ARITHMETICALLY EXCEPTIONAL LATTÈS MAPS ATTACHED TO ELLIPTIC CURVES WITHOUT COMPLEX MULTIPLICATION

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES
OF
MIDDLE EAST TECHNICAL UNIVERSITY

BY

OĞUZHAN ODABAŞ

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR
THE DEGREE OF MASTER OF SCIENCE
IN
MATHEMATICS

JUNE 2023

Approval of the thesis:

ARITHMETICALLY EXCEPTIONAL LATTÈS MAPS ATTACHED TO ELLIPTIC CURVES WITHOUT COMPLEX MULTIPLICATION

submitted by **OĞUZHAN ODABAŞ** in partial fulfillment of the requirements for the degree of **Master of Science in Mathematics Department, Middle East Technical University** by,

Prof. Dr. Halil Kalıpçılar
Dean, Graduate School of **Natural and Applied Sciences** ________________

Prof. Dr. Yıldıray Ozan
Head of Department, **Mathematics** ________________

Assoc. Prof. Dr. Ömer Küçüksakallı
Supervisor, **Mathematics, METU** ________________

Examining Committee Members:

Assoc. Prof. Dr. Burcu Gülmez Temür
Mathematics, Atılım University ________________

Assoc. Prof. Dr. Ömer Küçüksakallı
Mathematics, METU ________________

Assist. Prof. Dr. Özcan Yazıcı
Mathematics, METU ________________

Date:20.06.2023

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Surname: Oğuzhan Odabaş

Signature :

ABSTRACT

ARITHMETICALLY EXCEPTIONAL LATTÈS MAPS ATTACHED TO ELLIPTIC CURVES WITHOUT COMPLEX MULTIPLICATION

Odabaş, Oğuzhan
M.S., Department of Mathematics
Supervisor: Assoc. Prof. Dr. Ömer Küçüksakallı

June 2023, 69 pages

Let E be an elliptic curve given by $y^2 = x^3 + Ax + B$. If E has complex multiplication, then under certain conditions, there is a formula to compute the value sets of Lattès maps induced by such curves. However, when the endomorphism ring of E consists only of the integers, then there is no known method to compute the value sets of Lattès maps attached to such curves. In this thesis, we will introduce a Pari/GP code that computes the value sets of Lattès maps attached to elliptic curves without complex multiplication and discuss the arithmetic exceptionality of these maps experimentally.

Keywords: Elliptic curve, Lattès map, Arithmetically exceptional maps.

ÖZ

KOMPLEKS ÇARPIMI OLMAYAN ELİPTİK EĞRİLERDEN GELEN ARİTMETİK OLARAK İSTİSNAİ LATTÈS EŞLEMELERİ

Odabaş, Oğuzhan
Yüksek Lisans, Matematik Bölümü
Tez Yöneticisi: Doç. Dr. Ömer Küçüksakallı

Haziran 2023 , 69 sayfa

E, $y^2 = x^3 + Ax + B$ denklemi ile verilen eliptik eğri olsun. Belirli koşullar altında, eğer E eliptik eğrisinde kompleks çarpma varsa, bu tarz eğrilerden gelen Lattès fonksiyonlarının görüntü kümelerini hesaplamak için bir formül vardır. Fakat, eğer E'nin endomorfizma halkası sadece tamsayılardan oluşuyorsa, bu durumda bu tarz eğrilerden gelen Lattès fonksiyonlarının görüntü kümelerini hesaplamak için bilinen bir metot yoktur. Bu tezde, kompleks çarpma olmayan eliptik eğrilerden gelen Lattès fonksiyonlarının görüntü kümelerini hesaplayan bir Pari/GP kodu sunacak ve bu fonksiyonların aritmetiksel istisnailiklerini deneysel olarak tartışacağız.

Anahtar Kelimeler: Eliptik eğri, Lattès eşlemesi, Aritmetik olarak istisnai eşlemeler.

To my beloved mother, for her amazing queen sacrifices!!

ACKNOWLEDGMENTS

I am deeply grateful to my thesis supervisor, Assoc. Prof. Dr. Ömer Küçüksakallı, for his unwavering support and guidance throughout this process. His expertise and patience have been priceless to me and have played a crucial role in the completion of this thesis. I could not have undertaken this journey without his help.

I would also like to thank Assoc. Prof. Dr. Burcu Gülmez Temür and Assist. Prof. Dr. Özcan Yazıcı for serving on my thesis committee and providing helpful feedback and suggestions.

Finally, I would like to thank my whole family for their love and support during this process. Without them, this journey would not have been possible.

I am grateful to everyone who has supported me during this process. Without your help and guidance, this work would not have been possible.

TABLE OF CONTENTS

CHAPTERS

LIST OF TABLES

TABLES

CHAPTER 1

INTRODUCTION

1.1 Motivation and Problem Definition

Let $\mathbf{F}_q$ be the finite field of q elements. It is of interest to know whether an arbitrary map from $\mathbf{F}_q$ to itself gives a bijection. A polynomial f whose coefficients belong to $\mathbf{F}_q$ can be considered as a map from $\mathbf{F}_q$ to itself. We say that f is a permutation polynomial of $\mathbf{F}_q$ if this map induces a bijection from $\mathbf{F}_q$ onto itself. Since, in this case, the domain and the range of f is $\mathbf{F}_q$, which is a finite set, then each one of the following can also be used as an equivalent condition of being a permutation polynomial:

- the map f is injective,
- the map f is surjective,
- The equation $f(x) = a$ has a unique solution in $\mathbf{F}_q$ whenever $a \in \mathbf{F}_q$.

Among the simplest examples of permutation polynomials are the ones provided by power maps, which are defined by

$$f(x) = x^m$$

for certain integer $m \geq 1$ [5].

Another example of permutation polynomials comes from the family of Dickson polynomials considered over $\mathbf{F}_q$, which can be defined by the recurrence relation:

$$D_n(x, a) = xD_{n-1}(x, a) - aD_{n-2}(x, a)$$

with the initial conditions $D_0(x, a) = 2$ and $D_1(x, a) = x$, where a is an arbitrary element of $\mathbf{F}_q$ [5].

If $r(x)$ is a rational function whose coefficients belong to the finite field $\mathbf{F}_q$, then one can also discuss the bijectivity of $r(x)$ over $\mathbf{F}_q$. If $r(x)$ permutes $\mathbf{F}_q \cup \{\infty\}$, then we call $r(x)$ a permutation rational function. Here, the symbol ∞ denotes the point at infinity. The reason why we add the point at infinity is that there is a possibility that the denominator of $r(x)$ vanishes for some elements of $\mathbf{F}_q$. The images of such elements are mapped to the point at infinity [6].

In this thesis, we will be concerned with rational functions that are induced by some elliptic curve E, which can be defined by the graph of an equation of the form

$$E : y^2 = x^3 + Ax + B,$$

where the coefficients A and B are elements of some field [12].

Given two points

$$P_1 = (x_1, y_1), \;\; P_2 = (x_2, y_2)$$

on an elliptic curve E, another point P_3 lying on this curve can be obtained by drawing the line through P_1 and P_2 and then reflecting the intersection point (the point where the line intersects the curve) across the x-axis. If we denote this operation by $+_E$, then we can write $P_1 +_E P_2 = P_3$. This operation is called the elliptic curve point addition and makes $(E, +_E)$ into an abelian group [12].

An endomorphism of E is a group homomorphism from $(E, +_E)$ to itself which is given by rational functions. The simplest example of such maps is the multiplication by an integer n homomorphisms for some $n \geq 1$. We denote this endomorphism by the symbol $[n]$. Let $P = (a, b)$ be an arbitrary point of E. It turns out that the x-coordinate of $[n](P)$ can be expressed by some rational function that depends only on the first variable [12]. This rational function is called the n-th Lattès map attached to the elliptic curve E [9].

An elliptic curve E is said to have **complex multiplication** if it has endomorphisms other than the ones given by multiplication by an integer. If we denote the endomorphism ring of E by End(E), then we can say that E has complex multiplication if End(E) is strictly larger than the integers $\mathbf{Z}$ [12].

Let K be a number field and $r(x) \in K[x]$ be a rational function. We can write $r = f/g$ with $(f, g) = 1$ for some $f, g \in K[x]$. We can reduce the coefficients of the polynomials f and g modulo some prime ideal $\mathfrak{p}$ of K and further, for all but finitely many primes of K, the reduced function makes sense and induces a map on the projective 1-space $\mathbf{P}^1(K/\mathfrak{p}) = K/\mathfrak{p} \cup \{\infty\}$. The function r is then called **arithmetically exceptional** if this induced function, which we denote by $\bar{r}$, gives a bijection for infinitely many primes of K. If the residue field is $\mathbf{F}_q$ with $q = p^n$ for some integer n, then this is equivalent to saying that the value set of $\bar{r}$ contains exactly $p^n + 1$ elements [2].

In [3], Küçüksakallı shows that if E is an elliptic curve with complex multiplication, then under certain conditions, the projective 1-space $\mathbf{P}^1(\mathbf{F}_{q^m})$ can be expressed in terms of kernels of some extra endomorphisms (endomorphisms other than the ones given by multiplication by an integer) for each integer $m \geq 1$. Furthermore, there is also a formula to compute the value sets of Lattès maps that are induced by E. Having such a formula, one can determine if the Lattès maps induced by such elliptic curves are permutations and discuss their arithmetic exceptionality as well.

In the general case, however, there is no known formula. Namely, if E is an elliptic curve without complex multiplication, then there is no formula to compute the value sets of Lattès maps over finite fields.

In this thesis, our goal is to investigate the value sets of Lattès maps attached to elliptic curves without complex multiplication and discuss the arithmetic exceptionality of these maps. To accomplish this goal, we will introduce a computer-algebra program Pari/GP code, that computes the value sets of such maps. Moreover, within a specified range, we will look at the density of permutations for various primes to discuss the arithmetic exceptionality of such maps experimentally.

The organization of the thesis is as follows:

The first chapter is the introduction chapter, where we give some basic definitions and state the problem of the thesis.

In the second chapter, we first discuss the arithmetic exceptionality of power maps. There is a well-known criterion to determine under which condition power maps give a permutation [5]. Then we discuss the arithmetic exceptionality of Dickson polynomials. Again there is a well-known criterion to determine if a Dickson polynomial gives a permutation [5]. We review two alternative proofs of this fact that are due to [3] and [4]. The first proof relies on an approach that uses the fixed points of the Dickson polynomials over the complex numbers and expresses the projective 1-space $\mathbf{P}^1(\mathbf{F}_q)$ in terms of these fixed points. The second proof uses the endomorphisms of the singular cubic curve

$$y^2 = 4x^3 + x^2$$

and expresses $\mathbf{P}^1(\mathbf{F}_q)$ in terms of the kernels of these endomorphisms.

In the third chapter, we start by providing the theoretical background related to the theory of elliptic curves. Then we see that the method used for the singular cubic curve, which is described in the second chapter, can be generalized to certain elliptic curves with complex multiplication. More precisely, if E is an elliptic curve with complex multiplication, then under certain conditions, the projective 1-space $\mathbf{P}^1(\mathbf{F}_q)$ can be expressed in terms of some torsion points of E. Using this characterization, the formula for the value sets of Lattès maps is given, and further a criterion to determine the bijectivity of such maps is provided [3].

In the fourth chapter, we first introduce a code that computes the value sets of Dickson polynomials over finite fields as a motivating example in order to exemplify the computations in Pari/GP. Then we introduce two main codes, which we named `card` and `permdens`. Given inputs A, B, the integer k, and a prime p, the function `card` returns the size of the value set of the k-th Lattès map attached to the elliptic curve

$$E : y^2 = x^3 + Ax + B$$

over the finite field $\mathbf{F}_p$. Similarly, given A, B and the integer k, `permdens` returns the density of permutations of the k-th Lattès maps considered over $\mathbf{F}_p$'s where p is ranging over the first 1229 primes, i.e., primes less than 10000.

In the fifth chapter, we make some observations related to the computations done in the fourth chapter.

CHAPTER 2

REAL CYCLOTOMIC CASE

In this chapter, we describe the notion of arithmetic exceptionality and consider this notion for some particular functions. Firstly, the arithmetic exceptionality of power maps is discussed. Then we consider the arithmetic exceptionality of Dickson polynomials. There is a well-known criterion to determine if a Dickson polynomial permutes $\mathbf{F}_q$ or not [5]. Here, we give two alternative approaches that are due to [3] and [4]. The first method uses the fixed points of a Dickson polynomial over complex numbers. On the other hand, the second method relies on a method that uses the endomorphisms of some singular cubic curve.

2.1 Arithmetic exceptionality of power maps

In this section, we discuss the arithmetic exceptionality of monomials which are also called power maps. These maps constitute the simplest examples of exceptional maps.

Let K be a number field and $r(x) \in K[x]$ be a rational function so that we can write $r = f/g$ with $(f, g) = 1$ for some $f, g \in \mathcal{O}_K[x]$. Here $\mathcal{O}_K$ and $K[x]$ denote the ring of algebraic integers of K and the polynomial ring with coefficients in K, respectively. The coefficients of f can be reduced modulo some prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$. Moreover, for infinitely many primes of $\mathcal{O}_K$, the reduced function $\bar{r}$ induces a map on the projective 1-space $\mathbf{P}^1(\mathcal{O}_K/\mathfrak{p}) = \mathcal{O}_K/\mathfrak{p} \cup \{\infty\}$ [2].

Now we can give the following definition.

Definition 2.1. [2] The rational function r is called **arithmetically exceptional** if the induced function, which we denote by $\bar{r}$, is a bijection for infinitely many prime ideals of $\mathcal{O}_K$.

Before giving the general result related to the arithmetic exceptionality of power maps, we would like to consider some particular cases to motivate the situation. In order to do so, the following example is given.

Example 2.2. Consider the mapping $f(x) = x^5$ defined over the rational numbers $\mathbf{Q}$. Observe that for each prime p, the induced map $\bar{f}$ makes sense. Since the multiplicative group $\mathbf{F}_p^*$ is cyclic of order $p-1$, the condition for $\bar{f}$ to be injective (and hence bijective) is equivalent to the condition $\gcd(5, p-1) = 1$, where we denote by $\gcd(5, p-1) = 1$ the greatest common divisor of the integer 5 and $p-1$. In other words, we have the following

$$\bar{f} \text{ permutes } \mathbf{F}_p \Longleftrightarrow \gcd(5, p-1) = 1.$$

By Dirichlet's prime number theorem, we can find infinitely many prime p satisfying the condition $\gcd(5, p-1) = 1$. This implies that f is arithmetically exceptional.

Now we give the general result.

Proposition 2.3. *[5] Let $\mathbf{F}_q$ be a finite field of characteristic p. Then for each integer $n \geq 1$, the monomial $f(x) = x^n$ permutes $\mathbf{F}_q$ if and only if gcd$(n, q-1) = 1$.*

Proof. Since the function in question is considered over the finite field $\mathbf{F}_q$, then it suffices to show that it is surjective. Firstly, the zero element is clearly mapped to itself. Now take an arbitrary element $b \in \mathbf{F}_q^*$. Since the multiplicative group $\mathbf{F}_q^*$ of non-invertible elements is cyclic, then there must be an element $a \in \mathbf{F}_q^*$ such that $\langle a \rangle = \mathbf{F}_q^*$, where $\langle a \rangle$ denotes the cyclic group generated by the element a. For a given integer n, the order of the element a^n is given by $\frac{q-1}{\gcd(n,q-1)}$. Since the order of the group $\mathbf{F}_q^*$ is $q-1$, then the element a^n is a generator for that group if and only if the integers n and $q-1$ are coprime. Moreover, the element a^n generates $\mathbf{F}_q^*$ if and only if there exists and integer k with $1 \leq k \leq q-1$ such that we have

$$(a^n)^k = b$$

or equivalently,

$$(a^k)^n = b$$

so that we obtain an element $a^k \in \mathbf{F}_q^*$ such that $f(a^k) = b$. Consequently, we see that the monomial x^n maps $\mathbf{F}_q$ onto itself, and this is the desired result. □

Note that if n is an odd integer, then the map $g(x) = x^n$ is arithmetically exceptional. This is because Dirichlet's prime number theorem implies that the arithmetic progression $2 + nk$ with $k \in \mathbf{N}$ contains infinitely many primes since 2 and n are coprime. For each prime of the form $p = 2 + nk_0$, we have

$$\gcd(n, p-1) = \gcd(n, 1 + nk_0) = 1.$$

2.2 Arithmetic exceptionality of Dickson polynomials

Another important example of arithmetically exceptional maps comes from the family of Dickson polynomials. In this section, we consider two different approaches to derive the exceptionality of these polynomials.

We start with the definition of an important family of functions called Chebyshev polynomials.

Definition 2.4. [7] Let $k \geq 1$ be an integer. The k-th Chebyshev polynomial (of the first kind) T_k is defined as the unique polynomial satisfying the following trigonometric identity:

$$T_k(\cos\alpha) = \cos k\alpha.$$

For each integer $k \geq 1$, T_k is a polynomial in $\cos\alpha$ of degree k [7]. To see this, we start with the well-known de Moivre's formula:

$$(\cos\alpha + i\sin\alpha)^k = \cos k\alpha + i\sin k\alpha.$$

Expanding the left-hand side of this equation using the Binomial Theorem, one obtains

$$(\cos\alpha + i\sin\alpha)^k = \sum_{j=0}^{k} \binom{k}{j} (i)^j (\sin\alpha)^j (\cos\alpha)^{k-j}.$$

We wish to find the expression for $\cos k\alpha$, which is a real part of the left-hand side of the latter equation by de Moivre's formula. On the other hand, the real terms of the sum come from the summands with even indices. Since $i^2 = -1$ and $\cos^2\alpha + \sin^2\alpha =$

1, then for each j, we have $i^{2j} = (-1)^j$ and $\sin^{2j}\alpha = (1-\cos^2\alpha)^j$. Plugging these two identities in the sum in question, we obtain the expression for $\cos k\alpha$:

$$\cos k\alpha = \sum_{j=0}^{\lfloor \frac{k}{2} \rfloor} \binom{k}{2j} (\cos^2\alpha - 1)^j (\cos^{k-2j}\alpha),$$

which is the same as

$$T_k(\cos\alpha) = \sum_{j=0}^{\lfloor \frac{k}{2} \rfloor} \binom{k}{2j} (\cos^2\alpha - 1)^j (\cos^{k-2j}\alpha).$$

Finally, making the change of variable $\cos\alpha = x$ yields

$$T_k(x) = \sum_{j=0}^{\lfloor \frac{k}{2} \rfloor} \binom{k}{2j} (x^2 - 1)^j (x)^{k-2j}.$$

This shows that for each integer $k \geq 1$, $T_k(x)$ is a polynomial in x of degree k.

The Chebyshev polynomials can be normalized by defining $D_k(x) = 2T_k(\frac{x}{2})$ to obtain a new set of polynomials. Observe that for each $k \geq 1$, $D_k(x)$ satisfies a similar identity. That is, we have

$$D_k(2\cos\alpha) = 2\cos k\alpha.$$

This new family of polynomials has a special name.

Definition 2.5. [5] Let $k \geq 1$ be an integer. The k-th Dickson polynomial D_k (of the first kind) is defined by the sum

$$D_k(x) = \sum_{j=0}^{\lfloor \frac{k}{2} \rfloor} \frac{k}{k-j} \binom{k-j}{j} (-1)^j x^{k-2j}.$$

Below, we list the first few Chebyshev and Dickson polynomials:

$$\begin{aligned}
T_0(x) &= 1, & D_0(x) &= 2,\\
T_1(x) &= x, & D_1(x) &= x,\\
T_2(x) &= 2x^2 - 1, & D_2(x) &= x^2 - 2,\\
T_3(x) &= 4x^3 - 3x, & D_3(x) &= x^3 - 3x,\\
T_4(x) &= 8x^4 - 8x^2 + 1, & D_4(x) &= x^4 - 4x^2 + 2,\\
T_5(x) &= 16x^5 - 20x^3 + 5x, & D_5(x) &= x^5 - 5x^3 + 5x.
\end{aligned}$$

The family of Dickson polynomials possesses many important and remarkable properties. The following lemma lists some of them that are of our interest.

Lemma 2.6. *[5, 6] Dickson polynomials satisfy the following properties:*

1. *Let $k \geq 1$ be an integer. Then*

$$D_k(x + \frac{1}{x}) = x^k + \frac{1}{x^k}.$$

2. *For arbitrary integers $m, n \geq 1$, Dickson polynomials have the composition property:*

$$D_{mn} = D_m \circ D_n = D_n \circ D_m.$$

3. *Let $q = p^n$ where p is a prime and $n \geq 1$ an integer. Then*

$$D_q(x) \equiv x^q \text{ (mod } p).$$

Proof. 1. According to Edward Waring's method for expressing an arbitrary symmetric polynomial in terms of elementary symmetric polynomials [5], the symmetric polynomial $x_1^k + x_2^k$ has the following expression:

$$x_1^k + x_2^k = \sum_{j=0}^{\lfloor \frac{k}{2} \rfloor} \frac{k}{k-j} \binom{k-j}{j} (-x_1 x_2)^j x_1 + {x_2}^{k-2j}.$$

Putting $x_1 = x, x_2 = \frac{1}{x}$, we see that the right-hand side of the above equation is exactly the defining sum for $D_k(x)$. This finishes the proof of the first part.

2. We recall that D_k satisfies $D_k(2\cos\alpha) = 2\cos k\alpha$. It follows that we have

$$D_{mn}(2\cos\alpha) = 2\cos mn\alpha = D_m(2\cos n\alpha) = D_n(2\cos m\alpha)$$

and this proves second part of the lemma.

3. Expanding $(y + \frac{1}{y})^q$ by using the Binomial Theorem, one obtains

$$(y + \frac{1}{y})^q = \sum_{j=0}^{q} \binom{q}{j} y^{q-j} \frac{1}{y^j}.$$

We claim that for each j such that $1 \leq j \leq q-1$, the binomial coefficients $\binom{q}{j}$ are divisible by p. To see this, we first note that

$$\binom{q}{j} = \frac{q(q-1) \,...\, (q-j+1)}{j!}.$$

Now if the integer $j!$ is not divisible by p, then q and $j!$ must be coprime so that $j!$ divides the factor $(q-1)\ ...\ (q-j+1)$. This implies that the coefficient $\binom{q}{j}$ is divisible by p.

If, on the other hand, p divides $j!$, then the integer $j!$ must be of the form $j! = p^m a$ with $1 \leq m \leq n-1$ for some integer a. It follows that the coefficient $\binom{q}{j}$ is a multiple of p. Therefore, we obtain the following:

$$(y + \tfrac{1}{y})^q \equiv y^q + \tfrac{1}{y^q} \pmod{p}.$$

Combining this with the identity $D_q(y + \frac{1}{y}) = y^q + \frac{1}{y^q}$, which is proved in the first part, one gets

$$D_q(y + \tfrac{1}{y}) \equiv (y + \tfrac{1}{y})^q \pmod{p}.$$

Finally, making the change of variable $(y + \frac{1}{y}) = x$ yields the desired result.

□

The first method we will introduce in order to determine the value sets of Dickson polynomials over finite fields uses the fixed points of these polynomials over complex numbers. The method is due to [4].

We need a few definitions. We start with the following:

Definition 2.7. Let f be an arbitrary polynomial. The orbit of an element x under f is defined by

$$\mathcal{O}(x) = \{f^n(x) \ : \ n \geq 0\}.$$

Definition 2.8. The Julia set of a polynomial f over complex numbers is defined by

$$J(f) = \{x \in \mathbf{C} \ : \ \mathcal{O}(x) \ \text{ is bounded}\}.$$

Observe by definition that any periodic point must be contained in the Julia set since the orbits of such points contain a finite number of elements.

To begin with, we consider the following real-valued function of a real variable

$$\alpha(\sigma) = e^{2\pi i \sigma} + e^{-2\pi i \sigma} \quad , \sigma \in \mathbf{R}.$$

Now if the complex number $x \in \mathbf{C}$ is a fixed point of the k-th Dickson polynomial, then by definition of a fixed point, we have $D_k(x) = x$. Moreover, x must be contained in the Julia set of D_k since any fixed point is also a periodic point trivially. On the other hand, the Julia set of D_k over complex numbers is the closed interval $[-2, 2]$. Also, note that the value set of the function α over real numbers is also the closed interval $[-2, 2]$. It follows from these observations that one can write

$$J(D_k) = \{\alpha(\sigma) \ : \ \sigma \in \mathbf{R}\}.$$

Therefore, we must have $x = \alpha(\sigma)$ for some $\sigma \in \mathbf{R}$. Furthermore, using Euler's identity to expand the function $\alpha(\sigma)$, one obtains

$$\alpha(\sigma) = 2\cos 2\pi\sigma.$$

As we have mentioned before, D_k satisfies the trigonometric identity: $D_k(2\cos\theta) = 2\cos 2\theta$. This implies that we have

$$D_k(\alpha(\sigma)) = \alpha(k\sigma).$$

But since $x = \alpha(\sigma)$ is a fixed point by assumption, we must have

$$\alpha(\sigma) = \alpha(k\sigma).$$

The above equality is satisfied if and only if σ and $k\sigma$ differ by an integer. In other words, we have the following:

$$\alpha(\sigma) = \alpha(k\sigma) \Longleftrightarrow \sigma - k\sigma \in \mathbf{Z} \text{ or } \sigma + k\sigma \in \mathbf{Z}.$$

Now if $\sigma - k\sigma \in \mathbf{Z}$, then there exists some integer m_1 such that $\sigma(k-1) = m_1$ which is the same as $\sigma = m_1/(k-1)$. In a similar manner, if $\sigma + k\sigma \in \mathbf{Z}$, then we must have $\sigma = m_2/(k+1)$ for some integer m_2. It turns out that the fixed points of D_k over complex numbers can take two possible forms. More precisely, we have proved the following:

Theorem 2.9. *[4]*

$$\mathit{Fix}(D_k, \mathbf{C}) = \left\{\alpha\left(\frac{m}{k-1}\right) \ : \ m \in \mathbf{Z}\right\} \cup \left\{\alpha\left(\frac{m}{k+1}\right) \ : \ m \in \mathbf{Z}\right\}.$$

Now in order to determine the cardinality of the set $\mathrm{Fix}(D_k, \mathbf{C})$, we use the following procedure:

If k is even, then $\alpha\left(\frac{a}{k-1}\right)$ has $\frac{k}{2}$ elements and $\alpha\left(\frac{a}{k+1}\right)$ has $\frac{k+2}{2}$ elements. Moreover, their intersection contains only one point, which is $\alpha(0) = 2$. According to the Inclusion-exclusion principle, we have

$$|\mathrm{Fix}(D_k, \mathbf{C})| = \frac{k}{2} + \frac{k+2}{2} - 1.$$

If k is odd, then $\alpha\left(\frac{a}{k-1}\right)$ has $\frac{k+1}{2}$ elements and $\alpha\left(\frac{a}{k+1}\right)$ has $\frac{k+3}{2}$ elements. Also, in this case, the intersection of the two sets contains two points, which are $\alpha(0) = 2$ and $\alpha\left(\frac{1}{2}\right) = -2$. Again using the Inclusion-exclusion principle, we get

$$|\mathrm{Fix}(D_k, \mathbf{C})| = \frac{k+1}{2} + \frac{k+3}{2} - 2.$$

As a result, in both cases, we see that the set of fixed points of D_k over complex numbers contains exactly k elements. Since $D_k(x)$ is a polynomial of order k, this is equivalent to saying that the equation $D_k(x) - x = 0$ has k solutions in $\mathbf{C}$.

The following theorem shows that whenever $q = p^n$ for some prime p and an integer $n \geq 1$, the elements of the set $\mathrm{Fix}(D_q, \mathbf{C})$ and the finite field $\mathbf{F}_q$ are in one-to-one correspondence.

Theorem 2.10. *[4] Let $\mathbf{Q}(Fix(D_q, \mathbf{C}))$ be the field extension that is obtained by adjoining the elements of the set $Fix(D_k, \mathbf{C})$ to the field of rational numbers $\mathbf{Q}$, and let $\mathfrak{p}$ be a prime ideal of $\mathbf{Q}(Fix(D_q, \mathbf{C}))$ lying over p. Then we have*

$$\overline{Fix(D_q, \mathbf{C})} = \mathbf{F}_q$$

where $\overline{Fix(D_q, \mathbf{C})}$ is the set obtained by reducing the elements of $Fix(D_q, \mathbf{C})$ modulo $\mathfrak{p}$.

Proof. First of all, third part of the Lemma 2.6 implies that we have

$$D_q(x) \equiv x^q \pmod{p}.$$

So if we reduce an arbitrary element of $\mathrm{Fix}(D_q, \mathbf{C})$ modulo $\mathfrak{p}$, we obtain a solution to the polynomial $x^q - x = 0$ so that the fixed points of D_q modulo $\mathfrak{p}$ must be elements of the finite field $\mathbf{F}_q$. Moreover, we can obtain all elements of $\mathbf{F}_q$ by reducing the elements of Fix$(D_q, \mathbf{C})$ modulo $\mathfrak{p}$. It follows that the elements of the two sets are in one-to-one correspondence. We indicate this situation by writing

$$\text{Fix}(D_q, \mathbf{C}) \leftrightarrow \mathbf{F}_q.$$

□

Now combining our last result with the characterization of the fixed points given in theorem 2.9, the formula for the cardinality of the value sets of Dickson polynomials over finite fields can be found. Firstly, let $\eta(k, q)$ be the two variable piecewise function, which is defined by

$$\eta(k,q) = \begin{cases} 0 & \text{If} \quad \gcd(k, q-1) \equiv \gcd(k, q+1) \pmod 2 \\ \frac{1}{2} & \text{Otherwise} \end{cases}.$$

Applying the Inclusion-exclusion principle, one obtains

$$|V_{D_k(\mathbf{F}_q)}| = \frac{q-1}{2\gcd(k, q-1)} + \frac{q+1}{2\gcd(k, q+1)} + \eta(k, q)$$

where $V_{D_k(\mathbf{F}_q)}$ denotes the value set of D_k over the finite field $\mathbf{F}_q$.

An immediate consequence of the formula for the value set of D_k is the following well-known result:

Corollary 2.11. *[4] Let $k \geq 1$ be an integer, and let q be a power of some prime. Then D_k permutes $\mathbf{F}_q$ if and only if $(k, q^2 - 1) = 1$ where $(k, q^2 - 1)$ denotes the greatest common divisor of the integers k and $q^2 - 1$.*

Proof. Since D_k is considered over $\mathbf{F}_q$, which is a finite set, then the bijectivity of D_k is equivalent to its surjectivity. However, in order for this function to be surjective, the value set must contain exactly q elements. According to the formula for the value set, this is possible if and only if $(n, q-1) = 1$ and $(n, q+1) = 1$, which is the same as $(n, q^2 - 1) = 1$. □

Remark 2.12. Note that if k is a prime number such that $k \geq 5$, then the map $D_k(x)$ is arithmetically exceptional. To see this, note that there exists an integer $0 < k < m$ such that $m^2 \not\equiv 1 \pmod k$. There are infinitely many primes in the arithmetic progression $k + m, 2k + m, 3k + m, ...$ For each one of these primes, the condition of the above corollary is satisfied.

2.3 Endomorphisms of a singular cubic curve

This section is intended to determine the value sets of Dickson polynomials by using an alternative approach to the method described in the previous section. The method introduced in this section is also due to [3].

To begin with, let us denote by $\omega\mathbf{Z}$ the additive subgroup of the complex numbers $\mathbf{C}$ that is generated by the element $\omega = 2\pi i$. Here, we denote by $\mathbf{Z}$ the ring of integers. Now, consider the function defined by the infinite sum

$$\phi(z) = \sum_{\lambda \in \omega\mathbf{Z}} \frac{1}{(z-\lambda)^2}.$$

The following lemma lists some of the properties of $\phi(z)$ that are of our interest.

Lemma 2.13. *[3] The function $\phi(z)$ possess the following properties:*

1. *The defining sum for the function $\phi(z)$ converges uniformly on each compact subset of $\mathbf{C}\backslash\omega\mathbf{Z}$. Moreover, the only singularities of this function come from the points $\lambda \in \omega\mathbf{Z}$, which are all double poles.*

2. *For all $z \in \mathbf{C}\backslash\omega\mathbf{Z}$, we have*

$$\phi(z) = \frac{e^z}{(e^z-1)^2}.$$

3. *The function $\phi(z)$ defines an even function. That is, for all $z \in \mathbf{C}\backslash\omega\mathbf{Z}$, we have*

$$f(z) = f(-z).$$

4. *The function $\phi(z)$ defines a periodic function with period $2\pi i$. Namely, we have*

$$\phi(z + 2\pi i) = \phi(z)$$

   for all $z \in \mathbf{C}\backslash\omega\mathbf{Z}$.

5. *The function $\phi(z)$ and its derivative $\phi'(z)$ satisfy the following algebraic identity:*

$$\phi'(z)^2 = 4\phi(z)^3 + \phi(z)^2.$$

Proof. 1. From the triangle inequality, we have the following:

$$\left|\frac{1}{(z-\lambda)^2}\right| = \left|\frac{1}{(z-\lambda)^2} - \frac{1}{(\lambda)^2} + \frac{1}{(\lambda)^2}\right| \leq \left|\frac{1}{(z-\lambda)^2} - \frac{1}{(\lambda)^2}\right| + \left|\frac{1}{(\lambda)^2}\right|.$$

The sum defining the Weierstrass $\wp$- function (relative to the lattice $\omega\mathbf{Z}$) is given by

$$\wp(z;\omega\mathbf{Z}) = \frac{1}{z^2} + \sum_{\lambda\in\omega\mathbf{Z}\setminus\{0\}} \left(\frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2}\right)$$

so that the sum $\sum_{\lambda\in\omega\mathbf{Z}\setminus\{0\}}(\frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2})$ converges uniformly on compact subsets not containing the elements of the lattice $\omega\mathbf{Z}$ [10]. Moreover, we have:

$$\left|\sum_{k\in\mathbf{Z}} \frac{1}{(2\pi i - k)^2}\right| = \sum_{k\in\mathbf{Z}} \left|\frac{1}{4\pi^2}\frac{1}{(ik)^2}\right| = \frac{1}{4\pi^2}\sum_{k\in\mathbf{Z}}\left|\frac{1}{k^2}\right| = \frac{2\zeta(2)}{(2\pi)^2},$$

where $\zeta(s)$ denotes the Riemann-zeta function defined by

$$\zeta(s) = \sum_{n=1}^{\infty}\frac{1}{n^s} \quad , \; s\in\mathbf{C}.$$

It is a well known fact that $\zeta(2) = \frac{\pi^2}{6}$. Therefore, we have $\frac{2\zeta(2)}{4\pi^2} < \infty$. It follows that the sum defining the function $\phi(z)$ converges uniformly on compact subsets not containing the elements of $\omega\mathbf{Z}$. On the other hand, since a uniform limit of analytic functions is also analytic, then $\phi(z)$ is analytic for all $z\in\mathbf{C}$ such that $z\notin\omega\mathbf{Z}$. If $z\in\omega\mathbf{Z}$, then the sum of the terms for $\lambda\neq z$ is analytic at z so that the term $\frac{1}{(z-\lambda)^2}$ causes ϕ to have a double pole at z. Thus $\phi(z)$ is a meromorphic function of the complex plane with a double pole at each $\lambda\in w\mathbf{Z}$. Furthermore, these are the only poles of $\phi(z)$. This finishes the proof of the first part of the lemma.

2. First, we know that the Bernoulli numbers are defined by the exponential generating function. More precisely, we have

$$\frac{z}{e^z-1} = \sum_{j=0}^{\infty}\frac{B_j}{j!}z^j.$$

On the other hand, if n is an odd integer greater than 1, then $B_n = 0$. This is because the function $f(z) = \frac{z}{e^z-1} + \frac{z}{2}$ is even. This also implies that $B_1 = -\frac{1}{2}$.

Multiplying the both sides of the above equality by $\frac{1}{z}$ and then adding $\frac{1}{2}$ to both sides and using the fact that $B_n = 0$ for all $n < 1$, we obtain that

$$g(z) = \sum_{j=0}^{\infty} \frac{B_{2j}}{(2j)!} z^{2j-1},$$

where we set $g(z) = \frac{1}{e^z-1} + \frac{1}{2}$. Taking the derivative of the above sum term by term, we get

$$g'(z) = \sum_{j=0}^{\infty} (2j-1) \frac{B_{2j}}{(2j)!} z^{2j-2}.$$

On the other hand, recall from the first part of this Lemma that the function $\phi(z)$ has a double pole at the point $z = 0$ so that it has a Laurent series expansion there. Furthermore, as shown in [3], its Laurent expansion about $z = 0$ is given by

$$\phi(z) = -\sum_{j=0}^{\infty} (2j-1) \frac{B_{2j}}{(2j)!} z^{2j-2},$$

which implies that $g'(z) = -\phi(z)$. Since $g(z) = \frac{1}{e^z-1} + \frac{1}{2}$, then $g'(z) = \frac{-e^z}{(e^z-1)^2}$ and this yields $\phi(z) = \frac{e^z}{(e^z-1)^2}$. This proves the second part of the Lemma.

3. By definition of $\phi(z)$, we have

$$\phi(-z) = \sum_{k \in \mathbf{Z}} \frac{1}{(-z-k2\pi i)^2} = \sum_{k \in \mathbf{Z}} \frac{1}{(z+k2\pi i)^2}.$$

Since the sum is taken over all $k \in \mathbf{Z}$, the following equality trivially holds.

$$\sum_{k \in \mathbf{Z}} \frac{1}{(z+k2\pi i)^2} = \sum_{k \in \mathbf{Z}} \frac{1}{(z-k2\pi i)^2}.$$

Thus $\phi(z)$ is an even function. This proves the third part of the Lemma.

4. Using the expression for $\phi(z)$ that is obtained in the second part, one gets

$$\phi(z+2\pi i) = \frac{e^{z+2\pi i}}{(e^{z+2\pi i}-1)^2} = \frac{e^z e^{2\pi i}}{(e^z e^{2\pi i}-1)^2}.$$

But since by Euler's identity we have $e^{2\pi i} = \cos 2\pi + i \sin 2\pi = 1$, it follows that $\phi(z) = \phi(z+2\pi i)$. So the function $\phi(z)$ is periodic with period $w = 2\pi i$, and the proof of the fourth part is done.

5. Firstly, taking the derivative of the function $\phi(z) = \frac{e^z}{(e^z-1)^2}$, one gets

$$\phi'(z) = \frac{e^z(e^z-1)^2 - 2e^{2z}(e^z-1)}{(e^z-1)^4}.$$

Note that both the numerator and the denominator have the common factor $(e^z - 1)$. Simplifying this factor yields

$$\phi'(z) = \frac{e^z(e^z - 1) - 2(e^{2z})}{(e^z - 1)^3}.$$

After rearranging, we obtain

$$\phi'(z) = \frac{-(e^{2z}) - e^z}{(e^z - 1)^3}.$$

Furthermore, note that we have the relations $\phi' = -2\phi g$ and $g^2 = \phi + \frac{1}{4}$. Squaring both sides of the first one of these identities, we get

$$(\phi')^2 = 4(\phi)^2 g^2.$$

Now substituting $g^2 = \phi + \frac{1}{4}$ yields the following algebraic identity between the function $\phi(z)$ and its derivative:

$$\phi'(z) = 4(\phi(z))^3 + (\phi(z))^2.$$

and this proves the last part of the lemma.

□

Consider the singular cubic curve C, which is defined by the equation

$$C : y^2 = 4x^3 + x^2.$$

Then, this curve has a singularity at the origin since both partial derivatives vanish at that point. Now let C_{ns} denote the set of nonsingular points of this curve. Then C_{ns} forms an abelian group with group operation coming from the elliptic curve point addition [12]. Moreover, C_{ns} is isomorphic to the multiplicative subgroup of non-zero complex numbers $\mathbf{C}^* = \mathbf{C}\backslash\{0\}$ with the isomorphism obtained by the map $(x, y) \mapsto \frac{y-x}{y+x}$ [10].

Now since the multiplication of two complex numbers that have unit modulus results in a complex number with again modulus equal to 1, the elements of the unit circle in the complex plane form a multiplicative subgroup of $\mathbf{C}^*$. Let us denote the isomorphic image of this subgroup by C_1. Also, the last part of the Lemma 2.13 implies that the points on C can be parametrized by the function $\phi(z)$ and its derivative $\phi^{'}(z)$. More precisely, any point P on C is given by $P = (\phi(z), \phi^{'}(z))$ for some $z \in \mathbf{C}$. Also, the endomorphism $[n] : C_1 \longrightarrow C_1$ is given by the map $(\phi(z), \phi^{'}(z)) \mapsto (\phi(nz), \phi^{'}(nz))$ for each $n \in \mathbf{Z}$.

The subgroup of n-torsion points is defined by

$$C_1[n] = \{P \in C_1 : [n]P = \infty\}.$$

Now let $n \geq 1$ be an integer. These are the points of order dividing n. Observe that the n-torsion subgroup $C_1[n]$ is exactly the kernel of the homomorphism $[n] : C_1 \longrightarrow C_1$.

Now let $n \geq 1$ be an integer. Consider the function f_n defined by

$$f_n(\phi(z)) = \phi(nz) = x([n]P)$$

where $P = (\phi(z), \phi^{'}(z))$ and $x([n]P)$ denotes the x-coordinate of the point $[n]P$.

The following lemma establishes the relation between the function f_n and the n-th Dickson polynomial D_n.

Lemma 2.14. *[3] Let* $n \geq 1$ *be an integer. Then*

$$f_n(t) = \frac{1}{D_n\left(\frac{1}{t} + 2\right) - 2}.$$

Proof. As we have seen in the first section, the n-th Dickson polynomial satisfies

$$D_n(y + y^{-1}) = y^n + y^{-n}.$$

Using this and the relation $\frac{1}{\phi(z)} + 2 = e^z + e^{-z}$, one obtains the following:

$$D_n\left(\frac{1}{\phi(z)} + 2\right) = D_n(e^z + e^{-z}) = e^{nz} + e^{-nz} = \frac{1}{\phi(nz)} + 2$$

so that

$$D_n\left(\frac{1}{\phi(z)} + 2\right) = (f_n(\phi(z)))^{-1} + 2.$$

Now making the change of variable $t = \phi(z)$ yields

$$f_n(t) = \frac{1}{D_n\left(\frac{1}{t} + 2\right) - 2},$$

which is the desired result. □

Remark 2.15. Recall from the first section that $D_n(t)$ is a polynomial of degree n. It follows that $D_n(\frac{1}{t}+2)$ is a rational function of t, which implies that $f_n(t)$ is also a rational function of t by the preceding lemma.

Now we set the notation $C_1[n]_x$ to denote the set of x-coordinates of n-torsion points of C_1. More clearly, we have $C_1[n]_x = \{x(P) : P \in C_1[n]\}$ where $C_1[n]$ denotes the n-torsion subgroup of C_1 as defined before. The following theorem shows that the number of elements in this set can be expressed by a simple formula.

Theorem 2.16. *[3] Let $n \geq 1$ be an integer. Then the number of elements in the set $C_1[n]_x$ is given by*

$$|C_1[n]_x| = \frac{n+(n,2)}{2}.$$

Proof. Let P_1, P_2 be two points lying on C_1. Then the x-coordinates of these two points are equal if and only if $P_1 = P_2$ or $P_1 = -P_2$. Also, an arbitrary point P is contained in the 2-torsion subgroup of C_1 if and only if $P = -P$. On the other hand, since C_1 and the unit circle in the complex plane are isomorphic, it follows that the n-torsion subgroup $C_1[n]$ of C_1 and the multiplicative group of n-th roots of unity are also isomorphic. Therefore, the n-torsion subgroup $C_1[n]$ contains exactly n elements. Consequently, we can count the number of elements of $C_1[n]_x$ by

$$|C_1[n]_x| = \frac{|C_1[n] - C_1[(n,2)]|}{2} + |C_1[(n,2)]| = \frac{n-(n,2)}{2} + (n,2).$$

□

The following theorem shows that the projective space $\mathbf{P}^1(\mathbf{F}_q)$ can be expressed in terms of torsion points of C_1.

Theorem 2.17. *[3] Let $\mathbf{F}_q$ be the finite field with q elements where $q = p^k$ for some $k \geq 1$. Let $\mathfrak{p}$ be a prime ideal of the cyclotomic field $\mathbf{Q}(\zeta_{q^2-1})$ lying over p. Then we have the following:*

$$\mathbf{P}^1(\mathbf{F}_q) = \overline{C_1[q-1]_x} \cup \overline{C_1[q+1]_x} \cup \{0\}.$$

Proof. Recall from the previous section that whenever $q = p^k$, we have

$$D_q(t) \equiv t^q \pmod{p}.$$

Applying the Fermat's Little Theorem, we obtain

$$f_q(t) \equiv t^q \pmod{p}.$$

We see that each element of the finite field $\mathbf{F}_q$ satisfy the equation $f_q(t) = t$. This is because the elements of $\mathbf{F}_q$ come from the solutions of the polynomial $x^q - x = 0$. This implies that the equation $f_q(t) = t$ has $q + 1$ different solutions in the projective space $\mathbf{P}^1(\mathbf{F}_q)$, which also implies it has $q + 1$ different solutions in $\mathbf{P}^1(\mathbf{C})$ as well.

Now if $P \in C_1[q \mp 1]$, then $[q]P = [\mp 1]P$. It follows from the defining equation of the function f_q that we have $f_q(x(P)) = x(P)$. From this, we see that the x-coordinate of each such point P must satisfy the equation $f_q(t) = t$. Now the claim is that among the fixed points of the function f_q, those belonging to $\mathbf{P}^1(\mathbf{C})$ except 0 can be expressed by the union

$$C_1[q+1]_x \cup C_1[q-1]_x.$$

To prove the claim, it suffices to show that the above union contains q elements.

Now if q is even, then the intersection of the two sets $C_1[q+1]_x$ and $C_1[q-1]_x$ contains only one point, which is a point at infinity ∞. Applying the Inclusion-exclusion principle, one can see that the above union contains

$$\frac{q-1+1}{2} + \frac{q+1+1}{2} - 1$$

elements.

If q is odd, then the intersection is equal to the set of x-coordinates of the 2-torsion subgroup of C_1. In other words, we have $C_1[q+1]_x \cap C_1[q-1]_x = C_1[2]_x$. Then by Inclusion-exclusion principle, there are

$$\frac{q-1+2}{2} + \frac{q+1+2}{2} - 2$$

elements in this case. □

An important consequence of the preceding theorem is the following corollary, which allows for a determination of the value set of f_n over $\mathbf{P}^1(\mathbf{F}_q)$.

Corollary 2.18. *[3] Let $n \geq 1$ be an integer. Then the value set of the rational function f_n over $\mathbf{P}^1(\mathbf{F}_q)$ can be expressed by*

$$V_{f_n} = \overline{C_1[n^+]_x} \cup \overline{C_1[n^-]_x} \cup \{0\}.$$

Moreover, the cardinality of this set is given by the formula

$$|V_{f_n}| = \frac{(n^+ + n^-)}{2} + \eta(n,q) + 1,$$

where

$$n^- = \frac{q-1}{(n,q-1)}, \quad n^+ = \frac{q+1}{(n,q+1)}.$$

Proof. We start with considering the homomorphism

$$[n] : C_1[q-1] \longrightarrow C_1[q-1]$$

which has kernel $C_1[(n,q-1)]$. Then by First Isomorphism Theorem, the quotient group $C_1[q-1]/C_1[(n,q-1)]$ is isomorphic to the image set of $[n]$. Therefore, the image of the homomorphism $[n]$ is a subgroup of order $n^- = \frac{q-1}{(n,q-1)}$. This means that the map $f_n : C_1[q-1]_x \longrightarrow C_1[n^-]_x$ is surjective.

In a similar manner, the group homomorphism

$$[n] : C_1[q+1] \longrightarrow C_1[q+1]$$

has kernel $C_1[(n,q+1)]$. It follows by First Isomorphism Theorem that the quotient group $C_1[q+1]/C_1[(n,q+1)]$ is isomorphic to the image set of $[n]$.

According to the previous theorem, we have

$$V_{f_n} = \bar{C}_1[n^-]_x \cup \bar{C}_1[n^+]_x \cup \{0\}.$$

Furthermore, the cardinality of this set is given by

$$|V_{f_n}| = |C_1[n^-]_x| + |C_1[n^+]_x| - |C_1[(n^-,n^+)]_x| + 1.$$

Finally, by using the Theorem 2.16 we obtain the desired formula so that the proof is done. □

Recall that for each positive integer n, the rational function $f_n(t)$ and the n-th Dickson polynomial satisfy the relation

$$f_n(t) = \frac{1}{D_n\left(\frac{1}{t}+2\right) - 2},$$

which implies that $f_n(t)$ can be obtained from $D_n(t)$ via change of variables which are linear in $\frac{1}{t}$. It follows that the cardinality of the value sets of the two functions must be equal. Namely, we must have

$$|V_{f_n}|= |D_n|.$$

As a result, we conclude that f_n permutes $\mathbf{P}^1(\mathbf{F}_q)$ if and only if D_n permutes $\mathbf{P}^1(\mathbf{F}_q)$. Moreover, the same is also true if $\mathbf{P}^1(\mathbf{F}_q)$ is changed by $\mathbf{F}_q$ since both f_n and D_n fix the point at infinity. The following lemma is an immediate consequence of these observations.

Corollary 2.19. *[3]Let $n \geq 1$ be an integer. Then the cardinality of the value set of D_n over a finite field $\mathbf{F}_q$ is given by the formula*

$$\frac{(n^- + n^+)}{2} + \eta(k, q).$$

Proof. Applying the inclusion and exclusion principle to the representation of the set $\mathbf{P}^1(\mathbf{F}_q)$ given in 2.17, it is easy to see that the cardinality of the value set of D_n over a finite field F_q is

$$\frac{q-1}{2\text{gcd}(k, q-1)} + \frac{q+1}{2\text{gcd}(k, q+1)} + \eta(k, q)$$

where $\eta(k, q)$ as defined in Corollary 2.18. □

Corollary 2.20. *[3] For each integer $n \geq 1$, the n-th Dickson polynomial D_n permutes $\mathbf{F}_q$ if and only if $(n, q^2 - 1) = 1$.*

Proof. Using the formula for the value set of D_n given in the above corollary, it is easy to see that D_n permutes F_q if and only if $(n, q-1) = 1$ and $(n, q+1) = 1$. It is easy to see that this is true if and only if $(n, (q-1).(q+1)) = (n, q^2 - 1) = 1$ so that the proof is done. □

Remark 2.21. Recall that in the second section of this chapter, the above result is obtained by using the one-to-one correspondence between the fixed points of Dickson polynomials and the elements of the finite fields. On the other hand, the method here relies on the result, which states that the projective space $\mathbf{P}^1(\mathbf{F}_q)$ can be expressed by torsion points of the singular cubic curve $y^2 = 4x^3 + x^2$. As a result, we have seen two different approaches in order to discuss the arithmetic exceptionality of the Dickson polynomials.

CHAPTER 3

ELLIPTIC CASE

In this chapter, we first provide the theoretical background that we need related to the theory of elliptic curves. In the previous chapter, we have seen that the non-singular points of the singular cubic curve $C : y^2 = 4x^3 + x^2$ can be parametrized in terms of the function $\phi(z)$ and its derivative $\phi'(z)$. In a similar manner, points of an elliptic curve defined over complex numbers are parametrized by the Weierstrass $\wp$-function and its derivative. In this chapter, we will see that this analogy between $\phi(z)$ and the Weierstrass $\wp$-function can be used to generalize the methods given in the previous section to certain elliptic curves with complex multiplication. As we will see, the projective space $\mathbf{P}^1(\mathbf{F}_q)$ can be expressed in terms of torsion points of elliptic curves that have complex multiplication. As a result of this, value sets of Lattès maps are found, and further, a formula to compute the cardinality of these value sets is given. Furthermore, there is also a criterion to determine under which condition a Lattès map gives a bijection of $\mathbf{P}^1(\mathbf{F}_q)$.

3.1 Some Basic Definitions and Results

The basic definitions and results related to the theory of elliptic curves are presented in this section. Some of the results are given without proof. For details, we refer the reader to [8] or [12].

Definition 3.1. Given a field K, an elliptic curve E is defined as the set of points with coordinates in K satisfying the following equation

$$y^2 = x^3 + Ax + B, \quad A, B \in K.$$

In the definition given above, we put the restriction $4A^3 + 27B^2 \neq 0$ so that we assume that the cubic on the right-hand side has distinct roots. Also, we denote by $E(K)$ the set of points lying on E. More precisely, we have

$$E(K) = \{\infty\} \cup \{(x, y) \in K \times K \ : \ y^2 = x^3 + Ax + B\},$$

where ∞ denotes the point at infinity.

Given arbitrary two points $P, Q \in E(K)$, their sum $P+Q$ is defined by the following procedure: We draw the line through P and Q, which will intersect the curve in a third point. Then reflecting the intersection point across the x-axis, we obtain $P+Q$. With this operation, the set $E(K)$ forms an abelian group, where the point at infinity ∞ acts as an identity element.

Definition 3.2. Given an elliptic curve $E : y^2 = x^3 + Ax + B$, the j-invariant $j(E)$ of E is defined by

$$j(E) = 1728 \frac{4A^3}{4A^3 + 27B^2}.$$

Definition 3.3. Let E be an elliptic curve given by the equation $E : y^2 = x^3 + Ax + B$. An **endomorphism** of E is defined as a group homomorphism $\alpha : E(\bar{K}) \longrightarrow E(\bar{K})$, which is given by rational functions whose coefficients belong to the algebraic closure $\bar{K}$.

The simplest examples of endomorphisms are the multiplication by n homomorphisms for each integer $n \geq 1$.

Definition 3.4. Given an elliptic curve $E : y^2 = x^3 + Ax + B$, the divison polynomials $\psi_m \in \mathbf{Z}[x, y, A, B]$ corresponding to E are defined by the following recurrence relation:

$$\psi_0 = 0,$$

$$\psi_1 = 1,$$

$$\psi_2 = 2y,$$

$$\psi_3 = 3x^4 + 6Ax^2 + 12Bx - A^2,$$

$$\psi_4 = 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3),$$

$$\psi_{2m+1} = \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3 \text{ for each integer } m \geq 2,$$

$$\psi_{2m} = (2y)^{-1}\psi_m(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2) \text{ for each integer } m \geq 3.$$

Definition 3.5. For each integer $m \geq 0$, we define the family of polynomials ϕ_m and ω_m by

$$\phi_m = x\psi_m^2 - \psi_{m+1}\psi_{m-1},$$
$$\omega_m = (4y)^{-1}(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2).$$

As the following theorem shows, the multiplication by n homomorphism can be expressed in terms of the polynomials ψ_n, ω_n and ϕ_n.

Theorem 3.6. *Let E be an elliptic curve given by $y^2 = x^3 + Ax + B$, and let $P = (x, y)$ be an arbitrary point of E. For each integer $n \geq 1$, the multiplication by n endomorphism, which we denote by $[n]$, is given by*

$$[n](P) = (\frac{\phi_n(x)}{\psi_n^2(x)}, \frac{\omega_n(x,y)}{\psi_n^3(x,y)}).$$

Definition 3.7. Let E be an elliptic curve given by $y^2 = x^3+Ax+B$, where $A, B \in K$ for some field K. For each integer $n \geq 1$, the n-torsion subgroup of E, which we denote by $E[n]$, is defined as the group of points of order dividing n. More clearly, we have

$$E[n] = \{P \in E(\bar{K}) : [n](P) = \infty\}.$$

Observe from the previous definition that the n-torsion subgroup $E[n]$ consists of points with coordinates in the algebraic closure $\bar{K}$.

Definition 3.8. Let w_1, w_2 be two complex numbers, and let $\beta = \{w_1, w_2\}$ be a set that is linearly independent over the real numbers $\mathbf{R}$. Then the lattice generated by the set β is defined by

$$L = \mathbf{Z}_{w_1} + \mathbf{Z}_{w_2} = \{n_1w_1 + n_2w_2 \ : \ n_1, n_2 \in \mathbf{Z}\}.$$

Suppose we have a function defined on $\mathbf{C}/L$ for some lattice L. Note that we can also regard this function as a function with domain on $\mathbf{C}$ with the property that $f(z+w) = f(z)$ for all $z \in \mathbf{C}$ and all $w \in L$. After this observation, we can give the following definition.

Definition 3.9. Given a lattice L, let $f : \mathbf{C} \longrightarrow \mathbf{C} \cup \{\infty\}$ be a meromorphic function so that only singularities come from poles. We say that f is a doubly periodic function if

$$f(z+w) = f(z)$$

for all $z \in \mathbf{C}$ and all $w \in L$.

Observe that if L is generated by $\beta = \{w_1, w_2\}$, then the above condition is equivalent to saying that $f(z + w_i) = f(z)$ for $i = 1, 2$.

Definition 3.10. Let L be a lattice. The Weierstrass $\wp$-function corresponding to the lattice L is defined by the following sum

$$\wp(z; L) = \frac{1}{z^2} + \sum_{w \in L \setminus \{0\}} \left(\frac{1}{(z-w)^2} - \frac{1}{w^2} \right).$$

Immediately after the above definition, we give the following theorem, which is an elliptic analog of Lemma 2.13 given in Chapter 2.

Theorem 3.11. *Let L be a lattice. The Weierstrass $\wp$-function (relative to the lattice L) satisfies the following properties:*

1. *The defining series of $\wp(z)$ converges both absolutely and uniformly on compact subsets of $\mathbf{C} \setminus L$.*

2. *The only singularities of the function $\wp(z)$ are poles, which are all double poles occurring at each $w \in L$.*

3. *$\wp(z)$ is an even function, that is, $\wp(-z) = \wp(z)$ for all $z \in \mathbf{C}$.*

4. *$\wp(z)$ is periodic, with period at each $w \in L$. In other words, we have $\wp(z + w) = \wp(z)$ for all $z \in \mathbf{C}$ and $w \in L$.*

Remark 3.12. Recall that the function $\phi(z)$ defined in Lemma 2.13 can be used to express the points lying on the singular cubic curve $C : y^2 = 4x^3 + x^2$. In a similar manner, the complex points of an elliptic curve can be expressed in terms of the Weierstrass $\wp$-function $\wp(z)$.

Definition 3.13. Let L be a lattice and $k > 2$ be an integer. The Eisenstein series corresponding to the lattice L is defined by the following sum

$$G_k(L) = \sum_{0 \neq w \in L} w^{-k}.$$

Proposition 3.14. *Let L be a lattice. If* $0 < |z| < min(\{|w| : w \in L\})$*, then the Weierstrass* $\wp$*-function corresponding to the lattice L has the following characterization*

$$\wp(z) = \frac{1}{z^2} + \sum_{j=1}^{\infty}(2j+1)G_{2j+2}z^{2j}$$

where $min(\{|w| : w \in L\})$ *denotes the minimum of the modulus of elements of the lattice L.*

Proof. Firstly, we have

$$\left(\frac{1}{(z-w)^2} - \frac{1}{w^2}\right) = w^{-2}\left(\frac{1}{(z-(z/w))^2} - 1\right).$$

If $|z| < |w|$, then expressing the term $\frac{1}{(z-(z/w))^2}$ as a geometric sum, we see that the right side of the above equation is equal to

$$w^{-2}\left(\sum_{n=1}^{\infty}(n+1)\frac{z^n}{w^n}\right).$$

Then by definition of the Weierstrass $\wp$-function, we obtain

$$\wp(z) = \frac{1}{z^2} + \sum_{n \neq 0}\sum_{n=1}^{\infty}(n+1)\frac{z^n}{w^{n+2}}.$$

Finally summing over w first and then over n gives the desired result. □

Theorem 3.15. *Let L be a lattice and* $\wp(z)$ *be the Weierstrass* $\wp$*-function corresponding to L. Then* $\wp(z)$ *and its derivative satisfy the following algebraic identity:*

$$\wp^{'}(z)^2 = 4\wp(z)^3 - 60G_4\wp(z) - 140G_6.$$

Proof. Firstly, we have the following equalities:

$$\wp(z) = \frac{1}{z^2} + 3G_4z^2 + 5G_6z^4 + ... ,$$

$$\wp^{'}(z) = -\frac{2}{z^3} + 6G_4z + 20G_6z^3 + ...$$

Now taking the cube of the first equality and squaring the second one, one obtains

$$\wp(z)^3 = \frac{1}{z^6} + 9G_4\frac{1}{z^2} + 15G_6 + ...$$

$$\wp^{'}(z)^2 = \frac{4}{z^6} - 24G_4\frac{1}{z^2} - 80G_6 + ...$$

Combining the last two equalities that we obtain, we get

$$\wp'(z)^2 - 4\wp(z)^3 + 60G_4\wp(z) + 140G_6 = c_1z + c_2z^2 + ...$$

so that we have a power series with only positive powers of z and with the constant term equal to zero. The only possible poles of this power series are at lattice points, namely, the points of L. But since the sum is doubly periodic and has no pole at 0, it follows that the defining function of the sum has no pole. Therefore, it defines an entire function of **C**. By Liouville's Theorem, it must be constant. But since the constant term of the series is equal to zero, then it must be identically 0. □

If we set

$$g_2 = 60G_4$$

$$g_3 = 140G_6$$

then the identity given in the above theorem takes the form

$$\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3.$$

As a result, $\wp(z)$ and its derivative can be used to parametrize the points lying on the curve

$$y^2 = 4x^3 - g_2x - g_3.$$

Observe that the right-hand side of the above equation is a cubic polynomial, and the discriminant of it is given by

$$16({g_2}^3 - 27{g_3}^2).$$

Proposition 3.16. *Let Δ be the discriminant of the cubic polynomial $4x^3 - g_2x - g_3$ where $g_2 = 60G_4$ and $g_3 = 140G_6$. Then $\Delta = 16({g_2}^3 - 27{g_3}^2) \neq 0$.*

Proof. Since $\wp'(z)$ is a doubly periodic function, then we have

$$\wp'\left(\frac{w_i}{2}\right) = \wp'\left(\frac{w_i}{2} - w_i\right)$$

which is the same as

$$\wp'\left(\frac{w_i}{2}\right) = \wp'\left(-\frac{w_i}{2}\right).$$

On the other hand, $\wp'(z)$ is an odd function so that it satisfies $\wp'(-z) = -\wp'(z)$. It follows that we must have

$$\wp'\left(\frac{w_i}{2}\right) = 0$$

for $i = 1, 2, 3$. This implies that $\wp(w_i/2)$ must be a root of the polynomial $4x^3 - g_2x - g_3$ for $i = 1, 2, 3$. Now define

$$h_i(z) = \wp(z) - \wp\left(\frac{w_i}{2}\right)$$

for $i = 1, 2, 3$. Then the first two derivatives of the function $h_i(z)$ vanish at the point $w_i/2$ so that it has a zero of order at least 2 at that point. But since the function $h_i(z)$ has only one pole, which is a double pole at $z = 0$, then the point $w_i/2$ must be the only zero of that function. It follows that if $i \neq j$, then we have

$$h_i\left(\frac{w_j}{2}\right) \neq 0.$$

Therefore the values $\wp(w_1/2), \wp(w_2/2)$ and $\wp(w_3/2)$ are pairwise distinct. This means that the cubic polynomial $4x^3 - g_2x - g_3$ has three distinct roots, which implies that its discriminant differs from zero. □

According to the proposition, the curve

$$E : y^2 = 4x^3 - g_2x - g_3$$

defines an elliptic curve so that we have a map

$$\mathbf{C} \longrightarrow E(\mathbf{C})$$

$$z \longrightarrow (\wp(z), \wp'(z))$$

from the complex numbers $\mathbf{C}$ to the complex points of the elliptic curve E. As mentioned before, we can regard this function as a function with domain $\mathbf{C}/L$ so that we have a map from the quotient space $\mathbf{C}/L$ to $E(\mathbf{C})$. As the following theorem shows, this map gives an isomorphism between the two groups.

Theorem 3.17. *Given a lattice L, let E be the elliptic curve defined by $y^2 = 4x^3 - g_2x - g_3$, where $g_2 = 60G_4(L)$ and $g_3 = 140G_6(L)$. Then the map*

$$\Phi : \mathbf{C}/L \longrightarrow E(\mathbf{C})$$

$$z \longrightarrow (\wp(z), \wp'(z))$$

is a group isomorphism.

Remark 3.18. Given a lattice L, the quotient space $\mathbf{C}/L$ is a group where the group operation is addition modulo L. On the other hand, the complex points $E(\mathbf{C})$ on the elliptic curve $E : y^2 = 4x^3 - g_2x - g_3$ also forms a group where the group operation is elliptic curve point addition as defined before. According to the theorem, the two group structures coincide, and we can say that to every torus $\mathbf{C}/L$, there corresponds an elliptic curve.

Theorem 3.19. *Let E be an elliptic curve over* $\mathbf{C}$ *defined by* $y^2 = 4x^3 - Ax - B$. *Then there exists a lattice L with*

$$g_2 = 60G_4(L) = A \quad \textit{and} \quad g_3 = 140G_6(L) = B$$

and a group isomorphism

$$\Phi : \mathbf{C}/L \longrightarrow E(\mathbf{C}).$$

Remark 3.20. The theorem says that when we have an elliptic curve $E : y^2 = 4x^3 - Ax - B$, there exists a lattice L such that the elliptic curve corresponding to the torus $\mathbf{C}/L$ is E. Therefore, every elliptic curve defined over $\mathbf{C}$ yields a torus.

3.2 Elliptic Case

In this section, the generalization of the method used in Section 2.3 is explained in detail. The result is due to [3].

Recall from Section 2.2 that the function $\phi(z) = \frac{e^z}{(e^z-1)^2}$ can be used to express the non-singular points of the singular cubic curve $C : y^2 = 4x^3 + x^2$. In a similar manner, we know from Theorem 3.19 that if E is an elliptic curve defined over $\mathbf{C}$, then there exists a lattice L such that the Weierstrass $\wp$-function (relative to the lattice L) can be used to parametrize $E(\mathbf{C})$. It turns out that this analogy can be used to generalize the approach described in Section 2.2 to certain elliptic curves with complex multiplication.

Before describing the generalization of the method, we need some preliminaries.

Definition 3.21. [11] Let K be an imaginary quadratic field and let $\alpha \in K$ be an arbitrary element. Then the norm of α, which we denote by $N(\alpha)$, is defined by $N(\alpha) = \alpha\alpha^{'}$ where $\alpha^{'}$ denotes the complex conjugate of the element α.

Theorem 3.22. *[11] Let K be an imaginary quadratic field and $\mathcal{O}_K$ denote its ring of algebraic integers. Suppose $\mathfrak{a}$ is a non-zero ideal of $\mathcal{O}_K$. Then the quotient ring $\mathcal{O}_K/\mathfrak{a}$ contains finitely many elements.*

Definition 3.23. [11] Let K be an imaginary quadratic field, and let $\mathfrak{a}$ be an arbitrary non-zero ideal of the ring of integers $\mathcal{O}_K$. Then the norm of the ideal $\mathfrak{a}$ is defined to be the cardinality of the quotient ring $\mathcal{O}_K/\mathfrak{a}$.

Definition 3.24. [9] Let E be an elliptic curve defined over the complex numbers $\mathbf{C}$, and let $\mathcal{O}$ denote its endomorphism ring. Given $\alpha \in \mathcal{O}$, consider the function F_α defined by the following functional equation:

$$F_\alpha(\wp(z)) = \wp(\alpha z) = x([\alpha]P)$$

where $P = (\wp(z), \wp^{'}(z))$. The function F_α is called the Lattès map corresponding to the element α.

For the rest of this section, we set the followings:

Let E be an elliptic curve defined by

$$y^2 = x^3 + Ax + B, \quad A, B \in H$$

that has complex multiplication by $\mathcal{O}_K$ where we denote by K and H some imaginary quadratic field and its Hilbert class field, respectively.

The following lemma is proved by considering the three cases where p splits, ramifies or remains inert in K separately. For more details, we refer the reader to [3].

Lemma 3.25. *[3] Let $E : y^2 = x^3 + ax + b$, $a, b \in H$. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ lying above p and let $\mathfrak{P}$ be a prime ideal of $\mathcal{O}_H$ lying over $\mathfrak{p}$. By the finiteness of the class group, $\mathfrak{p}^n$ is principal for some $n \geq 1$. Then there is some $\pi \in \mathcal{O}_K$ such that the principal ideal $\mathfrak{p}^n$ is generated by π and the reduction of the map $[\pi] : E \longrightarrow E$ modulo $\mathfrak{P}$ gives the Frobenius map Frob$_{N(\pi)}$ defined by $(x, y) \longrightarrow (x^{N(\pi)}, y^{N(\pi)})$. Moreover, the element $\pi \in \mathcal{O}_K$ is uniquely determined.*

Recall that in Section 2.2, we have seen a formula for the number of elements in the set $C_1[n]_x$. The next lemma is an elliptic analog of it.

Lemma 3.26. *[3] Let $\mathfrak{a}$ be a non-zero ideal of $\mathcal{O}_K$. Then the number of elements in the set $E[\mathfrak{a}]_x$ is expressed by the formula*

$$|E[\mathfrak{a}]_x| = \frac{|E[\mathfrak{a}]\backslash E[\mathfrak{a}+(2)]|}{2} + |E[\mathfrak{a}+(2)]| = \frac{N(\mathfrak{a}) - N(\mathfrak{a}+(2))}{2} + N(\mathfrak{a}+(2)).$$

Proof. Suppose that P_1, P_2 are two points lying on E such that $x(P_1) = x(P_2)$. Since E is in Weierstrass form, then either P_1 and P_2 are equal, or their y-coordinates differ by a sign. More precisely, we have $P_1 = P_2$ or $P_1 = -P_2$. The converse is also true. On the other hand, recall from the first section that the 2-torsion points of E are the points with y-coordinates equal to zero. It follows that if $P \in E[2]$, then we must have $P = -P$. From these observations, we conclude that for any element x' of the set $E[a]_x$, there are two corresponding points of E : (x', y) and $(x', -y)$ where $y^2 = x'^3 + ax' + b$ except the x-coordinates of the 2-torsion subgroup. Furthermore, note that for each element x'' of the set $E[2]_x$, there is only one point of E, which is $(x'', 0)$. Note also that $E[2] \cup E[a] = E[a + (2)]$ where (2) denotes the principal ideal of $\mathcal{O}_K$ generated by the element 2. Therefore, the cardinality of the set $E[a]_x$ is given by

$$|E[\mathfrak{a}]_x| = \frac{|E[\mathfrak{a}]\backslash E[\mathfrak{a}+(2)]|}{2} + |E[\mathfrak{a}+(2)]| = \frac{N(\mathfrak{a}) - N(\mathfrak{a}+(2))}{2} + N(\mathfrak{a}+(2)).$$

□

The following theorem shows that for each integer $m \geq 1$, the projective space $\mathbf{P}^1(\mathbf{F}_{q^m})$ can be expressed via the torsion points of E.

Theorem 3.27. *[3] Let m be an integer with $m \geq 1$. Then*

$$\mathbf{P}^1(\mathbf{F}_{q^m}) = \overline{E[\pi^m - 1]_x} \cup \overline{E[\pi^m + 1]_x}.$$

Proof. [3] Lemma 3.25 implies we have $p^n = (\pi)$ and $[\bar{\pi}] = \text{Frob}_{N(\pi)}$ for some uniquely determined $\pi \in \mathcal{O}_K$. Then we have $F_{\pi^m}(t) = t^{N(\pi^m)} = t^{N(\pi^m)} \pmod{\mathfrak{P}}$. On the other hand, it is a well-known fact that the elements of the projective space $\mathbf{P}^1(\mathbf{F}_q)$ are the solutions of the monic polynomial $x^q - x = 0$. Setting $q = N(\pi)$ and $\beta = \pi^m$, we see that the equation $\bar{F_\beta}(t) = t$ has $q^m + 1$ distinct solutions in the projective space $\mathbf{P}^1(\mathbf{F}_q)$ where $\bar{F_\beta}(t) = t$ denotes the map obtained by reducing the coefficients of F_β modulo $\mathfrak{P}$. It follows that the equation $F_\beta(t) = t$ has $q^m + 1$ distinct solutions in the extended complex plane $\mathbf{P}^1(\mathbf{C}) = \mathbf{C} \cup \{\infty\}$.

Now let $P \in E[\beta + 1]$. Then we have $[\beta]P = -P$ where $[\beta]$ denotes the map defined by $(\wp(z), \wp'(z)) \longrightarrow (\wp(\beta z), \wp'(\beta z))$. Similarly if $P \in E[\beta - 1]$, then we have $[\beta]P = P$. In both cases, we have $F_\beta(x(P)) = x(P)$. Therefore the elements of the union $E[\beta + 1]_x \cup E[\beta - 1]_x$ satisfy the equation $F_\beta(t) = t$. On the other hand, observe that any point contained in the union $E[\beta + 1] \cup E[\beta - 1]$ must also be contained in the 2-torsion subgroup $E[2]$. This is because if some point is an element of both $\beta - 1$-torsion subgroup and $\beta + 1$-torsion subgroup, then the x-coordinate of this point must be equal to zero so that it must be an element of the 2-torsion subgroup. Thus, using the inclusion and exclusion principle, the cardinality of the union $E[\beta + 1]_x \cup E[\beta - 1]_x$ is given by

$$\frac{N(\beta - 1) + N(\mathfrak{P})}{2} + \frac{N(\beta + 1) + N(\mathfrak{P})}{2} - N(\mathfrak{P}) = \frac{N(\beta - 1) + N(\beta + 1)}{2}.$$

This shows that the union $E[\beta + 1]_x \cup E[\beta - 1]_x$ contains exactly q^m elements. This proves the theorem. □

Immediate consequences of Theorem 3.27 are the following two corollaries:

Corollary 3.28. *[3] Let $\alpha \in \mathcal{O}_K$. Then the value set of the Lattès map F_α has the following characterization:*

$$V_{F_\alpha} = \bar{E}[\mathfrak{a}^-]_x \cup E[\mathfrak{a}^+]_x.$$

Moreover, the cardinality of the value set is given by

$$|V_{F_\alpha}| = (N(\mathfrak{a}^-) + N(\mathfrak{a}^+))/2 + \xi,$$

where $\mathfrak{a}^- = \frac{(\pi^m - 1)}{(\alpha, \pi^m - 1)}$, $\mathfrak{a}^+ = \frac{(\pi^m + 1)}{(\alpha, \pi^m + 1)}$ *and* $\xi = \frac{N(\mathfrak{a}^- + (2)) + N(\mathfrak{a}^+ + (2))}{2} - N(\mathfrak{a}^- + \mathfrak{a}^+)$.

Corollary 3.29. *[3] Let $\alpha \in \mathcal{O}_K$. Then the reduced map $\bar{F}_\alpha$ permutes $\mathbf{P}^1(\mathbf{F}_q^m)$ if and only if $(\alpha, \pi^{2m} - 1) = (1)$.*

Remark 3.30. The criterion given in Corollary 3.29 can be used to show the existence of infinitely many Lattès maps. For instance, let $\alpha \in \mathcal{O}_K$ be an element whose norm, say $l = N(\alpha)$, is bigger than or equal to 5 and prime in $\mathbf{Z}$. Then there exists an integer $0 < l < m$ such that $m^2 \not\equiv 1$ (mod k). By Dirichlet's prime number theorem, there are infinitely many primes in the arithmetic progression $l + m, 2l + m, 3l + m, \ldots$. For infinitely many certain primes in this list, the condition of Corollary 3.29 is satisfied.

CHAPTER 4

COMPUTATIONS AND REMARKS

In the previous chapter, we have seen that there is a formula to compute the cardinalities of the value sets of Lattès maps induced by elliptic curves that have complex multiplication. But when the endomorphism ring consists only of the integers, there is no known formula to compute the size of the value sets of such maps so that the situation is ambiguous in that case. To handle this problem, we put on a computational approach and use a computer-algebra program Pari/GP code to determine the cardinalities of such maps.

4.1 Motivating Example

In Chapter 2, we have seen that there is a well-known formula to determine the value sets of Dickson polynomials. Using this formula for the value set, we introduce a piece of code that compute value sets of Dickson polynomials. In this section, we give several examples to illustrate how the computations in Pari/GP related to the value sets can be done.

To start with, let $k \geq 1$ be an integer and p be a prime. In order to evaluate the size of the image set of the k-th Dickson polynomial D_k over the finite field $\mathbf{F}_p$, we introduce the following piece of computer code:

```
Dicksoncount(k,p)={
        local(chebypol=cheby(k));
        local(valuevec);
        local(valueset);
        valuevec=vector(p,i,subst(chebypol,x,Mod(i,p)));
```

```
                valueset=Set(valuevec);
                return(length(valueset));}
```

Before giving some examples, we would like to explain the content of the code in detail. First of all, the name `Dicksoncount` stands for counting the elements in the image set, and it has inputs k and p, which corresponds to the k-th Dickson polynomial D_k and a prime number p. In the first line, we define `chebypol` to be `cheby`(k) as can be understood by the defining relation `chebypol=cheby`(k) where the function `cheby`(k) is defined by the following piece of code:

```
cheby(k)={
          if(k==0,
          return(2));
          if(k==1,
          return(x));
          return(x*cheby(k-1)-cheby(k-2));}
```

In the second and third lines, we put the notions valueset and valuevec which will then be defined in the fourth and fifth lines. Notice that all three of the notions are given under `local` to create a local scope for these functions. In other words, the notions defined under local are valid only for the function `Dicksoncount`(k,p).

In the fourth line, we define valuevec to be the 3-tuple of elements

(p,i, `subst(chebypol`,x, `Mod`(i,p))).

Here p is a prime number, i is an integer with $0 \leq i \leq p-1$. Also, `Mod`(i,p) is the function that returns the value of the integer i modulo p and `subst(chebypol`,x, `Mod`(i,p)) is the function that plugges `Mod`(i,p) for x in `chebypol` and returns the resulting value.

In the fifth line, we define valueset to be equal to `Set`(valuevec) where `Set`(valuevec) is the function that returns the set of 3-tuple of elements (p,i, `subst(chebypol`,x, `Mod`(i,p))). The function `length`(valueset) evaluates the cardinality of the value set and returns the resulting value.

In the last line, we use the function `return(length`(valueset)) so that the function `Dicksoncount`(k,p) returns the size of the image set of D_k over $\mathbf{F}_p$ where k and p are arbitrarily chosen integer and a prime, respectively.

4.2 The twist of an elliptic curve

In this section, we describe the notion of the twist of an elliptic curve. As we will see in the next section, it is an essential tool for our piece of code to compute the value sets of Lattès maps.

Definition 4.1. [12] Let E be an elliptic curve defined over K, which is given by the equation $y^2 = x^3 + Ax + B$. Let $d \in K^\times$. Then the twist of E by d is defined as the curve that has the equation

$$y^2 = x^3 + Ad^2x + Bd^3$$

and is denoted by $E^{(d)}$.

Theorem 4.2. *[12] Let E be an elliptic curve given by the equation $y^2 = x^3+Ax+B$ where the coefficients A, B are elements of some field K and let $d \in K^\times$. Then*

1. $j(E^{(d)}) = j(E)$.
2. *$E^{(d)}$ is isomorphic over $K(\sqrt{d})$ to E.*
3. *$E^{(d)}$ is isomorphic over K to $E^{(d^{'})}$ where $E^{(d^{'})}$ is given by*

$$dy^2 = x^3 + Ax + B.$$

Remark 4.3. The first part of the above theorem implies that the two curves E and $E^{(d)}$ are isomorphic over the algebraic closure of the field K. This means that both of the two curves can be transformed to each other by using the rational functions with coefficients coming from the algebraic closure of K. The second part says that these coefficients can be chosen from the field $K(\sqrt{d})$ so that we have

$$E(K(\sqrt{d})) \cong E^{(d)}(K(\sqrt{d})).$$

The third part of the theorem says that the two curves $E^{(d)}$ and $E^{(d^{'})}$ can be transformed to each other by rational change of variables with coefficients coming from the field K so that the two curves are isomorphic over K. In other words, we have

$$E^{(d)}(K) \cong E^{(d^{'})}(K).$$

Theorem 4.4. *[12] Let E be an elliptic curve given by the equation $y^2 = x^3 + A + B$ where the coefficients A, B are elements of the finite field $\mathbf{F}_q$ and let $d \in \mathbf{F}_q^{\times}$. Then the number of points in the twist of E by d can be expressed by the following formula:*

$$\#E^{(d)}(\mathbf{F}_q) = q + 1 - \left(\frac{d}{\mathbf{F}_q}\right) a,$$

where $\left(\frac{x^3+Ax+B}{\mathbf{F}_q}\right)$ denotes the Legendre symbol defined by

$$\left(\frac{x}{\mathbf{F}_q}\right) = \begin{cases} 1 & \textit{If } x \textit{ is a square in } \mathbf{F}_q \\ -1 & \textit{If } x \textit{ is not a square in } \mathbf{F}_q \\ 0 & \textit{If } x = 0 \end{cases} .$$

Proof. Suppose q is odd and let $d \in \mathbf{F}_q^{\times} = \mathbf{F}_q \backslash \{0\}$. It can easily be shown that the curve $E^{(d)}$ can be transformed to the curve of the form $d{y_1}^2 = {x_1}^3 + Ax_1 + B$ by rational transformations. So if d is a square of some element in $\mathbf{F}_q$, then the curve $E^{(d)}$ takes the form $y'^2 = {x_1}^3 + Ax_1 + B$. Using the above formula, we see that the number of points in $E^{(d)}(\mathbf{F}_q)$ is equal to $q + 1 - a$ where

$$a = -\sum_{x \in \mathbf{F}_q} \left(\frac{x^3 + Ax + B}{\mathbf{F}_q}\right).$$

If d is not a square in $\mathbf{F}_q$, then the number of points in $E^{(d)}(\mathbf{F}_q)$ is equal to $q + 1 + a$. This is because the product of two non-square elements in a finite field is a square element.

As a result, the number of points in $E^{(d)}(\mathbf{F}_q)$ is given by the following formula:

$$\#E^{(d)}(\mathbf{F}_q) = q + 1 - \left(\frac{d}{\mathbf{F}_q}\right) a.$$

□

Let E be an elliptic curve given by

$$E : y^2 = x^3 + Ax + B,$$

where the coefficients $A, B \in \mathbf{F}_q$. Given a non-square element $d \in \mathbf{F}_q^{\times}$, the twist of E by d is given by

$$E^{(d)} : y^2 = x^3 + Ad^2x + Bd^3,$$

which is isomorphic over $\mathbf{F}_q$ to the curve

$$E^{(d^{'})} : dy^2 = x^3 + Ax + B.$$

Now let $a \in \mathbf{F}_q$ be an arbitrary element. If the element $a^3 + Aa + B$ is square in $\mathbf{F}_q$, then we have $a \in [E(\mathbf{F}_q)]_x$ where $[E(\mathbf{F}_q)]_x$ denotes the set of x-coordinates of the points of the curve E. On the other hand if the element $a^3 + Aa + B$ is non-square in $\mathbf{F}_q$, then we have $a \in [E^{(d^{'})}(\mathbf{F}_q)]_x$ so that the projective space $\mathbf{P}^1(\mathbf{F}_q)$ can be expressed by the x-coordinates of the two curves E and $E^{(d^{'})}$. In other words, we have the following characterization:

$$\mathbf{P}^1(\mathbf{F}_q) = [E(\mathbf{F}_q)]_x \cup [E^{(d^{'})}(\mathbf{F}_q)]_x$$

4.3 Arithmetically exceptional Lattès maps

As we have mentioned in Chapter 3, the endomorphism ring of an elliptic curve always includes multiplication by integers.

Within some specified range for the parameters A and B, some of the outputs can be explained beforehand. More precisely, we can compute the value sets of Lattès maps attached to certain elliptic curves with complex multiplication by using the known theory explained before. For instance, elliptic curves of the form

$$y^2 = x^3 + Ax$$

with $A \neq 0$ have complex multiplication by Gaussian integers $Z[i]$ [12]. Therefore, we can determine the value sets of Lattès maps that are induced by certain elliptic curves without using the code. Similarly, elliptic curves of the form

$$y^2 = x^3 + B$$

with $B \neq 0$ has complex multiplication by the order $Z[\zeta_3]$ [12]. Again we can determine the value sets of Lattès maps that are induced by certain elliptic curves without using the code.

Recall that if E is an elliptic curve given by

$$E : y^2 = x^3 + Ax + B,$$

then the j-invariant of E is

$$j(E) = 1728\frac{4A^3}{4A^3 + 27B^2}.$$

Therefore, our choice for the parameters A and B forces the j-invariant to be an element of the rational numbers $\mathbf{Q}$. However, this is possible only if the endomorphism ring is an order which has class number one. For details, see [8]. It follows that in our range, the elliptic curves with non-integer j-invariants have no complex multiplication. The following table lists all of the orders which have class number one [1].

Table 4.1: Orders with class number 1

$\mathcal{O}$	$j(\mathcal{O})$
$\mathbf{Z}[i]$	12^3
$\mathbf{Z}[\frac{1+\sqrt{-7}}{2}]$	-15^3
$\mathbf{Z}[\frac{1+\sqrt{-11}}{2}]$	-32^3
$\mathbf{Z}[\frac{1+\sqrt{-19}}{2}]$	-96^3
$\mathbf{Z}[\frac{1+\sqrt{-43}}{2}]$	-960^3
$\mathbf{Z}[\frac{1+\sqrt{-67}}{2}]$	-5280^3
$\mathbf{Z}[\frac{1+\sqrt{-163}}{2}]$	-640323^3
$\mathbf{Z}[\frac{1+\sqrt{-3}}{2}]$	0
$\mathbf{Z}[\frac{1+3\sqrt{-3}}{2}]$	-12288000
$\mathbf{Z}[\sqrt{-3}]$	54000
$\mathbf{Z}[\sqrt{-7}]$	255^3
$\mathbf{Z}[\sqrt{-2}]$	20^3
$\mathbf{Z}[2i]$	66^3

Let E be an elliptic curve given by the equation

$$E : y^2 = x^3 + Ax + B, \quad A, B \in K$$

where K is some imaginary quadratic field with ring of integers denoted by $\mathcal{O}_K$. Suppose that the elliptic curve E has complex multiplication by $\mathcal{O}_K$. As noted in the previous chapter, if $\pi \in \mathcal{O}_K$, then there is a formula to compute the size of the value set of F_π defined over a finite field where F_π denotes the Lattès map corresponding to $\pi \in \mathcal{O}_K$. But this formula works for some special cases. To put a finer point on it, the formula given in [3] applies to the Lattès maps of elliptic curves with endomorphism ring isomorphic to the ring of integers of some imaginary quadratic field. In the case that an elliptic curve has no complex multiplication, the situation is ambiguous. More precisely, there's no known formula to determine the sizes of the Lattès maps induced from elliptic curves without complex multiplication. As mentioned before, the aim of this thesis is to determine the value sets of Lattès maps that are induced by elliptic curves without complex multiplication. Recall that in this case, the endomorphism ring is isomorphic to the integers $\mathbf{Z}$. To determine the cardinalities of such Lattès maps, we'll use a computational approach via Pari/GP source code which we introduce as:

```
card(A,B,k,p)={
          local(E=ellinit([A,B]));
          local(f=ellxn(E,k));
          local(r1num=f[1]);
          local(r1den=f[2]);
          local(r1=r1num/r1den);
          local(infinity=[]);
          local(valuevec=vector(p+1));
          local(valueset);
          valuevec[p+1]=infinity;
          for(i=1,p,
          if(subst(r1den,x,Mod(i,p))!=0,
          valuevec[i]=subst(r1,x,Mod(i,p)),
          valuevec[i]=infinity););
          valueset=Set(valuevec);
          return(length(valueset));}
```

The inputs A and B stand for the elliptic curve E defined by $E : y^2 = x^3+Ax+B$, the integer k stand for the k-th Lattès map f_k corresponding to E and finally p denotes the finite field $\mathbf{F}_p$ of p elements. Therefore, card(A, B, k, p) computes the cardinality of the image set of the k-th Lattès map f_k over $\mathbf{F}_p$. Before giving some examples, let us examine the content of the code defined above in a little more detail.

Given $A, B \in \mathbf{Z}$, the function E =`ellinit`($[A, B]$) initializes an elliptic curve E which has the equation $E : y^2 = x^3 + Ax + B$.

For each $k \in \mathbf{Z}$, the function `ellxn`(E,k) returns a vector including the numerator and the denominator of the k-th Lattès map:

$$f_k = \frac{\phi_k(x)}{(\psi_k(x))^2}.$$

Namely, if f=`ellxn`(E,k), then $f[1] = \phi_k(x)$ and $f[2] = (\psi_k(x))^2$. Therefore, the functions $f[1]$ and $f[2]$ return the numerator and the denominator of the k-th Lattès map f_k=`ellxn`(E,k), respectively.

The symbol [] stands for the point at infinity ∞ of E. In the above Pari code, it is named infinity, as can be seen from the defining equality `infinity`=[].

The for loop in the code computes the image of `Mod`(i, p) under the division polynomial $(\psi_k(x))^2$ for each $i \in \{1, 2, ..., p\}$. If the resulting value is not equal to 0, then it evaluates the image of `Mod`(i, p) under the k-th Lattès map. Otherwise, namely, if the image of `Mod`(i, p) under $(\psi_k(x))^2$ is equal to 0, then the image of `Mod`(i, p) under the Lattès map f_k is counted as infinity.

Now, we introduce another code that has the same inputs. For given A, B, k and a prime p such that the elliptic curve $y^2 = x^3 + Ax + B$ has good reduction over $\mathbf{F}_p$, if the Lattès map f_k permutes $\mathbf{F}_p$, it returns 1. Otherwise, the code returns 0. It uses the trace of the Frobenius endomorphism, which we denote by a in the code. The code is as follows:

```
permtest(A,B,k,p)={
            local(E=ellinit([A,B]));
            local(a);
            local(result);
            if(E.disc%p!=0,
            a=ellap(E,p),
            return(0););
```

```
          if(gcd((p+1-a)*(p+1+a),k)==1,
          result=1,
          result=0);
          return(result);}
```

Again before moving on to the examples, we would like to explain the code.

The function `ellinit`([A, B]) initializes an elliptic curve given by the equation $y^2 = x^3 + Ax + B$. In the first line, we define E to be `ellinit`([A, B]) so that E is the elliptic curve with equation $y^2 = x^3 + Ax + B$.

In the next two lines, we put the notions a, `card`p, `card`m, and result, which then will be defined in the following lines.

The function `E.disc` evaluates the discriminant of the elliptic curve E. If E is defined over the finite field $\mathbf{F}_p$, the function `ellap`(E,p) returns the trace of the Frobenius $a = q + 1-$ $E(\mathbf{F}_q)$. The if loop given in the fourth line evaluates the discriminant of E and considers it modulo p. If the resulting value is not zero, then it defines a to be equal to the trace of the Frobenius as can be inferred from the defining relation a=`ellap`(E,p). Otherwise, that is, if the discriminant is equal to zero, then the function `permtest`(A,B,k,p) returns 0.

To determine the density of permutations within some specified range, we introduce the following piece of code:

```
permdens(A,B,k=3,bnd=1229)={
          local(D=4A^3+27B^2);
          local(ctrperm=0, ctrbadred=0);
          if(D==0, return([]););
          for(i=1,bnd,
          p=prime(i);
          if(D%p!=0,
          if(permtest(A,B,k,p)==1, ctrperm++),
          ctrbadred++););
          return((ctrperm)/(bnd-ctrbadred) 1.);}
```

In the first line, we define D to be the discriminant of the elliptic curve given by $y^2 = x^3 + Ax + B$ as can be seen by the defining relation $D = 4A^3 + 27B^2$.

In the second line, we define both the `ctrperm` and `ctrbadred` to be 0. Notice that all of the definitions that are made in the first two lines are given under local. Therefore, it creates a local scope in the sense that they are valid only for the function `permdens`.

The if loop given in the third line evaluates the discriminant of the elliptic curve with equation $y^2 = x^3 + Ax + B$. If the discriminant is equal to zero, then the function `permdens` returns ∞ where we have used the symbol [] as a shorthand for the point at infinity of the elliptic curve in question.

For the first 1229 primes, i.e., the prime integers less than 10000, the for loop given in the fourth line first evaluates the discriminant of the elliptic curve and considers it modulo each such prime p. If the resulting value differs from zero, then it evaluates the cardinality of the k-th Lattès map. If the Lattès map in question is a bijection of $\mathbf{F}_p$, then it increases the permutation counter `ctrperm` by one. Otherwise, it increases the bad reduction counter `ctrbadred` by one.

In the last line, we put the formula

(ctrperm)/(bnd-ctrbadred)*1.

which is a quotient with the numerator being equal to the number of permutations and the denominator being equal to the number obtained by extracting the number of bad reductions from the bound, which is denoted by bnd=1229.

Therefore, the function `permdens` returns the value of what percentage of the given curves are bijections.

Example 4.5. For $A, B \in [-3, 3]$ we can determine the density of permutations of the third Lattès maps by using the following code:

```
for(A= 3 ,3 , for(B= 3 ,3 ,  print([A,B,permdens(A,B,3)])))
```

Then the output of the above code is:

```
[−3, −3, 0.3700081499592502037489812551]
[ 3,  2, []]
[ 3,  1, 0.3672638436482084690553745928]
[ 3, 0, 0.6299918500407497962510187449]
[ 3, 1, 0.3672638436482084690553745928]
[ 3, 2, []]
[ 3, 3, 0.3700081499592502037489812551]
[ 2,  3, 0.3835504885993485342019543974]
[ 2,  2, 0.3879380603096984515077424613]
[ 2,  1, 0.3705211726384364820846905538]
[ 2, 0, 0.6343648208469055374592833876]
[ 2, 1, 0.3705211726384364820846905538]
[ 2, 2, 0.3879380603096984515077424613]
[ 2, 3, 0.3835504885993485342019543974]
[ 1,  3, 0.3908794788273615635179153095]
[ 1,  2, 0.3911980440097799511002444988]
[ 1,  1, 0.3786644951140065146579804560]
[ 1, 0, 0.6302931596091205211726384365]
[ 1, 1, 0.3786644951140065146579804560]
[ 1, 2, 0.3911980440097799511002444988]
[ 1, 3, 0.3908794788273615635179153095]
[0,  3, 0]
[0,  2, 0]
[0,  1, 0]
[0, 0, []]
[0, 1, 0]
[0, 2, 0]
[0, 3, 0]
[1,  3, 0.3773431132844335778321108395]
[1,  2, 0.3748981255093724531377343113]
[1,  1, 0.3819218241042345276872964169]
[1, 0, 0.6302931596091205211726384365]
```

```
[1, 1, 0.3819218241042345276872964169]
[1, 2, 0.3748981255093724531377343113]
[1, 3, 0.3773431132844335778321108395]
[2,  3 , 0.3814180929095354523227383863]
[2,  2 , 0.3817292006525285481239804242]
[2,  1 , 0.3697068403908794788273615635]
[2, 0, 0.6343648208469055374592833876]
[2, 1, 0.3697068403908794788273615635]
[2, 2, 0.3817292006525285481239804242]
[2, 3, 0.3814180929095354523227383863]
[3,  3 , 0.3691931540342298288508557457]
[3,  2 , 0.3781581092094539527302363488]
[3,  1 , 0]
[3, 0, 0.6299918500407497962510187449]
[3, 1, 0]
[3, 2, 0.3781581092094539527302363488]
[3, 3, 0.3691931540342298288508557457]
```

Remark 4.6. Observe that there are three types of returns that we see in the output of the function `permdens`. The first one is [A, B, δ] with $\delta \neq 0$. The second one is [A, B, []], and the third type of output that we see is of the form [A, B, 0] where $A, B \in \mathbf{Z}$.

Initially, we consider the first case. As an example, we can consider the case $A = 3, B = 3$, which corresponds to the output

$$[-3, -3, 0.3700081499592502037489812551].$$

In this case, we have an elliptic curve that is given by the equation

$$y^2 = x^3 - 3x - 3$$

, and the Lattès map

$$f_3 = \frac{\phi_3(x)}{(\psi_3(x))^2}$$

where $\phi_3(x)$ and $\psi_3(x)$ are the third division polynomials corresponding to the elliptic curve in question. The value

$$0.370008149959250203748981 2551$$

that we see in the third entry implies that when we consider the rational function $f_3(x)$ over the finite field $\mathbf{F}_p$ where p is ranging over the first 1229 primes, thirty-seven percent of them gives a permutation, approximately.

Moreover, among the first type of outputs, there are some elliptic curves with complex multiplication. The table given below lists all such curves. In each case, the j-invariant is 1728, and End(E)= $\mathbf{Z}[i]$.

Table 4.2: Densities of the third Lattès maps attached to elliptic curves with CM

Output	Elliptic Curve	Lattès map
[-3, 0, 0.62999185004074979 62]	$y^2 = x^3 - 3x$	$\frac{\phi_3(x,-3,0)}{{\psi_3}^2(x,-3,0)}$
[-2, 0, 0.63436482084690553 74]	$y^2 = x^3 - 2x$	$\frac{\phi_3(x,-2,0)}{{\psi_3}^2(x,-2,0)}$
[-1, 0, 0.63029315960912052 11]	$y^2 = x^3 - x$	$\frac{\phi_3(x,-1,0)}{{\psi_3}^2(x,-1,0)}$
[1, 0, 0.630293159609120521 17]	$y^2 = x^3 + x$	$\frac{\phi_3(x,1,0)}{{\psi_3}^2(x,1,0)}$
[2, 0, 0.634364820846905537459]	$y^2 = x^3 + 2x$	$\frac{\phi_3(x,2,0)}{{\psi_3}^2(x,2,0)}$
[3, 0, 0.629991850040749796251]	$y^2 = x^3 + 3x$	$\frac{\phi_3(x,3,0)}{{\psi_3}^2(x,3,0)}$

Note that the arithmetic exceptionality of the Lattès maps that are listed in the above-given table can be examined using Corollary 3.18 and Corollary 3.19 since they are induced by elliptic curves with complex multiplication.

The remaining cases from the first type of output cannot be explained using Corollary 3.18 and Corollary 3.19. This is because they are induced by elliptic curves without complex multiplication. We list all such Lattès maps and their permutation densities in the following table. Note that since, in this case, the elliptic curves in question have no complex multiplication, their endomorphism rings consist only of the integers. Moreover, by our choice, their j-invariants must be rational numbers. We can conclude that if these j-invariants are not integers, then such elliptic curves have no complex multiplication. This is because if E is an elliptic curve defined over $\mathbf{C}$ with complex multiplication, then its j-invariant must be an algebraic integer [12].

Table 4.3: Densities of the third Lattès maps from elliptic curves without CM

Output	Elliptic Curve	Lattès map	j-invariant
[-3, -3, 0.370008149959250]	$y^2 = x^3 - 3x - 3$	$\frac{\phi_3(x,-3,-3)}{{\psi_3}^2(x,-3,-3)}$	-6912/5
[-3, -1, 0.36726384364820]	$y^2 = x^3 - 3x - 1$	$\frac{\phi_3(x,-3,-1)}{{\psi_3}^2(x,-3,-1)}$	2304
[-3, 1, 0.367263843648208]	$y^2 = x^3 - 3x + 1$	$\frac{\phi_3(x,-3,1)}{{\psi_3}^2(x,-3,1)}$	2304
[-3, 3, 0.37000814995925]	$y^2 = x^3 - 3x + 3$	$\frac{\phi_3(x,-3,3)}{{\psi_3}^2(x,-3,3)}$	-6912/5
[-2, -3, 0.3835504885993]	$y^2 = x^3 - 2x - 3$	$\frac{\phi_3(x,-2,-3)}{{\psi_3}^2(x,-2,-3)}$	-55296/211
[-2, -2, 0.387938060309]	$y^2 = x^3 - 2x - 2$	$\frac{\phi_3(x,-2,-2)}{{\psi_3}^2(x,-2,-2)}$	-13824/19
[-2, -1, 0.370521172638]	$y^2 = x^3 - 2x - 1$	$\frac{\phi_3(x,-2,-1)}{{\psi_3}^2(x,-2,-1)}$	55296/5
[-2, 1, 0.3705211726384]	$y^2 = x^3 - 2x + 1$	$\frac{\phi_3(x,-2,1)}{{\psi_3}^2(x,-2,1)}$	55296/5
[-2, 2, 0.3879380603096]	$y^2 = x^3 - 2x + 2$	$\frac{\phi_3(x,-2,2)}{{\psi_3}^2(x,-2,2)}$	-13824/19
[-2, 3, 0.38355048859934]	$y^2 = x^3 - 2x + 3$	$\frac{\phi_3(x,-2,3)}{{\psi_3}^2(x,-2,3)}$	-55296/211
[-1, -3, 0.3908794788273]	$y^2 = x^3 - x - 3$	$\frac{\phi_3(x,-1,-3)}{{\psi_3}^2(x,-1,-3)}$	-6912/239
[-1, -2, 0.3911980440097]	$y^2 = x^3 - x - 2$	$\frac{\phi_3(x,-1,-2)}{{\psi_3}^2(x,-1,-2)}$	-864/13
[-1, -1, 0.37866449511400]	$y^2 = x^3 - x - 1$	$\frac{\phi_3(x,-1,-1)}{{\psi_3}^2(x,-1,-1)}$	-6912/23
[-1, 1, 0.37866449511400]	$y^2 = x^3 - x + 1$	$\frac{\phi_3(x,-1,1)}{{\psi_3}^2(x,-1,1)}$	-6912/23
[-1, 2, 0.39119804400977]	$y^2 = x^3 - x + 2$	$\frac{\phi_3(x,-1,2)}{{\psi_3}^2(x,-1,2)}$	-864/13
[-1, 3, 0.3908794788273]	$y^2 = x^3 - x + 3$	$\frac{\phi_3(x,-1,3)}{{\psi_3}^2(x,-1,3)}$	-6912/239
[1, -3, 0.3773431132844]	$y^2 = x^3 - x - 3$	$\frac{\phi_3(x,1,-3)}{{\psi_3}^2(x,1,-3)}$	6912/247
[1, -2, 0.3748981255093]	$y^2 = x^3 + x - 2$	$\frac{\phi_3(x,1,-2)}{{\psi_3}^2(x,1,-2)}$	432/7
[1, -1, 0.38192182410423]	$y^2 = x^3 + x - 1$	$\frac{\phi_3(x,1,-1)}{{\psi_3}^2(x,1,-1)}$	6912/31
[1, 1, 0.38192182410423]	$y^2 = x^3 + x + 1$	$\frac{\phi_3(x,1,1)}{{\psi_3}^2(x,1,1)}$	6912/31
[1, 2, 0.3748981255093]	$y^2 = x^3 + x + 2$	$\frac{\phi_3(x,1,2)}{{\psi_3}^2(x,1,2)}$	432/7
[1, 3, 0.3773431132844]	$y^2 = x^3 + x + 3$	$\frac{\phi_3(x,1,3)}{{\psi_3}^2(x,1,3)}$	6912/247
[2, -3, 0.381418092909]	$y^2 = x^3 - 2x - 3$	$\frac{\phi_3(x,2,-3)}{{\psi_3}^2(x,2,-3)}$	55296/275
[2, -2, 0.381729200652]	$y^2 = x^3 + 2x - 2$	$\frac{\phi_3(x,2,-2)}{{\psi_3}^2(x,2,-2)}$	13824/35
[2, -1, 0.369706840390]	$y^2 = x^3 + 2x - 1$	$\frac{\phi_3(x,2,-1)}{{\psi_3}^2(x,2,-1)}$	55296/59
[2, 1, 0.36970684039087]	$y^2 = x^3 + 2x + 1$	$\frac{\phi_3(x,2,1)}{{\psi_3}^2(x,2,1)}$	55296/59
[2, 2, 0.38172920065252]	$y^2 = x^3 + 2x + 2$	$\frac{\phi_3(x,2,2)}{{\psi_3}^2(x,2,2)}$	13824/35
[2, 3, 0.38141809290953]	$y^2 = x^3 + 2x + 3$	$\frac{\phi_3(x,2,3)}{{\psi_3}^2(x,2,3)}$	55296/275

As an example of the second type of output, we can consider the case $A = 3, B = 2$, which corresponds to the output

$$[-3, -2, []].$$

This time, the curve in question is given by the equation

$$y^2 = x^3 - 3x - 2.$$

The symbol [] implies that the discriminant of the curve in question is equal to zero so that there is nothing to consider in this case since this curve does not even define an elliptic curve. We list all such cases in the following table:

Table 4.4: The curves with vanishing discriminant

Output	Curve	Discriminant
[-3, -2, []]	$y^2 = x^3-3x-2$	0
[-3, 2, []]	$y^2 = x^3-3x+2$	0
[0, 0, []]	$y^2 = x^3$	0

As an example of the third type of output, we can consider the case $A = 3, B = 3$, which corresponds to the output

$$[0, 3, 0]$$

so that the elliptic curve in question is given by the equation

$$y^2 = x^3 - 3.$$

In the third entry of this output, the value we see is 0, which implies that for each of the first 1229 primes, the Lattès map $f_3(x)$ does not give a permutation of the finite field $\mathbf{F}_p$. The reason why not even one of them gives a permutation is that there is some 3-torsion point with rational x-coordinate that lies on the elliptic curve in question. For if $(x, y) \in E(\mathbf{Q})$ is a 3-torsion point, then the integer x must be a root of the division polynomial $\psi_3(x)$ whose square appears in the denominator of $f_3(x)$. Since x is a root of this polynomial, then the denominator of the resulting value of the Lattès map $f_3(x)$ vanishes at that point so that we must have

$$f_3(x) = \infty.$$

In the table given below, we list all of the elliptic curves that have some 3-torsion point with rational x-coordinate and corresponding outputs.

Table 4.5: The elliptic curves that have 3-torsion point with rational x-coordinate

Output	Elliptic Curve	Lattès map	3-torsion point
[0, -3, 0]	$y^2 = x^3 - 3$	$\frac{\phi_3(x,0,-3)}{\psi_3{}^2(x,0,-3)}$	$(0, \mp\sqrt{-3})$
[0, -2, 0]	$y^2 = x^3 - 2$	$\frac{\phi_3(x,0,-2)}{\psi_3{}^2(x,0,-2)}$	$(0, \mp\sqrt{-2})$
[0, -1, 0]	$y^2 = x^3 - 1$	$\frac{\phi_3(x,0,-1)}{\psi_3{}^2(x,0,-1)}$	$(0, \mp\sqrt{-1})$
[0, 2, 0]	$y^2 = x^3 + 2$	$\frac{\phi_3(x,0,2)}{\psi_3{}^2(x,0,2)}$	$(0, \mp\sqrt{2})$
[0, 3, 0]	$y^2 = x^3 + 3$	$\frac{\phi_3(x,0,3)}{\psi_3{}^2(x,0,3)}$	$(0, \mp\sqrt{3})$
[3, -1, 0]	$y^2 = x^3+3x-1$	$\frac{\phi_3(x,3,-1)}{\psi_3{}^2(x,3,-1)}$	$(1, \mp\sqrt{3})$
[3, 1, 0]	$y^2 = x^3+3x+1$	$\frac{\phi_3(x,3,1)}{\psi_3{}^2(x,3,1)}$	$(-1, \mp\sqrt{-3})$

Example 4.7. Now we consider the second Lattès map

$$f_2 = \frac{\phi_2(x)}{(\psi_2(x))^2}$$

and put

```
for(A= 3,3, for(B= 3,3,  print([A,B,permdens(A,B,2)])))
```

to get the permutation densities of the second Lattès maps attached to elliptic curves in our range. The resulting output is given by

```
[3,  3, 0.3357783211083944580277098615]
[3,  2, []]
[3,  1, 0.6701954397394136807817589577]
[3, 0, 0]
[3, 1, 0.6701954397394136807817589577]
[3, 2, []]
[3, 3, 0.3357783211083944580277098615]
[2,  3, 0.3257328990228013029315960912]
[2,  2, 0.3357783211083944580277098615]
[2,  1, 0]
[2, 0, 0]
```

```
[ 2,  1,  0]
[ 2,  2,  0.3357783211083944580277098615]
[ 2,  3,  0.3257328990228013029315960912]
[ 1,   3,  0.3314332247557003257328990228]
[ 1,   2,  0.3333333333333333333333333333]
[ 1,   1,  0.3314332247557003257328990228]
[ 1,  0,  0]
[ 1,  1,  0.3314332247557003257328990228]
[ 1,  2,  0.3333333333333333333333333333]
[ 1,  3,  0.3314332247557003257328990228]
[0,   3,  0.3420195439739413680781758958]
[0,   2,  0.3349633251833740831295843521]
[0,   1,  0]
[0,  0,  []]
[0,  1,  0]
[0,  2,  0.3349633251833740831295843521]
[0,  3,  0.3420195439739413680781758958]
[1,   3,  0.3268133659331703341483292584]
[1,   2,  0]
[1,   1,  0.3371335504885993485342019544]
[1,  0,  0]
[1,  1,  0.3371335504885993485342019544]
[1,  2,  0]
[1,  3,  0.3268133659331703341483292584]
[2,   3,  0]
[2,   2,  0.3393148450244698205546492659]
[2,   1,  0.3338762214983713355048859935]
[2,  0,  0]
[2,  1,  0.3338762214983713355048859935]
[2,  2,  0.3393148450244698205546492659]
[2,  3,  0]
[3,   3,  0.3317033414832925835370823146]
```

```
[3,  2,  0.3365933170334148329258353708]
[3,  1,  0.3357783211083944580277098615]
[3, 0, 0]
[3, 1, 0.3357783211083944580277098615]
[3, 2, 0.3365933170334148329258353708]
[3, 3, 0.3317033414832925835370823146]
```

Following the same procedure as in the previous example, we first list the outputs that correspond to the elliptic curves with complex multiplication:

Table 4.6: Densities of the second Lattès maps attached to elliptic curves with CM

Output	Elliptic Curve	Lattès map	$j(E)$	End(E)
[0, -3, 0.342019543973941]	$y^2 = x^3 - 3$	$\frac{\phi_2(x,0,-3)}{{\psi_2}^2(x,0,-3)}$	0	$\mathbf{Z}[\zeta_3]$
[0, -2, 0.334963325183374]	$y^2 = x^3 - 2$	$\frac{\phi_2(x,0,-2)}{{\psi_2}^2(x,0,-2)}$	0	$\mathbf{Z}[\zeta_3]$
[0, 2, 0.33496332518337408]	$y^2 = x^3 + 2$	$\frac{\phi_2(x,0,2)}{{\psi_2}^2(x,0,2)}$	0	$\mathbf{Z}[\zeta_3]$
[0, 3, 0.34201954397394136807]	$y^2 = x^3 + 3$	$\frac{\phi_2(x,0,3)}{{\psi_2}^2(x,0,3)}$	0	$\mathbf{Z}[\zeta_3]$

The outputs corresponding to the elliptic curves without complex multiplication are listed in the following table given below. Observe that each such elliptic curve has endomorphism ring, which is isomorphic to $\mathbf{Z}$. As before, this can easily be seen from the corresponding j-invariants. Recall that from our choice for the coefficients of the elliptic curves in our range, the j-invariants of these curves must be contained in the rational numbers $\mathbf{Q}$. We conclude that if E is an elliptic curve with non-integer j-invariant, then the endomorphism ring of the elliptic curve E must be isomorphic to the ring of integers $\mathbf{Z}$. In other words, we have

$$\text{End}(E) \cong \mathbf{Z}.$$

Therefore, we can determine all elliptic curves without complex multiplication in our range by using this methodology. In the table given below, we list all such elliptic curves with their corresponding j-invariants and the third Lattès maps attached to them. It also contains their corresponding permutation densities.

Table 4.7: Densities of the second Lattès maps from elliptic curves without CM

Output	Elliptic Curve	Lattès map	j-invariant
[-3, -3, 0.3357783211108394]	$y^2 = x^3{-}3x{-}3$	$\frac{\phi_2(x,-3,-3)}{{\psi_2}^2(x,-3,-3)}$	-6912/5
[-3, -1, 0.670195439739413680]	$y^2 = x^3{-}3x{-}1$	$\frac{\phi_2(x,-3,-1)}{{\psi_2}^2(x,-3,-1)}$	2304
[-3, 1, 0.67019543973941368O7]	$y^2 = x^3{-}3x{+}1$	$\frac{\phi_2(x,-3,1)}{{\psi_2}^2(x,-3,1)}$	2304
[-3, 3, 0.33577832110839445 80]	$y^2 = x^3{-}3x{+}3$	$\frac{\phi_2(x,-3,3)}{{\psi_2}^2(x,-3,3)}$	-6912/5
[-2, -3, 0.325732899022801302]	$y^2 = x^3{-}2x{-}3$	$\frac{\phi_2(x,-2,-3)}{{\psi_2}^2(x,-2,-3)}$	-55296/211
[-2, -2, 0.335778321108394458]	$y^2 = x^3{-}2x{-}2$	$\frac{\phi_2(x,-2,-2)}{{\psi_2}^2(x,-2,-2)}$	-13824/19
[-2, 2, 0.335778321108394458]	$y^2 = x^3{-}2x{+}2$	$\frac{\phi_2(x,-2,2)}{{\psi_2}^2(x,-2,2)}$	-13824/19
[-2, 3, 0.325732899022801302]	$y^2 = x^3{-}2x{+}3$	$\frac{\phi_2(x,-2,3)}{{\psi_2}^2(x,-2,3)}$	-55296/211
[-1, -3, 0.33143322475570032]	$y^2 = x^3 - x - 3$	$\frac{\phi_2(x,-1,-3)}{{\psi_2}^2(x,-1,-3)}$	-6912/239
[-1, -2, 0.333333333333333]	$y^2 = x^3 - x - 2$	$\frac{\phi_2(x,-1,-2)}{{\psi_2}^2(x,-1,-2)}$	-864/13
[-1, -1, 0.3314332247557003]	$y^2 = x^3 - x - 1$	$\frac{\phi_2(x,-1,-1)}{{\psi_2}^2(x,-1,-1)}$	-6912/23
[-1, 1, 0.331433224755700325]	$y^2 = x^3 - x + 1$	$\frac{\phi_2(x,-1,1)}{{\psi_2}^2(x,-1,1)}$	-6912/23
[-1, 2, 0.333333333333333333]	$y^2 = x^3 - x + 2$	$\frac{\phi_2(x,-1,2)}{{\psi_2}^2(x,-1,2)}$	-864/13
[-1, 3, 0.3314332247557003257]	$y^2 = x^3 - x + 3$	$\frac{\phi_2(x,-1,3)}{{\psi_2}^2(x,-1,3)}$	-6912/239
[1, -3, 0.3268133659331703341]	$y^2 = x^3 - x - 3$	$\frac{\phi_2(x,1,-3)}{{\psi_2}^2(x,1,-3)}$	6912/247
[1, -1, 0.337133550488599348]	$y^2 = x^3 + x - 1$	$\frac{\phi_2(x,1,-1)}{{\psi_2}^2(x,1,-1)}$	6912/31
[1, 1, 0.3371335504885993485]	$y^2 = x^3 + x + 1$	$\frac{\phi_2(x,1,1)}{{\psi_2}^2(x,1,1)}$	6912/31
[1, 3, 0.3268133659331703341]	$y^2 = x^3 + x + 3$	$\frac{\phi_2(x,1,3)}{{\psi_2}^2(x,1,3)}$	6912/247
[2, -2, 0.33931484502446982]	$y^2 = x^3{+}2x{-}2$	$\frac{\phi_2(x,2,-2)}{{\psi_2}^2(x,2,-2)}$	13824/35
[2, -1, 0.333876221498371335]	$y^2 = x^3{+}2x{-}1$	$\frac{\phi_2(x,2,-1)}{{\psi_2}^2(x,2,-1)}$	55296/59
[2, 1, 0.333876221498371335]	$y^2 = x^3{+}2x{+}1$	$\frac{\phi_2(x,2,1)}{{\psi_2}^2(x,2,1)}$	55296/59
[2, 2, 0.339314845024469820]	$y^2 = x^3{+}2x{+}2$	$\frac{\phi_2(x,2,2)}{{\psi_2}^2(x,2,2)}$	13824/35
[3, -3, 0.331703341483292583]	$y^2 = x^3{+}3x{-}3$	$\frac{\phi_2(x,3,-3)}{{\psi_2}^2(x,3,-3)}$	6912/13
[3, -2, 0.336593317033414832]	$y^2 = x^3{+}3x{-}2$	$\frac{\phi_2(x,3,-2)}{{\psi_2}^2(x,3,-2)}$	864

Lastly, the following table shows the third type of the outputs and their corresponding 2-torsion points with rational x- coordinate:

Table 4.8: The elliptic curves that have 2-torsion point with rational x-coordinate

Output	Elliptic Curve	Lattès map	2-torsion point
[-3, 0, 0]	$y^2 = x^3 - 3x$	$\frac{\phi_2(x,-3,0)}{{\psi_2}^2(x,-3,0)}$	$(0,0)$
[-2, -1, 0]	$y^2 = x^3 - 2x - 1$	$\frac{\phi_2(x,-2,-1)}{{\psi_2}^2(x,-2,-1)}$	$(-1,0)$
[0, -1, 0]	$y^2 = x^3 - 1$	$\frac{\phi_2(x,0,-1)}{{\psi_2}^2(x,0,-1)}$	$(1,0)$
[-2, 0, 0]	$y^2 = x^3 - 2x$	$\frac{\phi_2(x,-2,0)}{{\psi_2}^2(x,-2,0)}$	$(0,0)$
[-2, 1, 0]	$y^2 = x^3 - 2x + 1$	$\frac{\phi_2(x,-2,1)}{{\psi_2}^2(x,-2,1)}$	$(1,0)$
[-1, 0, 0]	$y^2 = x^3 - x$	$\frac{\phi_2(x,-1,0)}{{\psi_2}^2(x,-1,0)}$	$(0,0)$
[0, -1, 0]	$y^2 = x^3 - 1$	$\frac{\phi_2(x,0,-1)}{{\psi_2}^2(x,0,-1)}$	$(1,0)$
[0, 1, 0]	$y^2 = x^3 + 1$	$\frac{\phi_2(x,0,1)}{{\psi_2}^2(x,0,1)}$	$(-1,0)$
[1, -2, 0]	$y^2 = x^3 + x - 2$	$\frac{\phi_2(x,1,-2)}{{\psi_2}^2(x,1,-2)}$	$(1,0)$
[1, 0, 0]	$y^2 = x^3 + x$	$\frac{\phi_2(x,1,0)}{{\psi_2}^2(x,1,0)}$	$(0,0)$
[1, 2, 0]	$y^2 = x^3 + x + 2$	$\frac{\phi_2(x,1,2)}{{\psi_2}^2(x,1,2)}$	$(-1,0)$
[2, -3, 0]	$y^2 = x^3 + 2x - 3$	$\frac{\phi_2(x,2,-3)}{{\psi_2}^2(x,2,-3)}$	$(1,0)$
[2, 0, 0]	$y^2 = x^3 + 2x$	$\frac{\phi_2(x,2,0)}{{\psi_2}^2(x,2,0)}$	$(0,0)$
[2, 3, 0]	$y^2 = x^3 + 2x + 3$	$\frac{\phi_2(x,2,3)}{{\psi_2}^2(x,2,3)}$	$(-1,0)$
[3, 0, 0]	$y^2 = x^3 + 3x$	$\frac{\phi_2(x,3,0)}{{\psi_2}^2(x,3,0)}$	$(0,0)$

Example 4.8. Now we consider the fifth Lattès map

$$f_5 = \frac{\phi_5(x)}{(\psi_5(x))^2}$$

and put

```
for(A= 3,3,for(B= 3,3,  print([A,B,permdens(A,B,5)])))
```

to get the permutation densities of the fifth Lattès maps attached to elliptic curves in our range. The resulting output is as follows:

```
[ 3,  3,  0.5770171149144254278728606357]
[ 3,  2,  []]
[ 3,  1,  0.5952768729641693811074918567]
[ 3 ,  0,  0.5069274653626731866340668297]
[ 3 ,  1,  0.5952768729641693811074918567]
[ 3 ,  2,  []]
[ 3 ,  3,  0.5770171149144254278728606357]
[ 2 ,   3 ,  0.5895765472312703583061889251]
[ 2 ,   2 ,  0.5925020374898125509372453138]
[ 2 ,   1 ,  0.5977198697068403908794788274]
[ 2 ,  0,  0.5065146579804560260586319218]
[ 2 ,  1,  0.5977198697068403908794788274]
[ 2 ,  2,  0.5925020374898125509372453138]
[ 2 ,  3,  0.5895765472312703583061889251]
[ 1 ,   3 ,  0.5773615635179153094462540717]
[ 1 ,   2 ,  0.5802770986145069274653626732]
[ 1 ,   1 ,  0.5903908794788273615635179153]
[ 1 ,  0,  0.5024429967426710097719869707]
[ 1 ,  1,  0.5903908794788273615635179153]
[ 1 ,  2,  0.5802770986145069274653626732]
[ 1 ,  3,  0.5773615635179153094462540717]
[0,   3 ,  0.8265472312703583061889250814]
[0,   2 ,  0.8337408312958435207823960880]
[0,   1 ,  0.8355048859934853420195439739]
[0,  0,  []]
[0,  1,  0.8355048859934853420195439739]
[0,  2,  0.8337408312958435207823960880]
[0,  3,  0.8265472312703583061889250814]
[1,   3 ,  0.5941320293398533007334963325]
[1,   2 ,  0.5884270578647106764466177669]
[1,   1 ,  0.5944625407166123778501628665]
[1,  0,  0.5024429967426710097719869707]
[1,  1,  0.5944625407166123778501628665]
[1,  2,  0.5884270578647106764466177669]
[1,  3,  0.5941320293398533007334963325]
```

```
[2,  3, 0.5729421352893235533822330888]
[2,  2, 0.5986949429037520391517128874]
[2,  1, 0.5960912052117263843648208469]
[2, 0, 0.5065146579804560260586319218]
[2, 1, 0.5960912052117263843648208469]
[2, 2, 0.5986949429037520391517128874]
[2, 3, 0.5729421352893235533822330888]
[3,  3, 0.5802770986145069274653626732]
[3,  2, 0.6014669926650366748166259169]
[3,  1, 0.5819070904645476772616136919]
[3, 0, 0.5069274653626731866340668297]
[3, 1, 0.5819070904645476772616136919]
[3, 2, 0.6014669926650366748166259169]
[3, 3, 0.5802770986145069274653626732]
```

Following the same procedure, we list the CM cases and non-CM cases in the following two tables respectively:

Table 4.9: Densities of the fifth Lattès maps attached to elliptic curves with CM

Output	Elliptic Curve	Lattès map	$j(E)$	End(E)
[0, -3, 0.8265472312703583061]	$y^2 = x^3 - 3$	$\frac{\phi_5(x,0,-3)}{{\psi_5}^2(x,0,-3)}$	0	$\mathbf{Z}[\zeta_3]$
[0, -2, 0.8337408312958435207]	$y^2 = x^3 - 2$	$\frac{\phi_5(x,0,-2)}{{\psi_5}^2(x,0,-2)}$	0	$\mathbf{Z}[\zeta_3]$
[0, -1, 0.835504885993485342]	$y^2 = x^3 - 1$	$\frac{\phi_5(x,0,-1)}{{\psi_5}^2(x,0,-1)}$	0	$\mathbf{Z}[\zeta_3]$
[0, 1, 0.835504885993485342]	$y^2 = x^3 + 1$	$\frac{\phi_5(x,0,1)}{{\psi_5}^2(x,0,1)}$	0	$\mathbf{Z}[\zeta_3]$
[0, 2, 0.833740831295843520]	$y^2 = x^3 + 2$	$\frac{\phi_5(x,0,2)}{{\psi_5}^2(x,0,2)}$	0	$\mathbf{Z}[\zeta_3]$
[0, 3, 0.826547231270358306]	$y^2 = x^3 + 3$	$\frac{\phi_5(x,0,3)}{{\psi_5}^2(x,0,3)}$	0	$\mathbf{Z}[\zeta_3]$
[-3, 0, 0.506927465362673186]	$y^2 = x^3 - 3x$	$\frac{\phi_5(x,-3,0)}{{\psi_5}^2(x,-3,0)}$	1728	$\mathbf{Z}[i]$
[-2, 0, 0.506514657980456026]	$y^2 = x^3 - 2x$	$\frac{\phi_5(x,-2,0)}{{\psi_5}^2(x,-2,0)}$	1728	$\mathbf{Z}[i]$
[-1, 0, 0.502442996742671009]	$y^2 = x^3 - x$	$\frac{\phi_5(x,-1,0)}{{\psi_5}^2(x,-1,0)}$	1728	$\mathbf{Z}[i]$
[1, 0, 0.502442996742671009]	$y^2 = x^3 + x$	$\frac{\phi_5(x,1,0)}{{\psi_5}^2(x,1,0)}$	1728	$\mathbf{Z}[i]$
[2, 0, 0.506514657980456026]	$y^2 = x^3 + 2x$	$\frac{\phi_5(x,2,0)}{{\psi_5}^2(x,2,0)}$	1728	$\mathbf{Z}[i]$
[3, 0, 0.5069274653626731866]	$y^2 = x^3 + 3x$	$\frac{\phi_5(x,3,0)}{{\psi_5}^2(x,3,0)}$	1728	$\mathbf{Z}[i]$

Table 4.10: Densities of the fifth Lattès maps from elliptic curves without CM

Output	Elliptic Curve	Lattès map	j-invariant
[-3, -3, 0.57701711491442542]	$y^2 = x^3-3x-3$	$\frac{\phi_5(x,-3,-3)}{{\psi_5}^2(x,-3,-3)}$	-6912/5
[-3, -1, 0.59527687296416938]	$y^2 = x^3-3x-1$	$\frac{\phi_5(x,-3,-1)}{{\psi_5}^2(x,-3,-1)}$	2304
[-3, 1, 0.59527687296416938]	$y^2 = x^3-3x+1$	$\frac{\phi_5(x,-3,1)}{{\psi_5}^2(x,-3,1)}$	2304
[-3, 3, 0.57701711491442542]	$y^2 = x^3-3x+3$	$\frac{\phi_5(x,-3,3)}{{\psi_5}^2(x,-3,3)}$	-6912/5
[-2, -3, 0.58957654723127035]	$y^2 = x^3-2x-3$	$\frac{\phi_5(x,-2,-3)}{{\psi_5}^2(x,-2,-3)}$	-55296/211
[-2, -2, 0.592502037489812]	$y^2 = x^3-2x-2$	$\frac{\phi_5(x,-2,-2)}{{\psi_5}^2(x,-2,-2)}$	-13824/19
[-2, -1, 0.59771986970684039]	$y^2 = x^3-2x-1$	$\frac{\phi_5(x,-2,-1)}{{\psi_5}^2(x,-2,-1)}$	55296/5
[-2, 1, 0.59771986970684039]	$y^2 = x^3-2x+1$	$\frac{\phi_5(x,-2,1)}{{\psi_5}^2(x,-2,1)}$	55296/5
[-2, 2, 0.59250203748981255]	$y^2 = x^3-2x+2$	$\frac{\phi_5(x,-2,2)}{{\psi_5}^2(x,-2,2)}$	-13824/19
[-2, 3, 0.5895765472312703]	$y^2 = x^3-2x+3$	$\frac{\phi_5(x,-2,3)}{{\psi_5}^2(x,-2,3)}$	-55296/211
[-1, -3, 0.5773615635179153]	$y^2 = x^3-x-3$	$\frac{\phi_5(x,-1,-3)}{{\psi_5}^2(x,-1,-3)}$	-6912/239
[-1, -2, 0.580277098614506]	$y^2 = x^3-x-2$	$\frac{\phi_5(x,-1,-2)}{{\psi_5}^2(x,-1,-2)}$	-864/13
[-1, -1, 0.590390879478827]	$y^2 = x^3-x-1$	$\frac{\phi_5(x,-1,-1)}{{\psi_5}^2(x,-1,-1)}$	-6912/23
[-1, 1, 0.5903908794788273]	$y^2 = x^3-x+1$	$\frac{\phi_5(x,-1,1)}{{\psi_5}^2(x,-1,1)}$	-6912/23
[-1, 2, 0.5802770986145069]	$y^2 = x^3-x+2$	$\frac{\phi_5(x,-1,2)}{{\psi_5}^2(x,-1,2)}$	-864/13
[-1, 3, 0.5773615635179153]	$y^2 = x^3-x+3$	$\frac{\phi_5(x,-1,3)}{{\psi_5}^2(x,-1,3)}$	-6912/239
[1, -3, 0.59413202933985330]	$y^2 = x^3+x-3$	$\frac{\phi_5(x,1,-3)}{{\psi_5}^2(x,1,-3)}$	6912/247
[1, -2, 0.58842705786471067]	$y^2 = x^3+x-2$	$\frac{\phi_5(x,1,-2)}{{\psi_5}^2(x,1,-2)}$	432/7
[1, -1, 0.59446254071661237]	$y^2 = x^3+x-1$	$\frac{\phi_5(x,1,-1)}{{\psi_5}^2(x,1,-1)}$	6912/31
[1, 1, 0.5944625407166123]	$y^2 = x^3+x+1$	$\frac{\phi_5(x,1,1)}{{\psi_5}^2(x,1,1)}$	6912/31
[1, 2, 0.58842705786471067]	$y^2 = x^3+x+2$	$\frac{\phi_5(x,1,2)}{{\psi_5}^2(x,1,2)}$	432/7
[1, 3, 0.59413202933985330]	$y^2 = x^3+x+3$	$\frac{\phi_5(x,1,3)}{{\psi_5}^2(x,1,3)}$	6912/247
[2, -3, 0.5729421352893235]	$y^2 = x^3+2x-3$	$\frac{\phi_5(x,2,-3)}{{\psi_5}^2(x,2,-3)}$	55296/275
[2, -2, 0.598694942903752]	$y^2 = x^3+2x-2$	$\frac{\phi_5(x,2,-2)}{{\psi_5}^2(x,2,-2)}$	13824/35
[2, -1, 0.5960912052117263]	$y^2 = x^3+2x-1$	$\frac{\phi_5(x,2,-1)}{{\psi_5}^2(x,2,-1)}$	55296/59

Example 4.9. Now we consider the seventh Lattès map

$$f_7 = \frac{\phi_7(x)}{(\psi_7(x))^2}$$

and put

```
for(A= 3 ,3 , for(B= 3 ,3 ,  print([A,B,permdens(A,B,7)])))
```

to get the permutation densities of the seventh Lattès maps attached to elliptic curves in our range. The resulting output is as follows:

```
[ 3 ,   3 ,  0.5770171149144254278728606357]
[ 3 ,   2 ,  []]
[ 3 ,   1 ,  0.5952768729641693811074918567]
[ 3 ,  0 ,  0.5069274653626731866340668297]
[ 3 ,  1 ,  0.5952768729641693811074918567]
[ 3 ,  2 ,  []]
[ 3 ,  3 ,  0.5770171149144254278728606357]
[ 2 ,   3 ,  0.5895765472312703583061889251]
[ 2 ,   2 ,  0.5925020374898125509372453138]
[ 2 ,   1 ,  0.5977198697068403908794788274]
[ 2 ,  0 ,  0.5065146579804560260586319218]
[ 2 ,  1 ,  0.5977198697068403908794788274]
[ 2 ,  2 ,  0.5925020374898125509372453138]
[ 2 ,  3 ,  0.5895765472312703583061889251]
[ 1 ,   3 ,  0.5773615635179153094462540717]
[ 1 ,   2 ,  0.5802770986145069274653626732]
[ 1 ,   1 ,  0.5903908794788273615635179153]
[ 1 ,  0 ,  0.5024429967426710097719869707]
[ 1 ,  1 ,  0.5903908794788273615635179153]
[ 1 ,  2 ,  0.5802770986145069274653626732]
[ 1 ,  3 ,  0.5773615635179153094462540717]
[0 ,   3 ,  0.8265472312703583061889250814]
[0 ,   2 ,  0.8337408312958435207823960880]
[0 ,   1 ,  0.8355048859934853420195439739]
[0 ,  0 ,  []]
```

```
[0, 1, 0.835504885993485342019543973 9]
[0, 2, 0.833740831295843520782396088 0]
[0, 3, 0.826547231270358306188925081 4]
[1,  3, 0.594132029339853300733496332 5]
[1,  2, 0.588427057864710676446617766 9]
[1,  1, 0.594462540716612377850162866 5]
[1, 0, 0.502442996742671009771986970 7]
[1, 1, 0.594462540716612377850162866 5]
[1, 2, 0.588427057864710676446617766 9]
[1, 3, 0.594132029339853300733496332 5]
[2,  3, 0.572942135289323553382233088 8]
[2,  2, 0.598694942903752039151712887 4]
[2,  1, 0.596091205211726384364820846 9]
[2, 0, 0.506514657980456026058631921 8]
[2, 1, 0.596091205211726384364820846 9]
[2, 2, 0.598694942903752039151712887 4]
[2, 3, 0.572942135289323553382233088 8]
[3,  3, 0.580277098614506927465362673 2]
[3,  2, 0.601466992665036674816625916 9]
[3,  1, 0.581907090464547677261613691 9]
[3, 0, 0.506927465362673186634066829 7]
[3, 1, 0.581907090464547677261613691 9]
[3, 2, 0.601466992665036674816625916 9]
[3, 3, 0.580277098614506927465362673 2]
```

Remark 4.10. As in the previous example, there is no third type of output, which means there is no elliptic curve that has a 7-torsion point with a rational x-coordinate. Observe that this implies that the division polynomial ψ_7 has no rational root for elliptic curves in our range. In the following two tables, we list all CM and non-CM cases, respectively. As we have mentioned before, we first find all elliptic curves with complex multiplication by checking their corresponding j-invariants. We also determine their endomorphism rings by using Table 4.1. As can be seen from the table, there are two types of endomorphism rings, which are $\mathbf{Z}[\zeta_3]$ and $\mathbf{Z}[i]$.

Table 4.11: Densities of the seventh Lattès maps from elliptic curves with CM

Output	Elliptic Curve	Lattès map	$j(E)$	End(E)
[0, -3, 0.62785016286644951]	$y^2 = x^3 - 3$	$\frac{\phi_7(x,0,-3)}{{\psi_7}^2(x,0,-3)}$	0	$\mathbf{Z}[\zeta_3]$
[0, -2, 0.63814180929095354]	$y^2 = x^3 - 2$	$\frac{\phi_7(x,0,-2)}{{\psi_7}^2(x,0,-2)}$	0	$\mathbf{Z}[\zeta_3]$
[0, -1, 0.64332247557003257]	$y^2 = x^3 - 1$	$\frac{\phi_7(x,0,-1)}{{\psi_7}^2(x,0,-1)}$	0	$\mathbf{Z}[\zeta_3]$
[0, 1, 0.643322475570032573]	$y^2 = x^3 + 1$	$\frac{\phi_7(x,0,1)}{{\psi_7}^2(x,0,1)}$	0	$\mathbf{Z}[\zeta_3]$
[0, 2, 0.638141809290953545]	$y^2 = x^3 + 2$	$\frac{\phi_7(x,0,2)}{{\psi_7}^2(x,0,2)}$	0	$\mathbf{Z}[\zeta_3]$
[0, 3, 0.62785016286644951]	$y^2 = x^3 + 3$	$\frac{\phi_7(x,0,3)}{{\psi_7}^2(x,0,3)}$	0	$\mathbf{Z}[\zeta_3]$
[-3, 0, 0.89649551752241238]	$y^2 = x^3 - 3x$	$\frac{\phi_7(x,-3,0)}{{\psi_7}^2(x,-3,0)}$	1728	$\mathbf{Z}[i]$
[-2, 0, 0.899837133550488]	$y^2 = x^3 - 2x$	$\frac{\phi_7(x,-2,0)}{{\psi_7}^2(x,-2,0)}$	1728	$\mathbf{Z}[i]$
[-1, 0, 0.89820846905537]	$y^2 = x^3 - x$	$\frac{\phi_7(x,-1,0)}{{\psi_7}^2(x,-1,0)}$	1728	$\mathbf{Z}[i]$
[1, 0, 0.8982084690553745]	$y^2 = x^3 + x$	$\frac{\phi_7(x,1,0)}{{\psi_7}^2(x,1,0)}$	1728	$\mathbf{Z}[i]$
[2, 0, 0.899837133550488]	$y^2 = x^3 + 2x$	$\frac{\phi_7(x,2,0)}{{\psi_7}^2(x,2,0)}$	1728	$\mathbf{Z}[i]$
[3, 0, 0.896495517522412]	$y^2 = x^3 + 3x$	$\frac{\phi_7(x,3,0)}{{\psi_7}^2(x,3,0)}$	1728	$\mathbf{Z}[i]$

Finally, it remains to list all outputs corresponding to elliptic curves without complex multiplication. As we have indicated before, if E is one such elliptic curve, then

$$\text{End}(E) \cong \mathbf{Z}.$$

Note also that except the following two elliptic curves

$$y^2 = x^3 - 3x - 1$$

$$y^2 = x^3 - 3x + 1,$$

all elliptic curves in our range have non-integer j-invariants. Therefore, it immediately follows that all such elliptic curves have no complex multiplication. This is because j-invariant is an algebraic integer. In the case of the two curves given above, Table 4.1 implies that both have no complex multiplication. The following table illustrates this situation.

Table 4.12: Densities of the seventh Lattès maps from non-CM cases

Output	Elliptic Curve	Lattès map	j-invariant
[-3, -3, 0.69845150774246128]	$y^2 = x^3{-}3x{-}3$	$\frac{\phi_7(x,-3,-3)}{{\psi_7}^2(x,-3,-3)}$	-6912/5
[-3, -1, 0.6807817589576547]	$y^2 = x^3{-}3x{-}1$	$\frac{\phi_7(x,-3,-1)}{{\psi_7}^2(x,-3,-1)}$	2304
[-3, 1, 0.680781758957654]	$y^2 = x^3{-}3x{+}1$	$\frac{\phi_7(x,-3,1)}{{\psi_7}^2(x,-3,1)}$	2304
[-3, 3, 0.69845150774246128]	$y^2 = x^3{-}3x{+}3$	$\frac{\phi_7(x,-3,3)}{{\psi_7}^2(x,-3,3)}$	-6912/5
[-2, -3, 0.7035830618892508]	$y^2 = x^3{-}2x{-}3$	$\frac{\phi_7(x,-2,-3)}{{\psi_7}^2(x,-2,-3)}$	-55296/211
[-2, -2, 0.7017114914425427]	$y^2 = x^3{-}2x{-}2$	$\frac{\phi_7(x,-2,-2)}{{\psi_7}^2(x,-2,-2)}$	-13824/19
[-2, -1, 0.7239413680781758]	$y^2 = x^3{-}2x{-}1$	$\frac{\phi_7(x,-2,-1)}{{\psi_7}^2(x,-2,-1)}$	55296/5
[-2, 1, 0.7239413680781758]	$y^2 = x^3{-}2x{+}1$	$\frac{\phi_7(x,-2,1)}{{\psi_7}^2(x,-2,1)}$	55296/5
[-2, 2, 0.70171149144254278]	$y^2 = x^3{-}2x{+}2$	$\frac{\phi_7(x,-2,2)}{{\psi_7}^2(x,-2,2)}$	-13824/19
[-2, 3, 0.70358306188925081]	$y^2 = x^3{-}2x{+}3$	$\frac{\phi_7(x,-2,3)}{{\psi_7}^2(x,-2,3)}$	-55296/211
[-1, -3, 0.6889250814332247]	$y^2 = x^3 - x - 3$	$\frac{\phi_7(x,-1,-3)}{{\psi_7}^2(x,-1,-3)}$	-6912/239
[-1, -2, 0.6919315403422982]	$y^2 = x^3 - x - 2$	$\frac{\phi_7(x,-1,-2)}{{\psi_7}^2(x,-1,-2)}$	-864/13
[-1, -1, 0.7076547231270358]	$y^2 = x^3 - x - 1$	$\frac{\phi_7(x,-1,-1)}{{\psi_7}^2(x,-1,-1)}$	-6912/23
[-1, 1, 0.7076547231270358]	$y^2 = x^3 - x + 1$	$\frac{\phi_7(x,-1,1)}{{\psi_7}^2(x,-1,1)}$	-6912/23
[-1, 2, 0.6919315403422982]	$y^2 = x^3 - x + 2$	$\frac{\phi_7(x,-1,2)}{{\psi_7}^2(x,-1,2)}$	-864/13
[-1, 3, 0.6889250814332247]	$y^2 = x^3 - x + 3$	$\frac{\phi_7(x,-1,3)}{{\psi_7}^2(x,-1,3)}$	-6912/239
[1, -3, 0.6951915240423797]	$y^2 = x^3 + x - 3$	$\frac{\phi_7(x,1,-3)}{{\psi_7}^2(x,1,-3)}$	6912/247
[1, -2, 0.70660146699266503]	$y^2 = x^3 + x - 2$	$\frac{\phi_7(x,1,-2)}{{\psi_7}^2(x,1,-2)}$	432/7
[1, -1, 0.70928338762214983]	$y^2 = x^3 + x - 1$	$\frac{\phi_7(x,1,-1)}{{\psi_7}^2(x,1,-1)}$	6912/31
[1, 1, 0.70928338762214983]	$y^2 = x^3 + x + 1$	$\frac{\phi_7(x,1,1)}{{\psi_7}^2(x,1,1)}$	6912/31
[1, 2, 0.706601466992665036]	$y^2 = x^3 + x + 2$	$\frac{\phi_7(x,1,2)}{{\psi_7}^2(x,1,2)}$	432/7
[1, 3, 0.695191524042379788]	$y^2 = x^3 + x + 3$	$\frac{\phi_7(x,1,3)}{{\psi_7}^2(x,1,3)}$	6912/247
[2, -3, 0.71882640586797066]	$y^2 = x^3{+}2x{-}3$	$\frac{\phi_7(x,2,-3)}{{\psi_7}^2(x,2,-3)}$	55296/275
[2, -2, 0.69249592169657422]	$y^2 = x^3{+}2x{-}2$	$\frac{\phi_7(x,2,-2)}{{\psi_7}^2(x,2,-2)}$	13824/35
[2, -1, 0.6726384364820846]	$y^2 = x^3{+}2x{-}1$	$\frac{\phi_7(x,2,-1)}{{\psi_7}^2(x,2,-1)}$	55296/59
[1, 3, 0.695191524042379788]	$y^2 = x^3 + x + 3$	$\frac{\phi_7(x,1,3)}{{\psi_7}^2(x,1,3)}$	6912/247
[2, -3, 0.71882640586797066]	$y^2 = x^3{+}2x{-}3$	$\frac{\phi_7(x,2,-3)}{{\psi_7}^2(x,2,-3)}$	55296/275
[2, -2, 0.69249592169657422]	$y^2 = x^3{+}2x{-}2$	$\frac{\phi_7(x,2,-2)}{{\psi_7}^2(x,2,-2)}$	13824/35

CHAPTER 5

CONCLUSIONS AND FUTURE WORK

As we have indicated in the first chapter, the goal of this thesis was to study the value sets of Lattès maps that are induced by elliptic curves without complex multiplication and discuss the arithmetical exceptionality of such maps. To accomplish this goal, we have put on an experimental approach and used the computer algebra program Pari/GP codes.

There were two main pieces of code used in the fourth chapter, which we named `card` and `permdens`.

In order to determine the size of the value sets, we have used the function named `card` that has four inputs A, B, k and p, which corresponds to the elliptic curve

$$E : y^2 = x^3 + Ax + B,$$

the Lattès map

$$f_k(x) = \frac{\phi_k(A, B, x)}{\psi_k(A, B, x)^2}$$

and a prime p. Here we denote by $\psi_k(A, B, x)$ the k-th division polynomial corresponding to the elliptic curve E. When the elliptic curve E has a good reduction over the finite field $\mathbf{F}_p$, the function `card`(A, B, k, p) returns the size of the image set of the k-th Lattès map f_k over the projective space $\mathbf{P}^1(\mathbf{F}_p)$.

In order to discuss the arithmetic exceptionality of such maps, we have used the function `permdens` that has three inputs A, B and k, which again corresponds to the elliptic curve $y^2 = x^3 + Ax + B$ and the k-th Lattès map f_k.

In the fourth chapter, where we have made various computations using the Pari/GP codes, we have seen that there are three types of outputs of which the function `permdens` returns.

The first of these was the outputs of the form

$$[A, B, []].$$

As we have noted before, such cases occur when the discriminant of the curve $y^2 = x^3 + Ax + B$ is equal to zero, that is, when we have $4A^3 + 27B^2 = 0$. But we don't consider the Lattès maps that are induced by such curves because, in this case, the curve in question does not even define an elliptic curve. Therefore, we exclude such cases since they are beyond the scope of this thesis.

The second one is of the form

$$[A, B, 0],$$

which corresponds to zero density. This means that for a chosen integer $k \geq 1$, the k-th Lattès map does not give a permutation of $\mathbf{F}_p$'s where p is ranging over the first 1229 primes. This is because the elliptic curve

$$y^2 = x^3 + Ax + B$$

has k-torsion point with rational x-coordinate. The reason k-th Lattès map never permutes the projective space $\mathbf{P}^1(\mathbf{F}_p)$ can be clarified as follows: If the point $P = (a, b)$ is a k-torsion point with a belongs to the rational numbers, then a must be a root of the division polynomial

$$\psi_k(A, B, x)^2.$$

Therefore, when we reduce the coefficients A and B modulo p, then $\bar{a}$ must be root of the reduced polynomial

$$\psi_k(\bar{A}, \bar{B}, x)^2.$$

But this implies that when we consider the k-th Lattès map over the projective space $\mathbf{P}^1(\mathbf{F}_p)$, it is not an injection since it maps both $\bar{a}$ and ∞ to the point ∞. From this point of view, we conclude that if an elliptic curve E has k-torsion point with rational x-coordinate, then the k-th Lattès map attached to E is not arithmetically exceptional. In other words, the Lattès maps corresponding to the second type of the outputs of the function `permdens` are not arithmetically exceptional.

The third type of output has the form

$$[A, B, \delta]$$

with $\delta \neq 0$. This means that for a chosen integer $k \geq 1$, the k-th Lattès map permutes $\mathbf{F}_p$'s for some primes, and δ gives the density of these permutations. This is because there is no k-torsion point with rational x-coordinate lying on the elliptic curve

$$y^2 = x^3 + Ax + B.$$

In such cases, we experimentally believe that the k-th Lattès map attached to E is arithmetically exceptional. Immediately afterward the remarks noted above, one may expect the following: For each integer $k \geq 1$, the $k-$th Lattès map f_k is arithmetically exceptional if and only if the elliptic curve E has no k-torsion point whose x-coordinate is rational.

Note that one side of this statement is trivially true. Namely, if E has k-torsion point with rational x-coordinate, then f_k is not arithmetically exceptional.

Note also that the above-given statement can be alternatively stated as f_k is arithmetically exceptional if and only if the division polynomial ψ_k has no rational root. This is because, for each integer $k \geq 1$, the x-coordinates of the k-torsion points come from the roots of the k-th division polynomial ψ_k.

As a final remark, we emphasize two situations that we observed when using the function `permdens`:

The first observation is that when we increase the variable k, the average permutation density also increases proportionally. For instance, while the average permutation density for the second Lattès map f_2 is 0.35, the average value that we see for the seventh Lattès map f_7 is 0.65.

The second interesting point to note is that except for the Lattès maps f_2 and f_3, there is no third type of the outputs in the function `permdens`. This implies that when $k \neq 2, 3$, then in our range, the x-coordinates of the k-torsion points of the elliptic curves are not rational. Again this is equivalent to saying that if $k \neq 2, 3$, then the k-th division polynomial ψ_k has no rational root.

REFERENCES

[1] Cox, D.A., 2022. *Primes of the Form $x^2 + ny^2$: Fermat, Class Field Theory, and Complex Multiplication. with Solutions* (Vol. 387). American Mathematical Soc..

[2] Guralnick, R.M., Müller, P. and Saxl, J., 2003. *The rational function analogue of a question of Schur and exceptionality of permutation representations* (Vol. 773). American Mathematical Soc..

[3] Küçüksakallı, Ö., 2014. Value sets of Lattes maps over finite fields. *Journal of Number Theory, 143,* pp.262-278.

[4] Küçüksakallı, Ö., 2015. Value sets of bivariate Chebyshev maps over finite fields. *Finite Fields and Their Applications, 36,* pp.189-202.

[5] Lidl, R. and Niederreiter, H., 1997. *Finite fields* (No. 20). Cambridge University Press.

[6] Mullen, G.L. and Panario, D., 2013. *Handbook of finite fields.* CRC Press.

[7] Rivlin, T.J., 2020. *Chebyshev polynomials.* Courier Dover Publications.

[8] Silverman, J.H., 1994. *Advanced topics in the arithmetic of elliptic curves* (Vol. 151). Springer Science & Business Media.

[9] Silverman, J.H., 2007. *The arithmetic of dynamical systems* (Vol. 241). Springer Science & Business Media.

[10] Silverman, J.H., 2009. *The arithmetic of elliptic curves* (Vol. 106, pp. xx+-513). New York: Springer.

[11] Stewart, I. and Tall, D., 2015. *Algebraic number theory and Fermat's last theorem.* CRC Press.

[12] Washington, L.C., 2008. *Elliptic curves: number theory and cryptography.* CRC Press