THE Z-DENSITIES OF THE FIBONACCI SEQUENCE

BY

PAUL CUBRE

A Thesis Submitted to the Graduate Faculty of

WAKE FOREST UNIVERSITY GRADUATE SCHOOL OF ARTS AND SCIENCES

in Partial Fulfillment of the Requirements

for the Degree of

MASTER OF ARTS

Mathematics

May 2012

Winston-Salem, North Carolina

Approved By:

Jeremy Rouse, Ph.D., Advisor

Fred Howard, Ph.D., Chair

Ellen Kirkman, Ph.D.

Acknowledgments

I would like to thank my parents for supporting me and always encouraging me to pursue my passions. If it were not for my parents and siblings encouragement to gain new experiences, then I would not have pursed my degree across the country. Also, I want to especially thank my advisor, Dr. Rouse, for giving me a challenging problem and having the patience needed to work with me.

Table of Contents

Abstract

Paul S. Bruckman and Peter G. Anderson made a conjecture about the Z-densities of the Fibonacci sequence, F_n, based on computational results. For a prime p, $Z(p)$ is the "Fibonacci entry-point of n" or the smallest positive integer n such that $p \mid F_n$, $M(m, x)$ is the number of primes $p \leq x$ such that $m \mid Z(p)$, and $\pi(x)$ is the number of primes less than x. We may define the "Z-density of m" to be $\zeta(m) = \lim_{x\to\infty} M(m, x)/\pi(x)$. The conjecture gives a formula for $\zeta(m)$ for all $m \geq 1$. We will prove the conjecture of Bruckman and Anderson by connecting $Z(p)$ with the order of the point $\alpha = (3/2, 1/2)$ in $G(\mathbb{F}_p) = \{(x, y) \in \mathbb{F}_p \mid x^2 - 5y^2 = 1\}$ and using the Chebotarev density theorem to find the limit.

Chapter 1: Introduction

The argument outlined in this paper belongs to the field of arithmetic dynamics. Silverman [12] describes a dynamical system as a set S and a function $\phi : S \to S$. We are interested in iterations of the map ϕ. Given a point $\alpha \in S$, the orbit of α is the set $\mathcal{O}_\phi(\alpha) = \{\phi^n(\alpha) : n \geq 0\}$. The goal of dynamics is to classify the points α in the set S by their orbits. In particular, we are interested in the simplest maps on algebraic groups. Let G be a group, g an element of G and $\phi : G \to G$ given by $\phi(g) = g^n$ or the n-th power map.

In arithmetic dynamics, we wish to study the intersection of number theory and dynamical systems. Silverman describes arithmetic dynamics as the theory of Diophantine equations in dynamical systems, where rational and integral points on varieties are rational or integral points in orbits. Some natural Diophantine equations that can be studied are the torus over a field K, of the form $\{(x, y) : x, y \in K, xy = 1\}$, twisted tori, of the form $x^2 - dy^2 = 1$ or elliptic curves. We are interested in particular the torus over $\mathbb{C}$ and the twisted torus $G(F) = \{(x, y) : x, y \in F, x^2 - 5y^2 = 1\}$ over a field F with group law $(x_1, y_1) \star (x_2, y_2) = (x_1x_2 + 5y_1y_2, x_1y_2 + x_2y_1)$.

An interest in arithmetic dynamics comes from the discrete log problem. Let $\mathbb{F}_q^\times$ denote the multiplicative group of $\mathbb{F}_q$. This group is known to be cyclic. If α is a generator for it, then for any x, $1 \leq x \leq q - 1$, it is easy to compute α^x. However, given an arbitrary $y \in \mathbb{F}_q^\times$, there is a unique x so that $y = \alpha^x$ and the computation problem of determining x given y is quite challenging. This one way function has applications in cryptography and is used by the Diffie-Hellman key exchange algorithm [3].

This thesis will also delve into probabilistic number theory, in particular, the theory of densities. Given a sequence $\mathcal{A}$ and a set $S \subset \mathbb{N}$ it is natural to ask what the probability that some $a \in \mathcal{A}$ is in S. An example, if we fix a positive integer n, the probability that a randomly chosen positive integer m is a multiple of n is $1/n$. Let λ_n take a value when n is in S and 0 otherwise. Then Tenebaum [15] defines a density $d(\mathcal{A})$ of a sequence $\mathcal{A} \subset S$ as the limit, when it exists, of the ratio $d(\mathcal{A};x) = \sum_{a \leq x, a \in \mathcal{A}} \lambda_a / \sum_{n \leq x} \lambda_n$. If $S = \mathbb{N}$ and $\lambda_n = 1$ for all $n \geq 1$ then the natural density, if the limit exists is $d\mathcal{A} := \lim_{x \to \infty} x^{-1} |\{a \leq x : a \in \mathcal{A}\}|$.

Given a sequence $\mathcal{A}$ we say $p \mid \mathcal{A}$ if and only if $p \mid a$ for some $a \in \mathcal{A}$ and let λ_n be 1 if n is prime and 0 otherwise. Let $\pi\mathcal{A}(x) = \sum_{a \leq x : a | \mathcal{A}} \lambda_a$ or the number of primes $p \leq x$ where $p \mid \mathcal{A}$. Similarly define $\pi(x) = \sum_{n \leq x} \lambda_n$ to be the number of primes less than x. Then the density of $\mathcal{A}$ is $\theta\mathcal{A} = \lim_{x \to \infty} \pi\mathcal{A}(x)/\pi(x)$.

An example of the connection between arithmetic dynamics and densities is for untwisted tori. Let $\alpha = (g, 1/g)$ be a point on $H(K) = \{(x,y) : x, y \in K, xy = 1\}$. Asking how often d divides the order of $\alpha \in H(\mathbb{F}_p)$ is equivalent to asking the order of $g \in \mathbb{F}_p^\times$ denoted $\operatorname{ord}_p(g)$. Given g, a rational number, and d, an integer, let $N_g(d)$ be the set of primes p such that $\operatorname{ord}_p(g)$ is divisible by d. In [11], Moree builds on previous work to estimate $N_g(d)(x)$ which is the set of primes less than x in $N_g(d)$ and the natural densities $\delta_g(d)$.

It is often the case that the study of arithmetic dynamics can shed light on divisibility properties of certain sequences. Jones and Rouse showed for the Somos 4-sequence defined by $a_0 = a_1 = a_2 = a_3 = 1$ and $a_n = (a_{n-1}a_{n-2} + a_{n-3}^2)/a_{n-4}$ for $n \geq 4$, the density of primes dividing at least one term in the sequence is $11/21$. They demonstrated the density by showing for the elliptic curve $E(K) = \{(x,y) : x, y \in K, y^2 + y = x^3 - x\}$, the order of the point $(0,0) \in E(\mathbb{F}_p)$ is odd if and only if a prime p divides a term in the Somos 4-sequence.

We wish to study a density involving the Fibonacci sequence, $\mathcal{F} = \{F_n\}_{n=0}^{\infty}$, where $F_0 = 0$, $F_1 = 1$ and $F_n = F_{n-1} + F_{n-2}$ for $n \geq 2$ and the Lucas sequence, $\mathcal{L} = \{L_n\}_{n=0}^{\infty}$, where $L_0 = 2$, $L_1 = 1$ and $L_n = L_{n-1} + L_{n-2}$ for $n \geq 2$. We say $Z(p)$ is the "Fibonacci entry-point of p" or the smallest positive integer n such that $p \mid F_n$. Using the notation of Anderson and Bruckman in [1], let $M(m,x) = \sum_{p \le x : m | Z(p)} \lambda_p$ be the number of primes p less than x such that $m \mid Z(p)$. Then define $\zeta(m)$, the "Z-density of m as a divisor," as $\zeta(m) = \lim_{x \to \infty} M(m,x)/\pi(x)$.

It is obvious $\zeta(1) = 1$. Running numerical calculations similar to Anderson and Bruckman we find for $x = 10^6$ that $M(m,x)/\pi(x)$ is the following:

m	$M(m,10^6)/\pi(10^6)$	Approx.	m	$M(m,10^6)/\pi(10^6)$	Approx.
1	1	1.0000	11	3607/39249	0.091900
2	26170/39249	0.66677	12	9817/78498	0.12506
3	14726/39249	0.37519	13	339/4361	0.077734
4	26143/78498	0.33304	14	7643/78498	0.097365
5	16351/78498	0.20830	15	6175/78498	0.078664
6	19661/78498	0.25046	16	365/4361	0.083696
7	1639/11214	0.14616	17	773/13083	0.059084
8	13073/78498	0.16654	18	727/8722	0.083352
9	9781/78498	0.12460	19	1373/26166	0.052473
10	6844/39249	0.17437	20	153/4361	0.035084.

In [9], Lagarias showed $\zeta(2) = 2/3$ as $\zeta(2) = \theta\mathcal{L}$. As a consequence of the work by Jones and Rouse [8], if q is a prime, $\zeta(q) = q/(q^2-1)$. Anderson and Bruckman in [1], conjectured from numerical calculations,

Conjecture 1.1. *If q is a prime,*

$$\zeta(q^j) = \begin{cases} 1 & \textit{if } j = 0, \\ \frac{q^{2-j}}{q^2-1} & \textit{if } j \ge 1. \end{cases} \tag{1.1}$$

Furthermore $\zeta(m) = \rho(m) \prod_{q^j || m} \zeta(q^j)$ where

$$\rho(m) = \begin{cases} 1 & \textit{if } 10 \nmid m, \\ 5/4 & \textit{if } m \equiv 10 \pmod{20}, \\ 1/2 & \textit{if } 20 \mid m. \end{cases} \tag{1.2}$$

Now we may compare the conjecture to our numerical calculations:

m	$M(m,10^6)/\pi(10^6)$	Approx.	$\zeta(m)$	Approx.
1	1	1.0000	1	1.0000
2	26170/39249	0.66677	2/3	0.66667
3	14726/39249	0.37519	3/8	0.37500
4	26143/78498	0.33304	1/3	0.33333
5	16351/78498	0.20830	5/24	0.20833
6	19661/78498	0.25046	1/4	0.25000
7	1639/11214	0.14616	7/48	0.14583
8	13073/78498	0.16654	1/6	0.16667
9	9781/78498	0.12460	1/8	0.12500
10	6844/39249	0.17437	25/144	0.17361
11	3607/39249	0.091900	11/120	0.091667
12	9817/78498	0.12506	1/8	0.12500
13	339/4361	0.077734	13/168	0.077381
14	7643/78498	0.097365	7/72	0.097222
15	6175/78498	0.078664	5/64	0.078125
16	365/4361	0.083696	1/12	0.083333
17	773/13083	0.059084	17/288	0.059028
18	727/8722	0.083352	1/12	0.083333
19	1373/26166	0.052473	19/360	0.052778
20	153/4361	0.035084	5/144	0.034722.

The main result of this thesis is the proof of their conjecture; along the way we will prove an intermediate conjecture by Anderson and Bruckman in [1].

Conjecture 1.2. *Let p be a prime and $\epsilon_p = \left(\frac{p}{5}\right)$. Given q, x, i, j, with $i \geq j \geq 0$, let $M(q,x;i,j)$, denote the number of $p \leq x$ such that $q^i \mid\mid (p - \epsilon_p)$ and $q^j \mid\mid Z(p)$. Then the "$q^i, q^j Z$-density." denoted $\zeta(q;i,j)$, is given as follows $\zeta(q;i,j) = \lim_{x\to\infty} M(q,x;i,j)/\phi(x)$. Then*

$$\zeta(q;i,j) = \begin{cases} \frac{q-2}{q-1} & \text{if } i = j = 0, \\ q^{-2i} & \text{if } i \geq 1, j = 0, \\ \frac{q-1}{q^{2i-j+1}} & \text{if } i \geq j \geq 1. \end{cases} \tag{1.3}$$

The proof follows from the study of the group $G(F)$. Since this group is abelian we will refer to the group operation as addition. We will show that the element $\alpha = (3/2, 1/2)$ iterated n times under group addition is $(L_{2n}/2, F_{2n}/2)$ when char $F \neq 2$. Additionally when $F = \mathbb{F}_p$, if the order of α is n then $F_{2n} \equiv 0 \pmod{p}$ and $L_{2n} \equiv 1 \pmod{p}$. Thereby we can recover the divisibility properties of the Fibonacci sequence by considering the order α in $G(\mathbb{F}_p)$. Hence we can relate $Z(p)$ to the order of $\alpha = (3/2, 1/2)$ in $G(\mathbb{F}_p)$, as is shown in Theorem 3.5.

We define a n-th preimage of α under l to be an element β such that β multiplied by l^n equal is to α. Then we may view preimages of α under l as elements in the group where the iterated l-th power map has α in its orbit. Let the power of l dividing α be $\mathrm{ord}_l(|\alpha|)$ and the power of l dividing G be $\mathrm{ord}_l(|G|)$. In Section 2.2, we show that we can derive $\mathrm{ord}_l(|\alpha|)$, from $\mathrm{ord}_l(|G|)$, and the number of preimages. In particular by Theorem 3.5 we have an explicit connection between $Z(p)$ and the order of α.

Therefore, we take all the preimages of α and adjoin their coordinates to $\mathbb{Q}$ yielding a field K. If p is an unramified in K, the Galois group of the field extension then can be used to recover the preimages that are in $G(\mathbb{F}_p)$ by finding the Frobenius maps that fix the preimage. (All but a finitely many primes are unramified.) Therefore, we can count the number of preimages in $G(\mathbb{F}_p)$ and the Frobenius tells us the order of the $G(\mathbb{F}_p)$, hence we know the order of α. Meanwhile, the Frobenius automorphism is used to count the equidistribution of primes ideals in the $\mathcal{O}_K$ by the Chebotarev Density Theorem 2.35.

In Chapter 2, we review background material about the Fibonacci and Lucas sequences, Galois Theory, and algebraic number theory necessary for this paper. Furthermore in Section 2.2 we make the precise connections between the power of a prime l dividing $Z(p)$, the power of l dividing the order of $\alpha \in G(\mathbb{F}_p)$, and the number of preimages of α under multiplication by l present in $G(\mathbb{F}_p)$. We then find all the preimages in $G(\mathbb{C})$ in Section 2.3.

In Chapter 3, we find the relation between $\alpha \in G(F)$ for F a field of characteristic not equal to 2 and the Fibonacci and Lucas sequences. We use this to establish the exact connection between $Z(p)$ and the order of $\alpha \in G(\mathbb{F}_p)$ in Theorem 3.5. Then we calculate the order of the Galois group of the number field created by adjoining the components of the preimages of α over

$\mathbb{C}$ in Section 3.2. We then account for all the considerations to apply the Chebotarev Density Theorem in 3.5. We prove Conjecture 1.2 in Theorem 3.23. Then we proceed to count all the conjugacy classes relating to each case of $\zeta(m)$. Then we finish proving the main Conjecture 1.1 in Theorem 3.25.

Chapter 2: Background

Again we have the Fibonacci sequence recursively defined by $F_0 = 0$, $F_1 = 1$, and $F_n = F_{n-1} + F_{n-2}$ for $n \geq 2$. The Lucas sequence is also recursively defined by $L_0 = 2$, $L_1 = 1$, and $L_n = L_{n-1} + L_{n-2}$ for $n \geq 2$. The following are some useful identities:

$$L_n^2 - 5F_n^2 = 4(-1)^n, \tag{2.1}$$

$$L_n^2 = L_{2n} + 2(-1)^n, \tag{2.2}$$

$$F_{2n} = F_n L_n, \tag{2.3}$$

$$5F_n = L_{n+1} + L_{n-1}, \tag{2.4}$$

$$L_n = F_{n+1} + F_{n-1}, \tag{2.5}$$

$$\gcd(F_m, F_n) = F_{\gcd(n,m)}. \tag{2.6}$$

2.1 Galois Theory and Algebraic Number Theory

The proof of the main conjecture relies heavily on algebra and algebraic number theory. We use Galois theory, and some of the following consequences.

Proposition 2.1 (Proposition 9 on pg. 520 in [4])**.** *Let α be algebraic over F. Then there is a unique monic irreducible polynomial $min_F(\alpha) \in F[x]$ which has α as a root. A polynomial $f(x) \in F[x]$ has α as a root if and only if $min_F(\alpha)$ divides $f(x)$ in $F[x]$.*

Lemma 2.2 (Lemma 18.3 on pg. 277 in [6])**.** *Let $F \subset E$ and write $G = Gal(E/F)$. Let $f \in F[x]$ with $f \neq 0$ and write $\Omega = \{\alpha \in E : f(\alpha) = 0\}$. Assuming that Ω is nonempty, the following hold.*

1. *The action of G on E permutes the elements of Ω.*

2. *If we assume that f is irreducible and also that E is a splitting field over F for some polynomial in $F[x]$, then G acts transitively Ω.*

Theorem 2.3. *[Theorem 18.22 on pg 288 in [6]] (Natural Irrationalities) Let $F \subset E \subset K$ be fields and suppose that E is Galois over F. Let $F \subset L \subset K$ and write $M = L \cap E$. Assume that no proper subfield of K contains both L and E. Then K is Galois over L, and the restriction of automorphisms to E defines an isomorphism of Gal(K/L) onto Gal(E/M). In particular, $|K : L| = |E : M|$.*

Proposition 2.4. *[Proposition 21 on pg 592 in [4]] Let K_1 and K_2 be Galois extensions of a field F. Then*

1. *The intersection $K_1 \cap K_2$ is Galois over F.*

2. *The composite $\langle K_1, K_2 \rangle$ is Galois over F. The Galois group, Gal$(\langle K_1, K_2 \rangle / F)$, is isomorphic to the subgroup*

$$H = \{(\sigma, \tau) : \sigma|_{K_1 \cap K_2} = \tau|_{K_1 \cap K_2}\}$$

of the direct product Gal$(K_1/F) \times$ Gal(K_2/F) consisting of elements whose restriction to the intersection $K_1 \cap K_2$ are equal.

Moreover,

$$|\langle K_1, K_2 \rangle : F| = \frac{|K_1 : F|\,|K_2 : F|}{|K_1 \cap K_2 : F|}.$$

We have the following definitions and consequences in algebraic number theory.

Definition 2.5 (pg. 36 in [14])**.** *A complex number α is algebraic if it is algebraic over $\mathbb{Q}$.*

Theorem 2.6 (Theorem 2.1 pg. 36 in [14])**.** *The set $\mathbb{A}$ of algebraic numbers is a subfield of the complex field $\mathbb{C}$.*

Definition 2.7 (Definition 1.10 on pg. 5 in [10]). *If α is an algebraic number we form the field $\mathbb{Q}(\alpha)$, we call this an algebraic number field over $\mathbb{Q}$.*

Definition 2.8 (pg. 42 in [14]). *A complex number α is is an algebraic integer if α is a root of a monic polynomial with integer coefficients.*

Definition 2.9 (Theorem 2.9 on pg. 43 in [14]). *The algebraic integers of a number field F form a subring of the field of algebraic numbers called the ring of (algebraic) integers in F, denoted $\mathcal{O}_F$.*

We have that $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$. Other examples of the rings of integers is for ζ_n is a n-th root of unity $\mathcal{O}_{\mathbb{Q}(\zeta_n)} = \mathbb{Z}[\zeta_n]$ and for d square free, if $d \equiv 1 \pmod 4$, $\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \mathbb{Z}[(1+\sqrt{d})/2]$ and $\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \mathbb{Z}[\sqrt{d}]$ otherwise.

Definition 2.10 (pg. 48 in [10]). *In a commutative ring R with identity, the units form a multiplicative group, denoted $\mathcal{U}_R$.*

Definition 2.11 (Definition 1.57 on pg. 34 in [10]). *(Integral Bases) If $\mathcal{O}_F$ is the ring of integers of an algebraic number field F, then a basis for $\mathcal{O}_F$ over $\mathbb{Z}$, or simply a $\mathbb{Z}$-basis, is called an integral basis for F.*

Definition 2.12 (Definition 1.74 on pg. 41 in [10]). *Let $\mathcal{B}$ be an integral basis for an algebraic number field F. Then the discriminant of F is disc($\mathcal{B}$), denoted Δ_F.*

We have a simplified version of Dirichlet's Unit Theorem.

Theorem 2.13 (Theorem 2.19 on pg. 77,80 in [10]). *Let $F = \mathbb{Q}(\sqrt{D})$, where $D > 1$ is squarefree integer. Then there exists a unique smallest unit $\epsilon_{\Delta_F} > 1$ in $\mathcal{U}_F$ such that for any $u \in \mathcal{U}_F$, there exists an $n \in \mathbb{Z}$ such that $u = \pm\epsilon_{\Delta_F}^n$. Furthermore $\epsilon_{\Delta_F} = (1+\sqrt{5})/2$ if $D = 5$.*

Theorem 2.14 (Theorem 2.32 on pg. 88 in [10]). *(Discriminants of Prime-Power Cyclotomic Fields) Let ζ_n be a primitive n-th root of unity and $F = \mathbb{Q}(\zeta_n)$. If $n = p^a$, then $\Delta_F = (-1)^{\phi(p^a)/2} p^{p^{a-1}(a(p-1)-1)}$ where ϕ is the Euler totient.*

Definition 2.15 (Definition 3.50 on pg. 153 in [10]). *(Fractional Ideals) Let R be an integral domain with quotient field F. A nonzero R-module M contained in F is called a fractional R-ideal provided that there exists a nonzero $\alpha \in R$ such that $\alpha M \subset R$.*

Definition 2.16 (Lemma 3.56 on pg. 154 in [10]). *If R is a Dedekind domain, then the set of all fractional ideals forms a multiplicative abelian group, denoted $\mathfrak{F}(R)$.*

Definition 2.17 (Definition 4.3 on pg. 194 in [10]). *(Ramification, Inertia, and Decomposition Numbers) Let K/F be an extension of number fields, and let $\mathfrak{p}$ be a prime $\mathcal{O}_F$-ideal with*

$$\mathfrak{p}\mathcal{O}_K = \prod_{j=1}^{g} \mathfrak{B}_j^{e_j}, e_j \in \mathbb{N}$$

where the $\mathfrak{B}_j$ are distinct, prime $\mathcal{O}_K$-ideals. We say that the prime $\mathcal{O}_K$-ideals $\mathfrak{B}_j$ lie over $\mathfrak{p}$, or above $\mathfrak{p}$. Also, $\mathfrak{p}$ is said to lie under the $\mathfrak{B}_j$. The number e_j is called the ramification index of $\mathfrak{B}_j$ in $\mathcal{O}_K$, denoted by

$$e_{K/F}\left(\mathfrak{B}_j\right).$$

Also, $\mathfrak{B}_j$ is said to be ramified in $\mathcal{O}_K$ if $e_{K/F}\left(\mathfrak{B}_j\right) > 1$, and $\mathfrak{p}$ is also said to be ramified in $\mathcal{O}_K$ as well. Furthermore, $\mathfrak{p}$ is said to be unramified in $\mathcal{O}_K$ provided that $e_{K/F}\left(\mathfrak{B}_j\right) = 1$ for each $j = 1, 2, \ldots, g$. The number g is called the decomposition number of $\mathfrak{p}$ in $\mathcal{O}_K$, denoted by

$$g_{K/F}(\mathfrak{p}).$$

The degree $|\mathcal{O}_K/\mathfrak{B}_j : \mathcal{O}_F/\mathfrak{p}|$ is called the inertial degree, or relative degree, of $\mathfrak{B}$ in $\mathcal{O}_K$, denoted by

$$f_{K/F}\left(\mathfrak{B}_j\right).$$

The fields $\mathcal{O}_K/\mathfrak{B}_j$ and $\mathcal{O}_F/\mathfrak{p}$ are called the residue class fields or simply residue fields at $\mathfrak{B}_j$ and $\mathfrak{p}$, respectively. Thus, $f_{K/F}(\mathfrak{B}_j)$ is the degree of the extension of these finite fields.

Definition 2.18 (Definition 4.8 on pg. 196 in [10])**.** *Let K/F be an extension of number fields with $|K : F| = n$, and let θ_j for $j = 1, 2, \ldots, n$ be all of the F-isomorphisms of K. Let $\alpha \in K$ and let*

$$N_{K/F}(\alpha) = \prod_{j=1}^{n} \theta_j(\alpha),$$

be the relative norm of α in K/F. Also, let

$$T_{K/F}(\alpha) = \sum_{j=1}^{n} \theta_j(\alpha),$$

be the relative trace of α in K/F.

Definition 2.19 (Definition 4.12 on pg. 197 in [10])**.** *Let K/F be an extension of number fields, and let $\mathfrak{B}$ be a prime $\mathcal{O}_K$-ideal above the unique prime $\mathcal{O}_F$-ideal $\mathfrak{p} = \mathfrak{B} \cap \mathcal{O}_F$. Set*

$$N^{K/F}(\mathfrak{B}) = \mathfrak{p}^{f_{K/F}(\mathfrak{B})},$$

and extend $N^{K/F}$ to all $I \in \mathfrak{F}(\mathcal{O}_K)$ by

$$N^{K/F}(I) = \prod_{j=1}^{n} \mathfrak{p}_{\mathrm{j}}{}^{a_j f_{K/F}(\mathfrak{B}_j)},$$

where

$$I = \prod_{j=1}^{n} \mathfrak{B}_j^{a_j},$$

as a product of distinct prime powers in $\mathcal{O}_K$ and where $\mathfrak{B}_j \cap \mathcal{O}_F = \mathfrak{p}_j$.

We need properties of norms.

Theorem 2.20 (Theorem 4.10 on pg. 197 in [10])**.** *If $F \subset K \subset L$ is a tower of number fields, then for $\alpha \in L$ the following holds.*

$$N_{L/F}(\alpha) = N_{K/F}(N_{L/K}(\alpha)), \text{ and } N_{L/F}(\alpha) \in F.$$

.

Lemma 2.21. *[Exercise 28 on pg. 619 in [4]] Let α be a root of the irreducible polynomial $f(x) \in F[x]$ and let $K = F(\alpha)$. Let D be the discriminant of $f(x)$. Then $D = (-1)^{n(n-1)/2} N_{K/F}(f'(\alpha))$, where $f'(x)$ is the derivative of $f(x)$.*

Definition 2.22 (Definition 4.31 on pg. 209 in [10])**.** *(The Dual - Codifferent) Let K/F be an extension of number fields, and let $I \in \mathfrak{F}(\mathcal{O}_F)$. Then*

$$I^* = \{\beta \in K : T_{K/F}(\beta I) \subset \mathcal{O}_F\}$$

is called the dual or codifferent of I over F, where $T_{K/F}(\beta I) \subset \mathcal{O}_F$ means $T_{K/F}(\beta\alpha) \in \mathcal{O}_F$ for all $\alpha \in I$.

Definition 2.23 (Definition 4.32 on pg. 209 in [10])**.** *(The Different) Let K/F be an extension of number fields, and let $I \in \mathfrak{F}(\mathcal{O}_F)$. Then the ideal $(I^*)^{-1} \in \mathfrak{F}(\mathcal{O}_F)$ is called the different of I over F, denoted by*

$$\mathcal{D}_{K/F}(I),$$

If $I = \mathcal{O}_K$, then $\mathcal{D}_{K/F}(I)$ is called the different of the extension K/F, denoted by

$$\mathcal{D}_{K/F}.$$

Definition 2.24 (Definition 4.34 on pg. 210 in [10])**.** *(Discriminant of a Relative Extension) Let K/F be an extension of number fields. Then the discriminant of K/F is $N^{K/F}(\mathcal{D}_{K/F})$, denoted by $\Delta_{K/F}$. In particular, $\Delta_{K/\mathbb{Q}} = \Delta_K$ is called the absolute discriminant of K*

Theorem 2.25 (Theorem 4.62 on pg. 221 in [10]). *If $\mathfrak{B}$ is a prime $\mathcal{O}_K$-ideal, then $\mathfrak{B}$ ramifies in K/F if and only if $\mathfrak{B} \mid \mathcal{D}_{K/F}$. Consequently, there are only finitely many ramified primes in K/F.*

Theorem 2.26 (Theorem 4.63 on pg. 221 in [10]). *A prime $\mathcal{O}_F$-ideal $\mathfrak{p}$ ramifies in K if and only if $\mathfrak{p} \mid \Delta_{K/F}$.*

Theorem 2.27. *[Theorem 4.67 on pg. 223 in [10]] (Ramification in a Compositum of Number Fields) Let the number fields K_j for $j = 1, 2$ be extensions of the number field F, and let $L = K_1K_2$ be the compositum of K_1 and K_2 over F. Then a prime $\mathcal{O}_F$-ideal $\mathfrak{p}$ divides $\Delta_{L/F}$ if and only if it divides $\Delta_{K_1/F}\Delta_{K_2/F}$.*

Definition 2.28 (pg. 101 in [2]). *Let $K \subset L$ be Galois, and let $\mathfrak{B}$ be a prime of L. Then the decomposition group and the inertia group of $\mathfrak{B}$ are defined by*

$$D_{\mathfrak{B}} = \{\sigma \in \mathit{Gal}(L/K) : \sigma(\mathfrak{B}) = \mathfrak{B}\}, \tag{2.7}$$

$$I_{\mathfrak{B}} = \{\sigma \in \mathit{Gal}(L/K) : \sigma(\alpha) \equiv \alpha \mod \mathfrak{B} \text{ for all } \alpha \in \mathcal{O}_L\}. \tag{2.8}$$

Let $\tilde{G}$ denote the Galois group of $\mathcal{O}_K/\mathfrak{p} \subset \mathcal{O}_L/\mathfrak{B}$.

Proposition 2.29 (Proposition 5.10 on pg. 102 in [2]). *Let $D_{\mathfrak{B}}$, $I_{\mathfrak{B}}$ and $\tilde{G}$ be as above.*

1. *The homomorphism $D_{\mathfrak{B}} \to \tilde{G}$ is surjective. Thus $D_{\mathfrak{B}}/I_{\mathfrak{B}} \cong \tilde{G}$.*
2. *$|I_{\mathfrak{B}}| = e_{\mathfrak{B}|\mathfrak{p}}$ and $|D_{\mathfrak{B}}| = e_{\mathfrak{B}|\mathfrak{p}}f_{\mathfrak{B}|\mathfrak{p}}$.*

Definition 2.30. *[Definition 4.99 on pg. 240 in [10]] If K/F is a Galois extension of number fields, and $\mathfrak{B}$ is a prime $\mathcal{O}_K$-ideal unramified in K/F with $\mathfrak{B} \cap \mathcal{O}_F = \mathfrak{p}$, then $D_{\mathfrak{B}}$ is cyclic and has generator:*

$$\left(\frac{K/F}{\mathfrak{B}}\right),$$

called the Frobenius automorphism of $\mathfrak{B}$ *in* K/F*, given by*

$$\left(\frac{K/F}{\mathfrak{B}}\right)(\alpha) \equiv \alpha^{N^{F/\mathbb{Q}}(\mathfrak{p})} \pmod{\mathfrak{B}}.$$

When $Gal(K/F)$ *is abelian, then the Frobenius automorphism depends only on* $\mathfrak{p}$ *and we write*

$$\left(\frac{K/F}{\mathfrak{p}}\right)(\alpha) \equiv \alpha^{N^{F/\mathbb{Q}}(\mathfrak{p})} \pmod{\mathfrak{p}\mathcal{O}_K},$$

where as usual $\mathfrak{p}\mathcal{O}_K$ *is the product of the prime* $\mathcal{O}_K$*-ideals lying over* $\mathfrak{p}$*. In this abelian case,* $\left(\frac{K/F}{\mathfrak{p}}\right)$ *is also called the Artin symbol.*

Definition 2.31 (pg. 127 in [7])**.** *If* $K \subset E \subset L$ *and both* E *and* L *Galois extensions over* K*, then*

$$res_E : Gal(L/K) \to Gal(E/K)$$

is the map $res_E(\sigma) =$ *restriction of* σ *to* E *defined by* $res_E(\sigma)(x) = \sigma(x)$ *for* $x \in E$*.*

Claim 2.32. *[Property 2.3 on pg. 127 in [7]] (Change of Extension Field) Let* $K \subset E \subset L$ *be a chain of fields with both* E *and* L *Galois over* K*. Let* $\mathfrak{p} = \mathfrak{B} \cap E$*. Then*

$$\left(\frac{E/K}{\mathfrak{p}}\right) = res_E \left(\frac{L/K}{\mathfrak{B}}\right).$$

Claim 2.33. *[Property 2.4 on pg. 127 in [7]] Suppose* $K \subset E, F \subset L$ *with* E, F *and* L *Galois over* K*. Let* $\mathfrak{p}_E = \mathfrak{B} \cap E$ *and* $\mathfrak{p}_F = \mathfrak{B} \cap F$*. Assume* $L = EF$*. The mapping* $\sigma \to (res_E(\sigma), res_F(\sigma))$ *of* $Gal(L/K)$ *into* $Gal(E/K) \times Gal(F/K)$ *has the effect*

$$\left(\frac{EF/K}{\mathfrak{B}}\right) \to \left(\frac{E/K}{\mathfrak{p}_E}\right) \times \left(\frac{F/K}{\mathfrak{p}_F}\right).$$

Definition 2.34 (pg. 9 in [13]). *A set S of prime numbers has density δ if*

$$\lim_{x\to\infty} \frac{\#\{p \leq x : p \in S\}}{\#\{p \leq x : p \text{ prime}\}} = \delta.$$

This is called natural density.

Theorem 2.35 (pg. 15 in [13]). *(Chebotarev Density Theorem) Let f be a monic polynomial in $\mathbb{Z}[x]$. Assume that the discriminant $\Delta(f)$ of f does not vanish. Let $\mathcal{C}$ be a conjugacy class of the Galois group $Gal(K/\mathbb{Q})$ of f. Then the set of primes p not dividing $\Delta(f)$ for which the Frobenius automorphism belongs to $\mathcal{C}$ has a density, and this density equals $\#\mathcal{C}/\#Gal(K/\mathbb{Q})$ [13].*

Corollary 2.36 (Corollary 6.3.2 on pg. 114 in [5]). *(Dirichlet) Suppose a and n are relatively prime positive integers. Then the density of $\{p \in P(\mathbb{Q}) : p \equiv a \pmod{n}\}$ is $\frac{1}{\phi(n)}$, where $\phi(n)$ is the Euler totient function.*

2.2 Preimages

We motivate the theorem in this section as necessary to establish the relation between the order of $G(\mathbb{F}_p)$ and order of the element $\alpha = (3/2, 1/2) \in G(\mathbb{F}_p)$.

Definition 2.37. *Let G be a group, α an element of G, and n, l integers. Then a nth preimage of α under l exists if there exists a $\beta \in G$ such that $l^n\beta = \alpha$.*

In the following suppose G is a cyclic group, α is an element in G and l, i, j are integers.

Claim 2.38. *Suppose $\alpha, \beta \in G$ and $l^n\beta = \alpha$. If the order of α is a multiple of l, then the order of β is a multiple of l^{n+1}.*

Proof. Let $|\alpha|$ be the order of α. Then $ml = |\alpha|$ for some integer m. Then $1 = ml\alpha = ml \cdot l^n\beta$, hence $|\beta| \mid ml^{n+1}$. Therefore $|\beta|r = ml^{n+1}$. Suppose $r > 1$. We have $r \mid ml^{n+1}$ therefore

$\gcd(r, ml^{n+1}) = r$ and $\gcd(r, ml) \cdot s = r$. Then $1 = s\,|\beta|\,\beta = \frac{ml}{\gcd(r,ml)}\alpha$ which is a contradiction to the order of α unless $\gcd(r, ml) = 1$ but $r \mid ml^{n+1}$ implies $r = 1$. Hence $|\beta| = ml^{n+1}$. □

Lemma 2.39. *The number l is coprime to $|\alpha|$ if and only if there exist infinitely many preimages of α under l.*

Proof. Let $\phi : G \to \phi(G)$ be a homomorphism and let $H = \langle\alpha\rangle$ be the subgroup generated by α in G where $\phi|_H\colon \alpha \mapsto \alpha^l$.

Claim 2.40. *The map $\phi|_H\colon H \to H$ is a group isomorphism if and only if l is coprime to $|\alpha| = n$.*

Proof. $\to$ Suppose that l is not coprime to the order of α. Let $d > 1$ be a divisor of n and l. Then there is an element in H that has order d. This is a contradiction as ϕ is an isomorphism and 1 is the only element such that $1^l = 1$.
$\leftarrow$ If l is coprime to n then $1 = lx + ny$. Let $\psi : H \to \psi(H)$ be given by $\psi : \alpha \mapsto \alpha^x$. Then $(\psi \circ \phi|_H)(\alpha) = (\alpha^l)^x = \alpha^{1-ny} = \alpha$. Similarly $(\phi|_H \circ \psi)(\alpha) = \alpha$. We may conclude ψ is the inverse of $\phi|_H$, therefore $\phi|_H$ is an isomorphism. □

For any $n \geq 1$, let $\beta = \psi^n(\alpha)$. Then $\alpha = l^n\beta$. □

Lemma 2.41. *Suppose i is coprime to $|\alpha|$, and there exist n preimages of α under j. Then there exist n preimages of α under ij.*

Proof. Let β be a preimage of α under j. Then we know $1 = |\alpha|\,\alpha = |\alpha|\,j^n\beta$. This yields $|\beta|\,\big|\,j^n\,|\alpha|$ thus i and $|\beta|$ are coprime. We may write $ix + |\beta|\,y = 1$ for some x and y. Therefore letting $\bar{\beta} = x^n\beta$, we have $(ij)^n(\bar{\beta}) = (ji)^n(x^n\beta) = (j)^n(ix)^n\beta = j^n(1 - |\beta|\,y)^n\beta = j^n\beta = \alpha$. Hence for each preimage of α under j, we may construct a preimage of α under ij. □

Lemma 2.42. *Suppose G is a cyclic group, $\alpha \in G$, and l is a integer with $m = ord_l(|G|)$ and $n = ord_l(|\alpha|)$. Then there exist $m - n$ preimages of α under l.*

Proof. Let γ be a generator of G and let $\alpha = s\gamma$. As $1 = |\alpha|\,\alpha$, then $1 = s\,|\alpha|\,\gamma$. We know $|G|\big|s\,|\alpha|$ which implies $|G|\,t = s\,|\alpha|$ and $s = \frac{t|G|}{|\alpha|}$. Then $\alpha = \frac{t|G|}{|\alpha|}\gamma$ or $\alpha = l^k \frac{t|G|}{l^k|\alpha|}\gamma$ with $1 \leq k \leq m-n$. This implies that there exist $m-n$ preimages of α under l where $\beta_k = \frac{t|G|}{l^k|\alpha|}\gamma$. □

Theorem 2.43. *If G is a cyclic group, α is an element of G, and l, i, j integers,*

1. *if l coprime to $|\alpha|$, then there are infinitely many preimages of α under l.*
2. *if when $l = i * j$ with i coprime to $|\alpha|$, $n = ord_j(|\alpha|)$ and $m = ord_j(|G|)$, then there are $m - n$ preimages of α under l.*

Proof. Lemma 2.39 proves case i and Lemma 2.41 and 2.42 prove case ii. As there exist $m - n$ preimages of α for $l = j$, there are $m - n$ preimages of α for $l = ij$. □

2.3 The Group G Over $\mathbb{C}$

We wish to look at $G(\mathbb{C}) = \{(x, y) \in \mathbb{C} : x^2 - 5y^2 = 1\}$ such that when we can create number fields using that have all the preimages of α under m some positive integer.

Lemma 2.44. *Suppose K is a field and there is an element $a \in K$ with $a^2 = 5$. Let*

$$G(K) = \left\{(x, y) \in K : x^2 - 5y^2 = 1\right\}, \tag{2.9}$$

$$H(K) = \{(u, v) \in K : uv = 1\}. \tag{2.10}$$

The set $G(K)$ is a group with the group operation $(x_1, y_1) \star (x_2, y_2) = (x_1x_2 + 5y_1y_2, x_1y_2 + x_2y_1)$ and identity $(1, 0)$. The set $H(K)$ also is a group with the group operation given by $(u_1, v_1) \star (u_2, v_2) = (u_1u_2, v_1v_2)$ and identity $(1, 1)$. Then the map

$$\phi : G(K) \to H(K)$$

given by $\phi(x,y) = (x+ay, x-ay)$ is an isomorphism between $G(K)$ and $H(K)$.

Proof. It can be easily shown that $G(K)$ and $H(K)$ are groups and ϕ is a group homomorphism. We observe that if $(x,y) \in H(K)$ then $\phi(((x+y)/2, (x-y)/2a)) = (x,y)$ and $((x+y)/2, (x-y)/2a)$ satisfies $((x+y)/2)^2 - 5((x-y)/2a)^2 = (x^2+y^2+2xy-x^2-y^2+2xy)/(4) = 4xy/4 = xy = 1$. Therefore the homomorphism, ϕ, is surjective. We look at $\ker\phi = \{(x,y) \in G(K) \mid \phi(x,y) = (1,1)\} = \{(x,y) \in G(K) \mid x+ay = 1 \text{ and } x-ay = 1\}$. Subtracting $x+ay = 1$ and $x-ay = 1$ we have that $2ay = 0$. As K is an integral domain and $a \neq 0$ then $y = 0$. Hence $x = 1$ and the kernel has exactly 1 element and therefore ϕ is injective. □

Lemma 2.45. *The group $H(K)$ is isomorphic to $K^\times$.*

Proof. Let $\phi((u,v)) = u$. It can be easily checked that ϕ is a homomorphism. Moreover u are the units of K hence we have isomorphism. □

Now we explicitly compute elements of $G(\mathbb{C})$.

Lemma 2.46. *Let $\alpha = (3/2, 1/2) \in G(\mathbb{C})$ and let $m \geq 1$ be a positive integer. Then there are m points $\beta \in G(\mathbb{C})$ that satisfy $m\beta = \alpha$ and m points of order dividing $m \in G(\mathbb{C})$.*

Proof. We will map α to $H(\mathbb{C})$. Hence we may rewrite $\phi(\alpha) = \left(\frac{3+a}{2}, \frac{3-a}{2}\right)$. We then take the m-th root of $\phi(\alpha) \in H(\mathbb{C})$ yielding m elements of the form $(\gamma\zeta_m^r, \gamma^{-1}\zeta_m^{-r})$ for $0 \leq r \leq m-1$ where $\gamma = \sqrt[m]{\frac{3+a}{2}}$ and ζ_m is a mth root of unity.

Let β_r be the pullback of $\phi(\beta_r) = (\gamma\zeta_m^r, \gamma^{-1}\zeta_m^{-r})$. Thus there are m points β_r such that $m\beta_r = \alpha$. We will compute β_r. The inverse of ϕ is given by $\phi^{-1}(e,f) = ((e+f)/2, (e-f)/2a)$. Then $\beta_r = ((\gamma\zeta_m^r + \gamma^{-1}\zeta_m^{-r})/2, (\gamma\zeta_m^r - \gamma^{-1}\zeta_m^{-r}/2a)$. Define $Q_{i,j}$ to be $\beta_i - \beta_j$ which means $Q_{i,j}$

has order dividing m. Calculating $Q_{i,j}$ we have:

$$\phi(\beta_i - \beta_j) = \phi(\beta_i)\phi(\beta_j)^{-1} = (\zeta_m^{i-j}, \zeta_m^{-(i-j)}), \tag{2.11}$$

$$Q_{i,j} = \phi^{-1}(\zeta_m^{i-j}, \zeta_m^{-(i-j)}) = \left(\frac{\zeta_m^{i-j} + \zeta_m^{-(i-j)}}{2}, \frac{\zeta_m^{i-j} - \zeta_m^{-(i-j)}}{2a}\right). \tag{2.12}$$

Thus as $0 \le i - j \le m - 1$, we have m points of order dividing m. □

If let $k = i - j$, then $Q_k = Q_{i,j}$ and $P_i = \beta_i$. We can then also have the following computation:

$$tQ_1 = \phi(\beta_2)^t\phi(\beta_1)^{-t} = \phi(\beta_{2t})\phi(\beta_t)^{-1} = Q_t, \tag{2.13}$$

$$P_0 + Q_t = \phi(\beta_0 + \beta_{2t} - \beta_t) = \phi(\beta_0)\phi(\beta_2)^t\phi(\beta_1)^{-t} = \phi(\beta_t) = P_t. \tag{2.14}$$

Chapter 3: Proof of the Conjecture

3.1 The Group G Over a Finite Field

We begin the proof by looking at the arithmetic dynamics of a group over a finite field with equation $x^2 - 5y^2 = 1$.

Lemma 3.1. *Let F be a field of characteristic p. Then*

$$G(\mathbb{F}_p) = \{(x, y) : x, y \in \mathbb{F}_p : x^2 - 5y^2 = 1\}$$

with the binary operation $(x_1, y_1) \star (x_2, y_2) = (x_1x_2 + 5y_1y_2, x_1y_2 + x_2y_1)$ defines a group.

Proof. The group $G(\mathbb{F}_p)$ satisfies the associate law, with inverses that negate the second coordinate, and has the identity $(1, 0)$. □

In the following lemma we make the observation that the Fibonacci numbers and Lucas numbers are intertwined with the group.

Lemma 3.2. *Let $\alpha = (3/2, 1/2) \in G(\mathbb{F}_p)$. Let F_n be the sequence of Fibonacci numbers defined by $F_0 = 0$, $F_1 = 1$ and $F_n = F_{n-1} + F_{n-2}$, and let L_n be the sequence of Lucas numbers defined by $L_0 = 2$, $L_1 = 1$, and $L_n = L_{n-1} + L_{n-2}$. Let $n\alpha = \overbrace{\alpha \star \alpha \star \cdots \star \alpha}^{n \text{ times}}$ where $n\alpha$ is α added n times with itself under the group law. Then $n\alpha = (L_{2n}/2, F_{2n}/2)$.*

Proof. (Proof by induction on n). The base case for $n = 1$ is given by $1 * (3/2, 1/2) = (L_2/2, F_2/2)$. The induction hypothesis for n is $n(3/2, 1/2) = (L_{2n}/2, F_{2n}/2)$. Subsequently, we want to show that $(n+1)(3/2, 1/2) = (L_{2n+2}/2, F_{2n+2}/2)$ for the $n+1$ case. First, we break down $(n+1)(3/2, 1/2)$, apply the hypothesis and expand.

$$\begin{aligned}
(n+1)\left(\frac{3}{2}, \frac{1}{2}\right) &= n\left(\frac{3}{2}, \frac{1}{2}\right) \star \left(\frac{3}{2}, \frac{1}{2}\right) \\
&= \left(\frac{L_{2n}}{2}, \frac{F_{2n}}{2}\right) \star \left(\frac{3}{2}, \frac{1}{2}\right) \\
&= \left(\frac{3L_{2n} + 5F_{2n}}{4}, \frac{L_{2n} + 3F_{2n}}{4}\right). \qquad (3.1)
\end{aligned}$$

We work on the first component and apply the identity $5F_n = L_{n+1} + L_{n-1}$ and the definition of the Lucas sequence. We get

$$\begin{aligned}
3L_{2n} + 5F_{2n} &= 3L_{2n} + L_{2n+1} + L_{2n-1} \\
&= 3L_{2n} + 2L_{2n+1} - L_{2n} \\
&= 2(L_{2n} + L_{2n+1}) \\
&= 2L_{2n+2}. \qquad (3.2)
\end{aligned}$$

We apply the identity $L_n = F_{n+1} + F_{n-1}$ and the definition of the Fibonacci sequence to transform the second component. We get

$$\begin{aligned}
L_{2n} + 3F_{2n} &= F_{2n+1} + F_{2n-1} + 3F_{2n} \\
&= F_{2n+1} + F_{2n+1} - F_{2n} + 3F_{2n} \\
&= 2(F_{2n+1} + F_{2n}) \\
&= 2F_{2n+2}. \qquad (3.3)
\end{aligned}$$

Thus $\left(\frac{3L_{2n}+5F_{2n}}{4}, \frac{L_{2n}+3F_{2n}}{4}\right) = \left(\frac{L_{2n+2}}{2}, \frac{F_{2n+2}}{2}\right)$ and our induction is finished. □

Lemma 3.3. *The group $G(\mathbb{F}_p)$ is cyclic.*

Proof. We will prove this for two cases: $\sqrt{5} \in \mathbb{F}_p$, and $\sqrt{5} \notin \mathbb{F}_p$ that correspond to $p \equiv 1, 4 \pmod 5$ and $p \equiv 2, 3 \pmod 5$ respectively. The case $p = 5$ can be easily checked. If $\sqrt{5} \in \mathbb{F}_p$, then by Lemma 2.44 and 2.45, we have $G(\mathbb{F}_p) \cong \mathbb{F}_p^\times$ which is a cyclic group. If $\sqrt{5} \notin \mathbb{F}_p$, then $\sqrt{5} \in \mathbb{F}_p[\sqrt{5}] \cong \mathbb{F}_{p^2}$. By Lemma 2.44 and 2.45, we have $G(\mathbb{F}_{p^2}) \cong \mathbb{F}_{p^2}^\times$ which is cyclic. Then $G(\mathbb{F}_p)$ is a subgroup of $G(\mathbb{F}_{p^2})$. □

Theorem 3.4. *Let p be a prime and $G(\mathbb{F}_p)$ be as defined before. Then the order of $G(\mathbb{F}_p)$ is*

$$|G(\mathbb{F}_p)| = \begin{cases} 2 & \text{if } p = 2, \\ 10 & \text{if } p = 5, \\ p+1 & \text{if } p = 5k+2 \text{ or } 5k+3, \\ p-1 & \text{if } p = 5k+1 \text{ or } 5k+4. \end{cases} \tag{3.4}$$

Proof. We first proof the simple cases. If $p = 2$, then $(1, 0)$ and $(0, 1)$ are the only two elements of the group. When $p = 5$, then the order is 10 as the set restriction reduces to $x^2 = 1$ and there are two solutions for x and five choices for y.

In order to solve the general case we parametrize the solutions to $x^2 - 5y^2 = 1$ for $p \neq 2, 5$. We can do so by letting (a, b) be a solution to $x^2 - 5y^2 = 1$ and drawing a line through the point $(1, 0)$. The slope of the line is rational if and only if the point (a, b) is a rational solution. Note that $\pmod p$ and rational are interchangeable. Hence, for some $m \pmod p$, all elements in the group satisfy $y \equiv m(x-1) \pmod p$. Plugging in for y from the group law, we simplify to get the equation $(1-5m^2)x^2 = 10m^2x - (5m^2+1) = 0$. Solving the quadratic equation for x yields $x = \frac{5m^2+1}{5m^2-1}$ and $y = \frac{2m}{5m^2-1}$.

As m lives in $\mathbb{F}_p$, the formulas above yield p possible elements of which none are $(1, 0)$. However, it is possible that different values of m produce the same elements. Suppose we have $m_1 \neq m_2$. Then $(5m_1^2+1)(5m_2^2-1) \equiv (5m_2^2+1)(5m_1^2-1)$ and $(2m_1)(5m_2^2-1) \equiv (2m_2)(5m_1^2-1)$. These equations reduce to $(m_1 + m_2) \equiv 0$ and $5m_1m_2 + 1 \equiv 0$, respectively. This implies the p solutions are not unique only for the case when $5m^2 - 1 \equiv 0$. When $5m^2 - 1 \neq 0$ we have solutions $(1, 0)$ and $\left(\frac{5m^2+1}{5m^2-1}, \frac{2m}{5m^2-1}\right)$ or $p+1$ solutions. Additionally, when $5m^2-1 \equiv 0 \pmod p$, we lose two solutions from m and $-m$. This is the case when 5 is a quadratic residue. This occurs if and only if $p \equiv 1, 4 \pmod 5$. □

We now establish the relationship between the order of $G(\mathbb{F}_p)$, the order of $(3/2, 1/2)$ and $Z(p)$. We use the fact that $n(3/2, 1/2) = (L_{2n}/2, F_{2n}/2)$ and the identity in $G(\mathbb{F}_p)$ is $(1, 0)$.

Theorem 3.5. *Let $p \neq 2, 5$ and $\alpha = \left(\frac{3}{2}, \frac{1}{2}\right) \in G(\mathbb{F}_p)$. Let $o(p)$ be the order of $\alpha \in G(\mathbb{F}_p)$. Then*

$$Z(p) = \begin{cases} 2o(p) & \text{if } o(p) \text{ is odd} \\ \frac{o(p)}{2} & \text{if } o(p) \equiv 2 \pmod 4 \\ o(p) & \text{if } o(p) \equiv 0 \pmod 4. \end{cases}$$

Proof. If $p \mid F_n$, then $p \mid F_{2n}$ and $L_n^2 \equiv 4(-1)^n \pmod p$. If $p \mid F_{2n}$, then $p \mid F_n$ or $p \mid L_n$. However, from $L_n^2 \equiv 4(-1)^n \pmod p$ we may conclude $p \mid F_n$. Hence $p \mid F_n$ if and only if $p \mid F_{2n}$ and $L_n^2 \equiv 4(-1)^n \pmod p$. We have $L_{2n} + 2(-1)^n \equiv L_n^2 \equiv 4(-1)^n \pmod p$ hence $L_{2n} \equiv 2(-1)^n \pmod p$. Therefore we have the following:

$$\begin{aligned} p \mid F_n \text{ iff } & p \mid F_{2n} \text{ and } L_n^2 \equiv 4(-1)^n \pmod p \\ \text{iff } & p \mid F_{2n} \text{ and } L_{2n} \equiv 2(-1)^n \pmod p \\ \text{iff } & n\alpha \equiv ((-1)^n, 0) \pmod p. \end{aligned} \tag{3.5}$$

Clearly $(L_{2o(p)}/2, F_{2o(p)}/2) \equiv (1, 0) \pmod p$. And $Z(p)$ is the smallest positive integer n such that $n\alpha \equiv ((-1)^n, 0) \pmod p$. Since $G(\mathbb{F}_p)$ is cyclic then $(-1, 0)$ is the unique element of order 2. Then we may break up the proof into the three cases.

If $o(p)$ is odd, then $(-1, 0) \notin \langle\alpha\rangle$. Therefore, $n\alpha \equiv ((-1)^n, 0) \pmod p$ if and only if n is even and $o(p) \mid n$. This implies that $Z(p) = 2o(p)$.

If $o(p)$ is even, then $(-1, 0) \in \langle\alpha\rangle$ since $o(p)/2\alpha$ has order 2. Since the only points in $G(\mathbb{F}_p)$ that have y-coordinate zero are $(\pm 1, 0)$, then $n\alpha \equiv ((-1)^n, 0) \pmod p$ implies $o(p)/2 \mid n$.

If $o(p) \equiv 2 \pmod 4$, then $o(p)/2$ is odd. Moreover, $o(p)/2\alpha \equiv (-1,0) \equiv ((-1)^{o(p)/2}, 0) \pmod p$ so $Z(p) = o(p)/2$. If $o(p) \equiv 0 \pmod 4$, then $o(p)/2\alpha \equiv (-1,0) \not\equiv ((-1)^{o(p)/2}, 0) \pmod p$, but $o(p)\alpha \equiv (1,0) = ((-1)^{o(p)}, 1) \pmod p$, so $Z(p) = o(p)$.

Thus we have derived the relation between $Z(p)$ and the order of α in $G(\mathbb{F}_p)$. □

3.2 The Galois Group for the Field K over $\mathbb{Q}$

We will now adjoin the components of the preimages of α under l to $\mathbb{Q}$.

Lemma 3.6. *Let k be an integer, $a = \frac{1+\sqrt{5}}{2}$, $\gamma_k = \sqrt[k]{a^2}$, and $F = \mathbb{Q}(\sqrt{5})$. Then $\gamma_k \notin F$ for $k > 2$.*

Proof. Assume $\gamma_k \in F$. Note that for an integer k, γ_k is an algebraic integer because it is a root of $x^{2k} - 3x^k + 1$. The set of algebraic integers in F is $\mathbb{Z}[a]$ and the units of $\mathbb{Z}[a]$ are generated by $\langle -1, a \rangle$. Furthermore $\mathbb{Z}[a]^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$ via the isomorphism $\sigma : (i,j) \to (-1)^i(a)^j$. We observe that $\sigma((0, \frac{2}{k})) = \gamma_k$. But j must be an integer, so it is impossible for $k > 2$. Hence $\gamma_k \notin F$ for $k > 2$. □

Lemma 3.7. *Let m be an integer, $a = \frac{1+\sqrt{5}}{2}$, $\gamma_m = \sqrt[m]{a^2}$, and ζ_m be a primitive m-th root of unity, $F = \mathbb{Q}(\sqrt{5})$, and $E = F(\gamma_m)$. Then E has degree m over F for m odd and $m/2$ for m even.*

Proof. Let d be the degree of E over F. Then $g(x) = \min_F(\gamma_m) \mid x^m - a^2$ and $\deg g = d$. The product of the roots of g is in F. Therefore, $\prod \zeta_m^{e_i}\gamma_m \in \mathbb{Z}[a]$ with $1 \leq e_i \leq m$ for some subset of the e_i. We observe that there are d factors of γ_m. Suppose that the $\gcd(d,m) = 1$. Then there exist some x, y such that $dx + my = 1$. Then $((\gamma_m)^d)^x = (\gamma_m)^{1-my} = (\gamma_m)(\gamma_m)^{-my} = (\gamma_m)(a^2)^{-y}$. Therefore, γ_m is in F, a contradiction to the previous lemma. Suppose $\gcd(d,m) > 1$. Therefore, d is a divisor of m as $\deg g \mid deg(x^m - a^2)$. The the norm of $a^{\frac{2}{d}}$ over F is a^2, ie $N_{E/F}(a^{\frac{2}{d}}) = a^2$. However, $N_{E/F}(\sqrt[d]{a^2}) = N_{E/F}(\sqrt[m]{a^2} \dots \sqrt[m]{a^2})$. Therefore $\sqrt[m/d]{a^2}$ is in F, a contradiction for $m/n \neq 2, 1$. Hence E has degree m over F for m odd and $m/2$ for m even. □

Lemma 3.8. *Let m be an integer, $F = \mathbb{Q}(\sqrt{5})$, $E = F(\gamma_m)$ as before, $L = F(\zeta_m)$ where the ζ_m is a primitive m-th root of unity, and $M = E \cap L$. Then $M = F$.*

Proof. As E has degree m or $m/2$ over F then $|M : F| = d$ for some $d \mid m$ as it is an intermediate field.We will show $d = 1$. As L is Galois over F, it is represented by the abelian multiplicative group $(\mathbb{Z}/m\mathbb{Z})^\times$ of order $\phi(m)$ if $5 \nmid m$ or $\phi(m)/2$ if $5 \mid m$ as $\mathbb{Q}(\sqrt{5}) \subset \mathbb{Q}(\zeta_5) \subset \mathbb{Q}(\zeta_m)$. Then M is Galois over F as its representative subgroup is normal. Let g be the minimal polynomial of γ_m over M and f be the minimal polynomial of γ_m over F. Then $g \mid f$ in $M[x]$. Therefore $g(x) = \prod_I (x - \gamma_m \zeta_m^i)$ with I some subset of $\mathbb{Z}/m\mathbb{Z}$. Looking at the constant term of the polynomial $\prod_I \gamma_m \zeta_m^i \in M$. Since M is a subfield of $\mathbb{R}$, then $\prod_I \zeta_m^i = \pm 1$. We then know $(\gamma_m)^{\frac{m}{d}} = \pm(\sqrt[d]{a^2}) \in M$. Let $E_d = F(\sqrt[d]{a^2}) \subset M$. As E_d has degree d over F and M has degree d then $E_d = M$. This gives a contradiction because M is Galois over $\mathbb{Q}$ and E_d is not Galois over $\mathbb{Q}$ if $d > 2$. We may conclude $M = F$ as long as $d \neq 1$ or 2. □

Lemma 3.9. *Let m be an integer, $F = \mathbb{Q}(\sqrt{5})$, $E = F(\sqrt[m]{a^2})$ as before, $L = F(\zeta_m)$, $M = E \cap L$, and $K = \langle E, L \rangle$. Then K over F is Galois and furthermore $|K : F| = m\phi(m)$ for $\gcd(10, m) = 1$ and $|K : F| = m\phi(m)/2$ for $\gcd(10, m) = 2, 5$ and $|K : F| = m\phi(m)/4$ for $\gcd(10, m) = 10$. Moreover if $m = l_1^{k_1} \dots l_n^{k_n}$ the prime factorization with l_i prime and k_i positive integers with $L_i = F(\zeta_{l_i^{k_i}})$ and $E_i = F(\sqrt[l_i^{k_i}]{a})$ with $K_i = E_i L_i$, $E = E_1 \cdots E_n$ and $L = L_1 \cdots L_n$, then $K_n \cap \langle K_1, \dots, K_{n-1} \rangle = F$.*

Proof. By the natural irrationalities theorem, we may conclude K is Galois over E and $|K : E| = |L : M|$ and by Lemma 3.8, $M = F$. Then K is Galois over F as it is a splitting field for $x^m - a$. So $|K : F| = |K : E|\,|E : F| = |L : F|\,|E : F| = m\phi(m)$ for $\gcd(10, m) = 1$. Note $\sqrt{5} \in \mathbb{Q}(\zeta_5)$.

Then $|L:F|\,|E:F| = m\phi(m)/2$ for $\gcd(10,m) = 2,5$ and $|L:F|\,|E:F| = m\phi(m)/4$ for $\gcd(10,m) = 10$.

Again by the natural irrationalities theorem,

$$\begin{aligned} |\langle K_1, \ldots, K_n\rangle : F| &= |E:F|\,|L:F| \\ &= |E_1:F| \cdots |E_n:F|\,|L_1:F| \cdots |L_n:F| \\ &= |K_1:F| \cdots |K_n:F|\,. \end{aligned} \tag{3.6}$$

By another application of the natural irrationalities theorem, $K_{n+1} \cap \langle K_1, \ldots, K_n\rangle = F$. □

We wish to break up m into its respective prime powers l_i such that they are easier to analyze later. We utilize that for the compositum $\langle K_1, K_2\rangle$, $\mathrm{Gal}(\langle K_1, K_2\rangle/\mathbb{Q})$ is isomorphic to the subgroup $\{(\sigma_1, \sigma_2) : \sigma_1|_F = \sigma_2|_F\} \subset \mathrm{Gal}(K_1/\mathbb{Q}) \times \mathrm{Gal}(K_2/\mathbb{Q})$.

3.3 The Image of Gal$(K/\mathbb{Q})$

Let m be an integer, ζ_m be a primitive m-th root of unity, and γ_m and a be defined as before. Then $K = \mathbb{Q}(\sqrt{5}, \zeta_m, \gamma_m)$. In order to count specific elements of $\mathrm{Gal}(K/\mathbb{Q})$ we find a more convenient group, S.

Claim 3.10. *The set of maps from $(\mathbb{Z}/m\mathbb{Z}) \to (\mathbb{Z}/m\mathbb{Z})$ of the form $f(x) = ax + b$, where $a \in (\mathbb{Z}/m\mathbb{Z})^\times$ and $b \in (\mathbb{Z}/m\mathbb{Z})$ form a group $I(m)$. Moreover $|I(m)| = m \cdot \phi(m)$.*

Proof. Given $(a_1x + b_1), (a_2x + b_2) \in I(m)$, $(a_1x + b_1) \circ (a_2x + b_2) = (a_1a_2x + a_1b_2 + b_1) \in I(m)$ as $a_1, a_2 \in (\mathbb{Z}/m\mathbb{Z})^\times$ and $b_1, b_2, a_1b_2 + b_1 \in (\mathbb{Z}/m\mathbb{Z})$. Hence $I(m)$ is closed under composition. Clearly $f(x) = x$ is the identity and composition of functions is associative. Lastly if $f(x) = ax + b \in I(m)$, then its inverse is $f^{-1}(x) = a^{-1}x - a^{-1}b$ so $f(f^{-1}(x)) = a(a^{-1}x - a^{-1}b) + b = x$ and $f^{-1}(f(x)) = a^{-1}(ax + b) - a^{-1}b = x$. Clearly $|I(m)| = |(\mathbb{Z}/m\mathbb{Z})|\,|(\mathbb{Z}/m\mathbb{Z})^\times| = m\phi(m)$. □

For later convenience we will denote P_i and Q_j to be following the pair of points:

$$P_i = \left(\frac{\gamma\zeta_m^i + \gamma^{-1}\zeta_m^{-i}}{2}, \frac{\gamma\zeta_m^i - \gamma^{-1}\zeta_m^{-i}}{2\sqrt{5}}\right), Q_j = \left(\frac{\zeta_m^j + \zeta_m^{-j}}{2}, \frac{\zeta_m^j - \zeta_m^{-j}}{2\sqrt{5}}\right)$$

which correspond to the m preimages of α and m points of order dividing m respectively with their coordinates in K. For convention we pick $P = P_0$ and $Q = Q_1$.

Let $\delta \in \text{Gal}(K/\mathbb{Q})$. Then $\delta((x_1, y_1)\star(x_2, y_2)) = \delta((x_1x_2+5y_1y_2, x_1y_2+x_2y_1)) = (\delta(x_1)\delta(x_2)+5\delta(y_1)\delta(y_2), \delta(x_1)\delta(y_2) + \delta(x_2)\delta(y_1)) = \delta(x_1, y_1) \star \delta(x_2, y_2)$. This implies if $\delta(mP_i) = \delta(\alpha) = \alpha$, then $m\delta(P_i) = \alpha$. Therefore $\delta(P)$ must go to another preimage, so $\delta(P) = P_b = P + bQ$ where $b \in \mathbb{Z}/m\mathbb{Z}$ as there are m preimages. If Q_a has order m, then $\delta(mQ_a) = 0$ or $m\delta(Q_a) = 0$ and $a \in (\mathbb{Z}/m\mathbb{Z})^\times$. Hence $\delta(Q)$ must go to another preimage of order m or $\delta(Q) = aQ$. Therefore, for any r such that $0 \leq r \leq m - 1$, we have $\delta(P + rQ) = \delta(P) + r\delta(Q) = P + (ar + b)Q$.

Claim 3.11. *Let m and K defined as before. For $\delta \in$ Gal$(K/\mathbb{Q})$ define $a, c \in (\mathbb{Z}/m\mathbb{Z})^\times$, and $b \in \mathbb{Z}/m\mathbb{Z}$ by $\delta(P + rQ) = P + (ar + b)Q$ and $\delta(\zeta) = \zeta^c$. The map $\phi :$ Gal$(K/\mathbb{Q}) \to I(m) \times (\mathbb{Z}/m\mathbb{Z})^\times$ given by $\phi(\delta) = (ax + b, c)$ is a homomorphism.*

Proof. Let $\delta_1, \delta_2 \in \text{Gal}(K/\mathbb{Q})$, where $\delta_i(P + rQ) = P + (a_ir + b_i)Q$ and $\delta_i(\zeta) = \zeta^{c_i}$ for $a_i, c_i \in (\mathbb{Z}/m\mathbb{Z})^\times$, $b_i \in (\mathbb{Z}/m\mathbb{Z})$ and $i = 1, 2$. Then $\delta_1 \circ \delta_2$ yields $\delta_1(\delta_2(P+rQ)) = \delta_1(P+(a_2r+b_2)Q) = P + (a_1(a_2r + b_2) + b_1)Q$ and $\delta_1(\delta_2(\zeta)) = \delta_1(\zeta_2^c) = \zeta^{c_1c_2}$. Hence $\phi(\delta_1 \circ \delta_2) = (a_1a_2x + a_1b_2 + b_1, c_1c_2) = (a_1x + b_1, c_1) \circ (a_2x + b_2, c_2) = \phi(\delta_1) \circ \phi(\delta_2)$. □

Claim 3.12. *The homomorphism $\phi :$ Gal$(K/\mathbb{Q}) \to I(m) \times (\mathbb{Z}/m\mathbb{Z})^\times$ is injective.*

Proof. The kernel of ϕ is the set $\{\delta \in \text{Gal}(K/\mathbb{Q}) : \phi(\delta) = (x, 1)\}$. This implies ζ, Q, P are fixed. This implies that as Q and ζ are fixed then $\sqrt{5}$ is fixed. Lastly as P, Q, ζ, and $\sqrt{5}$ are fixed, γ is fixed. Hence $\ker(\phi)$ fixes the generators K over $\mathbb{Q}$ or $K^{\langle\ker(\phi)\rangle} = K$. Therefore $\ker(\phi)$ is the identity. □

Claim 3.13. *Let $m = \prod_{i=1}^{s} l_i^{e_i}$. Then $I(m) \times (\mathbb{Z}/m\mathbb{Z})^\times \cong \prod_{i=1}^{s} I(l_i^{e_i}) \times (\mathbb{Z}/l_i^{e_i}\mathbb{Z})^\times$.*

Proof. The proof follows from the Chinese Remainder Theorem. □

We proceed by breaking into four cases for $m = l^k$: $l \neq 2, 5$ is a prime, $m = 2^k$, $m = 5^k$ and $m = 10^k$.

Claim 3.14. *Let l be a prime not equal to 2 or 5, $m = l^k$, and*

$$S = \left\{(ax+b, c) : a, c \in (\mathbb{Z}/l^k\mathbb{Z})^\times, b \in \mathbb{Z}/l^k\mathbb{Z}, a = \pm c\right\} \subset I(l^k) \times (\mathbb{Z}/l^k\mathbb{Z})^\times. \tag{3.7}$$

The Im $\phi \subset S$. Moreover $|Gal(K/\mathbb{Q})| = |S|$, therefore $\phi : Gal(K/\mathbb{Q}) \to S$ is an isomorphism. Moreover ϕ restricted to $Gal(K/F)$ implies $a = c$.

Proof. We have $\mathrm{Gal}(K/F(\zeta_{l^k}))$ is isomorphic to $\mathrm{Gal}(\mathbb{Q}(\zeta_{l^k})/\mathbb{Q})$ which have automorphisms of the form $x \to x^c$ where $c \in (\mathbb{Z}/l^k\mathbb{Z})^\times$. If $\delta(\zeta_m) = \zeta_m^c$, then $\delta(Q) = cQ$ if $\sqrt{5}$ is fixed and $-cQ$ if $\sqrt{5}$ is conjugated. Hence we split into two cases. If $\delta(Q) = cQ$, then $\delta(P+rQ) = P+(ar+b)Q$ then $\delta(P) = P + bQ$. Hence $P + bQ = \delta(P) = \delta(P + rQ) - \delta(rQ) = P + (ar + b)Q - crQ = P + ((a - c)r + b)Q$ means $a \equiv c \pmod m$. If $\delta(Q) = -cQ$, then $\delta(P + rQ) = P + (ar + b)Q$ and $\delta(P) = P + bQ$. Hence $P + bQ = \delta(P) = \delta(P + rQ) - \delta(rQ) = P + (ar + b)Q + crQ = P + ((a + c)r + b)Q$ means $a \equiv -c \pmod m$.

Clearly $|S| = 2m\phi(m)$ which is the size of $\mathrm{Gal}(K/\mathbb{Q})$. Since, ϕ is injective of the same size, then ϕ is an isomorphism. Moreover we have shown δ restricted to $\mathrm{Gal}(K/F)$ implies $a = c$. □

Claim 3.15. *Let $m = 5^k$, and*

$$S = \left\{(ax+b, c) : a, c \in (\mathbb{Z}/5^k\mathbb{Z})^\times, b \in \mathbb{Z}/5^k\mathbb{Z}, a = \left(\frac{c}{5}\right)c\right\} \subset I(5^k) \times (\mathbb{Z}/5^k\mathbb{Z})^\times. \tag{3.8}$$

The Im $\phi \subset S$. Moreover $|Gal(K/\mathbb{Q})| = |S|$, therefore $\phi : Gal(K/\mathbb{Q}) \to S$ is an isomorphism. Moreover ϕ restricted to $Gal(K/F)$ implies $a = c$ as $\left(\frac{c}{5}\right) = 1$.

Proof. Let $\delta(\zeta_m) = \zeta_m^c$. We have $\delta(\sqrt{5}) = \sqrt{5}$ if and only if $\left(\frac{c}{5}\right) = 1$ which is shown by applying δ to the Gaussian sum of $\sqrt{5}$. Therefore $\delta(Q) = cQ$ if $\left(\frac{c}{5}\right) = 1$ and $\delta(Q) = -cQ$ if $\left(\frac{c}{5}\right) = -1$ and we arrive at the same conclusion as the previous claim. □

Claim 3.16. *Let $m = 2^k$ and*

$$S = \left\{(ax+b, c) : a, c \in (\mathbb{Z}/2^k\mathbb{Z})^\times, b \in \mathbb{Z}/2^k\mathbb{Z}, a = (-1)^b c\right\} \subset I(l^k) \times (\mathbb{Z}/l^k\mathbb{Z})^\times. \tag{3.9}$$

The Im $\phi \subset S$. Moreover $|Gal(K/\mathbb{Q})| = |S|$, therefore $\phi : Gal(K/\mathbb{Q}) \to S$ is an isomorphism. Moreover ϕ restricted to $Gal(K/F)$ implies $a = c$ as b is even.

Proof. Since $\delta(P + rQ) = P + (ar + b)Q$ for any r, then we may say

$$P + bQ = \delta(P) = \left(\frac{\gamma_m\zeta_m^d + \gamma_m^{-1}\zeta_m^{-d}}{2}, \frac{\gamma_m\zeta_m^d - \gamma_m^{-1}\zeta_m^{-d}}{2\delta(\sqrt{5}}\right).$$

Therefore if $b = d$ then $\delta(\sqrt{5}) = \sqrt{5}$ and if $b = -d$ then $\delta(\sqrt{5}) = -\sqrt{5}$. Let $f(x) = x^{2*2^k} - 3x^{2^k} + 1 = (x^{2^k} - x^{2^k/2} - 1)(x^{2^k} + x^{2^k/2} - 1) = (x^{2^k/2} - ((1+\sqrt{5})/2))(x^{2^k/2} - ((1-\sqrt{5})/2))(x^{2^k/2} + ((1+\sqrt{5})/2))(x^{2^k/2} + ((1-\sqrt{5})/2))$. Therefore $\gamma_{2^k}\zeta^{2i}$ and $\gamma_{2^k}^{-1}\zeta^{2i+1}$ are roots of $(x^{2^k} - x^{2^k/2} - 1)$. Moreover d is even if $\delta(\sqrt{5}) = \sqrt{5}$ and d is odd if $\delta(\sqrt{5}) = -\sqrt{5}$. Moreover $a = c$ if and only if $\delta(\sqrt{5}) = \sqrt{5}$ by our calculation in the case $l \neq 2, 5$. Therefore we have shown our claim. □

Claim 3.17. *Let $m = 10^k$ and*

$$S = \left\{(ax+b, c) : a, c \in (\mathbb{Z}/10^k\mathbb{Z})^\times, b \in \mathbb{Z}/10^k\mathbb{Z}, a = \left(\frac{a}{5}\right)c, (-1)^b = \left(\frac{a}{5}\right)\right\} \tag{3.10}$$

with $S \subset I(m) \times (\mathbb{Z}/m\mathbb{Z})^\times$ and S is closed under multiplication. The Im $\phi \subset S$. Moreover $|Gal(K/\mathbb{Q})|\,|S| = \phi(10^k)10^k/2$. Moreover ϕ restricted to $Gal(K/F)$ implies $a = c$ as b is even and $\left(\frac{a}{5}\right) = 1$.

Proof. Since $\delta(P + rQ) = P + (ar + b)Q$ for any r, then we may say

$$P + bQ = \delta(P) = \left(\frac{\gamma_m \zeta_m^d + \gamma_m^{-1} \zeta_m^{-d}}{2}, \frac{\gamma_m \zeta_m^d - \gamma_m^{-1} \zeta_m^{-d}}{2\delta(\sqrt{5})} \right).$$

Therefore if $b = d$ then $\delta(\sqrt{5}) = \sqrt{5}$ and if $b = -d$ then $\delta(\sqrt{5}) = -\sqrt{5}$. Let $f(x) = x^{2*10^k} - 3x^{10^k} + 1 = (x^{10^k} - x^{10^k/2} - 1)(x^{10^k} + x^{10^k/2} - 1) = (x^{10^k/2} - ((1 + \sqrt{5})/2))(x^{10^k/2} - ((1 - \sqrt{5})/2))(x^{10^k/2} + ((1 + \sqrt{5})/2))(x^{10^k/2} + ((1 - \sqrt{5})/2))$. Therefore $\gamma_{10^k} \zeta^{2i}$ and $\gamma_{10^k}^{-1} \zeta^{2i+1}$ are roots of $(x^{10^k} - x^{10^k/2} - 1)$. We have d is even if $\delta(\sqrt{5}) = \sqrt{5}$ and d is odd if $\delta(\sqrt{5}) = -\sqrt{5}$ and $\delta(\sqrt{5}) = \sqrt{5}$ if and only if $\left(\frac{a}{5}\right) = 1$. Moreover $a = c$ if and only if $\delta(\sqrt{5}) = \sqrt{5}$ by our calculation in the case $l \neq 2, 5$. Therefore we have shown our claim. □

3.4 General S

Let m be an integer and $t = ul_1 \dots l_s$ where t is square free such that l_i is a prime $\neq 2, 5$, $l_i \mid m$, $u \mid 10$ and $u \mid m$. Let k be an integer and $\gamma_{t^k} = \sqrt[t^k]{\frac{3+\sqrt{5}}{2}}$, and ζ_{t^k} be a primitive t^k-th root of unity. Define $K = \mathbb{Q}(\sqrt{5}, \zeta_{t^k}, \gamma_{t^k})$, $K_i = \mathbb{Q}(\sqrt{5}, \zeta_{l_i^k}, \gamma_{l_i^k})$, and $K_0 = \mathbb{Q}(\sqrt{5}, \zeta_{u^k}, \gamma_{u^k})$. We revisit the subgroup of $\mathrm{Gal}(K_1/\mathbb{Q}) \times \mathrm{Gal}(K_2/\mathbb{Q})$, $\{(\sigma, \tau) : \sigma|_{K_1 \cap K_2} = \tau|_{K_1 \cap K_2}\}$ in Proposition 2.4, that is isomorphic to the Galois group of the compositum. Therefore we may say $\mathrm{Gal}(K/F) \cong \prod_i \mathrm{Gal}(K_i/F)$. Moreover as the automorphisms that conjugate $\sqrt{5}$ form a coset of the same order therefore we the following:

1. If $u = 1$, then

$$\phi(\mathrm{Gal}(K/\mathbb{Q})) = \left\{ \textstyle\prod_i (a_i x + b_i, c_i) : a_i, c_i \in (\mathbb{Z}/l_i^k\mathbb{Z})^\times, b \in \mathbb{Z}/l_i^k\mathbb{Z}, a_i = \pm c_i, a_i/c_i = a_j/c_j \right\}.$$

2. If $u = 2$, then

$$\phi(\mathrm{Gal}(K/\mathbb{Q})) = \left\{ \begin{matrix} \prod_i (a_i x + b_i, c_i) : a_0, c_0 \in (\mathbb{Z}/u^k\mathbb{Z})^\times, b_0 \in \mathbb{Z}/u^k\mathbb{Z}, \\ a_i, c_i \in (\mathbb{Z}/l_i^k\mathbb{Z})^\times, b \in \mathbb{Z}/l_i^k\mathbb{Z}, a_i = \pm c_i, (-1)^{b_0} = a_i/c_i \end{matrix} \right\}.$$

3. If $u = 5$, then

$$\phi(\mathrm{Gal}(K/\mathbb{Q})) = \begin{Bmatrix} \prod_i (a_i x + b_i, c_i) : a_0, c_0 \in (\mathbb{Z}/u^k\mathbb{Z})^\times, b_0 \in \mathbb{Z}/u^k\mathbb{Z}, \\ a_i, c_i \in (\mathbb{Z}/l_i^k\mathbb{Z})^\times, b_i \in \mathbb{Z}/l_i^k\mathbb{Z}, a_i = \pm c_i, a_i = \left(\frac{a_0}{5}\right) c_i \end{Bmatrix}.$$

4. If $u = 10$, then

$$\phi(\mathrm{Gal}(K/\mathbb{Q})) = \begin{Bmatrix} \prod_i (a_i x + b_i, c_i) : a_0, c_0 \in (\mathbb{Z}/u^k\mathbb{Z})^\times, b_0 \in \mathbb{Z}/u^k\mathbb{Z}, a_i, c_i \in (\mathbb{Z}/l_i^k\mathbb{Z})^\times, \\ b_i \in \mathbb{Z}/l_i^k\mathbb{Z}, a_i = \pm c_i, a_i = \left(\frac{a_0}{5}\right) c_i, (-1)^{b_0} = a_i/c_i \end{Bmatrix}.$$

3.5 Considerations for the Chebotarev Density Theorem

First we must determine what primes ramify.

Lemma 3.18. *Let m be an odd integer. The discriminant of $f(x) = x^{2m^k} - 3x^{m^k} + 1$ is $\pm 5^{m^k}(m^k)^{2m^k}$.*

Proof. We showed in Lemma 3.7 that $f(x)$ is irreducible over $\mathbb{Q}$. Therefore we may apply Lemma 2.21. The roots of f are $\gamma_m \zeta_m^i$ and $\gamma_m^{-1}\zeta_m^i$. Let $E = F(\gamma_m)$. The discriminant $D = (-1)^{\frac{n(n-1)}{2}} N_{E/\mathbb{Q}}(f'(\gamma_m))$. We have $f'(\gamma_m) = 2m^k\gamma_m^{2m^k-1} - 3m^k\gamma_m^{m^k-1} = \sqrt{5}m^k\gamma_m^{m^k-1}$. As $N_{E/\mathbb{Q}}(\gamma_m) = \prod \sigma_i(\gamma_m)$, where $\sigma_i(\gamma_m)$ are the conjugates of γ_m, and the norm is the last coefficient of $f(x)$. Also $N_{E/\mathbb{Q}}(\sqrt{5}) = \pm \prod^{2m^k} \sqrt{5}$. Clearly

$$\begin{aligned} N_{E/\mathbb{Q}}(\sqrt{5}m^k\gamma_m^{m^k-1}) &= N_{E/\mathbb{Q}}(\sqrt{5})N_{E/\mathbb{Q}}(m^k)N_{E/\mathbb{Q}}(\gamma_m)^{m^k-1} \\ &= (\pm 5^{m^k})(m^k)^{2m^k}(1)^{m^k-1}. \end{aligned} \tag{3.11}$$

Hence $D = \pm 5^{m^k}(m^k)^{2m^k}$. □

Lemma 3.19. *Let m be an even integer. The discriminant of $f(x) = x^{m^k} - x^{m^k/2} - 1$ is $\pm 5^{m^k/2}(m^k/2)^{m^k}$.*

Proof. We showed in Lemma 3.7 that $f(x)$ is irreducible over $\mathbb{Q}$. Therefore we may apply Lemma 2.21. The roots of f are $\gamma_m\zeta_m^{2i}$ and $\gamma_m^{-1}\zeta_m^{2i+1}$. Let $E = F(\gamma_m)$. The discriminant $D = (-1)^{\frac{n(n-1)}{2}} N_{E/\mathbb{Q}}(f'(\gamma_m))$. We have $f'(\gamma_m) = m^k\gamma_m^{m^k-1} - m^k\gamma_m^{m^k/2-1}/2 = \sqrt{5}m^k\gamma_m^{m^k/2-1}/2$. As $N_{E/\mathbb{Q}}(\gamma_m) = \prod \sigma_i(\gamma_m)$, where $\sigma_i(\gamma_m)$ are the conjugates of γ_m, and the norm is the last coefficient of $f(x)$. Also $N_{E/\mathbb{Q}}(\sqrt{5}) = \pm \prod^{m^k} \sqrt{5}$. We have

$$\begin{aligned} N_{E/\mathbb{Q}}(\sqrt{5}m^k\gamma_m^{m^k-1}/2) &= N_{E/\mathbb{Q}}(\sqrt{5})N_{E/\mathbb{Q}}(m^k/2)N_{E/\mathbb{Q}}(\gamma_m)^{m^k/2-1} \\ &= (\pm 5^{m^k/2})(m^k/2)^{m^k}(-1)^{m^k/2-1}. \end{aligned} \tag{3.12}$$

Hence $D = \pm 5^{m^k/2}(m^k/2)^{m^k}$. □

Let K be defined in Section 3.4.

Lemma 3.20. *The prime divisors of m and 5 are the only primes that ramify in K.*

Proof. Let $L = \mathbb{Q}(\zeta_m)$ and $E = \mathbb{Q}(\gamma_m)$. Then $K = \langle L, E\rangle$. By the previous two lemmas we showed the prime divisors of m and 5 divide Δ_E. Theorem 2.14 shows the discriminant of a cyclotomic field extension $\mathbb{Q}(\zeta_{l^k})$ is a power of l. Hence only prime divisors of m divide Δ_L. By Theorem 2.27, the prime divisors of m and 5 ramify in K. □

Let l be a prime, k an integer, $\gamma^{l^k} = \frac{3+\sqrt{5}}{2}$, ζ_{l^k} is the l^k-th root of unity, $K = \mathbb{Q}(\sqrt{5}, \gamma, \zeta_{l^k})$, and P and Q are defined as before. Let $\mathcal{C}_{n,l} = \{\sigma \in \mathrm{Gal}(K/\mathbb{Q}) | \sigma(l^nP + rl^nQ) = l^nP + rl^nQ$ and $\sigma(l^{n-1}P + rl^{n-1}Q) \neq l^{n-1}P + rl^{n-1}Q$ for some $r\}$ and $\mathfrak{p}$ be a prime above p in O_K. We may define $D_\mathfrak{p}$ to be the decomposition group of $\mathrm{Gal}(K/\mathbb{Q})$. We know that l and 5 are the only primes that ramify. Hence for all other p, $|I_\mathfrak{p}| = e_{\mathfrak{p}|p} = 1$. Therefore, there is an isomorphism between $D_\mathfrak{p}$ and $\mathrm{Gal}(O_K/\mathfrak{p}/\mathbb{F}_p) = \tilde{G}$, with $\tilde{G}$ is generated by the Frobenius automorphism, $\left(\frac{K/\mathbb{Q}}{\mathfrak{p}}\right)$. Then $\left(\frac{K/\mathbb{Q}}{\mathfrak{p}}\right)(l^nP + rl^nQ) = (l^nP + rl^nQ)^p \mod \mathfrak{p}$ hence $l^nP + rl^nQ \in G(\mathbb{F}_p)$. Then under conjugation by σ, $l^nP + rl^nQ$ is fixed but then $\left(\frac{K/\mathbb{Q}}{\sigma(\mathfrak{p})}\right)(l^nP + rl^nQ) = (l^nP + rl^nQ)^p$ mod $\sigma(\mathfrak{p})$. Therefore, the equation holds for any choice of $\mathfrak{p}$ above p.

Lemma 3.21. *The preimage $l^nP + rl^nQ \in G(\mathbb{F}_p)$ if and only if $\left(\frac{K/\mathbb{Q}}{\mathfrak{p}}\right) \in \mathcal{C}_{n,l}$.*

Proof. Suppose that $l^nP + rl^nQ \in \mathbb{F}_p$. Then $\left(\frac{K/\mathbb{Q}}{\mathfrak{p}}\right)(l^nP + rl^nQ) \equiv l^nP + rl^nQ \mod \mathfrak{p}$. We want to show that the reduction map from $\{l^nP + rl^nQ \in K\}$ to $\{l^nP + rl^nQ \mod \mathfrak{p}\}$ is injective. Suppose not. Then there is a $l^nP + r_1l^nQ$ and a $l^nP + r_2l^nQ$ in K such that they map to the same element $l^nP + rl^nQ \in O_k/\mathfrak{p}$. Then their difference $(r_2 - r_1)l^nQ \equiv (1, 0)$ mod $\mathfrak{p}$. We calculate the norm $N_{K/Q}(\mathfrak{p}) = O_k \cap \prod_{\sigma \in G} \sigma(\mathfrak{p}) = p$. Hence the norm of the y coordinate of Q must exist in the ideal (p) in $\mathbb{Z}$. Let the y coordinate of Q be denoted $Q[y]$. We decompose the norm by the field extensions for convenience as follows: $N((r_1-r_2)l^nQ[y]) = (r_1 - r_2)l^nN(Q[y]) = (r_1 - r_2)l^nN_{K/L}(N_{L/Q}(Q[y]))$. Note that for $l \neq 2, 5$, we have

$$N_{L/Q}\left(\frac{\zeta - \zeta^{-1}}{2\sqrt{5}}\right) = \prod_{\sigma \in \mathrm{Gal}(L/Q)} \sigma\left(\frac{\zeta - \zeta^{-1}}{2\sqrt{5}}\right) = \frac{l}{(2\sqrt{5})^{l^{k-1}(l-1)}}. \tag{3.13}$$

Hence $N((r_1 - r_2)l^nQ_1[y]) = (r_1 - r_2)l^nN_{K/L}(l) = (r_1 - r_2)l^n\left(\frac{l^{l^k}}{(2\sqrt{5})^{l^{2k-1}(l-1)}}\right)$. If $(r_1 - r_2)l^nQ \equiv (1, 0) \mod \mathfrak{p}$, then $N_{K/Q}((r_1 - r_2)l^nQ[y]) \in N_{K/Q}(\mathfrak{p})$ or $(r_1 - r_2)l^n(l^{l^k}) \in (p)$. However the $\gcd(p, l) = 1$ thus we have a contradiction and we may conclude $r_1 = r_2$.

For the other direction, suppose that $\left(\frac{K/\mathbb{Q}}{\mathfrak{p}}\right) \in \mathcal{C}_{n,l}$. Therefore for each $\mathfrak{p}$ above p, there is a $\left(\frac{K/\mathbb{Q}}{\mathfrak{p}}\right)$ that fixes $l^nP + rl^nQ$ mod $\mathfrak{p}$. Therefore $l^nP + rl^nQ$ is in the fixed field of $\mathrm{Gal}(O_k/\mathfrak{p}/F_p)$ hence $l^nP + rl^nQ \in G(\mathbb{F}_p)$. □

3.6 Counting the Conjugacy Class

We begin with a simple case and prove a different conjecture by Anderson and Bruckman to give some motivation.

Theorem 3.22. *Let $G(\mathbb{F}_p) = \{(x,y) \in \mathbb{F}_p : x^2 - 5y^2 = 1\}$, $\alpha = \left(\frac{3}{2}, \frac{1}{2}\right)$ and l be a prime. Let $l^i \mid\mid |G(\mathbb{F}_p)|$ and $l^j \mid\mid |\alpha|$. Let $K = \mathbb{Q}(\gamma, \zeta)$ where $\gamma = \sqrt[l^k]{\frac{3+\sqrt{5}}{2}}$ and ζ is a l^k-th primitive root of unity and let $\delta \in Gal(K/\mathbb{Q})$. Let*

$$P = \left(\frac{\gamma + \gamma^{-1}}{2}, \frac{\gamma - \gamma^{-1}}{2\sqrt{5}}\right) \tag{3.14}$$

$$Q = \left(\frac{\zeta + \zeta^{-1}}{2}, \frac{\zeta - \zeta^{-1}}{2\sqrt{5}}\right). \tag{3.15}$$

Suppose that $\delta(\zeta) = \zeta^c$ and $\delta(P + rQ) = P + (ar + b)Q$ and $\mathcal{C}_{n,l}$ be defined as before. Then for each n, $1 \leq n \leq k$ we have the following:

$$\frac{|\mathcal{C}_{n,l}|}{|Gal(K/\mathbb{Q})|} = \begin{cases} \frac{l-2}{l-1} & \text{if } i = j = 0, \\ \frac{1}{l^{m+(k-n)}} & \text{if } i \geq 1, j = 0, \\ \frac{l-1}{l^{1+m+(k-n)}} & \text{if } i \geq 1, j \geq 1. \end{cases} \tag{3.16}$$

Proof. We have that there are $i - j$ preimages of α under l hence there are corresponding $k - n$ preimages of α under l. We have $\gcd(a-1, l^k) = l^m$ for $0 \leq m \leq k$ with $m = i$. For $m = 0$, there are solutions to r for $rl^n = (ar + b)l^n$ with any b as $rl^n \equiv -(a-1)bl^n \pmod{l^k}$ or $r \equiv -(a-1)b \pmod{l^{k-n}}$. Therefore there are l^k choices for b and $l^{k-1}(l-1) - l^{k-1}$ choices for a. Hence the density of solutions that have this property is the following:

$$\frac{(l^{k-1}(l-1) - l^{k-1})l^k}{l^{2k-1}(l-1)} = \frac{l-2}{l-1}.$$

Otherwise, the $gcd(a-1, l^k) = l^m$. Then we have $(a-1)r = -b \pmod{l^{k-n}}$ for $(l-1)l^{k-m-1}$ choices for a. We know that $(a-1)r = sl^m$. Hence $sl^m \equiv -b \pmod{l^{k-n}}$, which is impossible unless $l^{\min(k-n,m)} \mid b$. If $l^m < l^{k-n}$, then $l^m \mid b$ and there are l^{k-m} choices for b. If $l^m \geq l^{k-n}$, then $l^{k-n} \mid b$ and there are l^n choice for b.

When $l^{k-n} \mid\mid b$ the density of the solutions is the following:

$$\frac{l^{k-m-1}(l-1)l^{n-1}(l-1)}{l^{2k-1}(l-1)} = \frac{l-1}{l^{m+(k-n)+1}}.$$

When $l^n \mid b$ the density of the solutions is the following:

$$\frac{l^{k-m-1}(l-1)l^n}{l^{2k-1}(l-1)} = \frac{1}{l^{m+(k-n)}}.$$

For $l = 2, 5$, we count in the same manner as before. In the case of $l = 2$, a is always odd. Hence the ratio is $0/2^{2k-1}$ which corresponds to $\frac{l-2}{l-1}$. □

Theorem 3.23. *Let $G(\mathbb{F}_p) = \{(x,y) \in \mathbb{F}_p : x^2 - 5y^2 = 1\}$, $\alpha = \left(\frac{3}{2}, \frac{1}{2}\right)$ and l be a prime. Let $M(l,x;i,j)$ be the number of primes $p \leq x$ such that $l^i \mid\mid |G(\mathbb{F}_p)|$ and $l^j \mid\mid |\alpha|$. Then $\lim_{x\mapsto\infty} M(l,x;i,j)/\pi(x)$ is determined by the following:*

$$\lim_{x\to\infty} \frac{M(l,x;i,j)}{\pi(x)} = \begin{cases} \frac{l-2}{l-1} & \text{if } i = j = 0, \\ \frac{1}{l^{2i}} & \text{if } i \geq 1, j = 0, \\ \frac{l-1}{l^{1+2i-j}} & \text{if } i \geq 1, j \geq 1. \end{cases} \tag{3.17}$$

Proof. Let l, x, i, j be fixed. Choose some $p \leq x$ and k such that we have a field extension K of $\mathbb{Q}$ and its respective Galois group $\mathrm{Gal}(K/\mathbb{Q})$ as before. The number of preimages of α in $G(\mathbb{F}_p)$ is $i - j$ which is equal to $k - n$. Hence once k is fixed we know n. Let $\mathfrak{p}$ be an ideal above p with the respective Frobenius automorphism, $\left(\frac{K/\mathbb{Q}}{\mathfrak{p}}\right)$. We have the following according to Chebotarev's density theorem.

$$\lim_{x\to\infty} \frac{\sum_{p\leq x} I_{\left(\frac{K/\mathbb{Q}}{\mathfrak{p}}\right)\subset \mathcal{C}_{n,l}}}{\pi(x)} = \frac{|\mathcal{C}_{n,l}|}{|\mathrm{Gal}(K/\mathbb{Q})|}. \tag{3.18}$$

From the lemma above, there is a one to one relation between $I_{\left(\frac{K/\mathbb{Q}}{\mathfrak{p}}\right)\subset\mathcal{C}_{n,l}}$ and $l^nP + rl^nQ \in G(\mathbb{F}_p)$. □

3.7 Counting the Conjugacy Class II: Interlude

We have that $l^kP + rl^kQ = \alpha$. So the $(k-n)$-th preimage of α under l is $l^nP + rl^nQ$. We are interested in finding when the $(k-n)$-th preimage of α under l is fixed. In particular, we are motivated by finding when $\delta \in \mathrm{Gal}(K/\mathbb{Q})$ is the Frobenius automorphism to apply Theorem 2.35. If $p \equiv \pm 1 \pmod{l^m}$ or $m = \mathrm{ord}_l(|G(\mathbb{F}_p)|)$ and $n = \mathrm{ord}_l(|\alpha|)$ then we have $m-n$ preimages of α under l.

Claim 3.24. *Let Gal($K/\mathbb{Q}$) be defined as before. If $\delta \in$ Gal($K/\mathbb{Q}$) is the Frobenius automorphism and $\delta(l^nQ) = l^nQ$, then $p \equiv \pm 1 \pmod{l^{k-n}}$.*

Proof. We have $\delta(l^nQ) = l^nQ$, then $\delta(\zeta^{l^n}) = \zeta^{l^n}$ or $\delta(\zeta^{l^n}) = \zeta^{-l^n}$. By Claim 2.32, if $\mathfrak{p}$ is a prime above p, then $\mathrm{res}_{\mathbb{Q}(\zeta)}\left(\frac{K/\mathbb{Q}}{\mathfrak{p}}\right) = \left(\frac{\mathbb{Q}(\zeta)/\mathbb{Q}}{p}\right)$ as $p = \mathfrak{p} \cap \mathbb{Q}(\zeta)$. Hence $\left(\frac{\mathbb{Q}(\zeta)/\mathbb{Q}}{p}\right)$ is the Artin symbol and $\delta(\zeta) = \zeta^p$ by Definition 2.30. If $\delta(\zeta^{l^n}) = \zeta^{l^n}$, then $\delta(\zeta) = \zeta^p$ and $p \equiv 1 \pmod{l^{k-n}}$. In the other case $p \equiv -1 \pmod{l^{k-n}}$. □

Let t be a squarefree integer. If δ fixes $t^nP + rt^nQ$, then $t^nP + rt^nQ = t^nP + (ar+b)t^nQ$. Hence $rt^n \equiv art^n + bt^n \pmod{t^k}$ or $r \equiv ar + b \pmod{t^{k-n}}$ or $(a-1)r + b \equiv 0 \pmod{t^{k-n}}$. Therefore, if $d = \mathrm{ord}_l(a-1)$ and there are at most $d-e$ preimages of α under l, then we may say $e \leq \mathrm{ord}_l(|\alpha|)$.

Let t be squarefree such that $t \mid m$ with $t = ul_1 \cdots l_s$. For each $l_i \neq 2, 5$ a prime with $l_i^{e_i} \mid\mid m$, let $l_i \mid t$. For $2^{e_{0_2}} \mid\mid m$, let $2 \mid u$ and similarly for $5^{e_{0_5}} \mid\mid m$. Let k be some integer. Then for t^k we look at $\pmod{l^k}$ or $\pmod{u^k}$. Therefore, if $\mathrm{ord}_l(a-1) = d$, we wish to find at most $d-e$ preimages of α under l hence $b \not\equiv 0 \pmod{l^{d-e+1}}$.

If l is a prime to find $l^e \mid Z(p)$ then we are counting $\mathcal{C}_{l,e} = \{\delta \in \mathrm{Gal}(K/\mathbb{Q}) : \phi(\delta) = (ax+b,c), \mathrm{ord}_l(a-1) = d \geq e, b \not\equiv 0 \pmod{l^{d-e+1}}\}$. Moreover if $m \mid Z(p)$, then $\mathcal{C} = \{(\sigma_0, \ldots, \sigma_s) : \sigma_i \in \mathcal{C}_{e,l_i}\}$ by 2.33.

3.8 Counting the Conjugacy Class III: The Complete Case

Let t be squarefree such that $t \mid m$ with $t = ul_1 \cdots l_s$. For each $l_i \neq 2, 5$ a prime with $l_i^{e_i} \mid\mid m$, let $l_i \mid t$. For $2^{e_{0_2}} \mid\mid m$, let $2 \mid u$ and similarly for $5^{e_{0_5}} \mid\mid m$. Let $K = \mathbb{Q}(\gamma_{t^k}, \zeta_{t^k}, \sqrt{5})$ be defined as usual.

3.8.1 $u = 1$

Now, if $\mathrm{ord}_{l_i}(a_i - 1) = d_i$, then there are $\prod_i A_{d_i} = \prod_i l_i^{k-d_i} - l_i^{k-d_i-1} = \prod_i l^{k-d_i-1}(l_i - 1)$ possible choices of a_i. Additionally $(a_i - 1)r = r' l_i^{d_i}$, so $r' l_i^{d_i} + b_i \equiv 0 \pmod{l_i^{k-d_i}}$. Therefore we have $b_i \not\equiv 0 \pmod{l_i^{d_i - e_i + 1}}$ giving $\prod_i B_{(d_i,e_i)} = \prod_i l_i^k (l^{d_i - e_i + 1} - 1)/l_i^{d_i - e_i + 1} = \prod_i l_i^k (1 - l_i^{-(d_i - e_i + 1)})$ choices of b_i. Then as d_i ranges from e_i to k, we have the number of δ with $a_i = \pm c_i$ for all i is $2 \prod_i \sum_{d_i = e_i}^{k} A_{d_i} B_{(d_i,e_i)}$.

We can compute $|\mathcal{C}| \,/\, |\mathrm{Gal}(K/\mathbb{Q})|$ as follows:

$$
\begin{aligned}
\frac{2\prod_i \sum_{d_i=e_i}^k A_{d_i} B_{(d_i,e_i)}}{|\mathrm{Gal}(K/\mathbb{Q})|} &= \frac{2\prod_i \sum_{d_i=e_i}^k l^{k-d_i-1}(l_i-1)l_i^k(1-l_i^{-(d_i-e_i+1)})}{2t^k\phi(t^k)} \\
&= \frac{\prod_i \sum_{d_i=e_i}^k l^{k-d_i-1}(l_i-1)l_i^k(1-l_i^{-(d_i-e_i+1)})}{\prod_i l_i^k \phi(l_i^k)} \\
&= \frac{\prod_i \sum_{d_i=e_i}^k l^{k-d_i-1}(l_i-1)l_i^k(1-l_i^{-(d_i-e_i+1)})}{\prod_i l_i^k l_i^{k-1}(l_i-1)} \\
&= \prod_i \sum_{d_i=e_i}^k l^{-d_i}(1-l_i^{-(d_i-e_i+1)}) \\
&= \prod_i \sum_{d_i=e_i}^k \frac{l_i^{d_i-e_i+1}-1}{l_i^{2d_i-e_i+1}} l^{-d_i}(1-l_i^{-(d_i-e_i+1)}) \\
&= \prod_i l_i^{-e_i} \sum_{j_i=1}^k \frac{l_i^{j_i}-1}{l_i^{2j_i-1}}, j_i = d_i-e_i+1. \qquad (3.19)
\end{aligned}
$$

Noting that $\sum_{j=1}^\infty (l^j-1)/(l^{2j-1}) = l^2/(l^2-1)$, we arrive at the conjecture $\zeta(l^e) = l^{2-e}/(l^2-1)$.

3.8.2 $u = 2$

Hence if $\mathrm{ord}_{l_i}(a_i-1) = d_i$ and $\mathrm{ord}_2(a_0-1) = d_0$, then there are $\prod_i A_{d_i} = 2^{k-d_0-1}\prod_i l_i^{k-d_i} - l_i^{k-d_i-1} = 2^{k-d_0-1}\prod_i l^{k-d_i-1}(l_i-1)$ possible choices of a_i. Additionally $(a-1)r = r' l_i^{d_i}$, so $r' l_i^{d_i} + b \equiv 0 \pmod{l_i^{k-d_i}}$, $r' 2^{d_0} + b \equiv 0 \pmod{2^{k-d_0}}$ and b depends on if a/c is even or odd. This gives $\prod_i B_{(d_i,e_i)} = t^k(2^{d_0-e_0+1}-1)/2^{d_0-e_0+1}\prod_i (l^{d_i-e_i+1}-1)/l^{d_i-e_i+1}$ choices of b_i. Then as d_i ranges from e_i to k, we have number of δ with $a_i = \pm c_i$ for all i is $\prod_i \sum_{d_i=e_i}^k A_{d_i} B_{(d_i,e_i)}$.

We can compute $|\mathcal{C}| / |\mathrm{Gal}(K/\mathbb{Q})|$ as follows:

$$\begin{aligned}
\frac{\prod_i \sum_{d_i=e_i}^k A_{d_i} B_{(d_i,e_i)}}{|\mathrm{Gal}(K/\mathbb{Q})|} &= \frac{\sum_{d_0=e_0}^k 2^{k-d_0-1} t^k \frac{2^{d_0-e_0+1}-1}{2^{d_0-e_0+1}} \prod_i \sum_{d_i=e_i}^k l^{k-d_i-1}(l_i-1)\frac{(l^{d_i-e_i+1}-1)}{l^{d_i-e_i+1}}}{t^k\phi(t^k)} \\
&= \frac{\sum_{d_0=e_0}^k 2^{k-d_0-1} t^k \frac{2^{d_0-e_0+1}-1}{2^{d_0-e_0+1}} \prod_i \sum_{d_i=e_i}^k l^{k-d_i-1}(l_i-1)\frac{(l^{d_i-e_i+1}-1)}{l^{d_i-e_i+1}}}{2^{k-1}\prod_i l_i^k \phi(l_i^k)} \\
&= \frac{2\sum_{d_0=e_0}^k 2^{-d_0} \frac{2^{d_0-e_0+1}-1}{2^{d_0-e_0+1}} \prod_i \sum_{d_i=e_i}^k l^{k-d_i-1}(l_i-1)\frac{(l^{d_i-e_i+1}-1)}{l^{d_i-e_i+1}}}{\prod_i l_i^{k-1}(l_i-1)} \\
&= \sum_{d_0=e_0}^k 2^{-d_0} \frac{2^{d_0-e_0+1}-1}{2^{d_0-e_0+1}} \prod_i \sum_{d_i=e_i}^k l^{-d_i} \frac{(l^{d_i-e_i+1}-1)}{l^{d_i-e_i+1}} \\
&= \sum_{d_0=e_0}^k \frac{2^{d_0-e_0+1}-1}{2^{2d_0-e_0+1}} \prod_i \sum_{d_i=e_i}^k \frac{(l^{d_i-e_i+1}-1)}{l^{2d_i-e_i+1}}. \qquad (3.20)
\end{aligned}$$

3.8.3 $u = 5$

Now, if $\mathrm{ord}_{l_i}(a_i-1) = d_i$ and $\mathrm{ord}_5(a_0-1) = d_0$, then there are $\prod_i A_{d_i} = \prod_i l_i^{k-d_i} - l_i^{k-d_i-1} = \prod_i l^{k-d_i-1}(l_i-1)$ possible choices of a_i. Additionally $(a_i-1)r = r'l_i^{d_i}$, so $r'l_i^{d_i} + b_i \equiv 0 \pmod{l_i^{k-d_i}}$. Therefore we have $b_i \not\equiv 0 \pmod{l_i^{d_i-e_i+1}}$ giving $\prod_i B_{(d_i,e_i)} = \prod_i l_i^k(l^{d_i-e_i+1} - 1)/l_i^{d_i-e_i+1} = \prod_i l_i^k(1-l_i^{-(d_i-e_i+1)})$ choices of b_i. Then as d_i ranges from e_i to k then we have $\prod_i \sum_{d_i=e_i}^k A_{d_i} B_{(d_i,e_i)}$ is the number of δ with $a_i = \left(\frac{a_i}{5}\right) c_i$ for all i.

We can compute $|\mathcal{C}| / |\mathrm{Gal}(K/\mathbb{Q})|$ as follows:

$$\begin{aligned}
\frac{\prod_i \sum_{d_i=e_i}^k A_{d_i} B_{(d_i,e_i)}}{|\mathrm{Gal}(K/\mathbb{Q})|} &= \frac{\prod_i \sum_{d_i=e_i}^k l^{k-d_i-1}(l_i-1) l_i^k (1-l_i^{-(d_i-e_i+1)})}{t^k\phi(t^k)} \\
&= \prod_i l_i^{-e_i} \sum_{j_i=1}^k \frac{l_i^{j_i}-1}{l_i^{2j_i-1}}, j_i = d_i - e_i + 1. \qquad (3.21)
\end{aligned}$$

3.8.4 $u = 10$

In the case that $u = 10$, then

$$S = \left\{ \begin{matrix} \prod_i (a_i x + b_i, c_i) : a_0, c_0 \in (\mathbb{Z}/u^k\mathbb{Z})^\times, b_0 \in \mathbb{Z}/u^k\mathbb{Z}, a_i, c_i \in (\mathbb{Z}/l_i^k\mathbb{Z})^\times, \\ b_i \in \mathbb{Z}/l_i^k\mathbb{Z}, a_i = \pm c_i, a_i = \left(\frac{a_0}{5}\right) c_i, (-1)^{b_0} = a_i/c_i \end{matrix} \right\}.$$

If $\mathrm{ord}_{l_i}(a_i - 1) = d_i$, $\mathrm{ord}_2(a_0 - 1) = d_{0_2}$, $\mathrm{ord}_5(a_0 - 1) = d_{0_5}$ and $d_{0_2} > 1$, then there are $\prod_i A_{d_i} = \prod_i l_i^{k-d_i} - l_i^{k-d_i-1} = \prod_i l^{k-d_i-1}(l_i - 1)$ possible choices of a_i. As $b_i \not\equiv 0 \pmod{l_i^{d_i-e_i+1}}$ and b_0 is even if $\left(\frac{a_0}{5}\right)$ and odd otherwise. Then

$$\prod_i B_{(d_i,e_i)} = t^k(2^{d_{0_2}-e_{0_2}+1} - 2^{d_{0_2}-e_{0_2}} - 1)/2^{d_{0_2}-e_{0_2}+1} \prod_i (l^{d_i-e_i+1} - 1)/l^{d_i-e_i+1}. \tag{3.22}$$

Then as d_i ranges from e_i to k, we have the number of δ with $a_i = \left(\frac{a_i}{5}\right) c_i$ for all i is $\prod_i \sum_{d_i=e_i}^k A_{d_i} B_{(d_i,e_i)}$.

$$\begin{aligned}
&\frac{\prod_i \sum_{d_i=e_i}^k A_{d_i} B_{(d_i,e_i)}}{|\mathrm{Gal}(K/\mathbb{Q})|} \\
&= \frac{\sum_{d_{0_2}=e_{0_2}}^k 2^{k-d_{0_2}-1} t^k \frac{2^{d_{0_2}-e_{0_2}+1} - 2^{d_{0_2}-e_{0_2}} - 1}{2^{d_{0_2}-e_{0_2}+1}} \prod_{i=0_5,1,\ldots,s} \sum_{d_i=e_i}^k l^{k-d_i-1}(l_i - 1) \frac{(l^{d_i-e_i+1}-1)}{l^{d_i-e_i+1}}}{t^k \phi(t^k)/2} \\
&= \frac{2\sum_{d_0=e_0}^k 2^{k-d_0-1} t^k \frac{2^{d_0-e_0+1} - 2^{d_0-e_0} - 1}{2^{d_0-e_0+1}} \prod_i \sum_{d_i=e_i}^k l^{k-d_i-1}(l_i - 1) \frac{(l^{d_i-e_i+1}-1)}{l^{d_i-e_i+1}}}{2^{k-1} \prod_i l_i^k \phi(l_i^k)} \\
&= \frac{2\sum_{d_0=e_0}^k 2^{-d_0} \frac{2^{d_0-e_0+1} - 2^{d_0-e_0} - 1}{2^{d_0-e_0+1}} \prod_i \sum_{d_i=e_i}^k l^{k-d_i-1}(l_i - 1) \frac{(l^{d_i-e_i+1}-1)}{l^{d_i-e_i+1}}}{\prod_i l_i^{k-1}(l_i - 1)} \\
&= 2 \sum_{d_0=e_0}^k 2^{-d_0} \frac{2^{d_0-e_0} - 1}{2^{d_0-e_0+1}} \prod_i \sum_{d_i=e_i}^k l^{-d_i} \frac{(l^{d_i-e_i+1} - 1)}{l^{d_i-e_i+1}} \\
&= 2 \sum_{d_0=e_0}^k \frac{2^{d_0-e_0} - 1}{2^{2d_0-e_0+1}} \prod_i \sum_{d_i=e_i}^k \frac{(l^{d_i-e_i+1} - 1)}{l^{2d_i-e_i+1}}.
\end{aligned} \tag{3.23}$$

If $e_{0_2} = 1$, then if $5^{e_{0_5}} \mid\mid |\alpha|$ and $2 \nmid |\alpha|$, then $2^{e_{0_2}}5^{e_{0_5}} \mid\mid Z(p)$. We need b to be even or odd depending on a, $2^{d_{0_2}}5^{d_{0_5}} \mid\mid a-1$, and $b \not\equiv 0 \pmod{5^{d_{0_5}-e_{0_5}+1}}$ as we can have infinitely many preimages of α under 2. Hence $\prod_i A_{d_i} = \prod_i l_i^{k-d_i} - l_i^{k-d_i-1} = \prod_i l^{k-d_i-1}(l_i-1)$. And $\prod_i B_{(d_i,e_i)} = t^k/2\prod_i(l^{d_i-e_i+1}-1)/l^{d_i-e_i+1}$.

$$
\begin{aligned}
\frac{\prod_i \sum_{d_i=e_i}^k A_{d_i}B_{(d_i,e_i)}}{|\mathrm{Gal}(K/\mathbb{Q})|} &= \frac{\sum_{d_0=e_0}^k 2^{k-d_0-1}t^k\frac{1}{2}\prod_i\sum_{d_i=e_i}^k l^{k-d_i-1}(l_i-1)\frac{(l^{d_i-e_i+1}-1)}{l^{d_i-e_i+1}}}{t^k\phi(t^k)/2} \\
&= \frac{2\sum_{d_0=e_0}^k 2^{k-d_0-1}t^k\frac{1}{2}\prod_i\sum_{d_i=e_i}^k l^{k-d_i-1}(l_i-1)\frac{(l^{d_i-e_i+1}-1)}{l^{d_i-e_i+1}}}{2^{k-1}\prod_i l_i^k\phi(l_i^k)} \\
&= \frac{2\sum_{d_0=e_0}^k 2^{-d_0}\frac{1}{2}\prod_i\sum_{d_i=e_i}^k l^{k-d_i-1}(l_i-1)\frac{(l^{d_i-e_i+1}-1)}{l^{d_i-e_i+1}}}{\prod_i l_i^{k-1}(l_i-1)} \\
&= 2\sum_{d_0=e_0}^k 2^{-d_0}\frac{1}{2}\prod_i\sum_{d_i=e_i}^k l^{-d_i}\frac{(l^{d_i-e_i+1}-1)}{l^{d_i-e_i+1}} \\
&= \sum_{d_0=e_0}^k \frac{1}{2^{d_0}}\prod_i\sum_{d_i=e_i}^k \frac{(l^{d_i-e_i+1}-1)}{l^{2d_i-e_i+1}}. \qquad (3.24)
\end{aligned}
$$

3.9 Z-Densities

We begin by restating the main conjecture of Anderson and Bruckman. Let q be a prime such that $q^j \mid\mid m$. Then $\zeta(m) = \rho(m)\prod_{q^j||m}\zeta(q^j)$.

$$
\zeta(q^j) = \begin{cases} 1 & \text{if } j = 0, \\ \frac{q^{2-j}}{q^2-1} & \text{if } j \geq 1. \end{cases} \qquad (3.25)
$$

$$\rho(m) = \begin{cases} 1 & \text{if } 10 \nmid m, \\ 5/4 & \text{if } m \equiv 10 \pmod{20}, \\ 1/2 & \text{if } 20 \mid m. \end{cases} \tag{3.26}$$

Theorem 3.25. *For positive integers m and prime divisors q of m, we have $\zeta(m) = \rho(m)\prod_{q^j||m}\zeta(q^j)$.*

Proof. Let t be squarefree such that $t \mid m$ with $t = ul_1 \cdots l_s$. For each $l_i \neq 2, 5$ a prime, if $l_i^{e_i} \mid\mid m$, then let $l_i \mid t$. For $2^{e_{02}} \mid m$, let $2 \mid u$ and similarly for $5^{e_{05}} \mid m$. Let $K = \mathbb{Q}(\gamma_{t^k}, \zeta_{t^k}, \sqrt{5})$ be defined as usual.

We don't know how many preimages there are when $p \pm 1 \equiv 0 \pmod{m^k}$. In this instance we do not know if there are a fixed number of preimages or infinitely many. Similarly for $p \equiv \pm 1 \pmod{l_i^k}$ for some prime $l_i \mid m$. Let $u = 1, 2$ or 5, $\epsilon > 0$, and $L_i = \sum_{j_i=1}^{\infty} \frac{l_i^{j_i}-1}{l_i^{2j_i-1}}$ where $j_i = d_i - e_i + 1$. Note this sum converges and $L_0 = \zeta(2^{e_{02}})\zeta(2^{e_{05}})$ and $L_i = \zeta(l_i^{e_i})$ otherwise. From Corollary 2.36, the density of primes such that $p \pm 1 \equiv 0 \pmod{l_i^k}$ is $2/\phi(l_i^k)$. We choose k such that $\left| L_i - \sum_{j_i=1}^{k-1} \frac{l_i^{j_i}-1}{l_i^{2j_i-1}} \right| < \epsilon$ and $2/\phi(l_i^k) < \epsilon$ for all i. For a fixed k and then there exists some $C(k)$, such that for $x > C(k)$ then $|\{p \leq x : p \text{ prime and } m \mid Z(p)\}/\pi(x) - |\mathcal{C}| / |\mathrm{Gal}(K/\mathbb{Q})|| < \epsilon$ by Theorem 2.35 and $\left|\{p \leq x : p \text{ prime and } p \equiv \pm 1 \pmod{l_i^k} - 2/\phi(l_i^k)\}\right| < \epsilon$.

$$-\epsilon + \frac{|\mathcal{C}|}{|\mathrm{Gal}(K/\mathbb{Q})|} < \frac{\{p \leq x : p \text{ prime and } m \mid Z(p)\}}{\pi(x)} < \frac{|\mathcal{C}|}{|\mathrm{Gal}(K/\mathbb{Q})|} + \epsilon. \tag{3.27}$$

For the right hand side we must account for the number of bad primes where we do not know the number of preimages. Therefore the right hand side gives the following inequality:

$$\begin{aligned}\frac{|\mathcal{C}|}{|\mathrm{Gal}(K/\mathbb{Q})|}+\epsilon &= \prod_i(\sum_{j_i=1}^{k}\frac{l_i^{j_i}-1}{l_i^{2j_i-1}})+\sum_i\frac{2}{\phi(l_i^k)}+\epsilon \\ &< (L_0+\epsilon)\cdots(L_s+\epsilon)+\sum_i\epsilon+\epsilon \\ &< L_0\cdots L_s+(2^{s+1}-1)\epsilon+(s+1)\epsilon+\epsilon \\ &= L_0\cdots L_s+(2^{s+1}+s+1)\epsilon. \qquad (3.28)\end{aligned}$$

We will have $(2^{s+1}-1)$ monomial cross terms in $(L_0+\epsilon)\cdots(L_s+\epsilon)$ which are each less than ϵ. For the left hand side we do not throw out the bad primes for a lower bound. This gives the following inequality:

$$\begin{aligned}-\epsilon+\frac{|\mathcal{C}|}{|\mathrm{Gal}(K/\mathbb{Q})|} &= -\epsilon+\prod_i\sum_{j_i=1}^{k}\frac{l_i^{j_i}-1}{l_i^{2j_i-1}} \\ &> -\epsilon+(L_0-\epsilon)\cdots(L_s-\epsilon) \\ &> -\epsilon-(2^{s+1}-1)\epsilon+L_0\cdots L_s. \qquad (3.29)\end{aligned}$$

Combining we have the following:

$$-2^{s+1}\epsilon+L_0\cdots L_s<\frac{\{p\leq x: p \text{ prime and } m \mid Z(p)\}}{\pi(x)}<L_0\cdots L_s+(2^{s+1}+s+1)\epsilon. \qquad (3.30)$$

Therefore we may conclude that for $\epsilon>0$ there exists a C for $x>C$ then

$$\left|\frac{\#\{p\leq x: p \text{ prime and } m \mid Z(p)\}}{\pi(x)}-L_0\cdots L_s\right|<(2^{s+1}+s+1)\epsilon. \qquad (3.31)$$

The proof of $u=10$ follows similarly. Hence we have shown the conjecture is true. □

Chapter 4: Further Research

We proved that the conjecture by Anderson and Bruckman was indeed true and furthermore we developed a methodology to attack problems of of similar nature. A question one could further study is entry points of other sequences. Given a recursive sequence, and a corresponding group law under what conditions could one find similar dynamics to solve the natural density question? In particular, we would be interested looking at $x^2 + ny^2 = 1$ and viewing the corresponding sequences with generators satisfying the equation.

Let $E(\mathbb{F}_p) = \{(x, y) : x, y, a, b \in \mathbb{F}_p, y^2 = x^3 + ax + b\}$ be an elliptic curve over $\mathbb{F}_p$. Then $E(\mathbb{F}_p)$ is a cyclic group or a product of cyclic groups. Therefore, we would be interested in preimages, which could have implications in elliptic curve cryptography. However, it may be difficult to generalize the order of a point based on it's preimages and the group size, as the conclusions reached in Theorem 2.43 rely on the group being solely cyclic.

Bibliography

[1] Paul S. Bruckman and Peter G. Anderson. Conjectures on the Z-densities of the Fibonacci sequence. *Fibonacci Quart.*, 36(3):263–271, 1998.

[2] David A. Cox. *Primes of the form* x^2+ny^2. A Wiley-Interscience Publication. John Wiley & Sons Inc., New York, 1989. Fermat, class field theory and complex multiplication.

[3] Whitfield Diffie and Martin E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6):644–654, November 1976.

[4] David S. Dummit and Richard M. Foote. *Abstract algebra.* John Wiley & Sons Inc., Hoboken, NJ, third edition, 2004.

[5] Michael D. Fried and Moshe Jarden. *Field arithmetic*, volume 11 of *Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics].* Springer-Verlag, Berlin, third edition, 2008. Revised by Jarden.

[6] I. Martin Isaacs. *Algebra: a graduate course.* Mathematics Series. Brooks/Cole Publishing Company, Pacific Grove, California, 1994.

[7] Gerald J. Janusz. *Algebraic number fields*, volume 7 of *Graduate Studies in Mathematics.* American Mathematical Society, Providence, RI, second edition, 1996.

[8] Rafe Jones and Jeremy Rouse. Galois theory of iterated endomorphisms. *Proc. Lond. Math. Soc. (3)*, 100(3):763–794, 2010. Appendix A by Jeffrey D. Achter.

[9] J. C. Lagarias. The set of primes dividing the Lucas numbers has density 2/3. *Pacific J. Math.*, 118(2):449–461, 1985.

[10] Richard A. Mollin. *Algebraic number theory.* CRC Press Series on Discrete Mathematics and its Applications. Chapman & Hall/CRC, Boca Raton, FL, 1999.

[11] Pieter Moree. On primes p for which d divides $\mathrm{ord}_p(g)$. *Funct. Approx. Comment. Math.*, 33:85–95, 2005.

[12] Joseph H. Silverman. *The arithmetic of dynamical systems*, volume 241 of *Graduate Texts in Mathematics.* Springer, New York, 2007.

[13] P. Stevenhagen and H. W. Lenstra, Jr. Chebotarëv and his density theorem. *Math. Intelligencer*, 18(2):26–37, 1996.

[14] Ian Stewart and David Tall. *Algebraic number theory and Fermat's last theorem.* A K Peters Ltd., Natick, MA, third edition, 2002.

[15] Gérald Tenenbaum. *Introduction to analytic and probabilistic number theory*, volume 46 of *Cambridge Studies in Advanced Mathematics.* Cambridge University Press, Cambridge, 1995. Translated from the second French edition (1995) by C. B. Thomas.

Vita

Paul Cubre

Date of Birth: January 21, 1986

Place of Birth: Fair Oaks, California

Education:

- Master of Arts in Mathematics,

  Wake Forest University, expected May 2012.

  Thesis title: The Z-Densities of the Fibonacci Sequence

  Advisor: Jeremy A. Rouse

- Bachelor of Science in Mathematics,

  University of California, Los Angeles, June 2008.