^{w-1} - 1$. They called this method the *general width-w τ-adic NAF*. We now expand on this idea by generating all possible values of α_u such that the $N(\alpha_u) < 2^w$.

The calculations were done as follows. Let

$$\alpha_u = \beta_u + \gamma_u \tau. \tag{3.36}$$

Since

$$\alpha_u \equiv u \; mod \; \tau^w \Rightarrow \alpha_u = q\tau^w + u \tag{3.37}$$

where $\alpha_u, q \in \mathbb{Z}[\tau]$. Let

$$q = q_0 + q_1 \tau. \tag{3.38}$$

Then we have

$$\beta_u + \gamma_u \tau = (q_0 + q_1 \tau)\tau^w + u. \tag{3.39}$$

Recall by the Lucas sequence 3.11, τ^w can be reduced to its canonical form $c_0 + c_1\tau$ so that

$$\begin{aligned} (q_0 + q_1\tau)\tau^w &= (q_0 + q_1\tau)(c_0 + c_1\tau) \\ &= q_0c_0 + q_0c_1\tau + q_1c_0\tau + q_1c_1\tau^2. \end{aligned} \tag{3.40}$$

But $\tau^2 = \mu\tau - 2$ so that

$$\begin{aligned} &= q_0c_0 + q_0c_1\tau + q_1c_0\tau + q_1c_1\mu\tau - 2q_1c_1 \\ &= (q_0c_0 - 2q_1c_1) + (q_0c_1 + q_1c_0 + q_1c_1\mu)\tau. \end{aligned} \tag{3.41}$$

Therefore,

$$(q_0 + q_1\tau)\tau^w + u = (q_0c_0 - 2q_1c_1) + (q_0c_1 + q_1c_0 + q_1c_1\mu)\tau + u. \tag{3.42}$$

Equating terms in τ, we have

$$\begin{aligned} \beta_u &= q_0c_0 - 2q_1c_1 + u \quad and \\ \gamma_u &= q_0c_1 + q_1c_0 + q_1c_1\mu. \end{aligned} \tag{3.43}$$

w, c_0, c_1, u and μ are known so one merely varies the values for q_0 and q_1 validating that

$N(\alpha_u) = \beta_u^2 + \mu\beta_u\gamma_u + 2\gamma_u^2 < N(\tau^w) = 2^w$.

As an example, we perform a calculation for α_3 ($u = 3$) for the elliptic curve $\mathrm{E}_1(a = 1,\ \mu = 1)$ for a window size $w = 4$. Thus $N(\tau^4) = 2^4 = 16$ so that we will have four odd equivalence classes or residues.

In order to get the c_0 and c_1 terms, we need to reduce τ^4 to its canonical form. This is easily done using the Lucas sequence for U[*], equation 3.11, where $\tau^4 = U_4\tau - 2U_3$. We find that $\tau^4 = -3\tau + 2 => c_0 = 2$ and $c_1 = -3$. Let's choose $q_0 = 1$ and $q_1 = 1$. Then

$$\begin{aligned} \beta_u &= q_0c_0 - 2q_1c_1 + u = 11 \quad \textit{and} \\ \gamma_u &= (q_0c_1 + q_1c_0 + q_1c_1\mu) = -4 \end{aligned} \tag{3.44}$$

so that $u\ \mathit{mod}\ \tau^4 = 11 - 4\tau$. However, $N(11 - 4\tau) = 109 > 16$ and, hence, this does not qualify. Let's try $q_0 = 1$ and $q_1 = -1$. Then

$$\begin{aligned} \beta_u &= q_0c_0 - 2q_1c_1 + u = -1 \quad \textit{and} \\ \gamma_u &= (q_0c_1 + q_1c_0 + q_1c_1\mu) = -2 \end{aligned} \tag{3.45}$$

so that $u\ \mathit{mod}\ \tau^4 = -1 - 2\tau$ with $N(-1 - 2\tau) = 11 < 16$.

We present the entire table for E_1 for a window size $w = 4$, following the modus operandi outlined above, by varying q_0 and q_1 between large values such that the norm is well outside the acceptable range, and discarding those values whose norm is outside this range.

TABLE 3.1: E_1: $w = 4, N(\tau^w) = 16, \tau^w(\mathit{reduced}) = -3\tau + 2$

u	norm	q_0	q_1	$u\ \mathit{mod}\ \tau^w$	α_u
1	1	0	0	1	1
3	8	0	-1	$\tau - 3$	$\tau^2 - 1$
3	9	0	0	3	$\tau^5 + \tau^2 - 1$
3	11	1	-1	$-2\tau - 1$	$\tau^4 + \tau^2 - 1$
5	2	0	-1	$\tau - 1$	$\tau^2 + 1$
5	7	1	-1	$-2\tau + 1$	$\tau^4 + \tau^2 + 1$
7	4	0	-1	$\tau + 1$	$-\tau^3 - 1$
7	11	1	-1	$-2\tau + 3$	$\tau^5 + \tau^3 - 1$
7	14	1	-2	$-\tau - 3$	$\tau^3 - 1$

[*] $U_0 = 0, U_1 = 1, U_2 = 1, U_3 = -1, U_4 = -3$.

Solinas in [19] worked with a window width of $w = 5$ for E$_1$ and presented the following values for α_u based on the least norm:

Table 3.2: E$_1$: $w = 5, N(\tau^w) = 32, \tau^w(\mathit{reduced}) = -\tau + 6$

u	norm	q_0	q_1	$u\ mod\ \tau^w$	α_u	Reduction
1	1	0	0	1	1	
3	8	-1	0	$\tau - 3$	$\tau^2 - 1$	
5	2	-1	0	$\tau - 1$	$\tau^2 + 1$	
7	4	-1	0	$\tau + 1$	$-\tau^3 - 1$	
9	11	-2	0	$2\tau - 3$	$-\tau^5 - \tau^3 + 1$	$-\tau^3\alpha_5 + 1$
11	7	-2	0	$2\tau - 1$	$-\tau^4 - \tau^2 - 1$	$-\tau^2\alpha_5 - 1$
13	11	-2	0	$2\tau + 1$	$-\tau^4 - \tau^2 + 1$	$-\tau^2\alpha_5 + 1$
15	16	-2	-1	$-3\tau + 1$	$\tau^4 - 1$	

Since each term in α_u involves an *elliptic curve addition* it is desirable, to the extent possible, to reduce these terms in combinations of other α_u values, taking advantage of the fact that they have already been calculated.

Solinas was able to show an efficient arrangement for the terms α_9, α_{11}, and α_{13}. However, α_{15} has a large power of τ, viz. τ^4. Of course, it is undesirable to use terms such as $-3\tau + 1$, favoring the τ mapping $\tau^4 - 1$, since, again, scalar multiplication is substantially more expensive. Furthermore, since $\alpha_u \equiv u\ mod\ \tau^w$, it would be equally valid to have chosen the $u\ mod\ \tau^w$ of $\tau - 1$ for α_5 and $\tau + 1$ for α_7, since these values are also valid congruence class representatives*.

Larger table sizes have α_u terms requiring longer τ-NAF representation, with high powers of τ, each requiring an elliptic curve addition. For example, a window width size of 8 has τ terms ranging as high as ten, with up to four elliptic curve additions. Window width sizes of 7 and 8 have not been studied extensively in the literature, and smaller table sizes show suboptimal arrangements. [2] produced a better pre-computation ar-

*Easily seen since $\tau^2 = \mu\tau - 2$.

rangement than that of Solinas in that the power of τ was reduced to 2. They were able to do this by picking terms that were not of least norm. However, we have improved upon this with no equation containing a term higher than a single power of τ. Furthermore, these terms all involve least norms!

The following is one such arrangement for a = 1 and w = 5 which is an improvement over any known arrangements.

$$\begin{aligned} \alpha_1 &= 1, & \alpha_3 &= \tau - 3 \\ \alpha_5 &= \tau - 1, & \alpha_7 &= \tau + 1 \\ \alpha_9 &= 2\tau - 3, & \alpha_{11} &= 2\tau - 1 \\ \alpha_{13} &= 2\tau + 1, & \alpha_{15} &= 3\tau - 3 \end{aligned}$$

with arrangement

$$\begin{aligned} \alpha_1 &= 1, & \alpha_5 &= \tau - 1 \\ \alpha_7 &= \tau + 1, & \alpha_3 &= \alpha_5 + \tau\alpha_5 \\ \alpha_{11} &= \alpha_5 + \tau, & \alpha_{13} &= \alpha_7 + \tau \\ \alpha_9 &= \alpha_3 + \tau, & \alpha_{15} &= \alpha_9 + \tau \end{aligned}$$

We verify this result as follows using the fact that $\tau^2 = \tau - 2$ for $a = 1$:

$\alpha_1 = 1$

$\alpha_5 = \tau - 1$

$\alpha_7 = \tau + 1$

$\alpha_3 = \alpha_5 + \tau\alpha_5 = \tau - 1 + \tau(\tau - 1) = \tau - 1 + \tau^2 - \tau = \tau - 3$

$\alpha_{11} = \alpha_5 + \tau = \tau - 1 + \tau = 2\tau - 1$

$\alpha_{13} = \alpha_7 + \tau = \tau + 1 + \tau = 2\tau + 1$

$\alpha_9 = \alpha_3 + \tau = \tau - 3 + \tau = 2\tau - 3$

$\alpha_{15} = \alpha_9 + \tau = 2\tau - 3 + \tau = 3\tau - 3$

Chapter 4

Pre-Computation

4.1 Efficient Table Calculation

Our goal was to examine the various *width-w* τ-NAF tables, and, based on observations, determine if we could find a pattern to producing more efficient arrangements, as well as examining width sizes of 7 and 8. Based on the work by [2], we did not restrict ourselves to least norm values. The tables exhibited in appendix A: and B: reflect all those values such that $N(\alpha_u) < \tau^w$.

Based on observation of smaller tables, it appeared that we could compute an efficient arrangement, not necessarily using least norms, such that all terms were combinations of $\alpha_j = \pm\alpha_i \pm \tau$ or $\alpha_j = \pm\alpha_i \pm \tau\alpha_i$. Favoring the former equation in terms of $\pm\tau$, we can save some computational time and memory by precalculating $\pm\tau P$. α_i is any previously determined arrangement from previous stages of reasoning, so we required initial starting values. It made sense to start with initial values of $\alpha_1 = 1$ and $\alpha_i' s = \pm\tau \pm 1$ and begin deliberations from there.

We were able to write a computer program which did most of the heavy lifting following the above paradigm. This program implements a greedy algorithm insofar that it looks for terms in the next stage with $\alpha_j = \pm\alpha_i \pm \tau$ first, followed by terms of the form $\alpha_j = \pm\alpha_i \pm \tau\alpha_i$, if no match was found. The program moves on to the next term on the very first match, i.e. we do not attempt to discover every conceivable permutation of terms, since our goal was to find just one optimal arrangement. These arrangements are not unique in that we can find other similar arrangements, but none of more efficiency in elliptic curve operations.

After generating many sets of arrangements using assorted combinations of terms (not necessarily of least norm) it appeared feasible that we could generate an efficient arrangement by using least norms. After some additional experimentation and observation, we were finally able to achieve our ultimate goal of generating efficient equations using least norms.

The following arrangements are the culmination of our work. These arrangements are better than any previously published results as they only use least norms and demand just $2^{w-2}-1$ elliptic curve operations with single powers of τ. They are optimal insofar as no values exist of the form $\alpha_j = -\alpha_i$, where $N(\alpha_u) < \tau^w$, so the best we can hope for is two term equations as presented below.

In addition, we present the same efficient arrangements for window widths of 7 and 8 which have never before been presented in the literature. It is interesting to note that the order of the arrangements are the same for the same width with the only deviation being the difference in the sign on the τ term. This is due to the fact that $\mu = 1$ when $a = 0$ and $\mu = -1$ when $a = 1$.

According to table 2 in [19], there is a diminishing return on precalculation. Based on the number of operations, the break even point, on average, between standard τ-NAF vs *window-w* τ-NAF occurs with a window width of 8. However, with a field size of $m = 521$ we have

$$m/3 = 521/3 \approx 174$$

additions for standard τ-NAF and

$$2^{w-2} - 1 + m/(w+1) = 2^7 - 1 + 521/10 \approx 180$$

additions for *window-w* τ-NAF where $w = 9$. Thus, for larger field sizes, corresponding to larger key sizes in data encryption, it may be advantageous to apply larger window width sizes.

The following are our arrangements for windows size of $5 \leq w \leq 8$ for $a = 0, 1$. Notice that each table has exactly $2^{w-2} - 1$ elliptic curve operations which is optimal since, again, no terms exist of the form $\alpha_j = -\alpha_i$ where $\alpha_u < N(\tau^w)$. Moreover, these tables were produced by picking the term of least norm from the congruence classes. Also take note that the arrangements are not in order, i.e. α terms with lower indices may appear later in the arrangements. Furthermore, as an added improvement in computational time, one can pre-compute τP.

Verification was performed by hand on table sizes up to $w = 6$ and then by random sampling on widths of 7 and 8. In addition, all arrangements were tested programmatically.

4.2 $\mathrm{E}_0, w = 5$

Congruence class representative:

$$\begin{aligned} \alpha_1 &= 1, & \alpha_3 &= -\tau - 3 \\ \alpha_5 &= -\tau - 1, & \alpha_7 &= -\tau + 1 \\ \alpha_9 &= -2\tau - 3, & \alpha_{11} &= -2\tau - 1 \\ \alpha_{13} &= -2\tau + 1, & \alpha_{15} &= 3\tau + 1 \end{aligned}$$

Arrangement:

$$\begin{aligned} \alpha_1 &= 1, & \alpha_5 &= -\tau - 1 \\ \alpha_7 &= -\tau + 1, & \alpha_3 &= \alpha_5 - \tau\alpha_5 \\ \alpha_{11} &= \alpha_5 - \tau, & \alpha_{13} &= \alpha_7 - \tau \\ \alpha_{15} &= -\alpha_7 + \tau\alpha_7, & \alpha_9 &= \alpha_3 - \tau \end{aligned}$$

4.3 $\mathrm{E}_1, w = 5$

Congruence class representative:

$$\begin{aligned} \alpha_1 &= 1, & \alpha_3 &= \tau - 3 \\ \alpha_5 &= \tau - 1, & \alpha_7 &= \tau + 1 \\ \alpha_9 &= 2\tau - 3, & \alpha_{11} &= 2\tau - 1 \\ \alpha_{13} &= 2\tau + 1, & \alpha_{15} &= -3\tau + 1 \end{aligned}$$

Arrangement:

$$\begin{aligned} \alpha_1 &= 1, & \alpha_5 &= \tau - 1 \\ \alpha_7 &= \tau + 1, & \alpha_3 &= \alpha_5 + \tau\alpha_5 \\ \alpha_{11} &= \alpha_5 + \tau, & \alpha_{13} &= \alpha_7 + \tau \\ \alpha_{15} &= -\alpha_7 - \tau\alpha_7, & \alpha_9 &= \alpha_3 + \tau \end{aligned}$$

4.4 $\mathrm{E}_0, w = 6$

Congruence class representative:

$$\begin{aligned}
\alpha_1 &= 1, & \alpha_3 &= 3\\
\alpha_5 &= 5, & \alpha_7 &= -2\tau - 5\\
\alpha_9 &= -2\tau - 3, & \alpha_{11} &= -2\tau - 1\\
\alpha_{13} &= -2\tau + 1, & \alpha_{15} &= 3\tau + 1\\
\alpha_{17} &= 3\tau + 3, & \alpha_{19} &= 3\tau + 5\\
\alpha_{21} &= -4\tau - 3, & \alpha_{23} &= \tau - 3\\
\alpha_{25} &= \tau - 1, & \alpha_{27} &= \tau + 1\\
\alpha_{29} &= \tau + 3, & \alpha_{31} &= \tau + 5
\end{aligned}$$

Arrangement:

$$\begin{aligned}
\alpha_1 &= 1, & \alpha_{25} &= \tau - 1\\
\alpha_{27} &= \tau + 1, & \alpha_{13} &= -\alpha_{25} - \tau\\
\alpha_{15} &= \alpha_{25} - \tau\alpha_{25}, & \alpha_{29} &= -\alpha_{25} - \tau\alpha_{25}\\
\alpha_{11} &= -\alpha_{27} - \tau, & \alpha_{31} &= \alpha_{13} + \tau\alpha_{13}\\
\alpha_3 &= \alpha_{29} - \tau, & \alpha_9 &= -\alpha_{29} - \tau\\
\alpha_{19} &= -\alpha_{11} + \tau\alpha_{11}, & \alpha_{23} &= -\alpha_{11} - \tau\alpha_{11}\\
\alpha_5 &= \alpha_{31} - \tau, & \alpha_7 &= -\alpha_{31} - \tau\\
\alpha_{17} &= \alpha_3 + \tau\alpha_3, & \alpha_{21} &= -\alpha_{17} - \tau
\end{aligned}$$

4.5 $\mathrm{E}_1, w = 6$

Congruence class representative:

$$\begin{aligned} \alpha_1 &= 1, & \alpha_3 &= 3 \\ \alpha_5 &= 5, & \alpha_7 &= 2\tau - 5 \\ \alpha_9 &= 2\tau - 3, & \alpha_{11} &= 2\tau - 1 \\ \alpha_{13} &= 2\tau + 1, & \alpha_{15} &= -3\tau + 1 \\ \alpha_{17} &= -3\tau + 3, & \alpha_{19} &= -3\tau + 5 \\ \alpha_{21} &= 4\tau - 3, & \alpha_{23} &= -\tau - 3 \\ \alpha_{25} &= -\tau - 1, & \alpha_{27} &= -\tau + 1 \\ \alpha_{29} &= -\tau + 3, & \alpha_{31} &= -\tau + 5 \end{aligned}$$

Arrangement:

$$\begin{aligned} \alpha_1 &= 1, & \alpha_{25} &= -\tau - 1 \\ \alpha_{27} &= -\tau + 1, & \alpha_{13} &= -\alpha_{25} + \tau \\ \alpha_{15} &= \alpha_{25} + \tau\alpha_{25}, & \alpha_{29} &= -\alpha_{25} + \tau\alpha_{25} \\ \alpha_{11} &= -\alpha_{27} + \tau, & \alpha_{31} &= \alpha_{13} - \tau\alpha_{13} \\ \alpha_3 &= \alpha_{29} + \tau, & \alpha_9 &= -\alpha_{29} + \tau \\ \alpha_{19} &= -\alpha_{11} - \tau\alpha_{11}, & \alpha_{23} &= -\alpha_{11} + \tau\alpha_{11} \\ \alpha_5 &= \alpha_{31} + \tau, & \alpha_7 &= -\alpha_{31} + \tau \\ \alpha_{17} &= \alpha_3 - \tau\alpha_3, & \alpha_{21} &= -\alpha_{17} + \tau \end{aligned}$$

4.6 $\mathrm{E}_0, w = 7$

Congruence class representative:

$$\begin{aligned}
\alpha_1 &= 1, & \alpha_3 &= 3\\
\alpha_5 &= 5, & \alpha_7 &= 7\\
\alpha_9 &= 3\tau - 5, & \alpha_{11} &= 3\tau - 3\\
\alpha_{13} &= 3\tau - 1, & \alpha_{15} &= 3\tau + 1\\
\alpha_{17} &= 3\tau + 3, & \alpha_{19} &= 3\tau + 5\\
\alpha_{21} &= -4\tau - 3, & \alpha_{23} &= -4\tau - 1\\
\alpha_{25} &= -4\tau + 1, & \alpha_{27} &= -4\tau + 3\\
\alpha_{29} &= 6\tau + 1, & \alpha_{31} &= -\tau - 7\\
\alpha_{33} &= -\tau - 5, & \alpha_{35} &= -\tau - 3\\
\alpha_{37} &= -\tau - 1, & \alpha_{39} &= -\tau + 1\\
\alpha_{41} &= -\tau + 3, & \alpha_{43} &= -\tau + 5\\
\alpha_{45} &= -\tau + 7, & \alpha_{47} &= 2\tau - 5\\
\alpha_{49} &= 2\tau - 3, & \alpha_{51} &= 2\tau - 1\\
\alpha_{53} &= 2\tau + 1, & \alpha_{55} &= 2\tau + 3\\
\alpha_{57} &= 2\tau + 5, & \alpha_{59} &= 2\tau + 7\\
\alpha_{61} &= -5\tau - 1, & \alpha_{63} &= -5\tau + 1
\end{aligned}$$

Arrangement:

$$\begin{aligned}
\alpha_1 &= 1, & \alpha_{37} &= -\tau - 1\\
\alpha_{39} &= -\tau + 1, & \alpha_{35} &= \alpha_{37} - \tau\alpha_{37}\\
\alpha_{53} &= -\alpha_{37} + \tau, & \alpha_{15} &= -\alpha_{39} + \tau\alpha_{39}\\
\alpha_{51} &= -\alpha_{39} + \tau, & \alpha_3 &= -\alpha_{35} - \tau\\
\alpha_{43} &= -\alpha_{35} + \tau\alpha_{35}, & \alpha_{55} &= -\alpha_{35} + \tau\\
\alpha_{19} &= \alpha_{53} - \tau\alpha_{53}, & \alpha_{41} &= -\alpha_{53} - \tau\alpha_{53}\\
\alpha_{23} &= -\alpha_{15} - \tau, & \alpha_{13} &= \alpha_{51} + \tau\\
\alpha_{33} &= \alpha_{51} + \tau\alpha_{51}, & \alpha_{11} &= -\alpha_3 + \tau\alpha_3\\
\alpha_{17} &= \alpha_3 + \tau\alpha_3, & \alpha_5 &= \alpha_{43} + \tau\\
\alpha_{47} &= -\alpha_{43} + \tau, & \alpha_{31} &= -\alpha_{55} + \tau\alpha_{55}\\
\alpha_{57} &= \alpha_{19} - \tau, & \alpha_{63} &= -\alpha_{19} - \tau\alpha_{19}\\
\alpha_{49} &= -\alpha_{41} + \tau, & \alpha_{45} &= \alpha_{23} + \tau\alpha_{23}\\
\alpha_{61} &= \alpha_{23} - \tau, & \alpha_{25} &= -\alpha_{13} - \tau\\
\alpha_{27} &= -\alpha_{11} - \tau, & \alpha_{21} &= -\alpha_{17} - \tau\\
\alpha_9 &= \alpha_{47} + \tau, & \alpha_7 &= -\alpha_{31} - \tau\\
\alpha_{59} &= -\alpha_{31} + \tau, & \alpha_{29} &= -\alpha_{61} + \tau
\end{aligned}$$

4.7 $\mathrm{E}_1, w = 7$

Congruence class representative:

$$\begin{aligned}
\alpha_1 &= 1, & \alpha_3 &= 3 \\
\alpha_5 &= 5, & \alpha_7 &= 7 \\
\alpha_9 &= -3\tau - 5, & \alpha_{11} &= -3\tau - 3 \\
\alpha_{13} &= -3\tau - 1, & \alpha_{15} &= -3\tau + 1 \\
\alpha_{17} &= -3\tau + 3, & \alpha_{19} &= -3\tau + 5 \\
\alpha_{21} &= 4\tau - 3, & \alpha_{23} &= 4\tau - 1 \\
\alpha_{25} &= 4\tau + 1, & \alpha_{27} &= 4\tau + 3 \\
\alpha_{29} &= -6\tau + 1, & \alpha_{31} &= \tau - 7 \\
\alpha_{33} &= \tau - 5, & \alpha_{35} &= \tau - 3 \\
\alpha_{37} &= \tau - 1, & \alpha_{39} &= \tau + 1 \\
\alpha_{41} &= \tau + 3, & \alpha_{43} &= \tau + 5 \\
\alpha_{45} &= \tau + 7, & \alpha_{47} &= -2\tau - 5 \\
\alpha_{49} &= -2\tau - 3, & \alpha_{51} &= -2\tau - 1 \\
\alpha_{53} &= -2\tau + 1, & \alpha_{55} &= -2\tau + 3 \\
\alpha_{57} &= -2\tau + 5, & \alpha_{59} &= -2\tau + 7 \\
\alpha_{61} &= 5\tau - 1, & \alpha_{63} &= 5\tau + 1
\end{aligned}$$

Arrangement:

$$\begin{aligned}
\alpha_1 &= 1, & \alpha_{37} &= \tau - 1 \\
\alpha_{39} &= \tau + 1, & \alpha_{35} &= \alpha_{37} + \tau\alpha_{37} \\
\alpha_{53} &= -\alpha_{37} - \tau, & \alpha_{15} &= -\alpha_{39} - \tau\alpha_{39} \\
\alpha_{51} &= -\alpha_{39} - \tau, & \alpha_3 &= -\alpha_{35} + \tau \\
\alpha_{43} &= -\alpha_{35} - \tau\alpha_{35}, & \alpha_{55} &= -\alpha_{35} - \tau \\
\alpha_{19} &= \alpha_{53} + \tau\alpha_{53}, & \alpha_{41} &= -\alpha_{53} + \tau\alpha_{53} \\
\alpha_{23} &= -\alpha_{15} + \tau, & \alpha_{13} &= \alpha_{51} - \tau \\
\alpha_{33} &= \alpha_{51} - \tau\alpha_{51}, & \alpha_{11} &= -\alpha_3 - \tau\alpha_3 \\
\alpha_{17} &= \alpha_3 - \tau\alpha_3, & \alpha_5 &= \alpha_{43} - \tau \\
\alpha_{47} &= -\alpha_{43} - \tau, & \alpha_{31} &= -\alpha_{55} - \tau\alpha_{55} \\
\alpha_{57} &= \alpha_{19} + \tau, & \alpha_{63} &= -\alpha_{19} + \tau\alpha_{19} \\
\alpha_{49} &= -\alpha_{41} - \tau, & \alpha_{45} &= \alpha_{23} - \tau\alpha_{23} \\
\alpha_{61} &= \alpha_{23} + \tau, & \alpha_{25} &= -\alpha_{13} + \tau \\
\alpha_{27} &= -\alpha_{11} + \tau, & \alpha_{21} &= -\alpha_{17} + \tau \\
\alpha_9 &= \alpha_{47} - \tau, & \alpha_7 &= -\alpha_{31} + \tau \\
\alpha_{59} &= -\alpha_{31} - \tau, & \alpha_{29} &= -\alpha_{61} - \tau
\end{aligned}$$

4.8 $\mathrm{E}_0, w = 8$

Congruence class representative:

$$\begin{aligned}
\alpha_{1} &= 1, & \alpha_{3} &= 3\\
\alpha_{5} &= 5, & \alpha_{7} &= 7\\
\alpha_{9} &= 3\tau - 5, & \alpha_{11} &= 3\tau - 3\\
\alpha_{13} &= 3\tau - 1, & \alpha_{15} &= 3\tau + 1\\
\alpha_{17} &= 3\tau + 3, & \alpha_{19} &= 3\tau + 5\\
\alpha_{21} &= 3\tau + 7, & \alpha_{23} &= 3\tau + 9\\
\alpha_{25} &= 6\tau - 3, & \alpha_{27} &= 6\tau - 1\\
\alpha_{29} &= 6\tau + 1, & \alpha_{31} &= 6\tau + 3\\
\alpha_{33} &= 6\tau + 5, & \alpha_{35} &= 6\tau + 7\\
\alpha_{37} &= 6\tau + 9, & \alpha_{39} &= 6\tau + 11\\
\alpha_{41} &= -8\tau - 7, & \alpha_{43} &= -8\tau - 5\\
\alpha_{45} &= -8\tau - 3, & \alpha_{47} &= -8\tau - 1\\
\alpha_{49} &= -8\tau + 1, & \alpha_{51} &= -5\tau - 11\\
\alpha_{53} &= -5\tau - 9, & \alpha_{55} &= -5\tau - 7\\
\alpha_{57} &= -5\tau - 5, & \alpha_{59} &= -5\tau - 3\\
\alpha_{61} &= -5\tau - 1, & \alpha_{63} &= -5\tau + 1\\
\alpha_{65} &= -5\tau + 3, & \alpha_{67} &= -2\tau - 9\\
\alpha_{69} &= -2\tau - 7, & \alpha_{71} &= -2\tau - 5\\
\alpha_{73} &= -2\tau - 3, & \alpha_{75} &= -2\tau - 1\\
\alpha_{77} &= -2\tau + 1, & \alpha_{79} &= -2\tau + 3\\
\alpha_{81} &= -2\tau + 5, & \alpha_{83} &= \tau - 7\\
\alpha_{85} &= \tau - 5, & \alpha_{87} &= \tau - 3\\
\alpha_{89} &= \tau - 1, & \alpha_{91} &= \tau + 1\\
\alpha_{93} &= \tau + 3, & \alpha_{95} &= \tau + 5\\
\alpha_{97} &= \tau + 7, & \alpha_{99} &= \tau + 9\\
\alpha_{101} &= 4\tau - 3, & \alpha_{103} &= 4\tau - 1\\
\alpha_{105} &= 4\tau + 1, & \alpha_{107} &= 4\tau + 3\\
\alpha_{109} &= 4\tau + 5, & \alpha_{111} &= 4\tau + 7\\
\alpha_{113} &= 4\tau + 9, & \alpha_{115} &= 4\tau + 11\\
\alpha_{117} &= 7\tau - 1, & \alpha_{119} &= 7\tau + 1\\
\alpha_{121} &= 7\tau + 3, & \alpha_{123} &= 7\tau + 5\\
\alpha_{125} &= 7\tau + 7, & \alpha_{127} &= 7\tau + 9
\end{aligned}$$

Arrangement:

$$\begin{aligned}
\alpha_{1} &= 1, & \alpha_{89} &= \tau - 1 \\
\alpha_{91} &= \tau + 1, & \alpha_{15} &= \alpha_{89} - \tau\alpha_{89} \\
\alpha_{77} &= -\alpha_{89} - \tau, & \alpha_{93} &= -\alpha_{89} - \tau\alpha_{89} \\
\alpha_{75} &= -\alpha_{91} - \tau, & \alpha_{55} &= -\alpha_{15} + \tau\alpha_{15} \\
\alpha_{85} &= \alpha_{15} + \tau\alpha_{15}, & \alpha_{105} &= \alpha_{15} + \tau \\
\alpha_{13} &= -\alpha_{77} + \tau, & \alpha_{59} &= \alpha_{77} - \tau\alpha_{77} \\
\alpha_{95} &= \alpha_{77} + \tau\alpha_{77}, & \alpha_{3} &= \alpha_{93} - \tau \\
\alpha_{73} &= -\alpha_{93} - \tau, & \alpha_{19} &= -\alpha_{75} + \tau\alpha_{75} \\
\alpha_{87} &= -\alpha_{75} - \tau\alpha_{75}, & \alpha_{35} &= -\alpha_{55} + \tau \\
\alpha_{111} &= -\alpha_{55} - \tau, & \alpha_{5} &= -\alpha_{85} + \tau \\
\alpha_{81} &= -\alpha_{85} - \tau, & \alpha_{61} &= -\alpha_{105} - \tau \\
\alpha_{83} &= \alpha_{105} + \tau\alpha_{105}, & \alpha_{127} &= \alpha_{105} - \tau\alpha_{105} \\
\alpha_{97} &= -\alpha_{13} - \tau\alpha_{13}, & \alpha_{103} &= \alpha_{13} + \tau \\
\alpha_{123} &= \alpha_{13} - \tau\alpha_{13}, & \alpha_{31} &= -\alpha_{59} + \tau \\
\alpha_{107} &= -\alpha_{59} - \tau, & \alpha_{71} &= -\alpha_{95} - \tau \\
\alpha_{11} &= -\alpha_{3} + \tau\alpha_{3}, & \alpha_{17} &= \alpha_{3} + \tau\alpha_{3} \\
\alpha_{63} &= -\alpha_{19} - \tau\alpha_{19}, & \alpha_{109} &= \alpha_{19} + \tau \\
\alpha_{79} &= -\alpha_{87} - \tau, & \alpha_{125} &= \alpha_{35} + \tau \\
\alpha_{21} &= \alpha_{111} - \tau, & \alpha_{117} &= \alpha_{111} + \tau\alpha_{111} \\
\alpha_{57} &= -\alpha_{5} - \tau\alpha_{5}, & \alpha_{9} &= -\alpha_{81} + \tau \\
\alpha_{53} &= -\alpha_{81} - \tau\alpha_{81}, & \alpha_{29} &= -\alpha_{61} + \tau \\
\alpha_{7} &= -\alpha_{83} + \tau, & \alpha_{37} &= \alpha_{127} - \tau \\
\alpha_{69} &= -\alpha_{97} - \tau, & \alpha_{99} &= -\alpha_{103} - \tau\alpha_{103} \\
\alpha_{33} &= \alpha_{123} - \tau, & \alpha_{43} &= -\alpha_{123} - \tau \\
\alpha_{121} &= \alpha_{31} + \tau, & \alpha_{51} &= -\alpha_{107} + \tau\alpha_{107} \\
\alpha_{23} &= -\alpha_{11} - \tau\alpha_{11}, & \alpha_{101} &= \alpha_{11} + \tau \\
\alpha_{27} &= -\alpha_{63} + \tau, & \alpha_{65} &= -\alpha_{109} - \tau\alpha_{109} \\
\alpha_{119} &= -\alpha_{79} + \tau\alpha_{79}, & \alpha_{41} &= -\alpha_{125} - \tau \\
\alpha_{49} &= -\alpha_{117} - \tau, & \alpha_{113} &= -\alpha_{53} - \tau \\
\alpha_{67} &= -\alpha_{99} - \tau, & \alpha_{45} &= -\alpha_{121} - \tau \\
\alpha_{39} &= -\alpha_{51} + \tau, & \alpha_{115} &= -\alpha_{51} - \tau \\
\alpha_{25} &= -\alpha_{65} + \tau, & \alpha_{47} &= -\alpha_{119} - \tau
\end{aligned}$$

4.9 $\mathrm{E}_1, w = 8$

Congruence class representative:

$$\begin{aligned}
\alpha_1 &= 1, & \alpha_3 &= 3\\
\alpha_5 &= 5, & \alpha_7 &= 7\\
\alpha_9 &= -3\tau - 5, & \alpha_{11} &= -3\tau - 3\\
\alpha_{13} &= -3\tau - 1, & \alpha_{15} &= -3\tau + 1\\
\alpha_{17} &= -3\tau + 3, & \alpha_{19} &= -3\tau + 5\\
\alpha_{21} &= -3\tau + 7, & \alpha_{23} &= -3\tau + 9\\
\alpha_{25} &= -6\tau - 3, & \alpha_{27} &= -6\tau - 1\\
\alpha_{29} &= -6\tau + 1, & \alpha_{31} &= -6\tau + 3\\
\alpha_{33} &= -6\tau + 5, & \alpha_{35} &= -6\tau + 7\\
\alpha_{37} &= -6\tau + 9, & \alpha_{39} &= -6\tau + 11\\
\alpha_{41} &= 8\tau - 7, & \alpha_{43} &= 8\tau - 5\\
\alpha_{45} &= 8\tau - 3, & \alpha_{47} &= 8\tau - 1\\
\alpha_{49} &= 8\tau + 1, & \alpha_{51} &= 5\tau - 11\\
\alpha_{53} &= 5\tau - 9, & \alpha_{55} &= 5\tau - 7\\
\alpha_{57} &= 5\tau - 5, & \alpha_{59} &= 5\tau - 3\\
\alpha_{61} &= 5\tau - 1, & \alpha_{63} &= 5\tau + 1\\
\alpha_{65} &= 5\tau + 3, & \alpha_{67} &= 2\tau - 9\\
\alpha_{69} &= 2\tau - 7, & \alpha_{71} &= 2\tau - 5\\
\alpha_{73} &= 2\tau - 3, & \alpha_{75} &= 2\tau - 1\\
\alpha_{77} &= 2\tau + 1, & \alpha_{79} &= 2\tau + 3\\
\alpha_{81} &= 2\tau + 5, & \alpha_{83} &= -\tau - 7\\
\alpha_{85} &= -\tau - 5, & \alpha_{87} &= -\tau - 3\\
\alpha_{89} &= -\tau - 1, & \alpha_{91} &= -\tau + 1\\
\alpha_{93} &= -\tau + 3, & \alpha_{95} &= -\tau + 5\\
\alpha_{97} &= -\tau + 7, & \alpha_{99} &= -\tau + 9\\
\alpha_{101} &= -4\tau - 3, & \alpha_{103} &= -4\tau - 1\\
\alpha_{105} &= -4\tau + 1, & \alpha_{107} &= -4\tau + 3\\
\alpha_{109} &= -4\tau + 5, & \alpha_{111} &= -4\tau + 7\\
\alpha_{113} &= -4\tau + 9, & \alpha_{115} &= -4\tau + 11\\
\alpha_{117} &= -7\tau - 1, & \alpha_{119} &= -7\tau + 1\\
\alpha_{121} &= -7\tau + 3, & \alpha_{123} &= -7\tau + 5\\
\alpha_{125} &= -7\tau + 7, & \alpha_{127} &= -7\tau + 9
\end{aligned}$$

Arrangement:

$$
\begin{aligned}
\alpha_{1} &= 1, & \alpha_{89} &= -\tau - 1\\
\alpha_{91} &= -\tau + 1, & \alpha_{15} &= \alpha_{89} + \tau\alpha_{89}\\
\alpha_{77} &= -\alpha_{89} + \tau, & \alpha_{93} &= -\alpha_{89} + \tau\alpha_{89}\\
\alpha_{75} &= -\alpha_{91} + \tau, & \alpha_{55} &= -\alpha_{15} - \tau\alpha_{15}\\
\alpha_{85} &= \alpha_{15} - \tau\alpha_{15}, & \alpha_{105} &= \alpha_{15} - \tau\\
\alpha_{13} &= -\alpha_{77} - \tau, & \alpha_{59} &= \alpha_{77} + \tau\alpha_{77}\\
\alpha_{95} &= \alpha_{77} - \tau\alpha_{77}, & \alpha_{3} &= \alpha_{93} + \tau\\
\alpha_{73} &= -\alpha_{93} + \tau, & \alpha_{19} &= -\alpha_{75} - \tau\alpha_{75}\\
\alpha_{87} &= -\alpha_{75} + \tau\alpha_{75}, & \alpha_{35} &= -\alpha_{55} - \tau\\
\alpha_{111} &= -\alpha_{55} + \tau, & \alpha_{5} &= -\alpha_{85} - \tau\\
\alpha_{81} &= -\alpha_{85} + \tau, & \alpha_{61} &= -\alpha_{105} + \tau\\
\alpha_{83} &= \alpha_{105} - \tau\alpha_{105}, & \alpha_{127} &= \alpha_{105} + \tau\alpha_{105}\\
\alpha_{97} &= -\alpha_{13} + \tau\alpha_{13}, & \alpha_{103} &= \alpha_{13} - \tau\\
\alpha_{123} &= \alpha_{13} + \tau\alpha_{13}, & \alpha_{31} &= -\alpha_{59} - \tau\\
\alpha_{107} &= -\alpha_{59} + \tau, & \alpha_{71} &= -\alpha_{95} + \tau\\
\alpha_{11} &= -\alpha_{3} - \tau\alpha_{3}, & \alpha_{17} &= \alpha_{3} - \tau\alpha_{3}\\
\alpha_{63} &= -\alpha_{19} + \tau\alpha_{19}, & \alpha_{109} &= \alpha_{19} - \tau\\
\alpha_{79} &= -\alpha_{87} + \tau, & \alpha_{125} &= \alpha_{35} - \tau\\
\alpha_{21} &= \alpha_{111} + \tau, & \alpha_{117} &= \alpha_{111} - \tau\alpha_{111}\\
\alpha_{57} &= -\alpha_{5} + \tau\alpha_{5}, & \alpha_{9} &= -\alpha_{81} - \tau\\
\alpha_{53} &= -\alpha_{81} + \tau\alpha_{81}, & \alpha_{29} &= -\alpha_{61} - \tau\\
\alpha_{7} &= -\alpha_{83} - \tau, & \alpha_{37} &= \alpha_{127} + \tau\\
\alpha_{69} &= -\alpha_{97} + \tau, & \alpha_{99} &= -\alpha_{103} + \tau\alpha_{103}\\
\alpha_{33} &= \alpha_{123} + \tau, & \alpha_{43} &= -\alpha_{123} + \tau\\
\alpha_{121} &= \alpha_{31} - \tau, & \alpha_{51} &= -\alpha_{107} - \tau\alpha_{107}\\
\alpha_{23} &= -\alpha_{11} + \tau\alpha_{11}, & \alpha_{101} &= \alpha_{11} - \tau\\
\alpha_{27} &= -\alpha_{63} - \tau, & \alpha_{65} &= -\alpha_{109} + \tau\alpha_{109}\\
\alpha_{119} &= -\alpha_{79} - \tau\alpha_{79}, & \alpha_{41} &= -\alpha_{125} + \tau\\
\alpha_{49} &= -\alpha_{117} + \tau, & \alpha_{113} &= -\alpha_{53} + \tau\\
\alpha_{67} &= -\alpha_{99} + \tau, & \alpha_{45} &= -\alpha_{121} + \tau\\
\alpha_{39} &= -\alpha_{51} - \tau, & \alpha_{115} &= -\alpha_{51} + \tau\\
\alpha_{25} &= -\alpha_{65} - \tau, & \alpha_{47} &= -\alpha_{119} + \tau
\end{aligned}
$$

Chapter 5

Discussion

5.1 Summary

Solinas [19] was able to develop a τ-NAF algorithm on Koblitz curves which provided a 50% improvement in scalar multiplication over previously known methods by exploiting the Frobenius endomorphism property of Koblitz curves. Furthermore, Solinas demonstrated an improvement in this algorithm by offering a *width-w* τ-NAF algorithm where he worked with a window width of 5, and showing well over a one third improvement in the work required over standard τ-NAF. He also offered an efficient arrangement of α_u terms which capitalizes on previous computation of terms. [2] later showed a further improvement over Solinas by relaxing the condition of least norm, offering a more efficient arrangement. However, one term involved a τ^2.

We further expanded on this work and provided more efficient arrangement utilizing single powers of τ, with just $2^{w-2} - 1$ elliptic curve operations and using least norms! Examining the tables in appendix A: and B:, we see that there are no terms such that $\alpha_j = -\alpha_i$. Hence, we would expect at least two term equations with the exception of $\alpha_1 = 1$.

Predecessors have worked with window width sizes of 6 or less. We have provided arrangements for window widths of 7 and 8, and we conjecture that such arrangements exist for larger window sizes. However, as mentioned previously, and based on current key size requirements, there is presently no advantage to applying larger window width sizes above 8.

Following the work of [2], and relaxing the requirement of least norm, we were able to provide a simplified rounding technique which led to a more elementary reduction modulo δ, algorithm 12, no less valid than that of using least norms. We provided mathematical proof via use of the division theorem.

Lastly, we discussed an $O(n)$ squaring algorithm that can be used in software which we presented in section 3.3.2.3. The disadvantage of this technique is that it requires a large memory footprint. An improvement but, at the expense of some efficiency, would be to apply a reduction each time the squared value exceeds the field size.

5.2 Future Work

We explored widths of size 7 and 8 and produced efficient arrangements. Although there is a diminishing return on larger window sizes, widths of 9 and 10 should be explored, especially since larger key sizes may be needed in the future, due to ever increasing computational power. In addition, by relaxing the condition of least norm as shown by [2], more equivalence class representatives are available, especially as width sizes get larger and, thus, a relationship of the form $\alpha_j = -\alpha_i$ may exist. This would reduce the number of elliptic curve operations.

Applying the approach in this thesis to find optimal arrangements for fields with characteristic 3 and larger.

Lastly, improvements in implementation by taking advantage of multi-core processors. For example, since elliptic curve addition forms an abelian group, we could easily parallel process a *width-w* τ-adic NAF by continuously taking widths of w and sending each to its own *thread of execution*. Results from each thread could then be summed to provide the final result. Note that there is no guarantee of the order in which a thread of execution completes, due to the nature of thread scheduling in a processor, but this does not matter since, again, elliptic curve addition forms an abelian group.

Bibliography

[1] Ian F. Blake, Kumar Murty, and Guangwu Xu. Efficient algorithms for koblitz curves over fields of charateristic three. *Journal of Discrete Algorithms 3 (2005) 113-124*, pages 113–124, 2005.

[2] Ian F. Blake, Kumar Murty, and Guangwu Xu. A note on window τ-naf algorithm. *Information Processing Letters 95*, pages 496–502, 2005.

[3] Ian F. Blake, Kumar Murty, and Guangwu Xu. Nonadjacent radix-τ expansions of integers in euclidean imaginary quadratic number fields. *Canadian Journal of Mathematics*, 60:1267–1282, 2008.

[4] Ricardo Dahab, Darrel Hankerson, Men Long, Julio López, and Alfred Menezes. Software multiplication using gaussian normal bases. *IEEE Trans. Comput*, 55:974–984, 2006.

[5] David Steven Dummit and Richard M. Foote. *Abstract algebra.* John Wiley & sons, Hoboken, NJ, 2004.

[6] Behrouz A. Forouzan. *Cryptography & Network Security.* McGraw-Hill, Inc., New York, NY, USA, 1 edition, 2008.

[7] L. Gilbert and J. Gilbert. *Elements of Modern Algebra.* BROOKS COLE Publishing Company, 2008.

[8] Darrel Hankerson, Alfred Menezes, and Scott Vanstone. *Guide to Elliptic Curve Cryptography.* Springer-Verlag, New York, NY, 2010.

[9] T.W. Judson. *Abstract Algebra: Theory and Applications.* The Prindle, Weber & Schmidt Series in Advanced Mathematics. PWS Publishing Company, 1994.

[10] Neal Koblitz. Elliptic curve cryptosystems. *Mathematics of Computation*, 48(177):203–209, 1 1987.

[11] Neal Koblitz. Cm-curves with good cryptographic properties. In *Proc. Crypto '91*, pages 279–287. Springer-Verlag, 1992.

[12] http : //csrc.nist.gov/groups/ST/toolkit/documents/dss/NISTReCur.pdf. Recommended elliptic curves for federal government use, 1999. Accessed: 2013-09-13.

[13] http : //en.wikipedia.org/wiki/Euclidean_domain. Euclidean domain, 2013. Accessed: 2013-09-25.

[14] http : //www.nsa.gov/business/programs/elliptic_curve.shtml. The case for elliptic curve cryptography, 2009. Accessed: 2013-05-08.

[15] Alfred J. Menezes, Paul C. Van Oorschot, Scott A. Vanstone, and R. L. Rivest. *Handbook of Applied Cryptography.* CRC Press, 1997.

[16] Victor S. Miller. Use of elliptic curves in cryptography. In *Lecture notes in computer sciences; 218 on Advances in cryptology—CRYPTO 85*, pages 417–426, New York, NY, USA, 1986. Springer-Verlag New York, Inc.

[17] Charles C. Pinter. *A Book of Abstract Algebra.* Dover Publications, Inc, Mineola, NY, 2 edition, 2010.

[18] Joseph H. Silverman and John Tate. *Rational Points on Elliptic Curves.* Springer-Verlag New York Inc., 2010.

[19] Jerome A. Solinas. Efficient arithmetic on Koblitz curves. *Designs, Codes, and Cryptography*, pages 195–249, 2000.

[20] Lawrence C. Washington. *Elliptic Curves: Number Theory and Cryptography.* Chapman & Hall/CRC, 2 edition, 2008.

Appendix A:

a = 0 Width-w τ-NAF Tables

This appendix lists the complete τ-NAF table for window sizes 3 to 8 for E$_0$.

Table A:.1: E$_0$: $w = 3, N(\tau^w) = 8, \tau^w(\mathit{reduced}) = -\tau + 2$

u	norm	q_0	q_1	$u \ \mathit{mod} \ \tau^w$	α_u
1	1	0	0	1	1
1	4	-1	0	$\tau - 1$	$-\tau^3 + 1$
3	2	-1	0	$\tau + 1$	$-\tau^2 - 1$
3	7	-1	-1	$-2\tau - 1$	$-\tau^4 - \tau^2 - 1$

Table A:.2: E$_0$: $w = 4, N(\tau^w) = 16, \tau^w(\mathit{reduced}) = 3\tau + 2$

u	norm	q_0	q_1	$u \ \mathit{mod} \ \tau^w$	α_u
1	1	0	0	1	1
3	8	0	1	$-\tau - 3$	$\tau^2 - 1$
3	9	0	0	3	$-\tau^5 + \tau^2 - 1$
3	11	1	1	$2\tau - 1$	$\tau^4 + \tau^2 - 1$
5	2	0	1	$-\tau - 1$	$\tau^2 + 1$
5	7	1	1	$2\tau + 1$	$\tau^4 + \tau^2 + 1$
7	4	0	1	$-\tau + 1$	$\tau^3 - 1$
7	11	1	1	$2\tau + 3$	$-\tau^5 - \tau^3 - 1$
7	14	1	2	$\tau - 3$	$-\tau^3 - 1$

Table A:.3: E_0: $w = 5, N(\tau^w) = 32, \tau^w(reduced) = -\tau - 6$

u	norm	q_0	q_1	$u\ mod\ \tau^w$	α_u
1	1	0	0	1	1
1	22	1	0	$-\tau - 5$	$\tau^5 + 1$
3	8	1	0	$-\tau - 3$	$\tau^2 - 1$
3	9	0	0	3	$-\tau^5 + \tau^2 - 1$
5	2	1	0	$-\tau - 1$	$\tau^2 + 1$
5	25	0	0	5	$-\tau^5 + \tau^2 + 1$
7	4	1	0	$-\tau + 1$	$\tau^3 - 1$
7	23	2	0	$-2\tau - 5$	$\tau^5 + \tau^3 - 1$
9	11	2	0	$-2\tau - 3$	$\tau^5 + \tau^3 + 1$
9	14	1	0	$-\tau + 3$	$\tau^3 + 1$
9	29	1	-1	$4\tau + 1$	$-\tau^6 + \tau^3 + 1$
11	7	2	0	$-2\tau - 1$	$-\tau^4 - \tau^2 - 1$
11	29	1	-1	$4\tau + 3$	$\tau^4 - \tau^2 - 1$
13	11	2	0	$-2\tau + 1$	$-\tau^4 - \tau^2 + 1$
13	22	2	-1	$3\tau - 1$	$-\tau^6 - \tau^4 - \tau^2 + 1$
13	28	3	0	$-3\tau - 5$	$-\tau^7 + \tau^4 - \tau^2 + 1$
15	16	2	-1	$3\tau + 1$	$\tau^4 - 1$
15	18	3	0	$-3\tau - 3$	$-\tau^4 - 1$
15	23	2	0	$-2\tau + 3$	$\tau^6 + \tau^4 - 1$

TABLE A:.4: E$_0$: $w = 6, N(\tau^w) = 64, \tau^w(reduced) = -5\tau + 2$

u	norm	q_0	q_1	$u \ mod \ \tau^w$	α_u
1	1	0	0	1	1
1	56	-1	0	$5\tau - 1$	$-\tau^6 + 1$
3	9	0	0	3	$-\tau^5 + \tau^2 - 1$
3	46	-1	0	$5\tau + 1$	$\tau^7 + \tau^5 + \tau^2 - 1$
5	25	0	0	5	$-\tau^5 + \tau^2 + 1$
5	43	-1	-1	$-2\tau - 7$	$\tau^5 + \tau^2 + 1$
5	44	-1	0	$5\tau + 3$	$\tau^7 + \tau^5 + \tau^2 + 1$
7	23	-1	-1	$-2\tau - 5$	$\tau^5 + \tau^3 - 1$
7	49	0	0	7	$-\tau^5 + \tau^3 - 1$
7	50	-1	0	$5\tau + 5$	$\tau^7 + \tau^5 + \tau^3 - 1$
9	11	-1	-1	$-2\tau - 3$	$\tau^5 + \tau^3 + 1$
9	58	-2	-1	$3\tau - 5$	$\tau^8 - \tau^5 + \tau^3 + 1$
11	7	-1	-1	$-2\tau - 1$	$-\tau^4 - \tau^2 - 1$
11	36	-2	-1	$3\tau - 3$	$-\tau^6 - \tau^4 - \tau^2 - 1$
13	11	-1	-1	$-2\tau + 1$	$-\tau^4 - \tau^2 + 1$
13	22	-2	-1	$3\tau - 1$	$-\tau^6 - \tau^4 - \tau^2 + 1$
15	16	-2	-1	$3\tau + 1$	$\tau^4 - 1$
15	23	-1	-1	$-2\tau + 3$	$\tau^6 + \tau^4 - 1$
17	18	-2	-1	$3\tau + 3$	$\tau^4 + 1$
17	43	-1	-1	$-2\tau + 5$	$\tau^6 + \tau^4 + 1$
17	53	-2	-2	$-4\tau - 7$	$-\tau^7 + \tau^4 + 1$
19	28	-2	-1	$3\tau + 5$	$\tau^7 - \tau^4 + \tau^2 - 1$
19	37	-2	-2	$-4\tau - 5$	$-\tau^4 + \tau^2 - 1$
19	58	-3	-2	$\tau - 7$	$-\tau^6 - \tau^4 + \tau^2 - 1$
21	29	-2	-2	$-4\tau - 3$	$-\tau^4 + \tau^2 + 1$
21	32	-3	-2	$\tau - 5$	$-\tau^6 - \tau^4 + \tau^2 + 1$
21	46	-2	-1	$3\tau + 7$	$\tau^7 - \tau^4 + \tau^2 + 1$
23	14	-3	-2	$\tau - 3$	$-\tau^3 - 1$
23	29	-2	-2	$-4\tau - 1$	$\tau^6 - \tau^3 - 1$
25	4	-3	-2	$\tau - 1$	$-\tau^3 + 1$
25	37	-2	-2	$-4\tau + 1$	$\tau^6 - \tau^3 + 1$
27	2	-3	-2	$\tau + 1$	$-\tau^2 - 1$
27	53	-2	-2	$-4\tau + 3$	$\tau^6 - \tau^2 - 1$
29	8	-3	-2	$\tau + 3$	$-\tau^2 + 1$
31	22	-3	-2	$\tau + 5$	$-\tau^5 - 1$
31	44	-4	-3	$-\tau - 7$	$\tau^5 - 1$
31	63	-4	-2	$6\tau + 3$	$\tau^7 + \tau^5 - 1$

Table A:.5: E_0: $w = 7, N(\tau^w) = 128, \tau^w(reduced) = 7\tau + 10$

u	norm	q_0	q_1	u *mod* τ^w	α_u
1	1	0	0	1	1
1	116	-1	0	$-7\tau - 9$	$-\tau^7 + 1$
3	9	0	0	3	$-\tau^5 + \tau^2 - 1$
3	98	-1	0	$-7\tau - 7$	$-\tau^7 - \tau^5 + \tau^2 - 1$
5	25	0	0	5	$-\tau^5 + \tau^2 + 1$
5	88	-1	0	$-7\tau - 5$	$-\tau^7 - \tau^5 + \tau^2 + 1$
5	126	0	1	$3\tau - 9$	$\tau^8 - \tau^5 + \tau^2 + 1$
7	49	0	0	7	$-\tau^5 + \tau^3 - 1$
7	86	-1	0	$-7\tau - 3$	$-\tau^7 - \tau^5 + \tau^3 - 1$
7	88	0	1	$3\tau - 7$	$\tau^8 - \tau^5 + \tau^3 - 1$
9	58	0	1	$3\tau - 5$	$\tau^8 - \tau^5 + \tau^3 + 1$
9	81	0	0	9	$-\tau^5 + \tau^3 + 1$
9	92	-1	0	$-7\tau - 1$	$-\tau^7 - \tau^5 + \tau^3 + 1$
11	36	0	1	$3\tau - 3$	$-\tau^6 - \tau^4 - \tau^2 - 1$
11	106	-1	0	$-7\tau + 1$	$\tau^6 - \tau^4 - \tau^2 - 1$
11	121	0	0	11	$-\tau^8 - \tau^6 - \tau^4 - \tau^2 - 1$
13	22	0	1	$3\tau - 1$	$-\tau^6 - \tau^4 - \tau^2 + 1$
13	109	-1	1	$-4\tau - 11$	$\tau^8 + \tau^6 - \tau^4 - \tau^2 + 1$
15	16	0	1	$3\tau + 1$	$\tau^4 - 1$
15	77	-1	1	$-4\tau - 9$	$-\tau^7 + \tau^4 - 1$
17	18	0	1	$3\tau + 3$	$\tau^4 + 1$
17	53	-1	1	$-4\tau - 7$	$-\tau^7 + \tau^4 + 1$
19	28	0	1	$3\tau + 5$	$\tau^7 - \tau^4 + \tau^2 - 1$
19	37	-1	1	$-4\tau - 5$	$-\tau^4 + \tau^2 - 1$
21	29	-1	1	$-4\tau - 3$	$-\tau^4 + \tau^2 + 1$
21	46	0	1	$3\tau + 7$	$\tau^7 - \tau^4 + \tau^2 + 1$
23	29	-1	1	$-4\tau - 1$	$\tau^6 - \tau^3 - 1$
23	72	0	1	$3\tau + 9$	$-\tau^8 - \tau^6 - \tau^3 - 1$
23	127	0	2	$6\tau - 5$	$-\tau^6 - \tau^3 - 1$
25	37	-1	1	$-4\tau + 1$	$\tau^6 - \tau^3 + 1$
25	99	0	2	$6\tau - 3$	$-\tau^6 - \tau^3 + 1$
25	106	0	1	$3\tau + 11$	$-\tau^8 - \tau^6 - \tau^3 + 1$
27	53	-1	1	$-4\tau + 3$	$\tau^6 - \tau^2 - 1$
27	79	0	2	$6\tau - 1$	$-\tau^6 - \tau^2 - 1$
27	112	-1	2	$-\tau - 11$	$\tau^8 + \tau^6 - \tau^2 - 1$
29	67	0	2	$6\tau + 1$	$-\tau^6 - \tau^2 + 1$
29	74	-1	2	$-\tau - 9$	$\tau^8 + \tau^6 - \tau^2 + 1$
29	77	-1	1	$-4\tau + 5$	$\tau^6 - \tau^2 + 1$
31	44	-1	2	$-\tau - 7$	$\tau^5 - 1$
31	63	0	2	$6\tau + 3$	$\tau^7 + \tau^5 - 1$
31	109	-1	1	$-4\tau + 7$	$-\tau^8 + \tau^5 - 1$
33	22	-1	2	$-\tau - 5$	$\tau^5 + 1$
33	67	0	2	$6\tau + 5$	$\tau^7 + \tau^5 + 1$

Continued on next page

Table A:.5 E$_0$**:** $w = 7, N(\tau^w) = 128, \tau^w(reduced) = 7\tau + 10$ **(continued from previous page)**

u	norm	q_0	q_1	u *mod* τ^w	α_u
35	8	-1	2	$-\tau - 3$	$\tau^2 - 1$
35	79	0	2	$6\tau + 7$	$\tau^7 + \tau^2 - 1$
37	2	-1	2	$-\tau - 1$	$\tau^2 + 1$
37	99	0	2	$6\tau + 9$	$\tau^7 + \tau^2 + 1$
39	4	-1	2	$-\tau + 1$	$\tau^3 - 1$
39	127	0	2	$6\tau + 11$	$\tau^7 + \tau^3 - 1$
41	14	-1	2	$-\tau + 3$	$\tau^3 + 1$
41	121	-2	2	$-8\tau - 7$	$-\tau^7 + \tau^3 + 1$
43	32	-1	2	$-\tau + 5$	$\tau^6 + \tau^4 - \tau^2 - 1$
43	107	-1	3	$2\tau - 9$	$\tau^8 + \tau^6 + \tau^4 - \tau^2 - 1$
43	113	-2	2	$-8\tau - 5$	$\tau^9 - \tau^6 + \tau^4 - \tau^2 - 1$
45	58	-1	2	$-\tau + 7$	$\tau^6 + \tau^4 - \tau^2 + 1$
45	71	-1	3	$2\tau - 7$	$\tau^8 + \tau^6 + \tau^4 - \tau^2 + 1$
45	113	-2	2	$-8\tau - 3$	$\tau^9 - \tau^6 + \tau^4 - \tau^2 + 1$
47	43	-1	3	$2\tau - 5$	$-\tau^6 - \tau^4 - 1$
47	92	-1	2	$-\tau + 9$	$-\tau^8 - \tau^6 - \tau^4 - 1$
47	121	-2	2	$-8\tau - 1$	$\tau^6 - \tau^4 - 1$
49	23	-1	3	$2\tau - 3$	$-\tau^6 - \tau^4 + 1$
51	11	-1	3	$2\tau - 1$	$\tau^4 + \tau^2 - 1$
51	116	-2	3	$-5\tau - 11$	$-\tau^7 + \tau^4 + \tau^2 - 1$
53	7	-1	3	$2\tau + 1$	$\tau^4 + \tau^2 + 1$
53	86	-2	3	$-5\tau - 9$	$-\tau^7 + \tau^4 + \tau^2 + 1$
55	11	-1	3	$2\tau + 3$	$-\tau^5 - \tau^3 - 1$
55	64	-2	3	$-5\tau - 7$	$-\tau^7 - \tau^5 - \tau^3 - 1$
57	23	-1	3	$2\tau + 5$	$-\tau^5 - \tau^3 + 1$
57	50	-2	3	$-5\tau - 5$	$-\tau^7 - \tau^5 - \tau^3 + 1$
59	43	-1	3	$2\tau + 7$	$-\tau^5 - \tau^2 - 1$
59	44	-2	3	$-5\tau - 3$	$-\tau^7 - \tau^5 - \tau^2 - 1$
61	46	-2	3	$-5\tau - 1$	$-\tau^7 - \tau^5 - \tau^2 + 1$
61	71	-1	3	$2\tau + 9$	$-\tau^5 - \tau^2 + 1$
61	100	-1	4	$5\tau - 5$	$\tau^8 - \tau^5 - \tau^2 + 1$
63	56	-2	3	$-5\tau + 1$	$\tau^6 - 1$
63	74	-1	4	$5\tau - 3$	$-\tau^6 - 1$
63	107	-1	3	$2\tau + 11$	$-\tau^8 - \tau^6 - 1$

TABLE A:.6: E_0: $w = 8, N(\tau^w) = 256, \tau^w(reduced) = 3\tau - 14$

u	norm	q_0	q_1	$u\ mod\ \tau^w$	α_u
1	1	0	0	1	1
1	226	1	0	$3\tau - 13$	$\tau^8 + 1$
3	9	0	0	3	$-\tau^5 + \tau^2 - 1$
3	172	1	0	$3\tau - 11$	$\tau^8 - \tau^5 + \tau^2 - 1$
5	25	0	0	5	$-\tau^5 + \tau^2 + 1$
5	126	1	0	$3\tau - 9$	$\tau^8 - \tau^5 + \tau^2 + 1$
7	49	0	0	7	$-\tau^5 + \tau^3 - 1$
7	88	1	0	$3\tau - 7$	$\tau^8 - \tau^5 + \tau^3 - 1$
9	58	1	0	$3\tau - 5$	$\tau^8 - \tau^5 + \tau^3 + 1$
9	81	0	0	9	$-\tau^5 + \tau^3 + 1$
11	36	1	0	$3\tau - 3$	$-\tau^6 - \tau^4 - \tau^2 - 1$
11	121	0	0	11	$-\tau^8 - \tau^6 - \tau^4 - \tau^2 - 1$
13	22	1	0	$3\tau - 1$	$-\tau^6 - \tau^4 - \tau^2 + 1$
13	169	0	0	13	$-\tau^8 - \tau^6 - \tau^4 - \tau^2 + 1$
15	16	1	0	$3\tau + 1$	$\tau^4 - 1$
15	225	0	0	15	$-\tau^8 + \tau^4 - 1$
17	18	1	0	$3\tau + 3$	$\tau^4 + 1$
19	28	1	0	$3\tau + 5$	$\tau^7 - \tau^4 + \tau^2 - 1$
19	207	2	0	$6\tau - 9$	$-\tau^9 - \tau^7 - \tau^4 + \tau^2 - 1$
21	46	1	0	$3\tau + 7$	$\tau^7 - \tau^4 + \tau^2 + 1$
21	163	2	0	$6\tau - 7$	$-\tau^9 - \tau^7 - \tau^4 + \tau^2 + 1$
23	72	1	0	$3\tau + 9$	$-\tau^8 - \tau^6 - \tau^3 - 1$
23	127	2	0	$6\tau - 5$	$-\tau^6 - \tau^3 - 1$
23	242	2	1	$-11\tau - 11$	$\tau^9 - \tau^6 - \tau^3 - 1$
25	99	2	0	$6\tau - 3$	$-\tau^6 - \tau^3 + 1$
25	106	1	0	$3\tau + 11$	$-\tau^8 - \tau^6 - \tau^3 + 1$
25	224	2	1	$-11\tau - 9$	$\tau^9 - \tau^6 - \tau^3 + 1$
27	79	2	0	$6\tau - 1$	$-\tau^6 - \tau^2 - 1$
27	148	1	0	$3\tau + 13$	$-\tau^8 - \tau^6 - \tau^2 - 1$
27	214	2	1	$-11\tau - 7$	$\tau^9 - \tau^6 - \tau^2 - 1$
29	67	2	0	$6\tau + 1$	$-\tau^6 - \tau^2 + 1$
29	198	1	0	$3\tau + 15$	$-\tau^8 - \tau^6 - \tau^2 + 1$
29	212	2	1	$-11\tau - 5$	$\tau^9 - \tau^6 - \tau^2 + 1$
31	63	2	0	$6\tau + 3$	$\tau^7 + \tau^5 - 1$
31	218	2	1	$-11\tau - 3$	$\tau^9 + \tau^7 + \tau^5 - 1$
33	67	2	0	$6\tau + 5$	$\tau^7 + \tau^5 + 1$
33	232	2	1	$-11\tau - 1$	$\tau^9 + \tau^7 + \tau^5 + 1$
33	233	3	1	$-8\tau - 15$	$-\tau^7 + \tau^5 + 1$
35	79	2	0	$6\tau + 7$	$\tau^7 + \tau^2 - 1$
35	193	3	1	$-8\tau - 13$	$-\tau^7 + \tau^2 - 1$
35	254	2	1	$-11\tau + 1$	$\tau^9 + \tau^7 + \tau^2 - 1$

Continued on next page

Table A:.6 E_0**:** $w = 8, N(\tau^w) = 256, \tau^w(\mathit{reduced}) = 3\tau - 14$ **(continued from previous page)**

u	norm	q_0	q_1	$u \bmod \tau^w$	α_u
37	99	2	0	$6\tau + 9$	$\tau^7 + \tau^2 + 1$
37	161	3	1	$-8\tau - 11$	$-\tau^7 + \tau^2 + 1$
37	232	3	0	$9\tau - 5$	$-\tau^9 - \tau^7 + \tau^2 + 1$
39	127	2	0	$6\tau + 11$	$\tau^7 + \tau^3 - 1$
39	137	3	1	$-8\tau - 9$	$-\tau^7 + \tau^3 - 1$
39	198	3	0	$9\tau - 3$	$-\tau^9 - \tau^7 + \tau^3 - 1$
41	121	3	1	$-8\tau - 7$	$-\tau^7 + \tau^3 + 1$
41	163	2	0	$6\tau + 13$	$\tau^7 + \tau^3 + 1$
41	172	3	0	$9\tau - 1$	$-\tau^9 - \tau^7 + \tau^3 + 1$
43	113	3	1	$-8\tau - 5$	$\tau^9 - \tau^6 + \tau^4 - \tau^2 - 1$
43	154	3	0	$9\tau + 1$	$-\tau^6 + \tau^4 - \tau^2 - 1$
43	207	2	0	$6\tau + 15$	$-\tau^8 - \tau^6 + \tau^4 - \tau^2 - 1$
45	113	3	1	$-8\tau - 3$	$\tau^9 - \tau^6 + \tau^4 - \tau^2 + 1$
45	144	3	0	$9\tau + 3$	$-\tau^6 + \tau^4 - \tau^2 + 1$
45	254	4	1	$-5\tau - 17$	$-\tau^{10} - \tau^8 - \tau^6 + \tau^4 - \tau^2 + 1$
47	121	3	1	$-8\tau - 1$	$\tau^6 - \tau^4 - 1$
47	142	3	0	$9\tau + 5$	$-\tau^9 + \tau^6 - \tau^4 - 1$
47	200	4	1	$-5\tau - 15$	$\tau^8 + \tau^6 - \tau^4 - 1$
49	137	3	1	$-8\tau + 1$	$\tau^6 - \tau^4 + 1$
49	148	3	0	$9\tau + 7$	$-\tau^9 + \tau^6 - \tau^4 + 1$
49	154	4	1	$-5\tau - 13$	$\tau^8 + \tau^6 - \tau^4 + 1$
51	116	4	1	$-5\tau - 11$	$-\tau^7 + \tau^4 + \tau^2 - 1$
51	161	3	1	$-8\tau + 3$	$\tau^9 + \tau^7 + \tau^4 + \tau^2 - 1$
51	162	3	0	$9\tau + 9$	$\tau^7 + \tau^4 + \tau^2 - 1$
53	86	4	1	$-5\tau - 9$	$-\tau^7 + \tau^4 + \tau^2 + 1$
53	184	3	0	$9\tau + 11$	$\tau^7 + \tau^4 + \tau^2 + 1$
53	193	3	1	$-8\tau + 5$	$\tau^9 + \tau^7 + \tau^4 + \tau^2 + 1$
55	64	4	1	$-5\tau - 7$	$-\tau^7 - \tau^5 - \tau^3 - 1$
55	214	3	0	$9\tau + 13$	$\tau^7 - \tau^5 - \tau^3 - 1$
55	233	3	1	$-8\tau + 7$	$\tau^9 + \tau^7 - \tau^5 - \tau^3 - 1$
57	50	4	1	$-5\tau - 5$	$-\tau^7 - \tau^5 - \tau^3 + 1$
57	252	3	0	$9\tau + 15$	$\tau^7 - \tau^5 - \tau^3 + 1$
59	44	4	1	$-5\tau - 3$	$-\tau^7 - \tau^5 - \tau^2 - 1$
61	46	4	1	$-5\tau - 1$	$-\tau^7 - \tau^5 - \tau^2 + 1$
61	203	5	1	$-2\tau - 15$	$-\tau^{10} + \tau^7 - \tau^5 - \tau^2 + 1$
61	253	4	0	$12\tau + 5$	$-\tau^9 - \tau^7 - \tau^5 - \tau^2 + 1$
63	56	4	1	$-5\tau + 1$	$\tau^6 - 1$
63	151	5	1	$-2\tau - 13$	$\tau^8 + \tau^6 - 1$
63	253	4	0	$12\tau + 7$	$-\tau^9 + \tau^6 - 1$
65	74	4	1	$-5\tau + 3$	$\tau^6 + 1$
65	107	5	1	$-2\tau - 11$	$\tau^8 + \tau^6 + 1$
67	71	5	1	$-2\tau - 9$	$\tau^5 + \tau^2 - 1$
67	100	4	1	$-5\tau + 5$	$-\tau^8 + \tau^5 + \tau^2 - 1$
69	43	5	1	$-2\tau - 7$	$\tau^5 + \tau^2 + 1$

Continued on next page

Table A:.6 E_0: $w = 8, N(\tau^w) = 256, \tau^w(reduced) = 3\tau - 14$ **(continued from previous page)**

u	norm	q_0	q_1	$u\ mod\ \tau^w$	α_u
69	134	4	1	$-5\tau + 7$	$-\tau^8 + \tau^5 + \tau^2 + 1$
71	23	5	1	$-2\tau - 5$	$\tau^5 + \tau^3 - 1$
71	176	4	1	$-5\tau + 9$	$-\tau^8 + \tau^5 + \tau^3 - 1$
73	11	5	1	$-2\tau - 3$	$\tau^5 + \tau^3 + 1$
73	226	4	1	$-5\tau + 11$	$-\tau^8 + \tau^5 + \tau^3 + 1$
75	7	5	1	$-2\tau - 1$	$-\tau^4 - \tau^2 - 1$
75	242	6	1	$\tau - 15$	$\tau^8 - \tau^4 - \tau^2 - 1$
77	11	5	1	$-2\tau + 1$	$-\tau^4 - \tau^2 + 1$
77	184	6	1	$\tau - 13$	$\tau^8 - \tau^4 - \tau^2 + 1$
79	23	5	1	$-2\tau + 3$	$\tau^6 + \tau^4 - 1$
79	134	6	1	$\tau - 11$	$\tau^8 + \tau^6 + \tau^4 - 1$
81	43	5	1	$-2\tau + 5$	$\tau^6 + \tau^4 + 1$
81	92	6	1	$\tau - 9$	$\tau^8 + \tau^6 + \tau^4 + 1$
83	58	6	1	$\tau - 7$	$-\tau^6 - \tau^4 + \tau^2 - 1$
83	71	5	1	$-2\tau + 7$	$-\tau^8 - \tau^6 - \tau^4 + \tau^2 - 1$
85	32	6	1	$\tau - 5$	$-\tau^6 - \tau^4 + \tau^2 + 1$
85	107	5	1	$-2\tau + 9$	$-\tau^8 - \tau^6 - \tau^4 + \tau^2 + 1$
87	14	6	1	$\tau - 3$	$-\tau^3 - 1$
87	151	5	1	$-2\tau + 11$	$-\tau^8 - \tau^3 - 1$
89	4	6	1	$\tau - 1$	$-\tau^3 + 1$
89	203	5	1	$-2\tau + 13$	$-\tau^8 - \tau^3 + 1$
91	2	6	1	$\tau + 1$	$-\tau^2 - 1$
91	253	7	1	$4\tau - 13$	$\tau^8 - \tau^2 - 1$
93	8	6	1	$\tau + 3$	$-\tau^2 + 1$
93	197	7	1	$4\tau - 11$	$\tau^8 - \tau^2 + 1$
95	22	6	1	$\tau + 5$	$-\tau^5 - 1$
95	149	7	1	$4\tau - 9$	$\tau^8 - \tau^5 - 1$
97	44	6	1	$\tau + 7$	$-\tau^5 + 1$
97	109	7	1	$4\tau - 7$	$\tau^8 - \tau^5 + 1$
99	74	6	1	$\tau + 9$	$-\tau^8 - \tau^6 + \tau^2 - 1$
99	77	7	1	$4\tau - 5$	$-\tau^6 + \tau^2 - 1$
101	53	7	1	$4\tau - 3$	$-\tau^6 + \tau^2 + 1$
101	112	6	1	$\tau + 11$	$-\tau^8 - \tau^6 + \tau^2 + 1$
103	37	7	1	$4\tau - 1$	$-\tau^6 + \tau^3 - 1$
103	158	6	1	$\tau + 13$	$-\tau^8 - \tau^6 + \tau^3 - 1$
105	29	7	1	$4\tau + 1$	$-\tau^6 + \tau^3 + 1$
105	212	6	1	$\tau + 15$	$-\tau^8 - \tau^6 + \tau^3 + 1$
107	29	7	1	$4\tau + 3$	$\tau^4 - \tau^2 - 1$
109	37	7	1	$4\tau + 5$	$\tau^4 - \tau^2 + 1$
109	242	8	1	$7\tau - 9$	$\tau^8 + \tau^4 - \tau^2 + 1$

Continued on next page

Table A:.6 E$_0$**:** $w = 8, N(\tau^w) = 256, \tau^w(reduced) = 3\tau - 14$ **(continued from previous page)**

u	norm	q_0	q_1	$u\ mod\ \tau^w$	α_u
111	53	7	1	$4\tau + 7$	$\tau^7 - \tau^4 - 1$
111	196	8	1	$7\tau - 7$	$-\tau^9 - \tau^7 - \tau^4 - 1$
111	239	8	2	$-10\tau - 13$	$-\tau^7 - \tau^4 - 1$
113	77	7	1	$4\tau + 9$	$\tau^7 - \tau^4 + 1$
113	158	8	1	$7\tau - 5$	$-\tau^9 - \tau^7 - \tau^4 + 1$
113	211	8	2	$-10\tau - 11$	$-\tau^7 - \tau^4 + 1$
115	109	7	1	$4\tau + 11$	$-\tau^8 - \tau^6 + \tau^4 + \tau^2 - 1$
115	128	8	1	$7\tau - 3$	$-\tau^6 + \tau^4 + \tau^2 - 1$
115	191	8	2	$-10\tau - 9$	$\tau^9 - \tau^6 + \tau^4 + \tau^2 - 1$
117	106	8	1	$7\tau - 1$	$-\tau^6 + \tau^4 + \tau^2 + 1$
117	149	7	1	$4\tau + 13$	$-\tau^8 - \tau^6 + \tau^4 + \tau^2 + 1$
117	179	8	2	$-10\tau - 7$	$\tau^9 - \tau^6 + \tau^4 + \tau^2 + 1$
119	92	8	1	$7\tau + 1$	$\tau^7 + \tau^5 - \tau^3 - 1$
119	175	8	2	$-10\tau - 5$	$\tau^9 + \tau^7 + \tau^5 - \tau^3 - 1$
119	197	7	1	$4\tau + 15$	$\tau^{10} - \tau^7 + \tau^5 - \tau^3 - 1$
121	86	8	1	$7\tau + 3$	$\tau^7 + \tau^5 - \tau^3 + 1$
121	179	8	2	$-10\tau - 3$	$\tau^9 + \tau^7 + \tau^5 - \tau^3 + 1$
121	253	7	1	$4\tau + 17$	$\tau^{10} - \tau^7 + \tau^5 - \tau^3 + 1$
123	88	8	1	$7\tau + 5$	$\tau^7 + \tau^5 - \tau^2 - 1$
123	191	8	2	$-10\tau - 1$	$\tau^9 + \tau^7 + \tau^5 - \tau^2 - 1$
123	218	9	2	$-7\tau - 15$	$-\tau^7 + \tau^5 - \tau^2 - 1$
125	98	8	1	$7\tau + 7$	$\tau^7 + \tau^5 - \tau^2 + 1$
125	176	9	2	$-7\tau - 13$	$-\tau^7 + \tau^5 - \tau^2 + 1$
125	211	8	2	$-10\tau + 1$	$\tau^9 + \tau^7 + \tau^5 - \tau^2 + 1$
127	116	8	1	$7\tau + 9$	$\tau^7 - 1$
127	142	9	2	$-7\tau - 11$	$-\tau^7 - 1$
127	239	8	2	$-10\tau + 3$	$\tau^9 + \tau^7 - 1$

Appendix B:

a = 1 Width-w τ-NAF Tables

This appendix lists the complete τ-NAF table for window sizes 3 to 8 for E$_1$.

Table B:.1: E$_1$: $w = 3, N(\tau^w) = 8, \tau^w(reduced) = -\tau - 2$

u	norm	q_0	q_1	$u\ mod\ \tau^w$	α_u
1	1	0	0	1	1
1	4	1	0	$-\tau - 1$	$\tau^3 + 1$
3	2	1	0	$-\tau + 1$	$-\tau^2 - 1$
3	7	1	-1	$2\tau - 1$	$-\tau^4 - \tau^2 - 1$

Table B:.2: E$_1$: $w = 4, N(\tau^w) = 16, \tau^w(reduced) = -3\tau + 2$

u	norm	q_0	q_1	$u\ mod\ \tau^w$	α_u
1	1	0	0	1	1
3	8	0	-1	$\tau - 3$	$\tau^2 - 1$
3	9	0	0	3	$\tau^5 + \tau^2 - 1$
3	11	1	-1	$-2\tau - 1$	$\tau^4 + \tau^2 - 1$
5	2	0	-1	$\tau - 1$	$\tau^2 + 1$
5	7	1	-1	$-2\tau + 1$	$\tau^4 + \tau^2 + 1$
7	4	0	-1	$\tau + 1$	$-\tau^3 - 1$
7	11	1	-1	$-2\tau + 3$	$\tau^5 + \tau^3 - 1$
7	14	1	-2	$-\tau - 3$	$\tau^3 - 1$

Table B:.3: E$_1$: $w = 5, N(\tau^w) = 32, \tau^w(reduced) = -\tau + 6$

u	norm	q_0	q_1	$u\ mod\ \tau^w$	α_u
1	1	0	0	1	1
					Continued on next page

Table B:.3 E$_1$: $w = 5, N(\tau^w) = 32, \tau^w(reduced) = -\tau + 6$ **(continued from previous page)**

u	norm	q_0	q_1	$u\ mod\ \tau^w$	α_u
1	22	-1	0	$\tau - 5$	$-\tau^5 + 1$
3	8	-1	0	$\tau - 3$	$\tau^2 - 1$
3	9	0	0	3	$\tau^5 + \tau^2 - 1$
5	2	-1	0	$\tau - 1$	$\tau^2 + 1$
5	25	0	0	5	$\tau^5 + \tau^2 + 1$
7	4	-1	0	$\tau + 1$	$-\tau^3 - 1$
7	23	-2	0	$2\tau - 5$	$-\tau^5 - \tau^3 - 1$
9	11	-2	0	$2\tau - 3$	$-\tau^5 - \tau^3 + 1$
9	14	-1	0	$\tau + 3$	$-\tau^3 + 1$
9	29	-1	-1	$-4\tau + 1$	$-\tau^6 - \tau^3 + 1$
11	7	-2	0	$2\tau - 1$	$-\tau^4 - \tau^2 - 1$
11	29	-1	-1	$-4\tau + 3$	$\tau^4 - \tau^2 - 1$
13	11	-2	0	$2\tau + 1$	$-\tau^4 - \tau^2 + 1$
13	22	-2	-1	$-3\tau - 1$	$-\tau^6 - \tau^4 - \tau^2 + 1$
13	28	-3	0	$3\tau - 5$	$\tau^7 + \tau^4 - \tau^2 + 1$
15	16	-2	-1	$-3\tau + 1$	$\tau^4 - 1$
15	18	-3	0	$3\tau - 3$	$-\tau^4 - 1$
15	23	-2	0	$2\tau + 3$	$\tau^6 + \tau^4 - 1$

Table B:.4: E$_1$: $w = 6, N(\tau^w) = 64, \tau^w(reduced) = 5\tau + 2$

u	norm	q_0	q_1	$u \ mod \ \tau^w$	α_u
1	1	0	0	1	1
1	56	-1	0	$-5\tau - 1$	$-\tau^6 + 1$
3	9	0	0	3	$\tau^5 + \tau^2 - 1$
3	46	-1	0	$-5\tau + 1$	$-\tau^7 - \tau^5 + \tau^2 - 1$
5	25	0	0	5	$\tau^5 + \tau^2 + 1$
5	43	-1	1	$2\tau - 7$	$-\tau^5 + \tau^2 + 1$
5	44	-1	0	$-5\tau + 3$	$-\tau^7 - \tau^5 + \tau^2 + 1$
7	23	-1	1	$2\tau - 5$	$-\tau^5 - \tau^3 - 1$
7	49	0	0	7	$\tau^5 - \tau^3 - 1$
7	50	-1	0	$-5\tau + 5$	$-\tau^7 - \tau^5 - \tau^3 - 1$
9	11	-1	1	$2\tau - 3$	$-\tau^5 - \tau^3 + 1$
9	58	-2	1	$-3\tau - 5$	$\tau^8 + \tau^5 - \tau^3 + 1$
11	7	-1	1	$2\tau - 1$	$-\tau^4 - \tau^2 - 1$
11	36	-2	1	$-3\tau - 3$	$-\tau^6 - \tau^4 - \tau^2 - 1$
13	11	-1	1	$2\tau + 1$	$-\tau^4 - \tau^2 + 1$
13	22	-2	1	$-3\tau - 1$	$-\tau^6 - \tau^4 - \tau^2 + 1$
15	16	-2	1	$-3\tau + 1$	$\tau^4 - 1$
15	23	-1	1	$2\tau + 3$	$\tau^6 + \tau^4 - 1$
17	18	-2	1	$-3\tau + 3$	$\tau^4 + 1$
17	43	-1	1	$2\tau + 5$	$\tau^6 + \tau^4 + 1$
17	53	-2	2	$4\tau - 7$	$\tau^7 + \tau^4 + 1$
19	28	-2	1	$-3\tau + 5$	$-\tau^7 - \tau^4 + \tau^2 - 1$
19	37	-2	2	$4\tau - 5$	$-\tau^4 + \tau^2 - 1$
19	58	-3	2	$-\tau - 7$	$-\tau^6 - \tau^4 + \tau^2 - 1$
21	29	-2	2	$4\tau - 3$	$-\tau^4 + \tau^2 + 1$
21	32	-3	2	$-\tau - 5$	$-\tau^6 - \tau^4 + \tau^2 + 1$
21	46	-2	1	$-3\tau + 7$	$-\tau^7 - \tau^4 + \tau^2 + 1$
23	14	-3	2	$-\tau - 3$	$\tau^3 - 1$
23	29	-2	2	$4\tau - 1$	$\tau^6 + \tau^3 - 1$
25	4	-3	2	$-\tau - 1$	$\tau^3 + 1$
25	37	-2	2	$4\tau + 1$	$\tau^6 + \tau^3 + 1$
27	2	-3	2	$-\tau + 1$	$-\tau^2 - 1$
27	53	-2	2	$4\tau + 3$	$\tau^6 - \tau^2 - 1$
29	8	-3	2	$-\tau + 3$	$-\tau^2 + 1$
31	22	-3	2	$-\tau + 5$	$\tau^5 - 1$
31	44	-4	3	$\tau - 7$	$-\tau^5 - 1$
31	63	-4	2	$-6\tau + 3$	$-\tau^7 - \tau^5 - 1$

TABLE B:.5: E_1: $w = 7, N(\tau^w) = 128, \tau^w(reduced) = 7\tau - 10$

u	norm	q_0	q_1	*u mod* τ^w	α_u
1	1	0	0	1	1
1	116	1	0	$7\tau - 9$	$\tau^7 + 1$
3	9	0	0	3	$\tau^5 + \tau^2 - 1$
3	98	1	0	$7\tau - 7$	$\tau^7 + \tau^5 + \tau^2 - 1$
5	25	0	0	5	$\tau^5 + \tau^2 + 1$
5	88	1	0	$7\tau - 5$	$\tau^7 + \tau^5 + \tau^2 + 1$
5	126	0	1	$-3\tau - 9$	$\tau^8 + \tau^5 + \tau^2 + 1$
7	49	0	0	7	$\tau^5 - \tau^3 - 1$
7	86	1	0	$7\tau - 3$	$\tau^7 + \tau^5 - \tau^3 - 1$
7	88	0	1	$-3\tau - 7$	$\tau^8 + \tau^5 - \tau^3 - 1$
9	58	0	1	$-3\tau - 5$	$\tau^8 + \tau^5 - \tau^3 + 1$
9	81	0	0	9	$\tau^5 - \tau^3 + 1$
9	92	1	0	$7\tau - 1$	$\tau^7 + \tau^5 - \tau^3 + 1$
11	36	0	1	$-3\tau - 3$	$-\tau^6 - \tau^4 - \tau^2 - 1$
11	106	1	0	$7\tau + 1$	$\tau^6 - \tau^4 - \tau^2 - 1$
11	121	0	0	11	$-\tau^8 - \tau^6 - \tau^4 - \tau^2 - 1$
13	22	0	1	$-3\tau - 1$	$-\tau^6 - \tau^4 - \tau^2 + 1$
13	109	1	1	$4\tau - 11$	$\tau^8 + \tau^6 - \tau^4 - \tau^2 + 1$
15	16	0	1	$-3\tau + 1$	$\tau^4 - 1$
15	77	1	1	$4\tau - 9$	$\tau^7 + \tau^4 - 1$
17	18	0	1	$-3\tau + 3$	$\tau^4 + 1$
17	53	1	1	$4\tau - 7$	$\tau^7 + \tau^4 + 1$
19	28	0	1	$-3\tau + 5$	$-\tau^7 - \tau^4 + \tau^2 - 1$
19	37	1	1	$4\tau - 5$	$-\tau^4 + \tau^2 - 1$
21	29	1	1	$4\tau - 3$	$-\tau^4 + \tau^2 + 1$
21	46	0	1	$-3\tau + 7$	$-\tau^7 - \tau^4 + \tau^2 + 1$
23	29	1	1	$4\tau - 1$	$\tau^6 + \tau^3 - 1$
23	72	0	1	$-3\tau + 9$	$-\tau^8 - \tau^6 + \tau^3 - 1$
23	127	0	2	$-6\tau - 5$	$-\tau^6 + \tau^3 - 1$
25	37	1	1	$4\tau + 1$	$\tau^6 + \tau^3 + 1$
25	99	0	2	$-6\tau - 3$	$-\tau^6 + \tau^3 + 1$
25	106	0	1	$-3\tau + 11$	$-\tau^8 - \tau^6 + \tau^3 + 1$
27	53	1	1	$4\tau + 3$	$\tau^6 - \tau^2 - 1$
27	79	0	2	$-6\tau - 1$	$-\tau^6 - \tau^2 - 1$
27	112	1	2	$\tau - 11$	$\tau^8 + \tau^6 - \tau^2 - 1$
29	67	0	2	$-6\tau + 1$	$-\tau^6 - \tau^2 + 1$
29	74	1	2	$\tau - 9$	$\tau^8 + \tau^6 - \tau^2 + 1$
29	77	1	1	$4\tau + 5$	$\tau^6 - \tau^2 + 1$
31	44	1	2	$\tau - 7$	$-\tau^5 - 1$
31	63	0	2	$-6\tau + 3$	$-\tau^7 - \tau^5 - 1$
31	109	1	1	$4\tau + 7$	$-\tau^8 - \tau^5 - 1$
33	22	1	2	$\tau - 5$	$-\tau^5 + 1$
33	67	0	2	$-6\tau + 5$	$-\tau^7 - \tau^5 + 1$

Continued on next page

Table B:.5 E$_1$: $w = 7, N(\tau^w) = 128, \tau^w(reduced) = 7\tau - 10$ **(continued from previous page)**

u	norm	q_0	q_1	$u \ mod \ \tau^w$	α_u
35	8	1	2	$\tau - 3$	$\tau^2 - 1$
35	79	0	2	$-6\tau + 7$	$-\tau^7 + \tau^2 - 1$
37	2	1	2	$\tau - 1$	$\tau^2 + 1$
37	99	0	2	$-6\tau + 9$	$-\tau^7 + \tau^2 + 1$
39	4	1	2	$\tau + 1$	$-\tau^3 - 1$
39	127	0	2	$-6\tau + 11$	$-\tau^7 - \tau^3 - 1$
41	14	1	2	$\tau + 3$	$-\tau^3 + 1$
41	121	2	2	$8\tau - 7$	$\tau^7 - \tau^3 + 1$
43	32	1	2	$\tau + 5$	$\tau^6 + \tau^4 - \tau^2 - 1$
43	107	1	3	$-2\tau - 9$	$\tau^8 + \tau^6 + \tau^4 - \tau^2 - 1$
43	113	2	2	$8\tau - 5$	$-\tau^9 - \tau^6 + \tau^4 - \tau^2 - 1$
45	58	1	2	$\tau + 7$	$\tau^6 + \tau^4 - \tau^2 + 1$
45	71	1	3	$-2\tau - 7$	$\tau^8 + \tau^6 + \tau^4 - \tau^2 + 1$
45	113	2	2	$8\tau - 3$	$-\tau^9 - \tau^6 + \tau^4 - \tau^2 + 1$
47	43	1	3	$-2\tau - 5$	$-\tau^6 - \tau^4 - 1$
47	92	1	2	$\tau + 9$	$-\tau^8 - \tau^6 - \tau^4 - 1$
47	121	2	2	$8\tau - 1$	$\tau^6 - \tau^4 - 1$
49	23	1	3	$-2\tau - 3$	$-\tau^6 - \tau^4 + 1$
51	11	1	3	$-2\tau - 1$	$\tau^4 + \tau^2 - 1$
51	116	2	3	$5\tau - 11$	$\tau^7 + \tau^4 + \tau^2 - 1$
53	7	1	3	$-2\tau + 1$	$\tau^4 + \tau^2 + 1$
53	86	2	3	$5\tau - 9$	$\tau^7 + \tau^4 + \tau^2 + 1$
55	11	1	3	$-2\tau + 3$	$\tau^5 + \tau^3 - 1$
55	64	2	3	$5\tau - 7$	$\tau^7 + \tau^5 + \tau^3 - 1$
57	23	1	3	$-2\tau + 5$	$\tau^5 + \tau^3 + 1$
57	50	2	3	$5\tau - 5$	$\tau^7 + \tau^5 + \tau^3 + 1$
59	43	1	3	$-2\tau + 7$	$\tau^5 - \tau^2 - 1$
59	44	2	3	$5\tau - 3$	$\tau^7 + \tau^5 - \tau^2 - 1$
61	46	2	3	$5\tau - 1$	$\tau^7 + \tau^5 - \tau^2 + 1$
61	71	1	3	$-2\tau + 9$	$\tau^5 - \tau^2 + 1$
61	100	1	4	$-5\tau - 5$	$\tau^8 + \tau^5 - \tau^2 + 1$
63	56	2	3	$5\tau + 1$	$\tau^6 - 1$
63	74	1	4	$-5\tau - 3$	$-\tau^6 - 1$
63	107	1	3	$-2\tau + 11$	$-\tau^8 - \tau^6 - 1$

TABLE B:.6: E$_1$: $w = 8, N(\tau^w) = 256, \tau^w(reduced) = -3\tau - 14$

u	norm	q_0	q_1	$u\ mod\ \tau^w$	α_u
1	1	0	0	1	1
1	226	1	0	$-3\tau - 13$	$\tau^8 + 1$
3	9	0	0	3	$\tau^5 + \tau^2 - 1$
3	172	1	0	$-3\tau - 11$	$\tau^8 + \tau^5 + \tau^2 - 1$
5	25	0	0	5	$\tau^5 + \tau^2 + 1$
5	126	1	0	$-3\tau - 9$	$\tau^8 + \tau^5 + \tau^2 + 1$
7	49	0	0	7	$\tau^5 - \tau^3 - 1$
7	88	1	0	$-3\tau - 7$	$\tau^8 + \tau^5 - \tau^3 - 1$
9	58	1	0	$-3\tau - 5$	$\tau^8 + \tau^5 - \tau^3 + 1$
9	81	0	0	9	$\tau^5 - \tau^3 + 1$
11	36	1	0	$-3\tau - 3$	$-\tau^6 - \tau^4 - \tau^2 - 1$
11	121	0	0	11	$-\tau^8 - \tau^6 - \tau^4 - \tau^2 - 1$
13	22	1	0	$-3\tau - 1$	$-\tau^6 - \tau^4 - \tau^2 + 1$
13	169	0	0	13	$-\tau^8 - \tau^6 - \tau^4 - \tau^2 + 1$
15	16	1	0	$-3\tau + 1$	$\tau^4 - 1$
15	225	0	0	15	$-\tau^8 + \tau^4 - 1$
17	18	1	0	$-3\tau + 3$	$\tau^4 + 1$
19	28	1	0	$-3\tau + 5$	$-\tau^7 - \tau^4 + \tau^2 - 1$
19	207	2	0	$-6\tau - 9$	$\tau^9 + \tau^7 - \tau^4 + \tau^2 - 1$
21	46	1	0	$-3\tau + 7$	$-\tau^7 - \tau^4 + \tau^2 + 1$
21	163	2	0	$-6\tau - 7$	$\tau^9 + \tau^7 - \tau^4 + \tau^2 + 1$
23	72	1	0	$-3\tau + 9$	$-\tau^8 - \tau^6 + \tau^3 - 1$
23	127	2	0	$-6\tau - 5$	$-\tau^6 + \tau^3 - 1$
23	242	2	-1	$11\tau - 11$	$-\tau^9 - \tau^6 + \tau^3 - 1$
25	99	2	0	$-6\tau - 3$	$-\tau^6 + \tau^3 + 1$
25	106	1	0	$-3\tau + 11$	$-\tau^8 - \tau^6 + \tau^3 + 1$
25	224	2	-1	$11\tau - 9$	$-\tau^9 - \tau^6 + \tau^3 + 1$
27	79	2	0	$-6\tau - 1$	$-\tau^6 - \tau^2 - 1$
27	148	1	0	$-3\tau + 13$	$-\tau^8 - \tau^6 - \tau^2 - 1$
27	214	2	-1	$11\tau - 7$	$-\tau^9 - \tau^6 - \tau^2 - 1$
29	67	2	0	$-6\tau + 1$	$-\tau^6 - \tau^2 + 1$
29	198	1	0	$-3\tau + 15$	$-\tau^8 - \tau^6 - \tau^2 + 1$
29	212	2	-1	$11\tau - 5$	$-\tau^9 - \tau^6 - \tau^2 + 1$
31	63	2	0	$-6\tau + 3$	$-\tau^7 - \tau^5 - 1$
31	218	2	-1	$11\tau - 3$	$-\tau^9 - \tau^7 - \tau^5 - 1$
33	67	2	0	$-6\tau + 5$	$-\tau^7 - \tau^5 + 1$
33	232	2	-1	$11\tau - 1$	$-\tau^9 - \tau^7 - \tau^5 + 1$
33	233	3	-1	$8\tau - 15$	$\tau^7 - \tau^5 + 1$
35	79	2	0	$-6\tau + 7$	$-\tau^7 + \tau^2 - 1$
35	193	3	-1	$8\tau - 13$	$\tau^7 + \tau^2 - 1$
35	254	2	-1	$11\tau + 1$	$-\tau^9 - \tau^7 + \tau^2 - 1$

Continued on next page

Table B:.6 E$_1$: $w = 8, N(\tau^w) = 256, \tau^w(reduced) = -3\tau - 14$ **(continued from previous page)**

u	norm	q_0	q_1	*u mod* τ^w	α_u
37	99	2	0	$-6\tau + 9$	$-\tau^7 + \tau^2 + 1$
37	161	3	-1	$8\tau - 11$	$\tau^7 + \tau^2 + 1$
37	232	3	0	$-9\tau - 5$	$\tau^9 + \tau^7 + \tau^2 + 1$
39	127	2	0	$-6\tau + 11$	$-\tau^7 - \tau^3 - 1$
39	137	3	-1	$8\tau - 9$	$\tau^7 - \tau^3 - 1$
39	198	3	0	$-9\tau - 3$	$\tau^9 + \tau^7 - \tau^3 - 1$
41	121	3	-1	$8\tau - 7$	$\tau^7 - \tau^3 + 1$
41	163	2	0	$-6\tau + 13$	$-\tau^7 - \tau^3 + 1$
41	172	3	0	$-9\tau - 1$	$\tau^9 + \tau^7 - \tau^3 + 1$
43	113	3	-1	$8\tau - 5$	$-\tau^9 - \tau^6 + \tau^4 - \tau^2 - 1$
43	154	3	0	$-9\tau + 1$	$-\tau^6 + \tau^4 - \tau^2 - 1$
43	207	2	0	$-6\tau + 15$	$-\tau^8 - \tau^6 + \tau^4 - \tau^2 - 1$
45	113	3	-1	$8\tau - 3$	$-\tau^9 - \tau^6 + \tau^4 - \tau^2 + 1$
45	144	3	0	$-9\tau + 3$	$-\tau^6 + \tau^4 - \tau^2 + 1$
45	254	4	-1	$5\tau - 17$	$-\tau^{10} - \tau^8 - \tau^6 + \tau^4 - \tau^2 + 1$
47	121	3	-1	$8\tau - 1$	$\tau^6 - \tau^4 - 1$
47	142	3	0	$-9\tau + 5$	$\tau^9 + \tau^6 - \tau^4 - 1$
47	200	4	-1	$5\tau - 15$	$\tau^8 + \tau^6 - \tau^4 - 1$
49	137	3	-1	$8\tau + 1$	$\tau^6 - \tau^4 + 1$
49	148	3	0	$-9\tau + 7$	$\tau^9 + \tau^6 - \tau^4 + 1$
49	154	4	-1	$5\tau - 13$	$\tau^8 + \tau^6 - \tau^4 + 1$
51	116	4	-1	$5\tau - 11$	$\tau^7 + \tau^4 + \tau^2 - 1$
51	161	3	-1	$8\tau + 3$	$-\tau^9 - \tau^7 + \tau^4 + \tau^2 - 1$
51	162	3	0	$-9\tau + 9$	$-\tau^7 + \tau^4 + \tau^2 - 1$
53	86	4	-1	$5\tau - 9$	$\tau^7 + \tau^4 + \tau^2 + 1$
53	184	3	0	$-9\tau + 11$	$-\tau^7 + \tau^4 + \tau^2 + 1$
53	193	3	-1	$8\tau + 5$	$-\tau^9 - \tau^7 + \tau^4 + \tau^2 + 1$
55	64	4	-1	$5\tau - 7$	$\tau^7 + \tau^5 + \tau^3 - 1$
55	214	3	0	$-9\tau + 13$	$-\tau^7 + \tau^5 + \tau^3 - 1$
55	233	3	-1	$8\tau + 7$	$-\tau^9 - \tau^7 + \tau^5 + \tau^3 - 1$
57	50	4	-1	$5\tau - 5$	$\tau^7 + \tau^5 + \tau^3 + 1$
57	252	3	0	$-9\tau + 15$	$-\tau^7 + \tau^5 + \tau^3 + 1$
59	44	4	-1	$5\tau - 3$	$\tau^7 + \tau^5 - \tau^2 - 1$
61	46	4	-1	$5\tau - 1$	$\tau^7 + \tau^5 - \tau^2 + 1$
61	203	5	-1	$2\tau - 15$	$-\tau^{10} - \tau^7 + \tau^5 - \tau^2 + 1$
61	253	4	0	$-12\tau + 5$	$\tau^9 + \tau^7 + \tau^5 - \tau^2 + 1$
63	56	4	-1	$5\tau + 1$	$\tau^6 - 1$
63	151	5	-1	$2\tau - 13$	$\tau^8 + \tau^6 - 1$
63	253	4	0	$-12\tau + 7$	$\tau^9 + \tau^6 - 1$
65	74	4	-1	$5\tau + 3$	$\tau^6 + 1$
65	107	5	-1	$2\tau - 11$	$\tau^8 + \tau^6 + 1$
67	71	5	-1	$2\tau - 9$	$-\tau^5 + \tau^2 - 1$
67	100	4	-1	$5\tau + 5$	$-\tau^8 - \tau^5 + \tau^2 - 1$
69	43	5	-1	$2\tau - 7$	$-\tau^5 + \tau^2 + 1$

Continued on next page

Table B:.6 E$_1$: $w = 8, N(\tau^w) = 256, \tau^w(reduced) = -3\tau - 14$ **(continued from previous page)**

u	norm	q_0	q_1	$u\ mod\ \tau^w$	α_u
69	134	4	-1	$5\tau + 7$	$-\tau^8 - \tau^5 + \tau^2 + 1$
71	23	5	-1	$2\tau - 5$	$-\tau^5 - \tau^3 - 1$
71	176	4	-1	$5\tau + 9$	$-\tau^8 - \tau^5 - \tau^3 - 1$
73	11	5	-1	$2\tau - 3$	$-\tau^5 - \tau^3 + 1$
73	226	4	-1	$5\tau + 11$	$-\tau^8 - \tau^5 - \tau^3 + 1$
75	7	5	-1	$2\tau - 1$	$-\tau^4 - \tau^2 - 1$
75	242	6	-1	$-\tau - 15$	$\tau^8 - \tau^4 - \tau^2 - 1$
77	11	5	-1	$2\tau + 1$	$-\tau^4 - \tau^2 + 1$
77	184	6	-1	$-\tau - 13$	$\tau^8 - \tau^4 - \tau^2 + 1$
79	23	5	-1	$2\tau + 3$	$\tau^6 + \tau^4 - 1$
79	134	6	-1	$-\tau - 11$	$\tau^8 + \tau^6 + \tau^4 - 1$
81	43	5	-1	$2\tau + 5$	$\tau^6 + \tau^4 + 1$
81	92	6	-1	$-\tau - 9$	$\tau^8 + \tau^6 + \tau^4 + 1$
83	58	6	-1	$-\tau - 7$	$-\tau^6 - \tau^4 + \tau^2 - 1$
83	71	5	-1	$2\tau + 7$	$-\tau^8 - \tau^6 - \tau^4 + \tau^2 - 1$
85	32	6	-1	$-\tau - 5$	$-\tau^6 - \tau^4 + \tau^2 + 1$
85	107	5	-1	$2\tau + 9$	$-\tau^8 - \tau^6 - \tau^4 + \tau^2 + 1$
87	14	6	-1	$-\tau - 3$	$\tau^3 - 1$
87	151	5	-1	$2\tau + 11$	$-\tau^8 + \tau^3 - 1$
89	4	6	-1	$-\tau - 1$	$\tau^3 + 1$
89	203	5	-1	$2\tau + 13$	$-\tau^8 + \tau^3 + 1$
91	2	6	-1	$-\tau + 1$	$-\tau^2 - 1$
91	253	7	-1	$-4\tau - 13$	$\tau^8 - \tau^2 - 1$
93	8	6	-1	$-\tau + 3$	$-\tau^2 + 1$
93	197	7	-1	$-4\tau - 11$	$\tau^8 - \tau^2 + 1$
95	22	6	-1	$-\tau + 5$	$\tau^5 - 1$
95	149	7	-1	$-4\tau - 9$	$\tau^8 + \tau^5 - 1$
97	44	6	-1	$-\tau + 7$	$\tau^5 + 1$
97	109	7	-1	$-4\tau - 7$	$\tau^8 + \tau^5 + 1$
99	74	6	-1	$-\tau + 9$	$-\tau^8 - \tau^6 + \tau^2 - 1$
99	77	7	-1	$-4\tau - 5$	$-\tau^6 + \tau^2 - 1$
101	53	7	-1	$-4\tau - 3$	$-\tau^6 + \tau^2 + 1$
101	112	6	-1	$-\tau + 11$	$-\tau^8 - \tau^6 + \tau^2 + 1$
103	37	7	-1	$-4\tau - 1$	$-\tau^6 - \tau^3 - 1$
103	158	6	-1	$-\tau + 13$	$-\tau^8 - \tau^6 - \tau^3 - 1$
105	29	7	-1	$-4\tau + 1$	$-\tau^6 - \tau^3 + 1$
105	212	6	-1	$-\tau + 15$	$-\tau^8 - \tau^6 - \tau^3 + 1$
107	29	7	-1	$-4\tau + 3$	$\tau^4 - \tau^2 - 1$
109	37	7	-1	$-4\tau + 5$	$\tau^4 - \tau^2 + 1$
109	242	8	-1	$-7\tau - 9$	$\tau^8 + \tau^4 - \tau^2 + 1$

Continued on next page

Table B:.6 E$_1$**:** $w = 8, N(\tau^w) = 256, \tau^w(reduced) = -3\tau - 14$ **(continued from previous page)**

u	norm	q_0	q_1	$u\ mod\ \tau^w$	α_u
111	53	7	-1	$-4\tau + 7$	$-\tau^7 - \tau^4 - 1$
111	196	8	-1	$-7\tau - 7$	$\tau^9 + \tau^7 - \tau^4 - 1$
111	239	8	-2	$10\tau - 13$	$\tau^7 - \tau^4 - 1$
113	77	7	-1	$-4\tau + 9$	$-\tau^7 - \tau^4 + 1$
113	158	8	-1	$-7\tau - 5$	$\tau^9 + \tau^7 - \tau^4 + 1$
113	211	8	-2	$10\tau - 11$	$\tau^7 - \tau^4 + 1$
115	109	7	-1	$-4\tau + 11$	$-\tau^8 - \tau^6 + \tau^4 + \tau^2 - 1$
115	128	8	-1	$-7\tau - 3$	$-\tau^6 + \tau^4 + \tau^2 - 1$
115	191	8	-2	$10\tau - 9$	$-\tau^9 - \tau^6 + \tau^4 + \tau^2 - 1$
117	106	8	-1	$-7\tau - 1$	$-\tau^6 + \tau^4 + \tau^2 + 1$
117	149	7	-1	$-4\tau + 13$	$-\tau^8 - \tau^6 + \tau^4 + \tau^2 + 1$
117	179	8	-2	$10\tau - 7$	$-\tau^9 - \tau^6 + \tau^4 + \tau^2 + 1$
119	92	8	-1	$-7\tau + 1$	$-\tau^7 - \tau^5 + \tau^3 - 1$
119	175	8	-2	$10\tau - 5$	$-\tau^9 - \tau^7 - \tau^5 + \tau^3 - 1$
119	197	7	-1	$-4\tau + 15$	$\tau^{10} + \tau^7 - \tau^5 + \tau^3 - 1$
121	86	8	-1	$-7\tau + 3$	$-\tau^7 - \tau^5 + \tau^3 + 1$
121	179	8	-2	$10\tau - 3$	$-\tau^9 - \tau^7 - \tau^5 + \tau^3 + 1$
121	253	7	-1	$-4\tau + 17$	$\tau^{10} + \tau^7 - \tau^5 + \tau^3 + 1$
123	88	8	-1	$-7\tau + 5$	$-\tau^7 - \tau^5 - \tau^2 - 1$
123	191	8	-2	$10\tau - 1$	$-\tau^9 - \tau^7 - \tau^5 - \tau^2 - 1$
123	218	9	-2	$7\tau - 15$	$\tau^7 - \tau^5 - \tau^2 - 1$
125	98	8	-1	$-7\tau + 7$	$-\tau^7 - \tau^5 - \tau^2 + 1$
125	176	9	-2	$7\tau - 13$	$\tau^7 - \tau^5 - \tau^2 + 1$
125	211	8	-2	$10\tau + 1$	$-\tau^9 - \tau^7 - \tau^5 - \tau^2 + 1$
127	116	8	-1	$-7\tau + 9$	$-\tau^7 - 1$
127	142	9	-2	$7\tau - 11$	$\tau^7 - 1$
127	239	8	-2	$10\tau + 3$	$-\tau^9 - \tau^7 - 1$

Appendix C:

Code Snippets

The following code snippets are examples of Java implementations for an $O(n)$ squaring algorithm along with Solina's modulo δ reduction algorithm using his rounding technique and our simplified reduction algorithm using our rounding technique. We also present the Java code used to produce the tables which appear in appendices A: and B:.

The $O(n)$ algorithm presented in 3.3.2.3 for arbitrary squares. This provides an efficient method for computing arbitrary powers of squares in software as would be needed for calculating τ^n, i.e. $\tau^2, \tau^3, \ldots$

```
public int[] square(int[] a) {
    int[] c = new int[2 * a.length];

    int aBitMask = 0x1;
    int cBitMask = 0x1;
    int aIntPtr = 0, cIntPtr = 0;
    for (int b = 0; b < a.length * 32; b++) {
    // Careful here. In Java all integer values are signed so that when
    // you shift the bitMask into the highest bit the number becomes
    // negative e.g. 0x40 (positive) << 1 = 0x80 (now negative)
    if ((a[aIntPtr] & aBitMask) != 0)
        c[cIntPtr] ^= cBitMask;

        aBitMask <<= 1;
        if (aBitMask == 0) {
          aIntPtr++;
          aBitMask = 0x1;
        }

        cBitMask <<= 2;
        if (cBitMask == 0) {
            cIntPtr++;
            cBitMask = 0x1;
        }
    }

    return trim(c);
}
```

This is an implementation of Solina's reduction algorithm along with his rounding technique as presented in [19]

```
/**
* Routine 74 - P. 225. Solinas's reduction algorithm.
*
* @param n - the scalar multiple
* @return - the parameters r<sub>0</sub> and r<sub>1</sub> representing the
*          reduction modulo delta.
* @throws Exception
*/
public BigInteger[] reductionModDelta(BigInteger n) throws Exception {
    BigDecimal s0 = new BigDecimal(this.s0);
    BigDecimal s1 = new BigDecimal(this.s1);
    BigDecimal mu = new BigDecimal(this.mu);

    BigDecimal d0 = s0.add(s1.multiply(mu));
    BigDecimal nn = new BigDecimal(n);

    BigDecimal rr = new BigDecimal(r);
    BigDecimal lambda0 = s0.multiply(nn).divide(rr);
    BigDecimal lambda1 = s1.multiply(nn).divide(rr);

    BigDecimal[] q = round(lambda0, lambda1); //Solina's rounding technique

    BigDecimal r0 = nn.subtract(d0.multiply(q[0])).subtract(
        BD_TWO.multiply(s1.multiply(q[1])));
    BigDecimal r1 = s1.multiply(q[0]).subtract(s0.multiply(q[1]));

    return new BigInteger[] { r0.toBigInteger(), r1.toBigInteger() };
}

/**
* This is an implementation of Solina's rounding algorithm which
* picks the closest value of least norm.
*
* Input: lamda = l<sub>0</sub> + l<sub>1</sub> * tau
*
* @param q<sub>0</sub>
*           - the rounded integer value of l<sub>0</sub>
* @param q<sub>1</sub>
*           - the rounded integer value of l<sub>1</sub>
* @return q<sub>0</sub>, q<sub>1</sub> specifying the complex
         number q<sub>0</sub> + q<sub>1</sub> * tau = round(lamda)
* @throws Exception
*/
public BigDecimal[] round(BigDecimal lambda0, BigDecimal lambda1) throws Exception {
    BigDecimal f0 = lambda0.add(new BigDecimal("0.5")).setScale(0, BigDecimal.ROUND_FLOOR);
    BigDecimal f1 = lambda1.add(new BigDecimal("0.5")).setScale(0, BigDecimal.ROUND_FLOOR);

    BigDecimal eta0 = lambda0.subtract(f0);
    BigDecimal eta1 = lambda1.subtract(f1);

    BigDecimal h0 = BigDecimal.ZERO;
    BigDecimal h1 = BigDecimal.ZERO;

    BigDecimal mu = new BigDecimal(this.mu);
    BigDecimal eta = BD_TWO.multiply(eta0).add(mu.multiply(eta1));

    if (eta.compareTo(BD_ONE) >= 0) {
        BigDecimal temp = eta0.subtract(BD_THREE.multiply(mu).multiply(eta1));
        if (temp.compareTo(BD_NEG_ONE) < 0)
            h1 = mu;
        else
            h0 = BD_ONE;
    } else {
        BigDecimal temp = eta0.add(BD_FOUR.multiply(mu).multiply(eta1));
        if (temp.compareTo(BD_TWO) >= 0)
            h1 = mu;
    }

    if (eta.compareTo(BD_NEG_ONE) < 0) {
        BigDecimal temp = eta0.subtract(BD_THREE.multiply(mu).multiply(eta1));
        if (temp.compareTo(BD_ONE) >= 0)
            h1 = mu.negate();
        else
            h0 = BD_NEG_ONE;
    } else {
        BigDecimal temp = eta0.add(BD_FOUR.multiply(mu).multiply(eta1));
        if (temp.compareTo(BD_TWO.negate()) < 0)
            h1 = mu.negate();
    }

    BigDecimal q0 = f0.add(h0);
    BigDecimal q1 = f1.add(h1);

    return new BigDecimal[] { q0, q1 };
}
```

This is an implementation of our reduction algorithm using our simplified rounding technique as presented in section 3.3.2.1.

```
/**
* Reduction modulo delta using simplified rounding.
*
* @param n - the scalar multiple
* @return - the parameters r<sub>0</sub> and r<sub>1</sub> representing the
*           reduction modulo delta.
* @throws Exception
*/
public BigInteger[] simplifiedReductionModDelta(BigInteger n)
    throws Exception {
    BigInteger d0 = s0.add(s1.multiply(mu));

    // We simply truncate the decimal.
    BigInteger q0 = s0.multiply(n).divide(r);
    BigInteger q1 = s1.multiply(n).divide(r);

    BigInteger r0 = n.subtract(d0.multiply(q0)).subtract(
    TWO.multiply(s1.multiply(q1)));
    BigInteger r1 = s1.multiply(q0).subtract(s0.multiply(q1));

    return new BigInteger[] { r0, r1 };
}
```

This code snippet was used to produce all of the tables which appear in appendices A: and B:. The snippet outputs its data in a latex format so that it can simply be cut/paste into a latex document.

```
/**
* Computes alpha<sub>u</sub> for a given "a". That is, E<sub>0</sub>
* or E<sub>1</sub>.
*
* Results are printed in latex format so that they can simply be copied into
* a latex document following the mantra "work smarter not harder".
*
* @param a
*            - the a constant from the elliptic curve 0 for E<sub>0</sub> 1
*            for E<sub>1</sub>
* @param w
*            - the window size
* @throws Exception
*/
public static void alphaAllWindows(int a) throws Exception {
    int mu = a == 0 ? -1 : 1;

    int table = 1;
    for (int w = 3; w <= 8; w++) {
        if (w >= 6)
            System.out.println("\\pagebreak");

            // returns the reduction of t^w = t0 + t1 * tau
            //This uses the Lucas sequence t<sup>k</sup> =
            //    U<sub>k</sub>t - 2U<sub>k-1</sub> for k >= 1
            //where t is tau.
            int[] t = tKReduction(w, mu);

            int uUpper = (int) Math.pow(2, w - 1) - 1;
            int tW = (int) Math.pow(2, w);

            System.out.println("\\begin{center}");
            System.out.println("\\begin{footnotesize}");

            StringBuilder caption = new StringBuilder("$E_" + a + "$: $w = "
                + w + ", N(\\uptau^w) = " + tW + ", \\uptau^w (reduced) = ");

            if (t[1] > 1)
                caption.append(t[1]).append("\\uptau");
            else if (t[1] == 1)
                caption.append("\\uptau");
            else if (t[1] == -1)
                caption.append("-\\uptau");
            else if (t[1] < -1)
                caption.append(t[1]).append("\\uptau");

            if (t[0] >= 1)
                caption.append(" + ").append(t[0]);
            else if (t[0] == -1)
                caption.append("- 1");
            else if (t[0] < -1)
                caption.append(" - ").append(Math.abs(t[0]));

            caption.append("$");

            System.out.println("\\caption[$E_" + a + "$: Width $" + w
                + "\\tau$-NAF Table]{" + caption.toString()
                + "\\\\\\label{tab:E" + a + "table" + (table++)
                + "}}\\\\ % **NB**");

            System.out.println("\\hline \\multicolumn{1}{|c|}{u} &"
                + "\\multicolumn{1}{c|}{norm} & \\multicolumn{1}{c|}{$q_0$}"
                + " & \\multicolumn{1}{c|}{$q_1$} & \\multicolumn{1}{c|}{$u ~mod ~\\uptau^w$}"
                + " & \\multicolumn{1}{c|}{$\\alpha_u$}\\\\ \\hline");
            System.out.println("\\endfirsthead");
            System.out.println("\\multicolumn{6}{c}%");

            System.out.println("{{\\bfseries \\tablename\\ \\thetable{} "
                + caption.toString()
                + " (continued from previous page) }} \\\\");
            System.out.println("\\hline \\multicolumn{1}{|c|}{u} &");
            System.out.println("\\multicolumn{1}{c|}{norm} &");
            System.out.println("\\multicolumn{1}{c|}{$q_0$} &");
            System.out.println("\\multicolumn{1}{c|}{$q_1$} &");
            System.out.println("\\multicolumn{1}{c|}{$u ~mod ~\\uptau^w$} &");

            System.out.println("\\multicolumn{1}{c|}{$\\alpha_u$}\\\\ \\hline");
            System.out.println("\\endhead");

            System.out.println("\\hline \\multicolumn{6}{|r|}"
                + "{{Continued on next page}} \\\\ \\hline");

            System.out.println("\\endfoot");

            System.out.println("\\hline \\hline");
            System.out.println("\\endlastfoot");

            System.out.println("% Now the regular content :");

            for (int u = 1; u <= uUpper; u++) {
                //TableRow is simply a convenience data structure
                //so that I can sort this information later.
                List<TableRow> rows = new ArrayList<>();

                //The real work horse section. We pick a range of q values
                //that generate norms way outside the range. Not the most
                //optimal but we only need to do this once.
                for (int q0 = -50; q0 <= 50; q0++)
                    for (int q1 = -50; q1 <= 50; q1++) {
                        int betau = t[0] * q0 + (-2 * t[1] * q1) + u;
                        int gammau = t[1] * q0 + (t[0] + mu * t[1]) * q1;

                        String nModTauW = "";

                        Integer[] tnaf = {};
                        int norm = norm(mu, betau, gammau);
                        if (norm < tW) {
                            if (gammau == 0)
                                nModTauW = Integer.toString(betau);
                            else if (gammau == 1)
                                nModTauW = "\\uptau"
                                    + (betau < 0 ? " - " + -betau : " + "
                                    + betau);
                            else if (gammau == -1)
                                nModTauW = "-\\uptau"
                                    + (betau < 0 ? " - " + -betau : " + "
                                    + betau);
                            else
                                nModTauW = ""
                                    + gammau
                                    + "\\uptau"
                                    + (betau < 0 ? " - " + -betau : " + "
                                    + betau);

                                rows.add(new TableRow(u, norm, q0, q1, nModTauW,
    tnaf));
                        }
                    }

                TableRow[] sortRows = new TableRow[rows.size()];
                rows.toArray(sortRows);
                Arrays.sort(sortRows);
```

```
                boolean isRow = false;
                for (TableRow r : sortRows)
                    if (r.u % 2 == 1) {
                        System.out.printf("%3s & %5s & %3s & %3s & $%15s$ & $%s$\\\\\n",
                            r.u, r.norm, r.q0, r.q1,
                            r.nModTauW, r.polyTNAF);

                    isRow = true;
                }

                if (isRow) {
                    System.out.println(" & & & & & \\\\");
                    isRow = false;
                }
            }

            System.out.println("\\end{longtable}");
            System.out.println("\\end{footnotesize}");
            System.out.println("\\end{center}");
        }
    }
}
```