5-1-2012

The Zeta Function of Generalized Markoff Equations over Finite Fields

Juan Mariscal
University of Nevada, Las Vegas, jcmariscal81@gmail.com

THE ZETA FUNCTION OF GENERALIZED MARKOFF EQUATIONS OVER FINITE FIELDS

by

Juan Carlos Mariscal

Thesis Submitted in Partial Fulfillment
of the Requirements for the

Master of Science in Mathematical Science

Department of Mathematical Science
College of Sciences
The Graduate College

University of Nevada, Las Vegas

May 2012

THE GRADUATE COLLEGE

We recommend the thesis prepared under our supervision by

Juan Carlos Mariscal

entitled

The Zeta Function of Generalized Markoff Equations Over Finite Fields

be accepted in partial fulfillment of the requirements for the degree of

Master of Science in Mathematical Science
Department of Mathematical Science

Arthur Baragar, Committee Chair

Peter Shiue, Committee Member

Gennady Bachman, Committee Member

Evangelos Yfantis, Graduate College Representative

Ronald Smith, Ph. D., Vice President for Research and Graduate Studies
and Dean of the Graduate College

May 2012

ABSTRACT

The study of this paper is based on the Markoff equation

$$x^2 + y^2 + z^2 = 3xyz. \tag{1}$$

Our goal is to derive the Hasse-Weil zeta function of a generalization of Equation (1) in dimensions 2 and 3. This algebraic variety $M_{a,b}(\mathbb{F}_q^n)$ is defined as the solutions to

$$x_1^2 + x_2^2 + +x_3^2 = ax_1x_2x_3 + b \tag{2}$$

over $\mathbb{F}_q$. We derive the zeta function by counting the number of solutions to Equation (2) over finite fields first by using a projection to $\mathbb{P}^2$ minus some lines and in all other cases by applying a slicing method from the two-dimensional cases. This enables us to derive a generating function for the number of solutions over the degree k extensions of the finite field $\mathbb{F}_q$ giving us the local zeta function

$$Z\left(M_{a,b}(\mathbb{F}_q^3), t\right) = \frac{1}{(1-q^2t)(1-\epsilon qt)^3(1-\epsilon\delta qt)(1-t)}$$

where ϵ and δ are ± 1 and depend on q.

ACKNOWLEDGEMENTS

I would like to thank all of my friends and family for their love and support throughout my academic career. This includes my colleagues I consulted with on the subject; Donald McGinn, Brandon Metz, Cody Palmer and Joy Sun. A special thanks to my committee for their time and advice despite the time restraints. Especially Dr. Peter Shiue for giving me so much of his time for which I am incredibly thankful for. I also wish to thank my advisor Dr. Arthur Baragar for his guidance throughout this paper and throughout every semester of my graduate studies up until this point. Lastly I would like to thank Joy Sun for her endless support, her helpful advice and food.

TABLE OF CONTENTS

Page

ABSTRACT . . . iii

ACKNOWLEDGEMENTS . . . iv

TABLE OF CONTENTS . . . v

LIST OF TABLES . . . vi

LIST OF FIGURES . . . vii

1 Introductory Material . . . 1

1.1 Finite Fields and Quadratic Residues . . . 1

1.2 Hasse-Weil Zeta Functions . . . 3

1.3 The Markoff Equation . . . 5

2 Generalized Markoff equations over $\mathbb{F}_q$ . . . 8

2.1 Generalized Markoff equations of degree 3 . . . 8

2.2 The Special case of $M_{1,4}(\mathbb{F}_q^3)$ . . . 10

2.3 The Two Dimensional Case . . . 14

2.4 The order of $M_{a,b}(\mathbb{F}_q^3)$ . . . 19

2.5 The Zeta Function of $M_{a,b}\left(\mathbb{F}_q^3\right)$ . . . 23

2.6 Discussion on Future Work . . . 25

BIBLIOGRAPHY . . . 27

VITA . . . 28

LIST OF TABLES

Table Page

2.1 $|M_{3,b}\left(\mathbb{F}_p^3\right)|$ for different b and small primes p 10

2.2 $|M_{a,b}(\mathbb{F}_{11}^2)|$ for all a and b 18

LIST OF FIGURES

Figure Page

1.1 The Markoff Tree Generated by (1,1,1). 6

2.1 Markoff Tree for $M_{3,2}(\mathbb{Z}_7^3)$. 8

2.2 Markoff Tree for $M_{1,3}(\mathbb{Z}_{11}^3)$. 9

Chapter 1

Introductory Material

The main topics of this paper include Number Theory, Finite Field Theory and a little algebraic geometry. It is assumed the reader has a basic knowledge of these areas.

1.1 Finite Fields and Quadratic Residues

Throughout the paper, we derive formulas based on whether or not certain constants are quadratic residues over finite fields. Recall, in number theory, an integer r is called a quadratic residue modulo p if it is congruent to a perfect square modulo p. I.e. there exists $x \in \mathbb{Z}_p$ such that $x^2 = r \pmod{p}$. We wish to apply the following well-known theorems whose proofs we omit.

Theorem 1.1: The set of quadratic residues form a subgroup of $\mathbb{Z}_p^*$.

Theorem 1.2: The quadratic residues of $\mathbb{Z}_p^*$ consist of $\left(\frac{p-1}{2}\right)$ elements for $p \neq 2$.

Since we will be working over arbitrary finite fields we wish to extend our definition and these theorems on quadratic residues to more than just the fields $\mathbb{Z}_p$.

Recall that if $\mathbb{F}_q$ is a finite field of order q then we have $q = p^m$ where the prime number p is the characteristic of the field and m is a positive integer. We also know that the multiplicative group $\mathbb{F}_q^*$ is cyclic and hence can be written as $\mathbb{F}_q^* = \langle \alpha \rangle$ for some generator α, implying that our group is isomorphic to $\mathbb{Z}_{q-1}$. Let us define R_q to be the set of quadratic residues in $\mathbb{F}_q^*$, where r is a quadratic residue of $\mathbb{F}_q^*$ if there exists an $x \in \mathbb{F}_q$ such that $x^2 = r$ over $\mathbb{F}_q$. This means that all quadratic residues of $\mathbb{F}_q$ are the even powers of the generator α. I.e. $(R_q, \cdot) = \langle \alpha^2 \rangle$. Therefore, if $2|(q-1)$

then we have that

$$[\mathbb{F}_q^* : \langle \alpha^2 \rangle] = 2$$

and therefore, exactly half of the elements of $\mathbb{F}_q^*$ belong to R_q. If 2 does not divide $q-1$ then $p = 2$ and $\gcd(2, q-1) = 1$ so α^2 must also be a generator of $\mathbb{F}_q^*$. Therefore all elements of $\mathbb{F}_q^*$ are quadratic residues. This leads us to the following analogs to Theorems 1.1 and 1.2 over finite fields:

Theorem 1.3: The set of quadratic residues R_q is a subgroup of $\mathbb{F}_q^*$.

Theorem 1.4: If $\mathbb{F}_q$ has odd characteristic, then there are $\frac{q-1}{2}$ elements of $\mathbb{F}_q^*$ that belong to R_q.

Theorem 1.5: If $\mathbb{F}_q$ has characteristic 2, then all elements of $\mathbb{F}_q^*$ belong to R_q.

For this reason, we will have to consider separate cases when deriving our class of zeta functions.

In Section 2.3, we make use of two theorems where we again define R_q to be the set of quadratic residues in $\mathbb{F}_q^*$ and introduce N_q for the set of quadratic non-residues in $\mathbb{F}_q^*$. Kelly proved the following theorems over fields of prime order but they can be easily generalized to arbitrary fields [6].

Theorem 1.6: Let $q \equiv 1 \pmod 4$, let r be an arbitrary quadratic residue and n an arbitrary nonresidue and assume $\mathbb{F}_q$ has characteristic not equal to 2. Then the sets $r + N_q$ and $n + R_q$ consist of $\frac{q-1}{4}$ quadratic residues and $\frac{q-1}{4}$ quadratic nonresidues.

Theorem 1.7: Let $q \equiv 3 \pmod 4$, assume $\mathbb{F}_q$ has characteristic not equal to 2 and r, n defined in the same manner. Then the sets $r + N_q$ and $n + R_q$ consist of the element 0 and $\frac{q-3}{4}$ quadratic residues along with $\frac{q-3}{4}$ nonresidues.

1.2 Hasse-Weil Zeta Functions

The Riemann Zeta function is defined as the complex valued function given by the series

$$\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s} \tag{1.1}$$

which is defined for complex numbers s with $\Re(s) > 1$. We can also write $\zeta(s)$ as the Euler product giving us the important property

$$\zeta(s) = \prod_{p \text{ prime}} \left(\frac{1}{1 - p^{-s}} \right).$$

Reimann was able to give a formula for the number of primes less then a given number in terms of the zeroes of the meromorphic continuation $\zeta(s)$. The search for the zeroes of such functions is reguarded as one of the most important problems in pure mathematics today.

It was only natural for mathmeticians to generalize $\zeta(s)$ in an attempt to gain more insight into the Reimann zeta function, and also because zeta functions themselves contain valuable information about the counting of certain geometric and algebraic objects. These zeta functions can be divided into two categories: local zeta functions and global zeta functions.

By local we mean that we are considering the series over finite fields $\mathbb{F}_q$. The local zeta function $Z(t)$ is a function whose logarithmic derivative is a generating function of some algebraic variety X over all k-extensions of the field $\mathbb{F}_q$. By this we mean that if we are given some algebraic variety X over $\mathbb{F}_q$ and let $|X_{q^k}|$ represent the number of solutions in $\mathbb{F}_{q^k}$, then we can build the generating function

$$G(t) = |X_q|t + \frac{|X_{q^2}|t^2}{2} + \frac{|X_{q^3}|t^3}{3} + ... \quad .$$

From here we are able to define the local zeta function of X paired with the initial finite field $\mathbb{F}_q$ as

$$\zeta(X_q, t) = \exp\left(\sum_{n=1}^{\infty} |X_{q^n}|\frac{t^n}{n}\right).$$

Enrico Bombieri showed that this function can be algorithmically determined for any variety X_{q^n} [3].

Deriving the number of solutions to polynomials over finite fields is a non-trivial problem. For example in 1925, Hasse put an upper bound on the number of solutions of elliptic curves over $\mathbb{F}_q$. His theorem states that if N is the number of solutions then we have

$$|N - (q + 1)| \leq 2\sqrt{q}.$$

This is equivalent to taking the absolute values of the zeroes of the local zeta function of the elliptic curve. Despite the importance of elliptic curves in modern mathematics, Hasse's theorem remains a fundamental result in counting the number of solutions of elliptic curves over $\mathbb{F}_q$. This demonstrates that finding the order of the variety X is an important problem for interesting cases of X.

Andre Weil [8] proposed several highly influential conjectures about the local zeta function $\zeta(X_q, t)$ with reguards to its rationality, functionality, and its connection to the Reimann hypothesis. Dwork [4] proved that if X is a non-singular projective algebraic variety than $\zeta(X_q, t)$ is a rational function. Grothendieck [5] proved that $\zeta(X_q, t)$ satisfies the functional equation

$$\zeta(X, n - t) = \pm q^{\frac{nE}{2} - Et}\zeta(X, t)$$

where E is the Euler characteristic of X.

Global zeta functions, like the Reimann zeta function, take into account all primes p. The understanding of zeta functions locally with respect to some prime gives information about the global zeta function analogous to how properties of certain integers can be determined by its prime factors. Local zeta functions can also be used to show that the global zeta function is defined in some region $\{s \in \mathbb{C} | \Re(s) > K\}$. In this paper we derive the Hasse-Weil zeta function, which is defined as the Euler-product of the local zeta functions for X_p for all prime numbers p. I.e.

$$\zeta(X, s) = \prod_{p \text{ prime}} \zeta\left(X_p, p^{-s}\right).$$

1.3 The Markoff Equation

In 1879 Markov considered the Diophantine equation

$$x^2 + y^2 + z^2 = 3xyz, \tag{1.2}$$

which was made famous when he observed the relationship between the Markoff triples and Diophantine approximation [7]. By a Markoff triple we mean the positive rational integral solutions (x, y, z) satisfying the equation above. Cleary if (x, y, z) is a Markoff triple then so are all other permutations. Less trivially if (x, y, z) is a solution to Equation (1.2) then we can obtain the solutions $(x, y, 3xy - z)$, $(x, 3xz - y, z)$, and $(3xyz - x, y, z)$ which we easily verify:

$$\begin{aligned} x^2 + y^2 + (3xy - z)^2 &= x^2 + y^2 + 9x^2y^2 - 6xyz + z^2 \\ &= 3xy + 9x^2y^2 - 6xyz \\ &= 3xy(3xy - z). \end{aligned}$$

The other two cases are identical. We can think of these substitutions as automorphisms on the curve defined in Equation (1.2) and define the group $G = \langle \sigma_1, \sigma_2, \sigma_3 \rangle$ where

$$\sigma_1(x, y, z) = (x, z, y)$$

$$\sigma_2(x, y, z) = (y, z, x)$$

$$\sigma_3(x, y, z) = (x, y, 3xy - z).$$

After applying these automorphisms to an arbitrary solution we naturally create a tree-like structure of integer solutions as seen below.

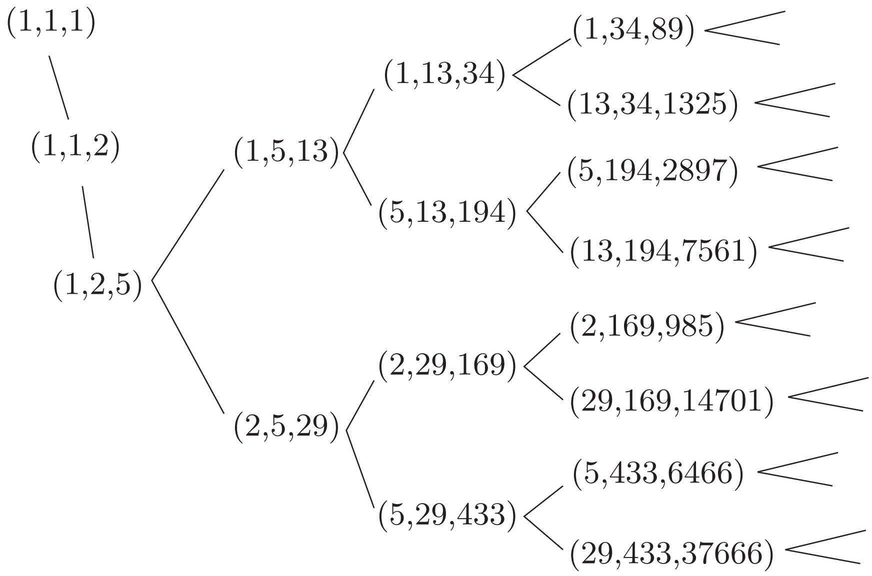

Figure 1.1: The Markoff Tree Generated by (1,1,1).

In Figure 1.3 we only consider one permutation of each triple ordered from least to greatest, and two triples are connected if the automorphism σ_3 was applied exactly once between the two triples. Using a descent argument, Markov showed that all integer solutions to Equation (1.2), aside from $(0, 0, 0)$, can be generated from the Group G acting on the fundamental solution $(1, 1, 1)$. Other than the first two triples, all Markov triples (a, b, c) consist of three distinct integers. The famous unicity conjecture states that for a Markov number c, there exists exactly one Markov triple (a, b, c) such that c is maximal.

Hurwitz (1907) was able to apply Markov's descent argument to the more general equation

$$x_1^2 + x_2^2 + \cdots + x_n^2 = a x_1 x_2 \ldots x_n. \tag{1.3}$$

Hurwitz was able to show that there are no integer solutions to Equation (1.3) if $a > n$.

The local zeta function for the Markoff equation over $\mathbb{F}_q$ was computed by Baragar [1] as

$$Z(M_{3,0}(\mathbb{F}_q^3), t) = \begin{cases} \frac{1}{(1-q^2t)(1-\epsilon qt)^3(1-t)} & \text{if the characteristic is not equal to 2 or 3} \\ \frac{1}{(1-q^2t)(1-t)} & \text{if the characteristic is equal to 2} \\ \frac{1}{(1-q^2t)} & \text{if the characteristic is equal to 3} \end{cases}$$

for $\epsilon = \left(\frac{-1}{p}\right)^m$ where $q = p^m$ and $\left(\frac{-1}{p}\right)$ is the Legendre symbol for -1 modulo p. This was done by using a birational map [2] between the set of solutions of Equation (1.3) over $\mathbb{F}_q$ and $\mathbb{P}^2$. In this projective mapping, the solution point $(0,0,0)$ acts as a point at infinite. We sought to attempt to count the number of solutions to the more generalized case $M_{a,b}(\mathbb{F}_q^3)$ using the same argument however we found that such a convenient projection only applied to the special case $M_{a,4a^{-2}}(\mathbb{F}_q^3)$.

Chapter 2

Generalized Markoff equations over $\mathbb{F}_q$

Throughout this paper we will refer to the algebraic variety of the more generalized Markoff (or Hurwitz) equation defined by

$$M_{a,b}(\mathbb{F}_q^n) = \left\{ (x_1, x_2, ..., x_n) \in \mathbb{F}_q^n \;\middle|\; \sum_{i=1}^{n} x_i^2 = a\left(\prod_{i=1}^{n} x_i\right) + b \right\}$$

over F_q for degree n. Within this chapter we restrict n to degree 2 and 3.

2.1 Generalized Markoff equations of degree 3

First we note a few basic properties of $M_{a,b}(\mathbb{F}_q^3)$ and the group G acting on $M_{a,b}(\mathbb{F}_q^3)$. First note that given a solution $(x, y, z) \in M_{a,b}(\mathbb{F}_q^3)$, we have that all permutations of (x, y, z) are also solutions and again less trivially we can show that $(x, y, axy - z)$ is also a solution by observing

$$\begin{aligned} x^2 + y^2 + (axy - z)^2 &= x^2 + y^2 + a^2x^2y^2 - 2axyz + z^2 \\ &= axyz + b + a^2x^2y^2 - 2axyz \\ &= axy(axy - z) + b. \end{aligned}$$

Hence we see that the group G acts on $M_{a,b}(\mathbb{F}_q^3)$ for any $b \in \mathbb{F}_q$ in the same manner as the set of integral solutions to the original Markoff equation $M_{3,0}(\mathbb{Z}^3)$. This means that the set $M_{a,b}(\mathbb{F}_q^3)$ can also be represented as a finite Markoff tree as seen below.

Here a given component represents a particular G-orbit (notated as $G\{(x_0, x_1, x_2)\}$) for some solution (x_0, x_1, x_2) of the set $M_{a,b}(\mathbb{F}_q^3)$. Baragar conjectured [1] that for the Markoff equation we have

$$M_{3,0}(Z_p) = G\{(1, 1, 1)\} \cup \{(0, 0, 0)\}$$

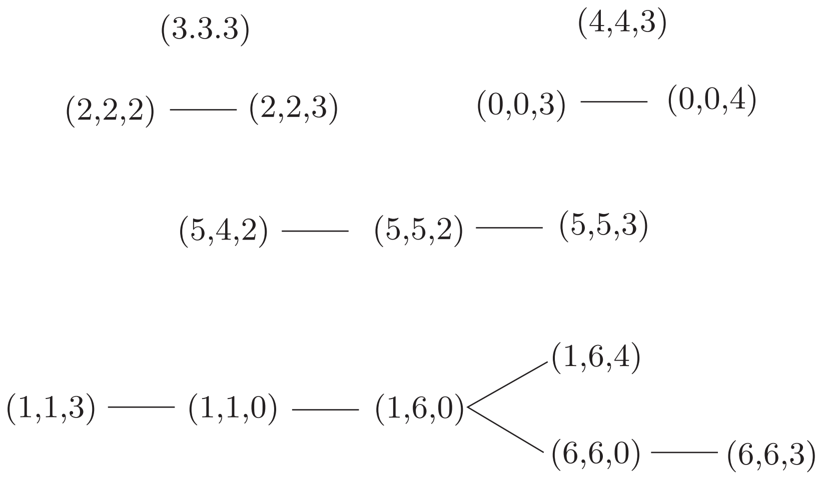

Figure 2.1: Markoff Tree for $M_{3,2}(\mathbb{Z}_7^3)$.

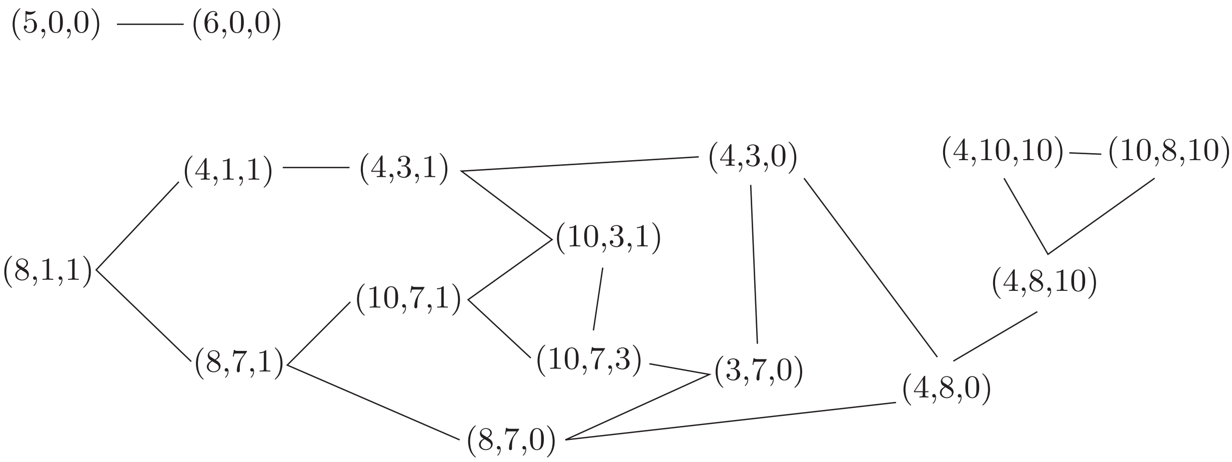

Figure 2.2: Markoff Tree for $M_{1,3}(\mathbb{Z}_{11}^3)$.

which we clearly see cannot hold when the a, b values are changed as seen by the trees for $M_{1,3}(\mathbb{F}_{11}^3)$ and $M_{3,2}(\mathbb{F}_7^3)$. The fact that the structure of the group G is difficult to determine brings interest to the following questions: How many G-orbits exist for the set $M_{a,b}(\mathbb{F}_q^3)$, can we obtain any information about G (i.e. subgroups, divisors of the order, etc.) by looking at the orbits, and what is the size of $M_{a,b}(\mathbb{F}_q^3)$. Throughout the next few sections we answer the last question.

Table 2.1: $|M_{3,b}\left(\mathbb{F}_p^3\right)|$ for different b and small primes p

$b\backslash p$	5	7	11	13	17	19
0	41	29	89	209	341	305
1	26	22	166	118	222	438
2	36	50	144	196	222	324
3	16	64	166	222	256	400
4	6	78	78	118	358	286
5		36	78	144	256	286
6		64	100	144	324	286
7			144	144	324	286
8			100	196	290	400
9			122	222	358	438
10			144	118	324	324
11				196	256	362
12				170	324	400
13					222	324
14					256	324
15					222	400
16					358	438
17						438
18						400

We have [2] that $|M_{3,0}(\mathbb{F}_q^3)| = q^2 + 3\left(\frac{-1}{q}\right)q + 1$. In table 2.1 we give the orders of $M_{3,b}(\mathbb{F}_q)$ for different values of b and over fields of order q.

To count the number of solutions to the generalized Hurwitz equation, it is advantageous to simplify the equation as much as possible.

Observation: $|M_{a,b}(\mathbb{F}_q^3)| = |M_{am^{-1},bm^2}(\mathbb{F}_q^3)|$ for any $m \in \mathbb{F}_q^*$.

Proof: We are able to show this using the fact that $(x, y, z) \rightarrow (mx, my, mz)$ is a bijective mapping and by assuming that $(x, y, z) \in M_{a,b}(\mathbb{F}_q^3)$. We observe that

$$\begin{aligned}(mx)^2 + (my)^2 + (mz)^2 &= m^2(x^2 + y^2 + z^2) \\ &= m^2(axyz + b) \\ &= am^{-1}(mx)(my)(mz) + bm^2\end{aligned}$$

Hence $(mx, my, mz) \in M_{am^{-1},bm^2}(\mathbb{F}_q^3)$. □

This means that the two degrees of freedom for choices of a and b can be broken down to just one. Using the mapping above, we have a bijection on the sets $M_{a,b}(\mathbb{F}_q^3)$ and $M_{1,ba^2}(\mathbb{F}_q^3)$, and because our goal is to find the order, we will only consider the set $M_{1,b}(\mathbb{F}_q^3)$ knowing there is a one-one correspondence to the generalized Hurwitz sets for other values of a.

2.2 The Special case of $M_{1,4}(\mathbb{F}_q^3)$

In this case, we can use the technique applied by Baragar [1] for the Markoff equation. In that case, the use of a birational map from $M_{3,0}(\mathbb{F}_q^3)$ to $\mathbb{P}^2$ was applied treating the singular point $(0, 0, 0)$ as a point at infinite. Note that $G\{(0, 0, 0)\}$ over this set consists of only one element. So to apply this technique we sought other points in $M_{1,b}(\mathbb{F}_q^3)$ whose G-orbit is also of order 1 over all fields. In other words

$$(x_0, x_1, x_2) = (x_1x_2 - x_0, x_1, x_2) = (x_0, x_0x_2 - x_1, x_2) = (x_0, x_1, x_0x_1 - x_2)$$

$$\Rightarrow \quad x_0 = x_1x_2 - x_0, \quad x_1 = x_0x_2 - x_1, \quad x_2 = x_0x_1 - x_2$$

$$\Rightarrow \quad 2x_0 = x_1x_2, \quad 2x_1 = x_0x_2, \quad 2x_2 = x_0x_1$$

Here we see that the only solutions to this system of equations over any finite field is $(0, 0, 0)$, which is always in $M_{1,0}(\mathbb{F}_q^3)$; and $(2, 2, 2)$, which is always an element of $M_{1,4}(\mathbb{F}_q^3)$. This suggests that the only candidate to use this technique is for the special case $M_{1,4}(\mathbb{F}_q^3)$ so we proceed in the same manner as Baragar using $(2,2,2)$ as a point at infinity in the birational mapping. (Note that for the fields $\mathbb{F}_q$ with characteristic 2, the triple $(2,2,2)$ is $(0,0,0)$.)

First let

$$\hat{x} = 2 - x \qquad \hat{y} = 2 - y \qquad \hat{z} = 2 - z$$

so our equation for $x^2 + y^2 + z^2 = xyz + 4$ becomes

$$(2-\hat{x})^2 + (2-\hat{y})^2 + (2-\hat{z})^2 = (2-\hat{x})(2-\hat{y})(2-\hat{z}) + 4$$

$$\hat{x}^2 + \hat{y}^2 + \hat{z}^2 - 4\hat{x} - 4\hat{y} - 4\hat{z} + 12 = 8 - 4\hat{x} - 4\hat{y} - 4\hat{z} + 2\hat{x}\hat{y} + 2\hat{x}\hat{z} + 2\hat{y}\hat{z} - \hat{x}\hat{y}\hat{z} + 4$$

and after cancellation we get

$$\hat{x}^2 + \hat{y}^2 + \hat{z}^2 = 2\hat{x}\hat{y} + 2\hat{x}\hat{z} + 2\hat{y}\hat{z} - \hat{x}\hat{y}\hat{z}.$$

Now suppose $\hat{z} \neq 0$, then we can write this equation as

$$\left(\frac{\hat{x}}{\hat{z}}\right)^2 + \left(\frac{\hat{y}}{\hat{z}}\right)^2 + 1 = 2\left(\frac{\hat{x}}{\hat{z}}\right)\left(\frac{\hat{y}}{\hat{z}}\right) + 2\left(\frac{\hat{x}}{\hat{z}}\right) + 2\left(\frac{\hat{y}}{\hat{z}}\right) - \left(\frac{\hat{x}}{\hat{z}}\right)\left(\frac{\hat{y}}{\hat{z}}\right)\hat{z}.$$

Now let

$$u = \frac{\hat{x}}{\hat{z}} = \frac{2-x}{2-z} \qquad v = \frac{\hat{y}}{\hat{z}} = \frac{2-y}{2-z}$$

giving us

$$u^2 + v^2 + 1 = 2uv + 2u + 2v - uv(2-z)$$

$$u^2 + v^2 + 1 = 2u + 2v + uvz.$$

Assuming that $uv \neq 0$ we solve for z

$$z = \frac{u^2 + v^2 + 1 - 2u - 2v}{uv}$$

which now enables us to put x and y in terms of u and v

$$x = \frac{u^2 + v^2 + 1 - 2uv - 2u}{v} \qquad y = \frac{u^2 + v^2 + 1 - 2uv - 2v}{u}.$$

We define the set L to be the set of elements taking into account our restrictions $uv \neq 0$ and $z \neq 2$

$$L = \left\{(u, v) \in \mathbb{F}_q^2 |\ uv \neq 0,\ u^2 + v^2 + 1 - 2u - 2v - 2uv \neq 0\right\}.$$

So now we have the one-to-one function

$$\varphi : L \to M_{1,4}(\mathbb{F}_q^3)$$

$$\varphi : (u, v) \longmapsto \left(\tfrac{u^2+v^2+1-2uv-2u}{v}, \tfrac{u^2+v^2+1-2uv-2v}{u}, \tfrac{u^2+v^2+1-2u-2v}{uv}\right)$$

where the elements of $M_{1,4}(\mathbb{F}_q^3)$ ommitted by φ is the set

$$S = \left\{(x, y, z) \in M_{1,4}(\mathbb{F}_q^3) |\ x = 2,\ y = 2,\ \text{or } z = 2\right\}.$$

This leads us to a partition of the set whose order we are interested in:

$$|M_{1,4}(\mathbb{F}_q^3)| = |L| + |S|.$$

We proceed by finding the order of S then L.

The set S is relatively easy to count. Assuming $x = 2$ we get

$$4 + y^2 + z^2 = 2yz + 4$$
$$y^2 - 2yx + z^2 = 0$$
$$(y - z)^2 = 0$$

but there are no zero-divisors in $\mathbb{F}_q$ which implies $y = z$, giving us q solutions. Thus letting $y = 2$ gives us q many solutions, and also $z = 2$ gives us q many more solutions, however the triple $(2, 2, 2)$ was over counted twice so

$$|S| = 3p - 2.$$

To count the size of L we consider the complement of L, the set

$$L^c = \left\{(u,v) \in \mathbb{F}_q^2 |\ uv = 0 \text{ or } u^2 + v^2 + 1 - 2u - 2v - 2uv = 0\right\}.$$

Knowing that $|L| + |L^c| = q^2$ it suffices to find $|L^c|$ in order to find $|L|$.

Counting the number of $(u,v) \in \mathbb{F}_q^2$ that satisfy the condition $uv = 0$ is not difficult. Again there are no zero-divisors in $\mathbb{F}_q$ so either $u = 0$ or $v = 0$. Assuming $u = 0$ there are q choices for v and like-wise for when $v = 0$. We double counted the single case where $(u,v) = (0,0)$ giving us $2p - 1$ such elements in L^c that satisfy the first condition.

To finish our count of L^c we must count the number of non-zero solutions to the equation given as the second condition of L^c. This is done by manipulating the equation

$$u^2 + v^2 + 1 - 2uv - 2u - 2v = 0$$

$$u^2 - 2uv + v^2 + 1 + 2u - 2v = 4u$$

$$(v-u)^2 - 2(v-u) + 1 = 4u$$

$$(v-u-1)^2 = 4u$$

$$v - u - 1 = \pm 2\sqrt{u}$$

$$v = u \pm 2\sqrt{u} + 1$$

$$v = (\sqrt{u} \pm 1)^2$$

implying that the $(u,v) \in L^c$ satisfying this condition must both be squares within $\mathbb{F}_q$ satisfying $(u, (\sqrt{u} \pm 1)^2)$. There are $\frac{q-1}{2}$ possibilities for u corresponding to the non-zero squares in $\mathbb{F}_q$ and for each u we have 2 unique v except for the case when $u = (\sqrt{u} \pm 1)^2$ which happens only when $u = 4^{-1}$. This means that we double count just once. Thus we have $2\left(\frac{q-1}{2}\right) - 1 = q - 2$ solutions to the second condition of L^c giving us

$$|L^c| = (2q-1) + (q-2) = 3q - 3$$

We now have enough information to compute $|M_{1,4}(\mathbb{F}_q^3)|$:

$$\begin{aligned} |M_{1,4}(\mathbb{F}_q^3)| &= |L| + |S| \\ &= q^2 - |L^c| + |S| \\ &= q^2 - (3q-3) + 3q - 2 \end{aligned}$$

so

$$|M_{1,4}(\mathbb{F}_q^3)| = q^2 + 1.$$

2.3 The Two Dimensional Case

So we have the order of the sets $M_{1,0}(\mathbb{F}_q^3)$ and $M_{1,4}(\mathbb{F}_q^3)$. To find the order of $M_{a,b}(\mathbb{F}_q^3)$ for all $a, b \in \mathbb{F}_q$ we first consider the two dimensional case of the generalized Hurwitz equation. That is, we consider

$$x^2 + y^2 = axy + b$$

over $\mathbb{F}_q$ and find $|M_{a,b}(\mathbb{F}_q^2)|$. The main result of this section is

Theorem 2.1: For $p \neq 2$, $q = p^m$, we have

$$|M_{a,b}(\mathbb{F}_q^2)| = \begin{cases} q & a = \pm 2,\ b = 0 \\ 2q & a = \pm 2,\ b \text{ is a nonzero quadratic residue} \\ 0 & a = \pm 2,\ b \text{ is a quadratic nonresidue} \\ 1 & b = 0,\ a^2 - 4 \text{ is a quadratic nonresidue} \\ 2q - 1 & b = 0,\ a^2 - 4 \text{ is a nonzero quadratic residue} \\ q - 1 & b \neq 0,\ a^2 - 4 \text{ is a nonzero quadratic residue} \\ q + 1 & b \neq 0,\ a^2 - 4 \text{ is a quadratic nonresidue} \end{cases}$$

For the first three cases, the number theory computations are elementary sowe omit their proof:

Case 1: $a = \pm 2$ and $b = 0$ yields q solutions.

Case 2: $a = \pm 2$ and b is a nonzero quadratic residue yields $2q$ solutions.

Case 3: $a = \pm 2$ and b is a quadratic nonresidue yields no solutions.

Next we compute the number of solutions to the less trivial cases.

Case 4 and **Case 5**: Let $b = 0$ and assume $a^2 - 4 \neq 0$.

Thus we have the equation $x^2 + y^2 = axy$. Note that $(0, 0)$ is the only solution in which y is zero. So assume $y \neq 0$ and write the equation $x^2 + y^2 = axy$ as

$$\left(\frac{x}{y}\right)^2 + 1 = a\left(\frac{x}{y}\right)$$

$$\left(\frac{x}{y}\right)^2 - a\frac{x}{y} + 1 = 0$$

$$\left(\frac{x}{y}\right)^2 - a\frac{x}{y} + \left(\frac{a}{2}\right)^2 - \left(\frac{a}{2}\right)^2 + 1 = 0$$

$$\left(\frac{x}{y} - \frac{a}{2}\right)^2 = \frac{a^2 - 4}{4}. \tag{2.1}$$

Thus the existence of any other solutions depend on whether the value $a^2 - 4$ is a square in $\mathbb{F}_q$. The case where a^2-4 is zero is covered in Case 1. If a^2-4 is a quadratic nonresidue, then Equation (2.1) has no solutions veryifying Case 4 where the only solution is $(0,0)$. If a^2-4 is a nonzero quadratic residue, then Equation (2.1) can be evaluated as

$$\frac{x}{y} = \frac{a}{2} \pm \frac{\sqrt{a^2-4}}{2}$$

implying that we are solving the two equations

$$\frac{x}{y} = \frac{a}{2} + \frac{\sqrt{a^2-4}}{2} \qquad \text{and} \qquad \frac{x}{y} = \frac{a}{2} - \frac{\sqrt{a^2-4}}{2}$$

or equivalently

$$\frac{x}{y} = c_1 \qquad \text{and} \qquad \frac{x}{y} = c_2$$

for $c_1, c_2 \in \mathbb{F}_q^*$ and $c_1 \neq c_2$. Knowing there are only $q-1$ choices for x and y (because we have ommited 0) we can deduce that there will be $2q-2$ solutions. Now taking into account the solution point $(0,0)$ implies that Case 5 gives $2q-1$ total solutions.

Before counting the number of solutions to Cases 6 and 7, we first simplify the equation $x^2 + y^2 = axyz + b$ by completing the square. So let $\bar{x} = x - \left(\frac{a}{2}\right) y$. Then

$$\begin{aligned} \left(\bar{x} + \frac{a}{2}y\right)^2 + y^2 &= a\left(\bar{x} + \frac{a}{2}y\right)y + b \\ \bar{x}^2 + a\bar{x}y + \left(\frac{a^2}{4}\right)y^2 + y^2 &= a\bar{x}y + \left(\frac{a^2}{2}\right)y^2 + b \\ \bar{x}^2 &= \left(\frac{a^2-4}{4}\right)y^2 + b. \end{aligned} \tag{2.2}$$

Thus in order to count the number of solutions to Cases 6 and 7 we need only count the number of solutions to Equation (2.2) under the same conditions. Note that if a^2-4 is a quadratic residue in $\mathbb{F}_q$ then so is $\frac{a^2-4}{4}$.

Case 6: Let $b \neq 0$ and assume a^2-4 is a non-zero quadratic residue.

By assumption we can let $k^2 = \frac{a^2-4}{4}$ with $k \in \mathbb{F}_q^*$. Using (2.2), we can apply another substitution where $u = k\left(\bar{x}+y\right)$ and $v = \bar{x} - y$ so (2.2) becomes

$$\begin{aligned}
\frac{a^2-4}{4}\left(u^2+2uv+v^2\right) &= \frac{a^2-4}{4}\left(u^2-2uv+v^2\right)+b \\
\frac{a^2-4}{4}(2uv)+\frac{a^2-4}{4}(2uv) &= b \\
uv &= \frac{b}{a^2-4}
\end{aligned}$$

By assumption we have that $\frac{b}{a^2-4} \neq 0$ and hence the equation above has exactly $q-1$ solutions over $\mathbb{F}_q$ verifying case 6.

Case 7: Let a^2-4 be a quadratic non-residue and $b \neq 0$.

To count the number of solutions to Equation (2.2), we note that it is equivalent to counting how often the term $\left(\frac{a^2-4}{4}\right)4y^2+b$ is a quadratic residue in $\mathbb{F}_q$ and how many times it is equal to zero. To do this we apply Theorems 1.13 and 1.14 depending on whether -1 and b are quadratic residues. We prove Case 7 for $-1 \in R_q$ and $b \in N_q$ and leave the other three cases to the reader, as the arguments are similar. So we want to know how often $\left(\frac{a^2-4}{4}\right)y^2+b$ or equivalently $N_q \cup \{0\}+n$, is a quadratic residue for some $n \in N_q$. We know that the set R_q+n consists of $\frac{q-1}{2}$ distinct elements exactly half of which are residues implying that the complement set $N_q \cup \{0\}+n$ must contain $\frac{q-1}{4}$ quadratic residues. Using the fact that the curve is symmetric with respect to x and y, we conclude that every quadratic residue in $n+N_q$ generates 4 solutions. Also note that based on our assumptions that $x=0$ is a solution and $y=0$ is not generating 2 more solutions giving us

$$4\left(\frac{q-1}{4}\right)+2(1) = q+1.$$

So again we have the total number of integral solutions to the generalized Hurwitz equation of two variables

Table 2.2: $|M_{a,b}(\mathbb{F}_{11}^2)|$ for all a and b

$b \backslash a$	0	1	2	3	4	5	6	7	8	9	10
0	1	1	11	21	21	1	1	21	21	11	1
1	1	1	11	10	10	12	12	10	10	22	12
2	12	12	22	10	10	12	12	10	10	0	12
3	12	12	0	10	10	12	12	10	10	22	12
4	12	12	22	10	10	12	12	10	10	22	12
5	12	12	22	10	10	12	12	10	10	22	12
6	12	12	22	10	10	12	12	10	10	0	12
7	12	12	0	10	10	12	12	10	10	0	12
8	12	12	0	10	10	12	12	10	10	0	12
9	12	12	0	10	10	12	12	10	10	22	12
10	12	12	22	10	10	12	12	10	10	0	12

$$|M_{a,b}(\mathbb{F}_q^2)| = \begin{cases} q & a = \pm 2,\ b = 0 \\ 2q & a = \pm 2,\ b \text{ is a nonzero quadratic residue} \\ 0 & a = \pm 2,\ b \text{ is a quadratic nonresidue} \\ 1 & b = 0,\ a^2 - 4 \text{ is a quadratic nonresidue} \\ 2q-1 & b = 0,\ a^2 - 4 \text{ is a nonzero quadratic residue} \\ q-1 & b \neq 0,\ a^2 - 4 \text{ is a nonzero quadratic residue} \\ q+1 & b \neq 0,\ a^2 - 4 \text{ is a quadratic nonresidue} \end{cases} . \tag{2.3}$$

Table 2.3 illustrates how the seven cases are visually clear as a and b change.

Note that we apply Case 6 exactly $\frac{q-3}{4}$ times and Case 7 exactly $\frac{q-1}{2}$ times. The way this is shown in general is by observing how often $a^2 - 4$ is a quadratic residue for all $a \in \mathbb{F}_q$ and this is done by applying Theorems 1.6 and 1.7.

2.4 The order of $M_{a,b}(\mathbb{F}_q^3)$

In this section we compute the order of the varieties $M_{1,b}(\mathbb{F}_q^3)$ by slicing the equation

$$x^2 + y^2 + z^2 = xyz + b \tag{2.4}$$

into two dimensional cases. Let us fix $z = k$ so Equation (2.4) becomes

$$x^2 + y^2 = kxy + (b - k^2). \tag{2.5}$$

This leads us to the formula

$$|M_{1,b}(\mathbb{F}_q^3)| = \sum_{k\in\mathbb{F}_q} |M_{k,b-k^2}(\mathbb{F}_q^2)|.$$

From here, we need to count how many times we apply each case from Equation (2.3). Clearly we can consider the cases when $k = \pm 2$ to arrive at

$$\begin{aligned} |M_{1,b}(\mathbb{F}_q^3)| &= \left|M_{2,b-4}(\mathbb{F}_q^2)\right| + \left|M_{-2,b-4}(\mathbb{F}_q^2)\right| + \sum_{k\in\mathbb{F}_q-\{\pm 2\}} |M_{k,b-k^2}(\mathbb{F}_q^2)| \\ &= 2\left|M_{2,b-4}(\mathbb{F}_q^2)\right| + \sum_{k\in\mathbb{F}_q-\{\pm 2\}} |M_{k,b-k^2}(\mathbb{F}_q^2)| \end{aligned} \tag{2.6}$$

but to continue isolating separate conditions of Equation (2.3), we consider four separate cases.

Case 1: Suppose b and $b-4$ are non-zero quadratic residues of $\mathbb{F}_q$.

If we want to isolate Cases 2 and 3 of Equation (2.3), then we let $k = \sqrt{b}$. Then Equation (2.6) becomes

$$\begin{aligned} |M_{1,b}(\mathbb{F}_q^3)| &= 2\left|M_{2,b-4}(\mathbb{F}_q^2)\right| + \left|M_{\sqrt{b},0}(\mathbb{F}_q^2)\right| + \left|M_{-\sqrt{b},0}(\mathbb{F}_q^2)\right| + \sum_{k\in\mathbb{F}_q-\left\{\pm 2,\pm\sqrt{b}\right\}} |M_{k,b-k^2}(\mathbb{F}_q^2)| \\ &= 2\left|M_{2,b-4}(\mathbb{F}_q^2)\right| + 2\left|M_{\sqrt{b},0}(\mathbb{F}_q^2)\right| + \sum_{k\in\mathbb{F}_q-\left\{\pm 2,\pm\sqrt{b}\right\}} |M_{k,b-k^2}(\mathbb{F}_q^2)|. \end{aligned}$$

Note that the term $\sum_{k\in\mathbb{F}_q-\{\pm 2,\pm\sqrt{b}\}} |M_{k,b-k^2}(\mathbb{F}_q^2)|$ is a sum of terms consisting of Case 6 and Case 7 of Equation (2.3). We know from Section 2.3 that Case 7 applies exactly $\left(\frac{q-1}{2}\right)$ times and that Case 6 applies exactly $\left(\frac{q-3}{2}-2\right)$, where we subtract 2 because we already considered the case when $k=\pm\sqrt{b}$. Lastly note the following equalities are based on Cases 2-5 of Equation (2.3)

$$|M_{2,b-4}(\mathbb{F}_q^2)| = \begin{cases} 0 & b-4 \text{ if is a quadratic nonresidue} \\ 2q & b-4 \text{ if is a non-zero quadratic residue} \end{cases}$$

$$|M_{\sqrt{b},0}(\mathbb{F}_q^2)| = \begin{cases} 1 & b-4 \text{ if is a quadratic nonresidue} \\ 2q-1 & b-4 \text{ if is a non-zero quadratic residue} \end{cases}$$

so since $b-4$ is a quadratic residue we have $|M_{2,b-4}(\mathbb{F}_q^2)| = 2q$ and $|M_{\sqrt{b},0}(\mathbb{F}_q^2)| = 2q-1$. Now we compute

$$\begin{aligned} |M_{1,b}(\mathbb{F}_q^3)| &= 2\left|M_{2,b-4}(\mathbb{F}_q^2)\right| + 2\left|M_{\sqrt{b},0}(\mathbb{F}_q^2)\right| + \sum_{k\in\mathbb{F}_q-\{\pm 2,\pm\sqrt{b}\}} |M_{k,b-k^2}(\mathbb{F}_q^2)| \\ &= 2\,(2q) + 2\,(2q-1) + \left(\frac{q-3}{2}-2\right)(q-1) + \left(\frac{q-1}{2}\right)(q+1) \\ &= 4q + 4q - 2 + \frac{q^2-8q+7}{2} + \frac{q^2-1}{2} \\ &= q^2+4q+1. \end{aligned}$$

Case 2: Suppose b is a quadratic residue of $\mathbb{F}_q$ and $b-4$ is a quadratic non-residue.

There are a couple of differences in calculation from these two cases. First note

$$|M_{2,b-4}(\mathbb{F}_q^2)| = \begin{cases} 0 & b-4 \text{ is a quadratic nonresidue} \\ 2q & b-4 \text{ is a non-zero quadratic residue} \end{cases}$$

$$|M_{\sqrt{b},0}(\mathbb{F}_q^2)| = \begin{cases} 1 & b-4 \text{ is a quadratic nonresidue} \\ 2q-1 & b-4 \text{ is a non-zero quadratic residue} \end{cases}$$

so since $b-4$ is a non-residue we have $|M_{2,b-4}(\mathbb{F}_q^2)| = 0$ and $|M_{\sqrt{b},0}(\mathbb{F}_q^2)| = 1$. The second difference is that $\left(\sqrt{b}\right)^2 - 4$ is not a quadratic residue and hence we must subtract 2 from the 4th term instead of the third, so

$$\begin{aligned} |M_{1,b}(\mathbb{F}_q^3)| &= 2\left|M_{2,b-4}(\mathbb{F}_q^2)\right| + 2\left|M_{\sqrt{b},0}(\mathbb{F}_q^2)\right| + \sum_{k\in\mathbb{F}_q - \left\{\pm 2, \pm\sqrt{b}\right\}} |M_{k,b-k^2}(\mathbb{F}_q^2)| \\ &= 2\,(0) + 2\,(1) + \left(\frac{q-3}{2}\right)(q-1) + \left(\frac{q-1}{2} - 2\right)(q+1) \\ &= 2 + \frac{q^2-4q+3}{2} + \frac{q^2-4q-5}{2} \\ &= q^2 - 4q + 1. \end{aligned}$$

Case 3: Suppose b is a quadratic nonresidue and $b-4$ is a non-zero quadratic residue of $\mathbb{F}_q$.

Note that the term $\left|M_{\sqrt{b},0}(\mathbb{F}_q^2)\right|$ in our first two cases will not exist when b is not a quadratic residue. This also means that we will not double count and hence not need to subtract by 2 as in the last two cases. Hence we have that

$$\begin{aligned} |M_{1,b}(\mathbb{F}_q^3)| &= 2\left|M_{2,b-4}(\mathbb{F}_q^2)\right| + \sum_{k\in\mathbb{F}_q - \left\{\pm 2, \pm\sqrt{b}\right\}} |M_{k,b-k^2}(\mathbb{F}_q^2)| \\ &= 2\,(2q) + \left(\frac{q-3}{2}\right)(q-1) + \left(\frac{q-1}{2}\right)(q+1) \\ &= 4q + \frac{q^2-4q+3}{2} + \frac{q^2-1}{2} \\ &= q^2 + 2q + 1. \end{aligned}$$

Case 4: Suppose b and $b-4$ are quadratic nonresidues of $\mathbb{F}_q$.

The computations in this case are similar to the previous case. The end result is

$$\begin{aligned}
|M_{1,b}(\mathbb{F}_q^3)| &= 2\left|M_{2,b-4}(\mathbb{F}_q^2)\right| + \sum_{k\in\mathbb{F}_q-\left\{\pm 2,\pm\sqrt{b}\right\}} |M_{k,b-k^2}(\mathbb{F}_q^2)| \\
&= 2\,(0) + \left(\frac{q-3}{2}\right)(q-1) + \left(\frac{q-1}{2}\right)(q+1) \\
&= 0 + \frac{q^2-4q+3}{2} + \frac{q^2-1}{2} \\
&= q^2 - 2q + 1.
\end{aligned}$$

We can also derive both $|M_{1,4}(\mathbb{F}_q^3)|$ and $|M_{1,0}(\mathbb{F}_q^3)|$ using this slicing method.

This gives us the formula

$$|M_{1,b}(\mathbb{F}_q^3)| = \begin{cases} q^2 + 3\epsilon q + 1 & b = 0 \\ q^2 + 2\epsilon q + 1 & b \text{ is a quadratic nonresidue} \\ q^2 + 4\epsilon q + 1 & b \text{ is a nonzero-quadratic residue} \end{cases}$$

where $\epsilon = \begin{cases} 1 & b-4 \text{ is a quadratic residue of } \mathbb{F}_q \\ -1 & b-4 \text{ is a quadratic nonresidue of } \mathbb{F}_q \\ 0 & b-4=0 \end{cases}$.

We showed in Section 2.1 that for $a \neq 0$ we have $|M_{a,b}(\mathbb{F}_q^3)| = |M_{1,ba^2}(\mathbb{F}_q^3)|$ but note that if b is a square in $\mathbb{F}_q$ then so is ba^2. Using these facts and the equation above, we can derive the order of $M_{a,b}(\mathbb{F}_q^3)$ for all $a, b \in \mathbb{F}_q$ given by

$$|M_{a,b}(\mathbb{F}_q^3)| = \begin{cases} q^2 + 3\epsilon q + 1 & b = 0 \\ q^2 + 2\epsilon q + 1 & b \text{ is a quadratic nonresidue} \\ q^2 + 4\epsilon q + 1 & b \text{ is a nonzero-quadratic residue} \end{cases}$$

where $\epsilon = \begin{cases} 1 & ba^2 - 4 \text{ is a quadratic residue of } \mathbb{F}_q \\ -1 & ba^2 - 4 \text{ is a quadratic nonresidue of } \mathbb{F}_q \\ 0 & ba^2 - 4 = 0 \end{cases}$.

In all cases we may write this formula in a more condensed manner as

$$|M_{a,b}(\mathbb{F}_q^3)| = q^2 + (3 + \delta)(\epsilon q) + 1 \tag{2.7}$$

by defining $\delta = \begin{cases} 1 & b \text{ is a quadratic residue of } \mathbb{F}_q \\ -1 & b \text{ is a quadratic nonresidue of } \mathbb{F}_q \\ 0 & b = 0 \end{cases}$.

We further note when $q = p^m$ we have $\epsilon = \left(\frac{ab^2-4}{p}\right)^m$ and $\delta = \left(\frac{b}{p}\right)^m$ (here we are using the Legendre symbol again).

2.5 The Zeta Function of $M_{a,b}\left(\mathbb{F}_q^3\right)$

Using Section 1.3, we compute the generating function of the variety $M_{a,b}(\mathbb{F}_q^3)$ to be

$$G(t) = \sum_{n=1}^{\infty} \left|M_{a,b}(\mathbb{F}_{q^n}^3)\right| \frac{t^n}{n}.$$

This series is computed over $\mathbb{Q}$, and our formula for $|M_{a,b}(\mathbb{F}_{q^n}^3)|$ depends on the quadratic reciprocity of b and $ab^2 - 4$ in $\mathbb{F}_{q^n}$ as the positive integer n increases. So again let us write $q = p^m$ with $p \neq 2$. Then we have

$$|M_{a,b}(\mathbb{F}_q^3)| = q^2 + (3 + \delta)(\epsilon q) + 1.$$

This gives us the generating function

$$G(t) = \sum_{n=1}^{\infty} \frac{\left(q^{2n} + (3 + \delta^n)(\epsilon q)^n + 1\right) t^n}{n}$$

$$G(t) = \sum_{n=1}^{\infty} \left(\frac{(q^2 t)^n}{n} + 3\frac{(\epsilon q t)^n}{n} + \frac{(\delta \epsilon q t)^n}{n} + \frac{t^n}{n}\right).$$

Using $\log(1-t) = -\sum_{k=1}^{\infty} \frac{t^k}{k}$

$$G(t) = -\log(1-q^2t) - 3\log(1-\epsilon qt) - \log(1-\epsilon\delta qt) - \log(1-t)$$

Which means we can solve for the local zeta function given by

$$\begin{aligned} Z\left(M_{a,b}(\mathbb{F}_q^3), t\right) &= e^{G(t)} \\ &= \frac{1}{(1-q^2t)(1-\epsilon qt)^3(1-\epsilon\delta qt)(1-t)}. \end{aligned}$$

A few more formulas that are necessary for the completion of the Hasse-Weil zeta function are for the case when $a = 0$ and when the characteristic is equal to 2.

The following is derived via the slicing technique on $\mathbb{F}_q$ with characteristic not equal to 2. The derivation for this formula is easier then that in section 2.5 so we omit the proof:

$$|M_{0,b}(\mathbb{F}_q^3)| = q^2 + \delta q.$$

When $q = 2^m$ with $a, b \in \mathbb{Z}_2$ we have

$$|M_{a,b}(\mathbb{Z}_2^3)| = \begin{cases} q^2 + \delta(-1)^m + 1 & \text{if } 2 \not| a \\ q^2 & \text{if } 2|a. \end{cases}$$

Thus the Hasse-Weil zeta function for the variety is

$$\zeta\left(M_{a,b}(\mathbb{Q}^3), s\right) =$$

$$Z_2(s) \prod_{p|a} \frac{1}{(1-p^{2-s})(1-\delta p^{1-s})} \prod_{p \not| a} \frac{1}{(1-p^{2-s})(1-\epsilon p^{1-s})^3(1-\epsilon\delta p^{1-s})(1-p^{-s})}$$

where

$$Z_2(s) = Z(M_{a,b}(\mathbb{Z}_2^3), s) = \begin{cases} \left(\frac{1}{(1-2^{2-s})(1-\delta 2^{1-s})(1-2^{-s})}\right) & \text{if } 2 \not| a \\ \left(\frac{1}{1-2^{2-s}}\right) & \text{if } 2|a. \end{cases}$$

2.6 Discussion on Future Work

We have $|M_{a,b}(\mathbb{F}_q^3)|$ for all a and b in $\mathbb{F}_q$ so a natural question is whether we can apply the same slicing method on the variety $M_{a,b}(\mathbb{F}_q^4)$ as well as higher values of n and we observe the difficulties that are encountered. Following the same technique in Section 2.4, we would proceed with the variety $|M_{1,0}(\mathbb{F}_q^4)|$ by fixing the variable $w = k$ like so;

$$x^2 + y^2 + z^2 + w^2 = xyzw$$

$$x^2 + y^2 + z^2 = kxyz - k^2$$

and after applying Equation (2.7) we get

$$\begin{aligned} |M_{1,0}(\mathbb{F}_q^4)| &= \sum_{k\in\mathbb{F}_q} |M_{k,-k^2}(\mathbb{F}_q^3)| \\ &= q^2 + \sum_{k\in\mathbb{F}_q^*} \left(q^2 + (3+\delta)(\epsilon q) + 1\right). \end{aligned}$$

Recall that

$$\epsilon = \begin{cases} 1 & -k^4 - 4 \text{ is a quadratic residue of } \mathbb{F}_q \\ -1 & -k^4 - 4 \text{ is a quadratic nonresidue of } \mathbb{F}_q \\ 0 & -k^4 - 4 = 0 \end{cases}$$

and

$$\delta = \begin{cases} 1 & -1 \text{ is a quadratic residue of } \mathbb{F}_q \\ -1 & -1 \text{ is a quadratic nonresidue of } \mathbb{F}_q \\ 0 & -1 = 0 \end{cases}.$$

so in order to find $|M_{1,0}(\mathbb{F}_q^4)|$ we would need to count how often the term $-k^4 - 4$ is a quadratic residue. We relied on Theorems 1.6 and 1.7 for previous cases but they cannot be applied here. This demonstrates that the difficulty in computing $|M_{a,b}(\mathbb{F}_q^n)|$

for higher values of n arise when trying to predict the terms that will be necessary to count.

Also there was a one-to-one correspondance between different varieties noticed in Section 2.1 that cannot always be applied here when $n > 3$ implying that there are still two degrees of freedom for $M_{a,b}(\mathbb{F}_q^n)$ in most cases.

BIBLIOGRAPHY

[1] A. Baragar, "The Markoff equation and equations of Hurwitz," (1991): Thesis (Ph.D.)Brown University

[2] A. Baragar, "The Markoff-Hurwitz equations over number fields," Rocky Mountain J. Math. **35** (2005): no. 3, 695-712.

[3] E. Bombieri, "Remarks on the analytic complexity of zeta functions," Analytic number theory **247** (1996): 21-30, London Math. Soc. Lecture Note Ser., Cambridge Univ. Press, Cambridge, 1997.

[4] B. Dwork, "On the rationality of the zeta function of an algebraic variety," Amer. J. Math. **82** (1960): 631-648.

[5] A. Grothendieck, "The cohomology theory of abstract algebraic varietie," Proc. Internat. Congress Math. (1960): Cambridge University Press, 103-118, (Edinburgh, 1958)

[6] J. Kelly, "A characteristic property of quadratic residues," Proc. Amer. Math. (1954): Soc. 5. 38-46.

[7] A. Markoff, *Sur les formes binaires indefinies*, Math. Ann. **17** (1880): 379-399.

[8] A. Weil, "Numbers of solutions of equations in finite fields," Bulletin of the AMS **55** (1949): 497-508.

VITA

Graduate College
University of Nevada, Las Vegas

Juan Mariscal

Degrees:
Bachelor of Science, 2009
University of California, Berkeley

Thesis Title:
The Zeta Function of Generalized Markoff Equations

Thesis Examination Committee:
Chairperson, Arthur Baragar, Ph.D.
Committee Member, Gennady Bachman, Ph.D.
Committee Member, Peter Shiue, Ph.D.
Graduate Faculty Representative, Evangelos Yfantis, Ph.D.