Universiteit Utrecht

Graphs of endomorphisms of elliptic curves over finite fields

An algebraic number-theoretic approach

Marlien Wennekes

Supervisor: Prof. Dr. Gunther Cornelissen
Second reader: Dr. Mikhail Hlushchanka

Master Thesis
Utrecht University
24-7-2022

Acknowledgements

First of all, I would like to thank my supervisor Gunther Cornelissen for always being able to motivate me with his enthusiasm.

Also many thanks to Mikhail Hlushchanka for the comments on my original draft, and for his questions and thoughts on the subject after the defence. I would like to thank Simone Ugolini for his willingness to answer my questions via email, which was of great help. Lastly I would like to thank Marc Houben and Gunther Corenlissen for the Mathematica code which I used for one of the graph examples.

Abstract

There is a growing body of research on dynamics of maps over finite sets; such a map $f : X \to X$ is described by a finite directed graph with vertex set X and edges from $x \in X$ to $f(x) \in X$. In general one finds that maps with algebraic properties give more symmetrical graphs than random graphs. In this context, we study endomorphisms of ordinary elliptic curves over finite fields with endomorphism ring equal to the maximal order of a quadratic number field. We translate the graph theory problem into an algebraic number-theoretic one. We use the theory of rational maps by x-coordinate projection of endomorphisms by Ugolini, and on dynamics of Dedekind domains by Qureshi and Reis, to derive precisely the cycles and trees that the graphs consist of. Next, we look at the curve $E : y^2 = x^3 - x$ over $\mathbb{F}_p$ to apply this theory. We run some computer experiments for endomorphisms $\alpha = a \pm bi$ with $1 \leq a, b \leq 9$ for the first 1000 prime numbers where E is ordinary. We look at two invariants: the number of points in cycles and the maximal cycle length. We study the proportion of points in cycles, looking at the density of primes where this proportion is maximal. Using congruence relations, we find a lower bound for endomorphisms which do not contain split primes. We also find more general results concerning the proportion of points experimentally. Next, we look at the proportion of cyclic points that are contained in the maximal cycle. We study experimentally how the proportion behaves as p increases in size; and find a big difference in the case where the norm of the endomorphism is even or odd. Further, we look into when the proportion is maximal. In the even case, the maximum proportion is 1; in the odd case it is < 1. For the odd case, we give a conjecture describing the value of the maximum proportion as a function of the endomorphism, which we base on the experimental data and on the case where the graph has only a minimal number of points.

Contents

Introduction

One can study maps of finite sets and their dynamics. Let X be a finite set and $f : X \to X$ a map. We consider the finite directed graph given by the vertex set X and edges from x to $f(x)$ for each $x \in X$. As the set is finite, it follows that each point is *preperiodic*, which means that there exist distinct $i, j > 0$ such that $f^i(x) = f^j(x)$ (if $j = 0$, we say x is *periodic*). In this thesis, we will call periodic points *cyclic* and consider cycles $\{x, f(x), f^2(x), \ldots, f^{k-1}(x)\}$ for periodic points x where k is the smallest positive integer such that $f^k(x) = x$. All non-cyclic points are parts of *trees* which are rooted in a cyclic point. For the finite set X we take the set of points on an elliptic curve over a finite field, and the map is an endomorphism of the curve.

In Figure 1 we see an example of such a graph. Take a look at each cyclic (i.e., periodic) point; they are all connected to an equal number of non-cyclic points, so all the trees are isomorphic. Maps that give graphs with such symmetrical properties have been studied, their symmetry often being explained by algebraic properties of the maps, for example in the case of Chebyshev polynomials [BCH20]. In our case the symmetry is also not suprising, as the point set of an elliptic curve forms a group with point addition.

The exact object of study is endomorphisms of ordinary elliptic curves over finite fields which have endomorphism ring equal to the maximal order of a quadratic number field. To be explicit, consider an endomorphism φ of an elliptic curve E over a finite field $\mathbb{F}_q$ with q a prime power. We consider a graph with vertices all the points on $E(\mathbb{F}_{q^n})$ and draw an arrow from a point P to Q if and only if $\varphi(P) = Q$. Because of previous results on rational maps from Ugolini in [Ugo18] and Qureshi & Reis in [QR19], we were quite confident that a nice description of the graphs would be possible. One interesting question is then how the endomorphisms act on growing sizes of points. What happens to the invariants of the graph? The behaviour of invariants of random graphs has been studied in [Bol01, p. 412-413], but our graphs are certainly not random. For example, an invariant to study is the proportion of points in cycles, i.e., periodic points. Take, e.g., $E : y^2 = x^3 + x$ to be an ordinary elliptic curve over $\mathbb{F}_p$; E has endomorphism ring $\mathbb{Z}[i]$, which is the maximal order. We can see already in Figure 2 that there is a difference in the proportion of points in cycles between $\alpha = 1 + i$ and $\alpha = 1 + 2i$. We can also see that as p grows, certain properties of the graphs do not change. Note that, (1) all trees in the graph are isomorphic; and (2), every point has a similar number of points in the pre-image: it is either 0, 1 or equal to the norm of α (2 or 5). These are things we will be able to explain once we have a general theory of the graphs.

Our first objective is then to describe the cycles and trees of the graphs. Later, we look at a specific elliptic curve and study them in terms of the theory. In Chapter 1, we will, as Ugolini does, use an important theorem of Lenstra to turn the graph theory problem into an algebraic number-theoretic problem. Because of this theorem it is important that we assume that the endomorphism ring is equal to the maximal order of the number field. This brings us to endomorphism rings modulo p in Chapter 2, where we will see that reducing the curve modulo p does not change the endomorphism ring in the cases we are interested in (where the curve has good reduction is ordinary at p, and the endomorphim ring is equal to the maximal order). This means we can vary p as we please and not worry about the endomorphism ring changing. It also implies that lots of curves could be studied in a similar way to how we studied the specific curve.

In Chapter 3 we completely describe the graphs of the endomorphisms. In the article [Ugo18] Ugolini discusses rational maps given by the projection onto the x-coordinate of maps of endomorphisms. This is

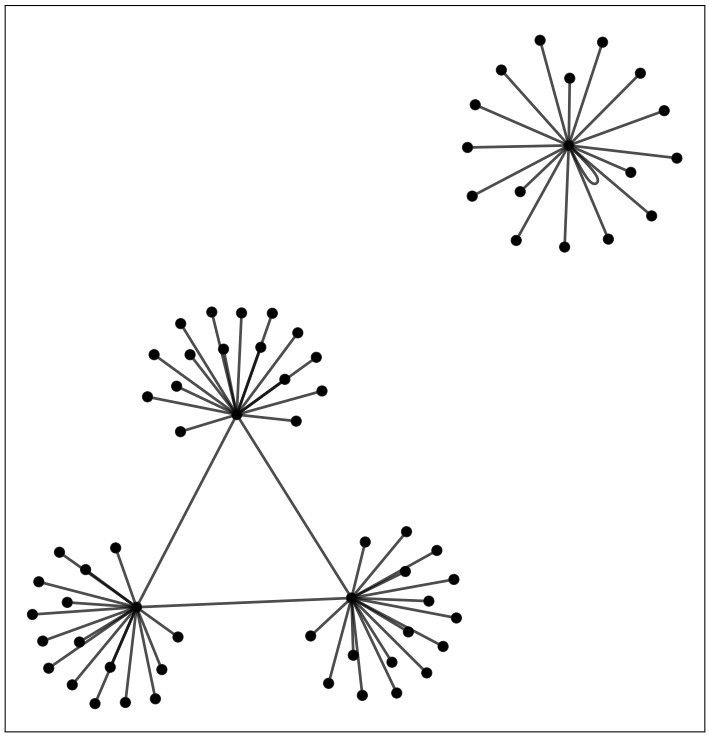


Figure 1: Let $E : y^2 = x^3 + 56x + 34$ be an elliptic curve over $\mathbb{F}_{83}$. This curve has endomorphism ring $R = \mathbb{Z}[\omega]$ for $\omega = \frac{1+\sqrt{-19}}{2}$. Above, we see the graph of the set $E(\mathbb{F}_{83})$ with map $\alpha = 3 + \omega \in R$. While this is a directed graph, we have omitted the arrows to make the image less cluttered. See Appendix C.2 for the Mathematica code and [Ugo18, Example 4.2] for the original example.

very similar to our goal here, so we follow this article closely, adapting the theorems and proofs to give a description of the cycles and trees of our graphs. There was one proof which, as it turned out after some communications with the author of [Ugo18], did not work in one (ramified) case. In this thesis a new proof is presented in Section 3.2, but we have included more details on the old proof in Appendix A. We have also adapted one of Ugolini's examples on a curve on $\mathbb{F}_{25^2}$.

In Chapter 4, we will apply our previous theory. We focus on an example of an elliptic curve, $E : y^2 = x^3 - x$ over $\mathbb{Q}$ to make things more concrete. We call a prime number 'ordinary', when the curve E has good reduction at p and the resulting curve mod p is ordinary. We will prove some results and also show results of a computer experiment.

The first invariant studied is the proportion of points in cycles

$$C = \frac{\#\text{ points in cycles}}{\#\text{ total points}}.$$

In particular we are looking for when this C is maximal, so when a lot of the points are in cycles. We try to find the density of primes where this proportion is maximal by looking at congruence relations. In this way, we can derive the statement 'for $\alpha = 1 + i$, the density of points that have the maximal $C = 1/8$ is $1/2$'. In general, we can give a certain lower bound of the lower density (infimum limit) of primes when we consider that the endomorphism α consists only of prime ideals which lie above inert and ramified primes (only 2). Then we have for $N(\alpha) = 2^k \cdot q_1^{r_1} q_2^{r_2} \cdots q_n^{r_n}$ with q_i inert, that the lower density of ordinary primes where C is maximal is at least

$$\frac{\prod_{i=1}^{n}(q_i - 2)}{\prod_{i=1}^{n}(q_i - 1)} \quad \text{or} \quad \frac{\prod_{i=1}^{n}(q_i - 2)}{2 \cdot \prod_{i=1}^{n}(q_i - 1)},$$

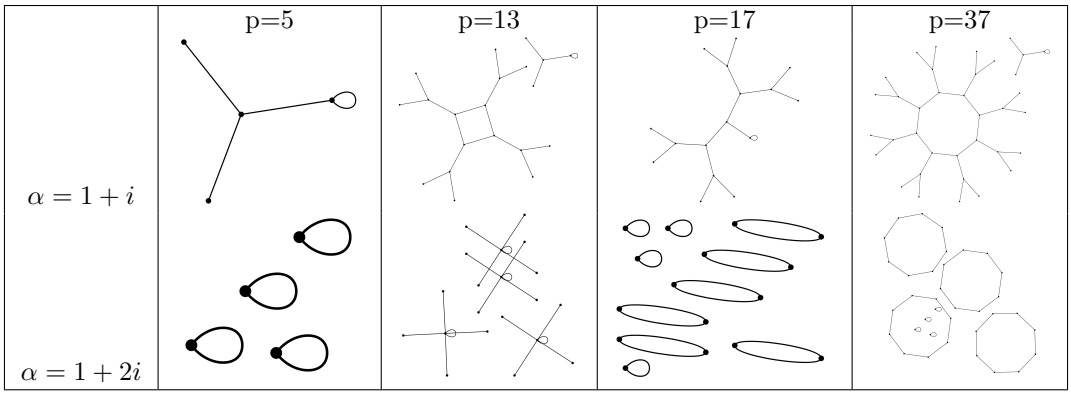


Figure 2: Let $E : y^2 = x^3 + x$ over $\mathbb{F}_p$. For the endomorphisms $\alpha = 1 + i$ and $\alpha = 1 + 2i$ we see the graphs of α acting on $E(\mathbb{F}_p)$ for $p = 5$, 13, 17 and 37. Note that (1) the trees have a symmetry to them; and (2) $\alpha = 1 + 2i$ has more cyclic points. See Appendix C.1 for the Sagemath code.

depending on whether $k = 0$ or not. Unfortunately, we cannot use the proof in the split case. We did make some experimental observations to see what happens in general. In fact we found that the fractions are a very good approximation of the density when α is not divisible by some rational prime number $p \neq 2$, see Section 4.2.2. However, for this we do not have a proof.

Next, we want to know how the cycles are distributed and to do this, we study the maximal cycle length. To study how the maximal cycle length changes as the number of points grows, we turned to

$$K = \frac{\text{maximal cycle length}}{\#\text{ number of points in cycles}}.$$

One thing that we observe is that the plots look very different for $N(\alpha)$ even or odd. In the even case, K is often much larger than in the odd case. We looked at when $K = 1$, which is the case with only one cycle. We noted that, as expected, when p grows we see less of $K = 1$. In general, there seems to be an increase for smaller cycles as p grows. Further, in the odd case we can say something about the maximal value of K when the number of points in cycles equals 8. Then we know that for $\alpha = a + bi$ and even a, $K = 1/2$, while if a is odd, we have $1/4$ when $a + b \equiv 3 \bmod 4$ and $1/8$ when $a + b \equiv 1 \bmod 4$. In all of the experimental cases, the maximal of K in the 495 ordinary prime numbers is always equal to the case with $p = 5$ (and thus also to the cases with exactly 8 points in cycles). However, we cannot prove this always holds.

Prerequisites

We assume the reader to be familiar with the basics of graph theory, elliptic curves and algebraic number theory.

Chapter 1

Elliptic curves over finite fields as modules of the endomorphism ring

Let E be an ordinary elliptic curve defined over a finite field $\mathbb{F}_q$. Let $R \coloneqq \mathrm{End}_{\mathbb{F}_q}(E)$ be the endomorphism ring of E over $\mathbb{F}_q$. The set of points $E(\mathbb{F}_{q^n})$ forms an abelian group on which the endomorphisms in R act by evaluation, making it into an R-module. In this chapter we will find an alternative description of this R-module.

As E is ordinary, R is an order of an imaginary quadratic number field. We consider the Frobenius endomorphism $\pi_q : (x, y) \mapsto (x^q, y^q)$.

With above notation, we can get from Theorem 1(a) in [Len96] that

Theorem 1.0.1. *There is an isomorphism of R-modules $E(\mathbb{F}_{q^n}) \cong R/(\pi_q^n - 1)$.*

In this chapter we will give an exposition of the proof of the above theorem, following closely Proposition 2.1 in [Len96].

Let $E[s] \coloneqq \{P \in E(\overline{\mathbb{F}_q}) | sP = \mathcal{O}\}$. The proof will consist of showing that for separable $s \in R$ there is an R-module isomorphism $E[s] \cong R/(s)$. Note that this result concerns ordinary elliptic curves and is not guaranteed in the supersingular case. Note that $\pi_q^n - 1$ is separable by [Sil09, p. 79, Corollary 5.5]. Now for any $P \in E(\overline{\mathbb{F}_q})$,

$$(\pi_q^n - 1)P = \mathcal{O} \iff P \in E(\mathbb{F}_{q^n}),$$

so $E[\pi_q^n - 1] \cong E(\mathbb{F}_{q^n})$. Then Theorem 1.0.1 follows by setting $s = \pi_q^n - 1$ in the following theorem.

Theorem 1.0.2. *For every separable $s \in R$, there is an isomorphism of R-modules $E[s] \cong R/(s)$.*

The remainder of this chapter is dedicated to proving Theorem 1.0.2. In the proof we will use two lemmas, Lemma 1.0.2 and 1.0.3. We will also need the following fact from [Wit01, p. 336, Corollary 2.2], for which we include a proof based on [Wit01, Lemma 2.1]:

Lemma 1.0.1. *Every endomorphism of E is defined over $\mathbb{F}_q$, so $R = \mathrm{End}(E)$.*

Proof. Let $\varphi \in R$, so $\varphi(x, y) = (\varphi_1(x, y), \varphi_2(x, y))$ with $\varphi_1(x, y), \varphi_2(x, y)$ rational maps with coefficients in $\mathbb{F}_q$. Then $(\varphi_1(x^q, y^q), \varphi_2(x^q, y^q)) = (\varphi_1(x, y)^q, \varphi_2(x, y)^q)$, as we are working in characteristic p and also $a^q = a$ for $a \in \mathbb{F}_q$. Now if $\psi \in \mathrm{End}(E)$ with coefficients not in $\mathbb{F}_q$, then there is a coefficient of ψ, say a_i with $a_i^q \neq a_i$. So the above does not hold in that case. Therefore $R = \{\psi \in \mathrm{End}(E) | \psi\pi_q = \pi_q\psi\}$. Now, as E is ordinary, $\mathrm{End}(E)$ is commutative, so in fact $R = \mathrm{End}(E)$. □

Lemma 1.0.2. *Let A be a finite commutative ring. Then the following two statements are equivalent:*
(i) each faithful A-module M contains a submodule that is free of rank 1 over A;
(ii) the number of maximal ideals of A is equal to the number of minimal ideals of A.

Proof. Assume (i). Consider the finite commutative ring A as an abelian group. By the classification theorem on finitely generated abelian groups, we have $A \cong C_{q_1} \oplus \cdots \oplus C_{q_t}$ where C_{q_i} is a cyclic group of order a prime power q_i. Let $M = \mathrm{Hom}(A, \mathbb{Q}/\mathbb{Z})$, the set of group homomorphisms from A to $\mathbb{Q}/\mathbb{Z}$. Let $f \in M$ and $a \in A$.

Let $(a_i)_i$ denote the image of a in $C_{q_1} \oplus \cdots \oplus C_{q_t}$ and f_i the restriction of f to C_{q_i}. Each C_{q_i} is cyclic so because f_i is an homomorphism, f_i is completely determined by $f(g_i)$ for a chosen generator g_i. There are $|C_{q_i}| = q_i$ choices for f_i to be a homomorphism in $\mathrm{Hom}(C_{q_i}, \mathbb{Q}/\mathbb{Z})$, namely $f_i(g_i) = 0$, $f_i(g_i) = 1/q_i$, $f_i(g_i) = 2/q_i$, ..., or $f_i(g_i) = (q_i - 1)/q_i$.

Now M is an A-module in the following way. Define the action of a_i on f_i for $a_i \in C_{q_i}$ as $a_i \circ f_i : x \mapsto f_i(a_i x)$. The action of $a = (a_i)_i$ on $f = (f_i)_i$ is defined in the obvious way, $a \circ f : x = (x_i)_i \mapsto (f_i(a_i x_i))_i$. Then M is an A-module because of the A-module structure on A (as a ring) and because each f_i is a homomorphism of abelian groups. We also want that M is faithful. If $aM = 0$, then it follows that for all $f \in M$ and $x \in A$, $f(ax) = 0$. With $x = 1$ we get $f(a) = 0$. So for each i, we have $f_i(a_i) = 0$. Take f_i so that $f_i(g_i) = 1/q_i$. Let $a_i = k \cdot g_i$, so we have $f_i(a_i) = k/q_i$. Then $f_i(a_i) = 0$ only if $k = 0$, so $a_i = 0$ for any i and thus $a = 0$.

We will also use that M is dual to A. To see this, consider a ideals I, J of A with $I \subset J$. Now the submodule $\mathrm{Hom}(I, \mathbb{Q}/\mathbb{Z})$ of M consists of homomorphisms $f \circ \iota$ where $f \in \mathrm{Hom}(A, \mathbb{Q}/\mathbb{Z})$ and $\iota : I \hookrightarrow A$ is the inclusion. Consider the image of I in $C_{q_1} \oplus \cdots \oplus C_{q_t}$, so that $I = (I_1, I_2, \ldots, I_t)$, and each I_i is generated by some element $k_i \cdot g_i$. Then $f_i(k_i \cdot g_i) = k_i \cdot f_i(g_i)$. Also $J = (J_1, J_2, \ldots, J_t)$, and J_i is generated by $l_i \cdot g_i$. There is an inclusion $I_i \subset J_i$, so k_i is a multiple of l_i for each i. From this it follows that $\mathrm{Hom}(J, \mathbb{Q}/\mathbb{Z}) \subset \mathrm{Hom}(I, \mathbb{Q}/\mathbb{Z})$.

We note that $|M| = \prod_i q_i = |A|$. Since by assumption, each faithful A-module contains a submodule that is free of rank 1 over A, it follows that $A \cong M$, so the number of minimal ideals of A is equal to the number of minimal submodules of M. Now by duality, it follows that the number of maximal ideals of A is equal to the number of minimal ideals of A.

Assume (ii). Let M be a faithful A-module. As A is a finite commutative ring, it is Artinian, so $A = \prod_m A_m$ with the product over the maximal ideals and A_m the localisation of A at the maximal ideal m [AM69, p. 90, Theorem 8.7]. Then $M = \prod_m M_m$ and each M_m is a faithful A_m-module. Of course, each A_m has a unique maximal ideal m. Because A_m is finite, it also has at least one minimal ideal. By the assumption, this implies each A_m has a unique minimal ideal. Let $r_m \neq 0$ be an element in the unique minimal ideal of A_m. Since M_m is faithful, there exists an $x_m \in M_m$ so that $r_m x_m \neq 0$. So $r_m \notin \mathrm{Ann}(x)$, and thus $\mathrm{Ann}(x_m)$ is an ideal in A_m which does not contain the unique minimal ideal of A_m, so by finiteness of A_m, $\mathrm{Ann}(x_m) = 0$. Then multiplication by x gives an injective map, so the submodules $x_m A_m$ and A_m of M_m are isomorphic. Now $\bigoplus_m x_m A_m$ is a submodule of M with $\bigoplus_m x_m A_m \cong A$, which completes the proof. □

Lemma 1.0.3. *Let $s \in R, s \neq 0$. Let $\hat{s}$ denote the dual endomorphism of s. Then $R/(s)$ is a finite ring of cardinality $s\hat{s}$, and the number of maximal ideals of $R/(s)$ is equal to the number of minimal ideals of $R/(s)$.*

Proof. First, note that $|R/(s)| = N(s) = s\hat{s}$. Let $A = R/(s)$ and let p be a prime number dividing $|A|$. We consider the element $p \in A$ of order $|A/p|$. There are partitions

$$\{m \subset A : m \text{ maximal ideal}\} = \bigcup_{p||A|} \{m \subset A : m \text{ maximal ideal and } p \in m\}$$

and

$$\{n \subset A : n \text{ minimal ideal}\} = \bigcup_{p||A|} \{n \subset A : n \text{ minimal ideal and } pn = 0\}.$$

The first follows since:
1) Let $p \neq p'$ be prime numbers dividing $|A|$, then $pA + p'A = A$. Therefore the sets are distinct.
2) If if $p \notin m$ for all p dividing $|A|$, then m is not maximal. So the sets also cover the maximal ideals.
And the second:
1) If $pn = 0$ and $p'n = 0$, then $pn + p'n = n = 0$, which implies distinct sets.
2) If n is a minimal ideal, n has prime order dividing $|A|$ so that n contains no subgroups. Now say n has order p, then $pn = 0$, so all minimal ideals are covered.

Let $A_p = \{a \in A : pa = 0\}$. A_p is a subset with exactly $|pA|$ cosets, so $|A| = |A_p| \cdot |pA|$. Since A is finite, $|A_p| = |A|/|pA| = |A/pA|$. Note that as E is ordinary, $[R : \mathbb{Z}] = 2$, so $|R/Rp| = p^2$. From the fact that there is a surjective map $R/Rp \to A/Ap$, it follows that $|A/Ap| = p$ or p^2.

First assume $|A_p| = |A/Ap| = p$. Since p is prime, and the order of a subgroup divides the order of the group, there is only one maximal ideal $m \subset A$ so that $Ap \subset m$, namely $m = Ap$. Similarly, there is only one minimal ideal n with $pn = 0$, namely $n = A_p$ (as A_p cannot contain subgroups).

Now let $|A_p| = |A/Ap| = p^2$. Then $R/Rp \cong A/Ap$, so we have that $s = rp$ for some $r \in R$. Then there is the following isomorphism of R-modules

$$A_p = \left(R \cap Rsp^{-1}\right)/Rs = Rr/Rrp \cong R/Rp \cong A/Ap.$$

Therefore, minimal ideals $n \subset A_p$ map to minimal ideals in A/Ap. Now it remains to show that in A/Aq, the number of minimal ideals equals the number of maximal ideals. This is clear, because if A/Ap has non-trivial ideals, then these have exactly p elements and are both maximal and minimal. □

Proof of Theorem 1.0.2. Let $M = E[s]$ and $A = R/(s)$. We define the action of the equivalence class $[a] \in A$ on a point $P \in M$ as $\varphi(P)$ for a representative $\varphi \in [a]$. We need to show that this is well-defined. If we take φ, ψ in the same equivalence class, we can write $\varphi = \psi + \kappa \circ s$ for some endomorphism κ. Then $\varphi(P) = (\psi + \kappa \circ s)(P) = \psi(P) + \kappa \circ s(P) = \psi(P)$ since $P \in M = E[s]$. Note that this makes M into an A-module. Next we claim that M is faithful. Let $0 \neq r \in R$ and $rM = 0$. We must show that $r \in (s)$. Note that s is separable and $\ker s = M$, so $\ker s \subset \ker r$. It follows from [Sil09, p. 73, Chapter III Corollary 4.11] that $r = t \cdot s$ for some $t \in \mathrm{End}(E)$. By Lemma 1.0.1, $R = \mathrm{End}(E)$. So $r = ts \in (s)$. This proves that M is faithful.

By Lemma 1.0.3, A is a finite ring and the number of maximal ideals of A is equal to the number of minimal ideals of A. Now as R is an order in an imaginary quadratic number field, A is also commutative. So by Lemma 1.0.2, it follows that each faithful A-module contains a submodule that is free of rank 1 over A. So M has a submodule that is free of rank 1 over A. Now $|\ker s| = \deg s$ by in [Sil09, p. 72, Chapter III Theorem 4.10c], so $|M| = \deg s$. Furthermore, $s\hat{s} = \deg s$ by [Sil09, p. 83, Chapter III Theorem 6.2a], so by Lemma 1.0.3 $|M| = |A|$. So M must be free of rank 1 over A. □

Chapter 2

Variation of the endomorphism ring modulo p

In this chapter, E is an elliptic curve over the rational numbers with complex multiplication. If E has good reduction at a prime p, we denote by $\tilde{E}_p$ the reduction of E at p. Further, we assume that the endomorphism ring $R \coloneqq \mathrm{End}(E)$ is the maximal order in the imaginary quadratic field $K \coloneqq \mathbb{Q}(\sqrt{-d})$. In this chapter we will see that whenever the reduction at a prime gives us a 'nice' elliptic curve, for any such prime we always get the same endomorphism ring. This is captured in the following theorem.

Theorem 2.0.1. *Let E have good reduction at the primes p and p' with $\tilde{E}_p, \tilde{E}_{p'}$ both ordinary. Furthermore, let $\mathrm{End}(E)$ be the maximal order of an imaginary quadratic field. Then in fact $\mathrm{End}(\tilde{E}_p) = \mathrm{End}(\tilde{E}_{p'})$.*

We will prove this in two parts.

The following theorem and proof is adapted from [Sil94, Proposition 4.4, p. 124].

Theorem 2.0.2. *Say E has good reduction at the prime p and $\tilde{E}_p$ is ordinary. The natural reduction map*

$$\mathrm{End}(E) \hookrightarrow \mathrm{End}(\tilde{E}_p)$$

is injective. Further, if $\mathrm{End}(E)$ is the maximal order of an imaginary quadratic field, then $\mathrm{End}(E) = \mathrm{End}(\tilde{E}_p)$.

Proof. Let m be an integer coprime to p. Let $T \in E[m]$ and $\varphi \in \mathrm{End}(E)$ with $\tilde{\varphi} = [0]$. We want to show that $\varphi = [0]$. Now

$$\widetilde{\varphi(T)} = \tilde{\varphi}(\tilde{T}) = \mathcal{O}$$

and we will first show that this reduction is injective so that $\varphi(T) = \mathcal{O}$. Note that

$$m\varphi(T) = \varphi(mT) = \varphi(\mathcal{O}) = \mathcal{O},$$

so $\varphi(T) \in E[m]$. Also, $E[m] = E(\overline{\mathbb{Q}})[m] \subset E(\overline{\mathbb{Q}}_p)[m]$, so it is enough to show that the reduction on $E(\overline{\mathbb{Q}}_p)[m]$ is injective. Define the algebraic extension L of $\mathbb{Q}$ by adjoining the roots of the polynomial equations stemming from $mP = P$ to $\mathbb{Q}$, so that $E(\overline{\mathbb{Q}}_p)[m] = E(L)[m]$. By [Sil09, Theorem VII.3.1b, p. 192], the reduction modulo p map $E(L_p)[m] \hookrightarrow \widetilde{E(L_p)}$ is injective for m coprime to p. As $E(L) \subset E(L_p)$, in particular the reduction $E(\overline{\mathbb{Q}_p})[m] \to \widetilde{E(\overline{\mathbb{Q}_p})}$ is injective. Therefore $\varphi(T) = \mathcal{O}$ so it follows that $E[m] \subset \ker(\varphi)$.

As $\#E[m] = \deg[m] = m^2$ for arbitrary m, it follows that that $\ker(\varphi)$ does not have finite kernel so $\varphi = [0]$.

Now consider the case where $\mathrm{End}(E)$ is a maximal order in $\mathbb{Q}(\sqrt{-d})$ for some positive integer d. We will show that $\mathrm{End}(\tilde{E}_p)$ is also an order in $\mathbb{Q}(\sqrt{-d})$. Then because the maximal order cannot inject into something smaller, it follows that $\mathrm{End}(E) = \mathrm{End}(\tilde{E}_p)$.

Note that the reduction map sends any multiplication map $[m]$ to itself. Consider a non-multiplication map α as an element of the maximal order of an imaginary quadratic field K. It is the root of some quadratic equation $x^2 + rx + s$ where r, s are integers (multiplication maps). This root depends on the discriminant $D = r^2 - 4s$, and in fact $K = \mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{D})$. Then the natural reduction map (a homomorphism) sends α to a root of $x^2 + rx + s$ and therefore $\mathrm{End}(\tilde{E}_p)$ is an order in $\mathbb{Q}(\sqrt{D})$. □

Proof of 2.0.1. Direct consequence of Theorem 2.0.2, namely we get $\mathrm{End}(\tilde{E}_p) = \mathrm{End}(E) = \mathrm{End}(\tilde{E}_{p'})$. □

Example 2.0.1. We have assumed here that we are considering elliptic curves E with complex multiplication. Indeed Theorem 2.0.2 does not hold otherwise. Consider the elliptic curve

$$E : y^2 = x^3 + 56x + 34$$

over $\mathbb{Q}$. This curve has j-invariant $j(E) = 303464448/183419$ and discriminant $\Delta(E) = -11738816$. As the j-invariant is not an integer, E does not have complex multiplication [1]. As $\Delta(E) \not\equiv 0 \bmod 13$ and 31, E has good reduction at $p = 13$ and $p = 31$. Also, $\tilde{E}_{13}$ and $\tilde{E}_{31}$ are not supersingular, so they are orders in imaginary quadratic fields. We now want to first find those imaginary quadratic fields K corresponding to $\mathrm{End}(\tilde{E}_p)$ with $p = 13$ and $p = 31$. Here we apply Theorem 2.4 from [Wit01] (this will also be described in Section 3.1): $K = \mathbb{Q}(\sqrt{-d})$ with

$$d = 4p - (p + 1 - |E(\mathbb{F}_p)|)^2.$$

It follows that $\tilde{E}_{13}$ is an order in $\mathbb{Q}(\sqrt{-1})$ and $\tilde{E}_{31}$ is an order in $\mathbb{Q}(\sqrt{-43})$. So the orders are certainly not equal in this case. ■

Now for an elliptic curve E with complex multiplication over $\mathbb{Q}$, theorem 2.0.1 gives conditions for when two primes p, p' give curves $\tilde{E}_p, \tilde{E}_{p'}$ with the same endomorphism rings. One thing to check is that there is good reduction at p and p'. We further need that $\tilde{E}_p, \tilde{E}_{p'}$ are ordinary. We can check this with Deuring's criterion [Sil94, p. 184, Exercise 2.30]:

Theorem 2.0.3 (Deuring's Criterion)**.** *Let E be an elliptic curve over $\mathbb{Q}$ with complex multiplication which has good reduction at the prime p. Then $\tilde{E}_p$ is ordinary if and only if p splits in K.*

Remember that we have the isomorphism

$$E(\mathbb{F}_{q^n}) \cong R/R(\pi_q^n - 1).$$

Theorem 2.0.1 implies that under reduction at different primes, R stays constant. Then the right-hand side only depends on π_q. This is useful when we want to compare the graphs of elliptic curve endomorphisms modulo different primes.

[1] See [Sil09, p. 427, Example 11.3.1]: For E/Q an elliptic curve with complex multiplication, and $\mathrm{End}(E)$ the full ring of integers R, we have that the class number of the imaginary quadratic field equals 1, and it follows that there are only 9 possible j-invariants, which can be computed and turn out to be integers (for example, one can find them in Sagemath).

Chapter 3

Dynamics of endomorphisms of elliptic curves over a finite field

3.1 Introduction

Let us return to considering an ordinary elliptic curve E over a finite field $\mathbb{F}_q$. Consider further the endomorphism

$$\alpha(x, y) \coloneqq (\alpha_1(x), y\alpha_2(x))$$

where $\alpha_1(x)$, $\alpha_2(x)$ are rational functions in $\mathbb{F}_q(x)$. Since E is ordinary, $R = \text{end}(E)$ is isomorphic to an order in an imaginary quadratic number field $K = \mathbb{Q}(\sqrt{-d})$. We assume that $R = \mathcal{O}_K$, the ring of integers and maximal order of K.

Let π_q be the Frobenius endomorphism $(x, y) \to (x^q, y^q)$. We know there is an isomorphism

$$F : E(\mathbb{F}_{q^n}) \to R/(\pi_q^n - 1)$$

of R-modules.

Note that, as R is a Dedekind domain, we can consider the decomposition of the ideal $(\pi_q^n - 1)$ into prime ideals. However first we consider the so-called α-decomposition of $(\pi_q^n - 1)$,

$$(\pi_q^n - 1) = I_c \times I_t,$$

where $(\alpha) \not\subset \mathfrak{B}_c$ for any prime factor $\mathfrak{B}_c$ of I_c while $(\alpha) \subset \mathfrak{B}_t$ for any prime factor $\mathfrak{B}_t$ of I_t. Equivalently we can say $\gcd(I_c, (\alpha)) = 1$ and $(\alpha) \subset \text{rad}(I_t)$. By the Chinese Remainder Theorem there is an isomorphism

$$R/(\pi_q^n - 1) \cong R/I_c \times R/I_t.$$

We will see that I_c determines the cycles of the graph and I_t the trees attached to nodes in the cycles. For an ideal I, we will denote by $N(I)$ the absolute norm of I, so

$$N(I) \coloneqq |R/I|.$$

Note that because of Lenstra's theorem (Theorem 1.0.1) it then follows that

$$|E(\mathbb{F}_{q^n})| = N(I_t)N(I_c).$$

The following holds in analogy with Lemma 3.6 of [Ugo18]:

Theorem 3.1.1. *The point (x, y) is α-periodic if and only if $F(x, y) = (P, [0]) \in R/I_c \times R/I_t$ for some $P \in R/I_c$.*

Proof. First assume (x, y) is α-periodic. Let m be an integer so that $\alpha^m(x, y) = (x, y)$ and let further $F(x, y) = (P, Q) \in R/I_c \times R/I_t$. Now since F is an R-module homomorphism

$$F(\alpha^m(x, y)) = [\alpha]^m F(x, y) = ([\alpha]^m P, [\alpha]^m Q) = (P, Q),$$

so $[\alpha]^m Q = Q$ in R/I_t. By the definition of I_t, $(\alpha) \subset \mathfrak{B}_t$ for any prime factor $\mathfrak{B}_t$ of I_t, so there exists an integer l so that $[\alpha]^l Q = [0]$ in R/I_t. Pick k so that $km \geq l$, and it follows that $[a]^{km} Q = Q$ and $[a]^{km} Q = [0]$, so $Q = [0]$.

Now assume we have $F(x, y) = (P, [0]) \in R/I_c \times R/I_t$. Note that we can just consider the point P in R/I_c. Consider integers i, j such that $\alpha^i P = \alpha^j P$ in R/I_c for $i \neq j$ and $i > j$ (these exist of course because R/I_c is finite). Then $(\alpha^i - \alpha^j)P = 0$ and $\alpha^j(\alpha^{i-j} - 1)P = 0$ in R/I_c, so as the ideal α and I_c are coprime, we must have $(\alpha^{i-j} - 1)P = 0$ in R/I_c. So we get $\alpha^{i-j} P = P$ so P is periodic. □

Representing rational maps as elements of the number ring

To study the cycles of the graph, we will need the image of the rational maps π_q and α in the number ring. The representation of π_q is given by [Wit01] as follows. Note that

$$N(\pi_q - 1) = (\pi_q - 1)\overline{(\pi_q - 1)} = (\pi_q - 1)(\overline{\pi_q} - 1) = N(\pi_q) - \mathrm{Trace}(\pi_q) + 1$$

and

$$N(\pi_q - 1) = |R/(\pi_q - 1)| = |E(\mathbb{F}_q)|.$$

Now $N(\pi_q) = \pi_q \circ \overline{\pi_q} = \pi_q \circ \hat{\pi_q} = \deg q = q$, so π_q is a root of

$$(X - \pi_q)(X - \overline{\pi}_q) = X^2 - (q + 1 - |E(\mathbb{F}_q)|)X + q.$$

The discriminant of this polynomial is given by $\Delta \coloneqq (q + 1 - |E(\mathbb{F}_q)|)^2 - 4q$, which is always negative. Set $d \coloneqq -\Delta$ so that

$$\pi_q = \frac{q + 1 - |E(\mathbb{F}_q)| + \sqrt{-d}}{2}.$$

Note that we also get from this that R is an order in $\mathbb{Q}(\sqrt{-d})$.

To determine the α-decomposition of $(\pi_q^n - 1)$, we also need to know the image of α in R. Say $\alpha = a + b\sqrt{-d}$ for $a, b \in \mathbb{Z}$. If we know the degree of α, we can find an $\alpha = a + bi$ satisfying

$$\deg(\alpha) = \alpha \circ \hat{\alpha} = \alpha \circ \overline{\alpha} = (a + b\sqrt{-d})(a - b\sqrt{-d}) = a^2 + db^2.$$

3.2 Cycles

In this section I will give the theory necessary to describe the cycles in the graph and present the main result in a theorem. The proof and notation is inspired by [Ugo18], but the context and the proof presented here is different. In the appendix (see Appendix A) I go into an alternative proof following Ugolini, which uses the algebraic structure of the rings $R/\mathfrak{B}_i$ where $\mathfrak{B}_i$ is a prime ideal of $(\pi_q^n - 1)$. After some communications with the author of [Ugo18], we came to the conclusion that this proof does not hold in all cases. He did have ideas on how to fix the proof which were very helpful. In this section then I present the final proof, which is also similar I believe to the approach in [QR19]. The notation is kept the same as in the paper [Ugo18].

We want to study points on an elliptic curve that are in cycles, so periodic points. We have seen a point in a cycle corresponds to a point $P \in R/(\pi_p - 1) \cong R/(I_c \times I_t)$ where $P \equiv 0 \bmod I_t$. Therefore this set of points is isomorphic to R/I_c. Consider the prime factorisation

$$R/I_c \cong R/\mathfrak{B}_1^{e_1} \times \cdots R/\mathfrak{B}_n^{e_n}.$$

Now each point corresponds to some $h = (h_1, h_2, \ldots, h_n) \in H \coloneqq H_1 \times H_2 \times \cdots \times H_n$ where $H_i = \{0, 1, \ldots, e_i\}$. We can write $P = (P_1, P_2, \ldots, P_n)$ where $P_i = 0$ if $h_i = 0$ and else $P_i \in (\mathfrak{B}_i^{e_i - h_i}/\mathfrak{B}_i^{e_i}) \setminus (\mathfrak{B}_i^{e_i - h_i + 1}/\mathfrak{B}_i^{e_i})$. Here we have $\mathfrak{B}_i^0 = R$.

Let us define

$$(n_h)_i = \begin{cases} 1 & \text{if } h_i = 0, \\ N(\mathfrak{B}_i^{h_i}) - N(\mathfrak{B}_i^{h_i - 1}) & \text{otherwise} \end{cases}$$

and $n_h = \prod_{i=1}^n (n_h)_i$. Also

$$s_h = \min_{v \geq 1} \{v : \alpha^v - 1 \in \prod_{i=1}^n \mathfrak{B}_i^{h_i}\}.$$

Theorem 3.2.1. *For each $h \in H$, there are n_h points in cycles of length s_h.*

Proof. A point P in a cycle corresponds to an $h \in H$ as noted above. With this notation, it holds that if $h_i = 0$, there is only one corresponding point in $R/\mathfrak{B}_i^{e_i}$, namely $P_i = 0$. Now let $P_i \neq 0$, so $P_i \in (\mathfrak{B}_i^{e_i - h_i}/\mathfrak{B}_i^{e_i}) \setminus (\mathfrak{B}_i^{e_i - h_i + 1}/\mathfrak{B}_i^{e_i})$ for some $h_i \neq 0$. So there are

$$|(\mathfrak{B}_i^{e_i - h_i}/\mathfrak{B}_i^{e_i}) \setminus (\mathfrak{B}_i^{e_i - h_i + 1}/\mathfrak{B}_i^{e_i})| = |\mathfrak{B}_i^{e_i - h_i}/\mathfrak{B}_i^{e_i}| - |\mathfrak{B}_i^{e_i - h_i + 1}/\mathfrak{B}_i^{e_i}| = N(\mathfrak{B}_i)^{h_i} - N(\mathfrak{B}_i)^{h_i - 1}$$

such points P_i. This brings the total to n_h points P. Now it remains to show that these points are in cycles of length s_h. For our endomorphism α and the point P on the curve, we want to find the minimal v so that $\alpha^v P = P$. This is equivalent to $(\alpha^v - 1)P = 0$. We can translate this to R/I_c and note that here this means that $(\alpha^v - 1)P \equiv 0 \bmod \mathfrak{B}_i^{e_i}$ for each i. By how we defined the point P, we need that $\alpha^v - 1 \in \mathfrak{B}_i^{h_i}$ for each i, so $\alpha^v - 1 \in \prod_{i=1}^n \mathfrak{B}_i^{h_i}$. □

Note that the theorem does not say that there are *exactly* n_h points in cycles of length s_h. To determine the cycles of the graph, one should consider sets of points that correspond to an $h \in H$. These points are divided into

$$C_h \coloneqq n_h / s_h$$

cycles of length s_h. After examination of each $h \in H$, we can determine the quantity and length of cycles of the graph.

3.3 Trees

Now we turn to the quotient ring R/I_t to determine the trees attached to nodes in the cycles. The question is how many times we can multiply an element $(P, Q) \in R/I_c \times R/I_t$ with $[\alpha]$ before the R/I_t part disappears. Let the prime factorizations be given by

$$I_t = R/\mathfrak{D}_1^{e_1} \times \cdots R/\mathfrak{D}_n^{e_n}$$

$$(\alpha) = \prod_{i=1}^{l} \mathfrak{D}_i^{f_i} \cdot \mathcal{R}$$

where the $\mathfrak{D}_i$ are prime ideals, $\mathcal{R} \not\subset \mathfrak{D}_i$ for each i and $f_i > 0$ and $e_i > 0$. Then the depth of the tree is given by

$$d \coloneqq \max_{i\in[1,l]} \left\{ \left\lceil \frac{e_i}{f_i} \right\rceil \right\}.$$

Let $T(P)$ denote the tree rooted in the point P and $T_h(P)$ denote the nodes on level h of that tree for $h \in [0, d]$. The preimage $\mathrm{Pre}(\tilde{x}, \tilde{y})$ denotes the set of elements $(x, y) \in E$ so that $\alpha(x, y) = (\tilde{x}, \tilde{y})$.

The following is an adaptation of Theorem 3.12 in [Ugo18]. Considering points on an elliptic curve simplifies this theorem considerably. The proofs are also based on Ugolini. The proof of (1) I have left essentially the same as in [Ugo18]. The theorem also implies that trees attached to different periodic points have the same structure.

Theorem 3.3.1. *(1) Let (x, y) be a periodic point in $E(\mathbb{F}_{q^n})$. The tree $T(x, y)$ has depth d and, for any $h \in [1, d]$, we have*

$$|T_h(x, y)| = \prod_{i=1}^{l} N\left(\mathfrak{D}_i^{\min\{e_i, f_i h\}}\right) - \prod_{i=1}^{l} N\left(\mathfrak{D}_i^{\min\{e_i, f_i (h-1)\}}\right)$$

.

(2) Let $(x_h, y_h) \in T_h(x, y)$ for some $h \in [0, d-1]$, then $|\operatorname{Pre}(x_h, y_h)| = 0$ or

$$|\operatorname{Pre}(x_h, y_h)| = \prod_{i=1}^{l} N\left(\mathfrak{D}_i^{\min\{f_i, e_i\}}\right).$$

Proof. Let $(P, [0]) \in R/I_c \times R/I_t \cong R/(\pi_q^n - 1)$ be the point corresponding to the periodic point $(x, y) \in E(\mathbb{F}_{q^n})$.
(1) The depth of the tree $T(x, y)$ is equal to the smallest integer k for which $[\alpha]^k U = (-, [0])$ (the tree part I_t is zero) for any point U corresponding to a node in $T(x, y)$. Note that by the definition of d we have $df_i \geq \frac{e_i}{f_i} f_i = e_i$ for any $i \in [1, l]$. Therefore the depth of $T(x, y)$ is at most d. Consider the point $V \coloneqq \left([\alpha]^{-d} P, [1]\right)$, which exists because $(P, [0])$ is periodic. By the definition of d we have that $[\alpha]^u V \neq (-, [0])$ if u is smaller than d, while $[\alpha]^d V = (P, [0])$. Hence we conclude that $T(x, y)$ has depth d.

For convenience we will denote

$$m_i^s \coloneqq \min\{e_i, f_i s\}$$

for any $i \in [1, l]$ and any non-negative integer s. Now consider a point $V \coloneqq (P', Q)$ belonging to $T_h(x, y)$ for some $h \geq 1$. Then h is the smallest positive integer so that $[\alpha]^h V = (P, [0])$ holds. Then we get $P' = [\alpha]^{-h} P$ and

$$Q \in \left(\prod_{i=1}^{l} \mathfrak{D}_i^{e_i - m_i^h} / \mathfrak{D}_i^{e_i} \right) \setminus \left(\prod_{i=1}^{l} \mathfrak{D}_i^{e_i - m_i^{(h-1)}} / \mathfrak{D}_i^{e_i} \right).$$

Now note that there is a surjective homomorphism of groups $R \to \mathfrak{D}_i^{e_i - m_i^h} / \mathfrak{D}_i^{e_i}$ with kernel $\mathfrak{D}_i^{m_i^h}$. It follows with the fundamental homomorphism theorem that

$$\left| \prod_{i=1}^{l} \mathfrak{D}_i^{e_i - m_i^h} / \mathfrak{D}_i^{e_i} \right| = \prod_{i=1}^{l} N\left(\mathfrak{D}_i^{m_i^h}\right)$$

$$\left| \prod_{i=1}^{l} \mathfrak{D}_i^{e_i - m_i^{(h-1)}} / \mathfrak{D}_i^{e_i} \right| = \prod_{i=1}^{l} N\left(\mathfrak{D}_i^{m_i^{(h-1)}}\right)$$

which finishes the proof that $T_h(x, y)$ has exactly $\prod_{i=1}^{l} N\left(\mathfrak{D}_i^{m_i^h}\right) - \prod_{i=1}^{l} N\left(\mathfrak{D}_i^{m_i^{(h-1)}}\right)$ elements.

(2) Let $V_h := \left([\alpha]^{-h}P, Q\right)$ be a point in $R/(\pi_q^n - 1)$ corresponding to (x_h, y_h) in $E(\mathbb{F}_{q^n})$. Imagine an element in the preimage $(\tilde{P}, \tilde{Q}) \in [\alpha]^{-1}V_h$.

We know how the endomorphism α acts on the periodic part R/I_c: $\tilde{P} = [\alpha]^{-h-1}P$ is fixed. On R/I_t, we should consider how α acts on each $\mathfrak{D}_i^{e_i-m_i^{h+1}}/\mathfrak{D}_i^{e_i}$. If $e_i > f_i$, α sends to 0 exactly the elements in $\mathfrak{D}_i^{e_i-f_i}/\mathfrak{D}_i^{e_i}$. There are

$$|\mathfrak{D}_i^{e_i-f_i}/\mathfrak{D}_i^{e_i}| = |R/\mathfrak{D}_i^{f_i}| = N(\mathfrak{D}_i^{f_i})$$

many of those. Now if $e_i \leq f_i$, then all elements in $R/\mathfrak{D}_i^{e_i}$ get send to 0. So in total, there are such $\prod_{i=1}^{l} N\left(\mathfrak{D}_i^{\min\{f_i,e_i\}}\right)$ elements in R/I_t that α sends to 0.

Now suppose there is $\tilde{Q}_i \in (\mathfrak{D}_i^{e_i-m_i^{h+1}}/\mathfrak{D}_i^{e_i})\backslash(\mathfrak{D}_i^{e_i-m_i^{h}}/\mathfrak{D}_i^{e_i})$ so that $\alpha\tilde{Q}_i = Q_i$. For any $R_i \in \mathfrak{D}_i^{e_i-\min\{f_i,e_i\}}/\mathfrak{D}_i^{e_i}$ we have

$$\tilde{Q}_i + R_i \in (\mathfrak{D}_i^{e_i-m_i^{h+1}}/\mathfrak{D}_i^{e_i}) \setminus (\mathfrak{D}_i^{e_i-m_i^{h}}/\mathfrak{D}_i^{e_i})$$

and further $\alpha(\tilde{Q}_i + R_i) = \alpha\tilde{Q}_i = Q_i$.

It follows that there are $\prod_{i=1}^{l} N\left(\mathfrak{D}_i^{\min\{f_i,e_i\}}\right)$ elements in R/I_t with image Q under α. □

3.4 Example on $\mathbb{F}_{25^2}$

Let us consider an example with multiple cycles and extensive trees. This example is adapted from Example 4.3 in [Ugo18]. It is restated to give an endomorphism graph instead of a graph of a rational map. We will also mention how to find such maps using Sagemath.

The elliptic curve is given by

$$E : y^2 = x^3 + x + \gamma$$

over $\mathbb{F}_{25}$ where γ is a primitive element of $\mathbb{F}_{25}$. The curve has endomorphism ring $R \coloneqq \mathbb{Z}[\omega]$ with $\omega = \sqrt{-21}$ which is the maximal order in $K \coloneqq \mathbb{Q}(\sqrt{-21})$. Consider an endomorphism $\alpha \in R$ of degree 22, specifically let us take $\alpha = 1 + \omega$, so that indeed

$$N(\alpha) = \alpha \circ \tilde{\alpha} = 1^2 + 1^2 \cdot 21 = 22.$$

Now $\alpha = 1 + \omega$ also corresponds to some rational maps. We can find these in Sagemath by using

```
alpha = EllipticCurveIsogeny(E,E(4,z))
```

where $(4, z) = (4, \gamma)$ is the point in the kernel of the isogeny. Then to get an endomorphism $E \to E$ we use

```
isom=alpha.codomain().isomorphism_to(E);phi.set_post_isomorphism(isom);.
```

Having the maps in Sagemath was very useful for generating graph pictures and checking the theory.

We want to find the graph of the action of α on $E(\mathbb{F}_{25^2})$. Now

$$\pi_{25} = \frac{q + 1 - |E(\mathbb{F}_{25})| + \sqrt{(q + 1 - |E(\mathbb{F}_{25})|)^2 - 4 \cdot q}}{2}$$

with $q = 25$ and $|E(\mathbb{F}_{25})| = 22$, from which it follows that $\pi_{25} = 2 + \omega$.

First, we need to check how the ideals $(\pi_{25}^2 - 1) = (-4\omega + 18)$ and $(\alpha) = (\omega + 1)$ factor in R, which gives:

$$(\pi_{25}^2 - 1) = I_1 \cdot I_2 \cdot I_3^2 \cdot I_4,$$
$$(\alpha) = I_2 \cdot I_3,$$

for

$$I_1 \coloneqq (5, \omega + 3),$$
$$I_2 \coloneqq (11, \omega + 1),$$
$$I_3 \coloneqq (2, \omega + 1),$$
$$I_4 \coloneqq (3, \omega),$$

and they are not inert so $N(I_1) = 5, N(I_2) = 11, N(I_3) = 2$ and $N(I_4) = 3$.

To determine the cycles, consider

$$R/I_c \coloneqq R/I_1 \times R/I_4.$$

Now $(3) = (3, \omega)^2 = I_4^2$ and $(5) = (5, \omega + 3)(5, \omega + 2)$, thus 3 is ramified and 5 splits in K. Note that, in the notation of Section 3.2, we have $e_1 = 1$ and $e_2 = 1$. Consider

$$H_1 = [0, 1], \quad H_2 = [0, 1].$$

Then any point lies in a set corresponding to some $h \in H = H_1 \times H_2$, and we have $h = (h_1, h_2) = (0, 0), (1, 0), (0, 1)$ or $(1, 1)$. Let $h_1 \in H_1$. We have that

$$s_{h_1} = \begin{cases} 1 & \text{if } h_1 = 0 \\ 4 & \text{if } h_1 = 1 \end{cases}$$

because $\alpha^2 + 1 \in I_1$, so $i = 4$ is the smallest integer so that $\alpha^i - 1 \in I_1$. Moreover

$$n_{h_1} = \begin{cases} 1 & \text{if } h_1 = 0 \\ 5 - 1 = 4 & \text{if } h_1 = 1. \end{cases}$$

Let $h_2 \in H_2$. We have that

$$s_{h_2} = \begin{cases} 1 & \text{if } h_2 = 0 \\ 1 & \text{if } h_2 = 1 \end{cases}$$

because $\alpha - 1 \in I_4$. Moreover

$$n_{h_2} = \begin{cases} 1 & \text{if } h_2 = 0 \\ 3 - 1 = 2 & \text{if } h_2 = 1 \end{cases}$$

Hence we get

$$C_{(0,1)} = \frac{n_{(0,1)}}{s_{(0,1)}} = \frac{1 \cdot 2}{\operatorname{lcm}(1, 1)} = 2,$$
$$C_{(1,0)} = \frac{n_{(1,0)}}{s_{(1,0)}} = \frac{4 \cdot 1}{\operatorname{lcm}(4, 1)} = 1,$$
$$C_{(1,1)} = \frac{n_{(1,1)}}{s_{(1,1)}} = \frac{4 \cdot 2}{\operatorname{lcm}(4, 1)} = 2,$$

so this results in two cycles of length 1 and three cycles of length 4. Naturally, the only point corresponding to the set with $h = (0, 0)$ is the point $([0], [0]) \in R/I_c$, which has order 1, which corresponds to $\mathcal{O} \in E$ forming a cycle of length 1.

Let us now determine the structure of the trees attached to each periodic point, by considering

$$R/I_t := R/I_2 \times R/I_3^2.$$

Note that the trees have depth 2, as two is the highest exponent. Let P be a periodic point on E, so that

$$|T_1(P)| = N(I_2)N(I_3) - N(R) = 11 \cdot 2 - 1 = 21$$
$$|T_2(P)| = N(I_2)N(I_3^2) - N(I_2)N(I_3) = 11 \cdot 4 - 11 \cdot 2 = 22$$

and both for points $Q \in T_1(P)$ and $\in T_2(P)$ it holds that

$$\text{either } |\text{Pre}(Q)| = N(I_2)N(I_3) = 22$$
$$\text{or } |\text{Pre}(Q)| = 0$$

which determines the structure of the trees attached to the cycles. We have determined that there are six connected components. Below in Figure 3.1 is a picture of one of them, containing the point at infinity $\mathcal{O}$. After that we see the total graph in Figure 3.2.

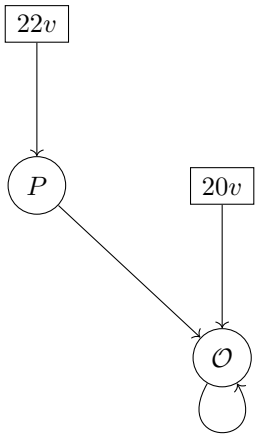


Figure 3.1: The rectangles reading 20v and 22v represent 20 vertices with arrows pointing to $\mathcal{O}$ and 22 vertices to the point P. Furthermore $P \in E$ represents the unique point on level 1 of the graph that has 22 points in the preimage.

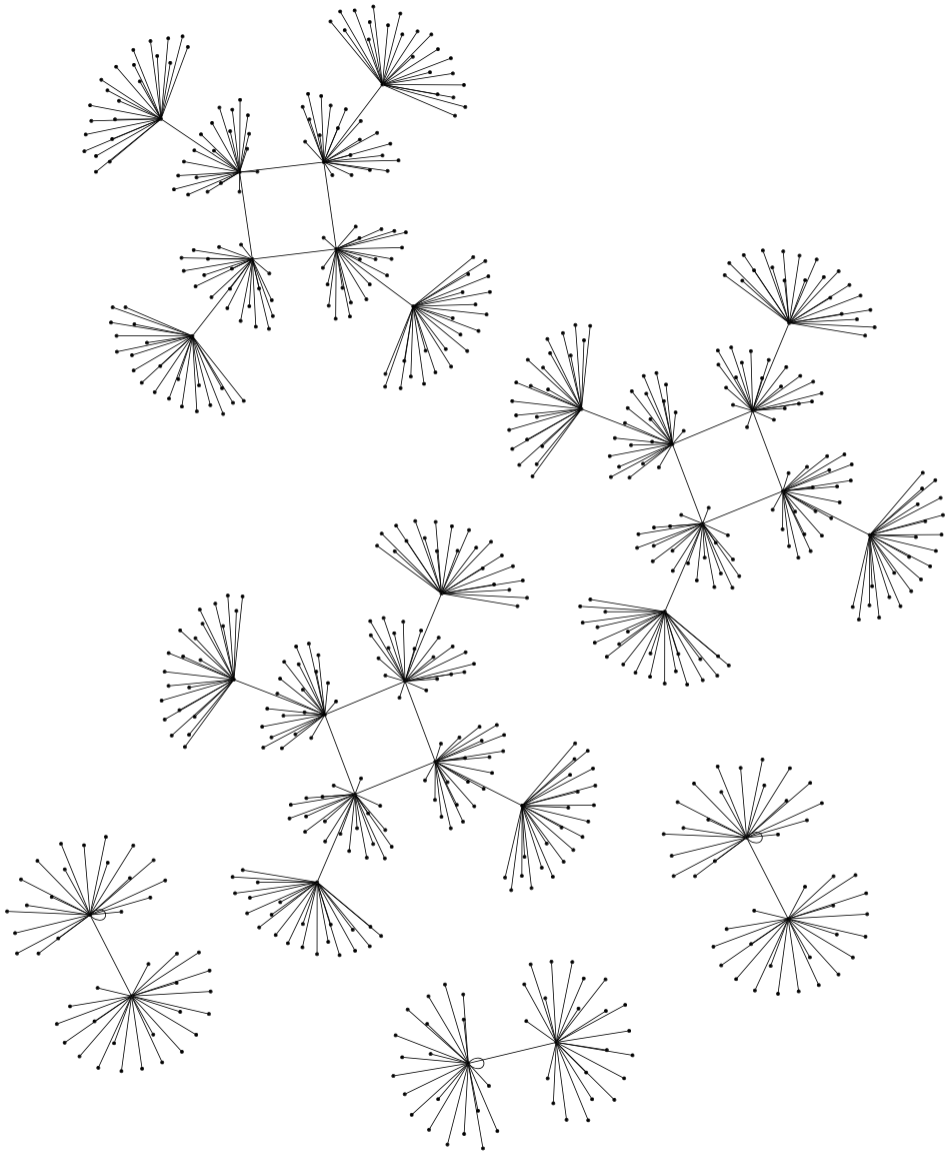


Figure 3.2: The total graph over $\mathbb{F}_{25^2}$. Note that there are three 4-cycles and three 1-cycles and all trees have identical structure to Figure 3.1. Figure is generated using Sagemath and Graphviz, see Appendix C.1.

Chapter 4

Variation of graphs with p: theory and experiments

4.1 Introduction

Let us now consider the elliptic curve

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

over the rationals. Note that it has complex multiplication $i : (x, y) \mapsto (-x, iy)$ and that the endomorphism ring is given by $R \coloneqq \mathbb{Z}[i]$. We consider a prime number p where E has good reduction and so that E over $\mathbb{F}_p$ is ordinary. We know that the endomorphism ring of E over $\mathbb{F}_p$ is also equal to $\mathbb{Z}[i]$ (this follows for example from Theorem 2.0.2 in Chapter 2). We want to study the action of some endomorphism α on the points $E(\mathbb{F}_p)$. This will yield a finite directed graph of which we want to study the cycles and the trees. We will denote this graph by $\mathcal{G}_{\alpha,p}$.

The curve E has discriminant $\Delta(E) = 64$ so it has good reduction everywhere except at $p = 2$. The reduction is ordinary if and only if p splits in $\mathbb{Q}(i)$ from Deuring's Criterion (Theorem 2.0.3), so if and only if p can be written as a sum of two squares or $p \equiv 1 \bmod 4$.

We will use that

$$|E(\mathbb{F}_p)| = N(\pi_p - 1)$$

where π_p denotes the p-Frobenius element in R because of Lenstra's Theorem 1.0.1. By previous theory (see Section 3.1) we know that we can write

$$\pi_p - 1 = I_c \times I_t$$

where I_c determines the cycle part of the graph and I_t determines the trees. We want to consider the prime ideals in the number ring $K = \mathbb{Q}(i)$ dividing $\pi_p - 1$ and check if these belong to I_c or I_t. Note that 2 is the only ramified prime, as 2 is the only prime number dividing the discriminant of the quadratic field $\Delta_K = -4$.

We can investigate a number of invariants of the graphs. For example the number of connected components, which is equal to the number of cycles. In this section we will look at two invariants; the proportion of points in cycles and the proportion of periodic points in the maximal cycle. For this part of my thesis, I wanted to look at such invariants and see for example what happens when varying p.

We generated the data for several endomorphisms and finite fields of hundreds of prime numbers. Going forward we will often say 'ordinary prime' for a prime number where E has ordinary reduction. The endomorphisms are $\alpha = a \pm bi$ for $1 \leq a, b \leq 9$, so 162 cases. Note that the graphs of $-a - bi$ and $a + bi$ look the

same, because $\alpha(-P) = -\alpha(P)$. We looked at the graphs while varying p over all ordinary prime numbers among the first 1000 ones, which is 495 prime numbers, up to 7901.

4.2 Proportion of points in cycles

We want to study

$$C_{\alpha,p} = \frac{\#\text{ periodic points of } \mathcal{G}_{\alpha,p}}{\#\text{ total points of } \mathcal{G}_{\alpha,p}}.$$

We can rewrite this as in the following theorem.

Theorem 4.2.1. *We have* $C_{\alpha,p} = \frac{1}{N(I_t)}$.

Proof. The statement follows because the number of total points is $|E(\mathbb{F}_p)| = N(I_c)N(I_t)$ and the number of periodic points $N(I_c)$, see Section 3.1 and in particular Theorem 3.1.1. □

Question 4.2.1. *For what density of ordinary primes is $C_{\alpha,p}$ maximal? Let p denote an ordinary prime number. What is*

$$\lim_{x\to\infty} \frac{\#\{p \mid p \leq x \wedge C_{\alpha,p} = \max_p\{C_{\alpha,p}\}\}}{\#\{p \mid p \leq x\}}?$$

Note that answering this question also means addressing whether or not the limit exists. What we will do in the next section, is find a lower bound for the lower density (infimum limit)

$$\liminf_{x\to\infty} \frac{\#\{p \mid p \leq x \wedge C_{\alpha,p} = \max_p\{C_{\alpha,p}\}\}}{\#\{p \mid p \leq x\}}.$$

4.2.1 Results from congruences

It is useful to know which primes divide $|E(\mathbb{F}_p)|$, as this gives a lot of information on primes dividing $N(I_t)$. Therefore, we can study the number of points on an elliptic curve modulo some prime. There have been some publications on this, for example modulo 8 and 24. We can extract a useful result from this, given in Theorem 4.2.2. To show how it follows we will need Lemma 4.2.1.

Lemma 4.2.1. *Let $p > 2$ be a prime number.*

- $p \equiv 1 \bmod 4$ *if and only if* -1 *is a quadratic residue* mod p.
- $p \equiv 1 \bmod 8$ *if and only if* -1 *is a quartic residue* mod p.

Proof.

- Let $x^2 \equiv -1 \bmod p$, so x has order 4 in the multiplicative group $\mathbb{F}_p^*$. Then by Lagrange's theorem, 4 divides $p-1$ so $p \equiv 1 \bmod 4$.

  For other way, assume $p = 1 + 4k$. By Wilson's theorem we have $(p-1)! \equiv -1 \bmod p$, which we can rearrange to get $1 \cdot (p-1) \cdots 4k(p-4k) \equiv -1 \bmod p$ and then

  $$-1 \cdot 1^{\cdot} - 1 \cdot 2^2 \cdots - 1 \cdot (4k)^2 \equiv (-1)^{4k}(4k)!^2 \equiv (4k)!^2 \equiv -1 \bmod p$$

  so -1 is a quadratic residue mod p.

- Let $x^4 \equiv -1 \bmod p$. Let g generate $\mathbb{F}_p^*$ and $g^y = x$. Note that also $g^{y+(p-1)/2} = -x$ is a solution to the quartic equation, so therefore we assume $0 < y < (p-1)/2$. Now $x^4 \equiv -1 \bmod p$ implies that also $4y \equiv (p-1)/2 \bmod p-1$ so $4y = (p-1)/2 + k(p-1)$. Since $0 < 4y < 2(p-1)$, we get $k = 0$ or $k = 1$. Then $y = (p-1)/8$ or $y = 3(p-1)/8$, and as y is an integer, it follows that $p \equiv 1 \bmod 8$.

  For the other implication, let 8 divide $p-1$. Let g generate $\mathbb{F}_p^*$. Now the equation $x^4 \equiv -1 \mod p$ with $g^y = x$ holds if and only if $4y \equiv (p-1)/2 \bmod p-1$. Because 8 divides $p-1$, we find that $y \equiv (p-1)/8 \bmod (p-1)/4$ and we can solve this to find y and thus x, so -1 is a quartic residue. □

Theorem 4.2.2. *Let $E : y^2 = x^3 - x$ be an ordinary elliptic curve over $\mathbb{F}_p$, then*

- *When $p \equiv 1 \bmod 8$, 16 divides $|E(\mathbb{F}_p)|$.*
- *When $p \equiv 5 \bmod 8$, 8 strictly divides $|E(\mathbb{F}_p)|$, which is to say that 8 divides $|E(\mathbb{F}_p)|$ but 16 does not.*

Proof. From [PKL03] and [İna+07, Theorem 2] we find the number of points on $E : y^2 = x^3 + cx$ over $\mathbb{F}_p$ modulo 8. We will need the following distinction: if p is a rational prime, then when $p \equiv 1 \bmod 8$,
$\begin{cases} \#E \equiv 0 \bmod 8 & \text{if } c \text{ is a quartic residue in } \mathbb{F}_p, \\ \#E \not\equiv 0 \bmod 8 & \text{else,} \end{cases}$
and when $p \equiv 5 \bmod 8$,
$\begin{cases} \#E \equiv 0 \bmod 8 & \text{if c is a quadratic residue but quartic non-residue in } \mathbb{F}_p, \\ \#E \not\equiv 0 \bmod 8 & \text{else.} \end{cases}$

For our purposes, we take $c = -1$. We know when -1 is a quartic or a quadratic residue from Lemma 4.2.1. It follows that -1 is a quartic residue if and only if $p \equiv 1 \bmod 8$, so we find that 8 always divides $|E(\mathbb{F}_p)|$ when $p \equiv 1 \bmod 4$ (so for ordinary curves). It further follows from [PKL03, p. 35-36] that 16 divides $|E(\mathbb{F}_p)|$ if and only if $p \equiv 1 \bmod 8$. □

Note that 2 is ramified in $\mathbb{Q}(i)$. So when $N(\alpha)$ is even, it follows from Theorem 4.2.2 that 8 divides $N(I_t)$ and further that 16 divides $N(I_t)$ when $p \equiv 1 \bmod 8$. Note that when a prime is split, such as 5, this means that we cannot automatically draw conclusions on $N(I_t)$ from observations of prime numbers dividing both $N(\alpha)$ and $|E(\mathbb{F}_p)|$. However, for inert primes just like ramified primes (which is only 2), it is as simple as that. Therefore it is useful to note the following.

Theorem 4.2.3. *Let q be a prime number, and say that the ideal (q) divides $\pi_p - 1$ in R. Then $p \equiv 1 \bmod q$.*

Proof. We have $\pi_p = 1 + kq$ in R and similar for the conjugate $\overline{\pi_p}$, so $p = \pi_p \overline{\pi_p} \equiv 1 \bmod q$. □

Let us consider the case where $N(\alpha)$ is divisible only by inert primes and by 2. We have:

Theorem 4.2.4. *Let q be an inert prime divisor of $N(\alpha)$. When q divides $|E(\mathbb{F}_p)|$, we get that $C \leq \frac{1}{q^2}$ and $p \equiv 1 \bmod q$.*

Proof. Assume q divides $|E(\mathbb{F}_p)| = N(\pi_p - 1)$. As q is inert, (q) occurs in the factorization of $\pi_p - 1$, so in fact $N(q) = q^2$ divides $|E(\mathbb{F}_p)|$. It also follows that q^2 divides $N(\alpha)$, so q^2 divides $N(I_t)$ and therefore $C \leq \frac{1}{q^2}$. It is also immediate from Theorem 4.2.3 that $p \equiv 1 \bmod q$. □

Example 4.2.1. Let us fix an endomorphism α. One can consider the question, what is the density within the ordinary primes of primes where the reduction of E has a maximal C. When $\alpha = 1 - i$, we see that $C = 1/8$ if and only if $p \equiv 5 \bmod 8$, so this density is $1/2$. ■

Example 4.2.2. Now take $\alpha = 3 - 3i$, which has $N(\alpha) = 3^2 + 3^2 = 2 \cdot 3^2$. Note that 3 is inert in $\mathbb{Z}[i]$ as we cannot write 3 as a sum of two squares. We want to consider when C is maximal, so when we have $C = \frac{1}{8}$. We know that this is true when $p \equiv 5 \bmod 8$ and $p \equiv 2 \bmod 3$ using Theorem 4.2.2 and Theorem 4.2.4. Therefore we need $p \equiv 5 \bmod 24$. We do not know exactly when $C = \frac{1}{8}$ if $p \equiv 1, 13, 17 \bmod 24$, but at least $1/4$ of the ordinary primes has the property that exactly $1/8$ of the points are periodic. ■

In general, we can say a lot when α is only divisible by 2 or inert primes.

Theorem 4.2.5. *Let α be an endomorphism so that $N(\alpha)$ is divisible only by the even or inert primes $q_1, q_2, \ldots, q_k$. If $N(\alpha)$ is even, the lower density of ordinary primes that have the maximal possible value $C_{\alpha,p} = 1/8$ is at least*

$$\frac{\prod_i (q_i - 2)}{2 \cdot \prod_i (q_i - 1)}.$$

On the other hand, if $N(\alpha)$ is odd, the lower density of these primes with $C_{\alpha,p} = 1$ is at least

$$\frac{\prod_i (q_i - 2)}{\prod_i (q_i - 1)}.$$

Proof. To maximize C, we should minimize $N(I_t)$. First assume $N(\alpha)$ is even and divisible by odd primes $q_1, q_2, \ldots, q_n$. So we want $p \equiv 5 \bmod 8$ and $p \not\equiv 1 \bmod q_i$ for $1 \leq i \leq k$. As q_i and p are prime, there are $q_i - 2$ options for each q_i. Set $q \coloneqq 2^3 q_1 q_2 \cdots q_k$. For each combination, there is a solution x so that $p \equiv x \bmod q$. Therefore there are $\prod_i (q_i - 2)$ such combinations. Note that there are $2 \cdot \prod_i (q_i - 1)$ options modulo q for ordinary primes p, as we need $p \equiv 1, 5 \bmod 8$ and $p \not\equiv 0 \bmod q_i$. So the lower density of ordinary primes that have $C = 1/8$ is at least

$$\frac{\prod_i (q_i - 2)}{2 \cdot \prod_i (q_i - 1)}.$$

If $N(\alpha)$ is odd, we should consider $q \coloneqq 4 \cdot q_1 q_2 \cdots q_n$. For any ordinary prime, we need $p \equiv 1 \bmod 4$. Again, if we want to maximize p we have $p \not\equiv 1 \bmod q_i$ for each $1 \leq i \leq n$. Now we consider again the number of solutions to $p \equiv x \bmod q$. It follows that the lower density of ordinary primes with $C = 1$ is at least

$$\frac{\prod_i (q_i - 2)}{\prod_i (q_i - 1)}.$$

□

4.2.2 Experiment

Is there anything to say for endomorphisms of split primes? In an effort of answering Question 4.2.1 in general, indeed assuming that this limit exists, we will check the density of primes with maximal $C_{\alpha,p}$ in the computed endomorphisms. For the 162 values $\alpha = a + bi$ ranging $1 \leq a, b \leq 9$, we computed the number of primes where $C_{\alpha,p}$ is maximal in the first 495 ordinary primes, and we denote the fraction of these in the total number of primes by R_α from now on. Further, we let

$$L_\alpha \coloneqq \begin{cases} \dfrac{\prod_i (q_i - 2)}{2 \cdot \prod_i (q_i - 1)} & \text{if } N(\alpha) \text{ is even,} \\ \dfrac{\prod_i (q_i - 2)}{\prod_i (q_i - 1)} & \text{else.} \end{cases}.$$

To compare these two values, we look at $\delta = 100 \cdot (R_\alpha - L_\alpha)$. Some of the results are included in Table 4.1 while the full table can be found in Appendix B.

What one sees is that surprisingly, the fractions actually give a good indication of the densities when α is not divisible by some full prime $p \neq 2$ (so, in particular, not by inert primes, but also not by 5 for example). This suggest for Question 4.2.1 that perhaps a limit does exists and is equal to L_α in this case, which leads us to the following conjecture.

Conjecture 4.2.1. *Let $E : y^2 = x^3 - x$ be an ordinary elliptic curve over a finite prime field. Let α be an endomorphism not divisible a a full prime $p \neq 2$. Then the density of ordinary primes with a maximal proportion of periodic points exists and is equal to L_α.*

When α does comprise of inert primes we see the computed density is bigger, which is as expected. It is suprising how well the computed value matches the fractions above when α is not divisible by a full prime. We do not have an explanation at this point. We also see that when $\alpha = 5$, the difference δ is negative, which is not contradictory. We know in this case that if 5 divides $|E(\mathbb{F}_p)|$, it divides $N(I_t)$, and we also know that $p \not\equiv 1 \bmod 5$ implies that (5) does not divide $(\pi_p - 1)$ from Theorem 4.2.3. However, we do not know whether P divides $(\pi_p - 1)$ for P a prime above 5 and so we cannot say that C_5 will be maximal when $p \not\equiv 0, 1 \bmod 5$.

α	N(α)	δ	α	N(α)	δ	α	N(α)	δ
2	2^2	1.31	8	2^6	1.31	5	5^2	-18.2
$i+1$	2	1.31	$7i+1$	$2 \cdot 5^2$	0.480	6	$2^2 \cdot 3^2$	20.9
$-i+2$	5	0.152	$6i+4$	$2^2 \cdot 13$	1.04	7	7^2	14.6
$3i+1$	$2 \cdot 5$	1.29	$7i+5$	$2 \cdot 37$	1.29	9	3^4	39.1
$-3i+1$	$2 \cdot 5$	0.480	$8i+5$	89	0.126	$-7i+7$	$2 \cdot 7^2$	8.23
$5i+1$	$2 \cdot 13$	1.04	$2i+9$	$5 \cdot 17$	2.01	$6i+3$	$3^2 \cdot 5$	29.4
$-5i+1$	$2 \cdot 13$	1.04	$9i+8$	$5 \cdot 29$	0.810	$6i+9$	$3^2 \cdot 13$	36.4

Figure 4.1: For a selected number of endomorphisms we portray $\delta = 100 \cdot (R_\alpha - L_\alpha)$ where R_α is as in Theorem 4.2.5 and L_α is the computed density among the first 495 ordinary primes. For the total table, see the appendix B.

4.3 Maximal cycle length

Another type of invariant concerns length of the cycles. One can look at the maximal cycle length or the average cycle length. Here, we want to analyse how the cycle lengths change for different finite fields $\mathbb{F}_p$. A problem is that when p increases in size, naturally one can expect that the cycle lengths will also increase. Therefore we will need to normalise ℓ = *maximal cycle length*. First, I tried studying l/p and $l/\sqrt{p}$ to find possible formulas for l. However, the results turn out much better when analysing $l/N(I_c)$. Note that $N(I_c)$ is equal to the number of points in a cycle. Therefore we study

$$K_{\alpha,p} = \frac{\text{maximal cycle length in } \mathcal{G}_{\alpha,p}}{\#\text{ points in cycles in } \mathcal{G}_{\alpha,p}}$$

so we have $K_{\alpha,p} = l/N(I_c)$ for $(\pi_p - 1) = I_c \times I_t$.

Note that when $N(\alpha)$ is odd, $N(I_c)$ is even, and when $N(\alpha)$ is even, $N(I_c)$ is odd, because of how we defined I_c and I_t. Furthermore, when $N(\alpha)$ is odd, $N(I_c)$ is divisible by 8 because of Theorem 4.2.2.This means we can only have $K_{\alpha,p} = l/N(I_c) = N(I_c) = 1$, so just one cycle, when $N(\alpha)$ is even.

Data and obvervations

I will discuss a few things that stand out regarding the invariant $K_{\alpha,p} = l/N(I_c)$. I will separately discuss the cases $N(\alpha)$ even or odd. We will plot $K_{\alpha,p}$ against the 495 ordinary prime numbers for each α.

Endomorphism with even norm

If $N(\alpha)$ is even, a question is how many times we can expect $N(I_c) = 1$, so that there is only one cycle in the graph. In general, we would expect this is less likely as p grows, and indeed this turns out to be the case for all the 82 even cases. Among the 495 primes, $N(I_c) = 1$ occurs mainly among the first 50 primes (we find 6 to 16 instances), and decreases rapidly towards the last 150 primes (< 4 instances). This is not

surprising, because as p grows, the cardinality of $E(\mathbb{F}_p)$ grows, and thus has more possible prime divisors, which means $N(I_c)$ has more too, and thus it is more likely that $N(I_c) \neq 1$. This also means that $N(I_c) = 1$ is more likely when $N(\alpha)$ has more prime divisors. This is indeed what we see when comparing Figure 4.3 and 4.2. The two plots are typical examples for the computed endomorphisms with even norm.

To see if it is true that the cases of $N(I_c) = 1$ generally go down with bigger prime numbers, we plot for every p, the average number of instances of $N(I_c) = 1$ among the 82 computed even endomorphisms α in Figure 4.4. We can indeed see that the average declines.

When looking at the plots, one might notice that many of the dots are located at smaller values. This is an indicator that there are a lot of points in smaller graphs, as the biggest cycle is rather small. We can see exactly how often this is the case for even endomorphisms. Let us take as a benchmark when $K_{\alpha,p} \leq 1/8$. One can see these cases do go up in Figure 4.8. However, it might not seem too spectacular. It is interesting though to compare this to odd endomorphisms, which is why the graph is included at the end of the chapter.

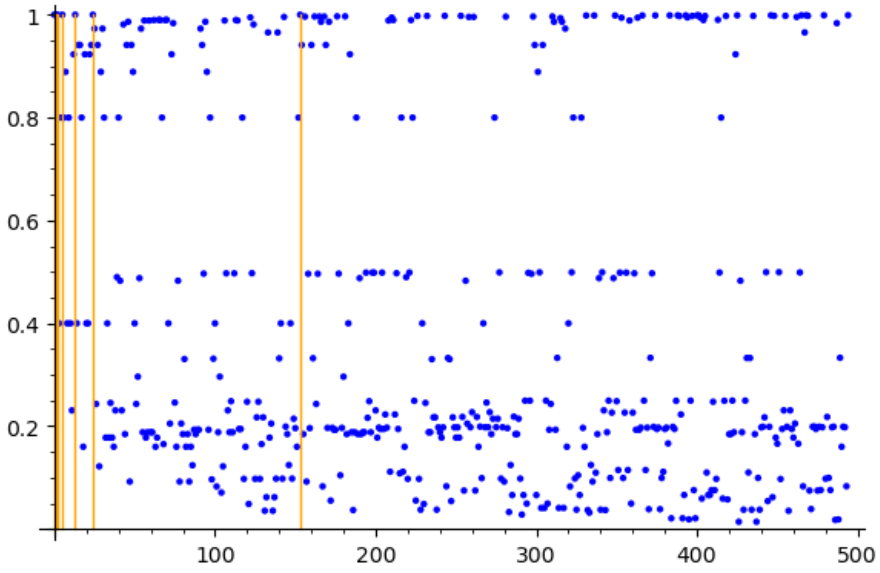


Figure 4.2: $K_{\alpha,p}$ plotted against the first 495 prime numbers p for $\alpha = i + 1$. A yellow line indicates that $K_{\alpha,p} = N(I_c) = 1$ at that prime number.

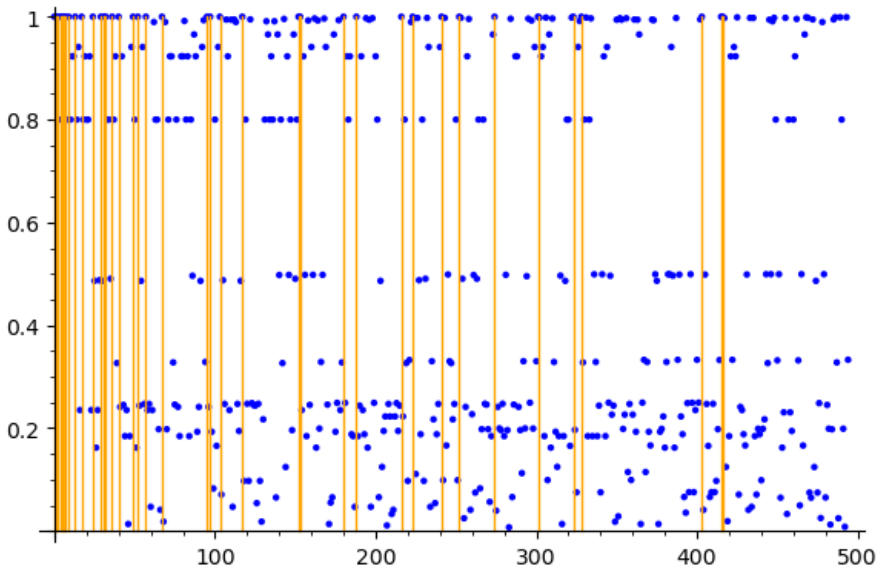


Figure 4.3: $K_{\alpha,p}$ plotted against the first 495 prime numbers for $\alpha = 3i + 9$. A yellow line indicates that $K_{\alpha,p} = N(I_c) = 1$ at that prime number. Note that there are a lot of points where $K_{\alpha,p}$ is almost 1, but not exactly.

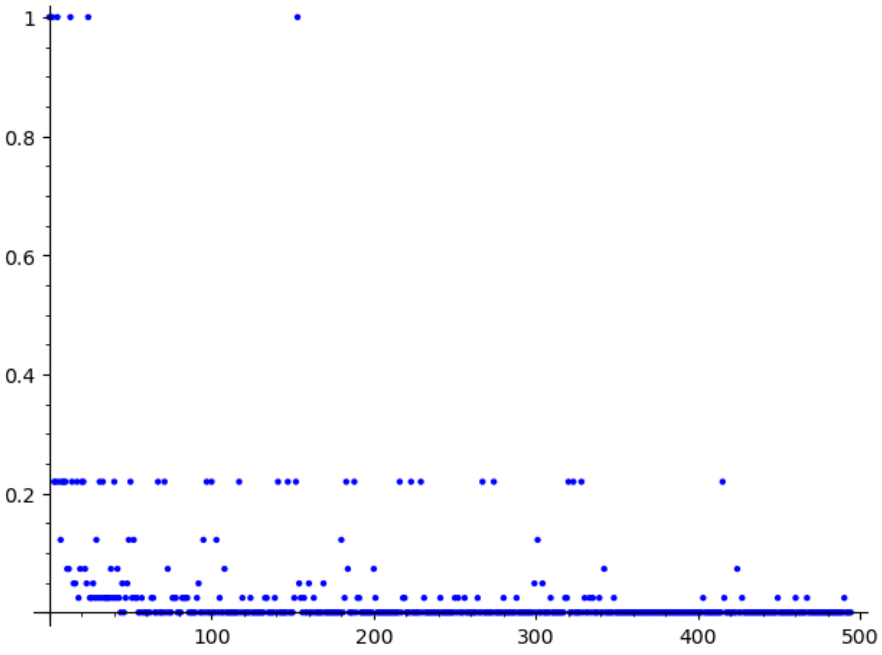


Figure 4.4: For every ordinary prime number p with index ≤ 495 on the x-axis, the average number of instances of $K_{\alpha,p} = 1$ among all computed endomorphisms ($\alpha = a + bi$ with $1 \leq a, b \leq 9$ and $N(\alpha)$ even) is portrayed.

Endomorphisms with odd norm

If $N(\alpha)$ is odd, for each α we found at most $K_{\alpha,p} = 1/2$. In all 80 cases we have the following division:

$\max_p K_{\alpha,p}$	number of cases found	$\mathrm{Re}(\alpha) = a$	$\mathrm{Im}(\alpha) = b$
1/2	40	even	odd
1/4	20	odd	for $a \equiv 1 \bmod 4$, $b \equiv 2 \bmod 4$, else $b \equiv 0 \bmod 4$
1/8	20	odd	for $a \equiv 1 \bmod 4$, $b \equiv 0 \bmod 4$, else $b \equiv 2 \bmod 4$

Figure 4.5: Table describing the occurence of different maxima $K_{\alpha,p}$ over the first 495 ordinary primes among endomorphisms $\alpha = a + bi$. The maximum equals either $1/2, 1/4$ or $1/8$ in all cases.

We can partially explain this with the following theorem.

Theorem 4.3.1. *Let $E : y^2 = x^3 - x$ be an ordinary elliptic curve over $\mathbb{F}_p$ and let $\alpha = a + bi$ be an endomorphism with odd norm with the property that the number of points in cycles is $N(I_c) = 8$ (e.g. at $p = 5$). Then*

- $K_{\alpha,p} = 1/2$ *when a is even,*
- $K_{\alpha,p} = 1/4$ *when a is odd and $a + b \equiv 3 \bmod 4$*
- $K_{\alpha,p} = 1/8$ *when a is odd and $a + b \equiv 1 \bmod 4$.*

Proof. Since we are considering ordinary curves, we have $p \equiv 1 \bmod 4$. This implies that -1 is a quadratic residue in $\mathbb{F}_p$ by Lemma 4.2.1. Note that the curve $E : y^2 = x^3 - x$ always contains the following 8 points

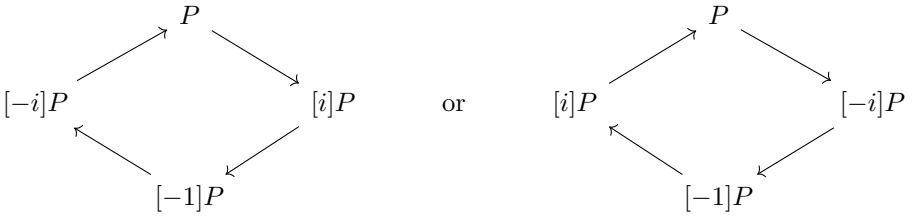
$$\mathcal{O}, (0,0), (-1,0), (1,0), (i, -i+1), (i, i-1), (-i, i+1), (-i, -i-1).$$

Consider the case when these are the only points, so $|E(\mathbb{F}_p)| = N(I_c) = 8$. Note that the points with y-coordinate 0 have order 2, the point $\mathcal{O}$ has order 1 and that the remaining 4 points have order 4: indeed for those points we can calculate that $2P = (0,0)$.

Now let $\alpha = a + bi$ for a even and b odd, say $a = 2k$ and $b = 2l + 1$. Also consider P is one of the points above of order 4; so that $2P = (0,0)$ and $P + (0,0) = -P$. Note that, if $P = (x, y)$ is one of these points, then so is $iP = (-x, iy)$. Then

$$\begin{aligned}
\alpha P = [2k + (2l+1)i]P &= 2kP + (2l+1)iP \\
&= 2kP + 2l(iP) + iP \\
&= k(0,0) + l(0,0) + iP \\
&= [(k+l)(0,0) + i]P \\
&= \begin{cases} [i]P \text{ when } k + l \equiv 0 \bmod 2 \\ [-i]P \text{ when } k + l \equiv 1 \bmod 2 \end{cases}
\end{aligned}$$

for any of the points $P = (i, -i+1), (i, i-1), (-i, i+1), (-i, -i-1)$. So for $\alpha = a + bi$, when a is even and b is odd, this implies that there is a 4-cycle:



depending if $k+l$ is even or odd. Now when a is odd, and b is even, we see that

$$\alpha P = \begin{cases} P \text{ when } k+l \equiv 0 \bmod 2 \\ [-1]P \text{ when } k+l \equiv 1 \bmod 2 \end{cases}$$

and so we see this determines whether the graph has 2-cycles or not. □

Now it is clear when $K_{\alpha,p} = 1/2, 1/4$ and $1/8$ occurs as a maximal value; $N(\alpha)$ needs to be odd and we need to choose a prime p such that $N(I_c) = 8$ – then we know for which α we get $1/2$, $1/4$ or $1/8$. In all computed cases, the maximum of $K_{\alpha,p}$ among the primes is always the same as the first entry ($p = 5$). It follows that we always have that the maximum of $K_{\alpha,p}$ is at least $1/8$. It seems likely that the maximum $K_{\alpha,p}$ will always be equal to the first entry. However, we cannot prove that this holds or that $K_{\alpha,p} > 1/2$ could be possible. Still, we conjecture that

Conjecture 4.3.1. *Let $E : y^3 = x^3 - x$ be the elliptic curve over $\mathbb{Q}$. Let $\alpha = a + bi$ be an endomorphism of E with an odd norm. Let p be an ordinary prime number; so that E over $\mathbb{F}_p$ is an ordinary elliptic curve. Then*

- $\max_p\{K_{\alpha,p}\} = 1/2$ *when a is even,*
- $\max_p\{K_{\alpha,p}\} = 1/4$ *when a is odd and $a + b \equiv 3 \bmod 4$*
- $\max_p\{K_{\alpha,p}\} = 1/8$ *when a is odd and $a + b \equiv 1 \bmod 4$.*

Next, we will show a typical example of the odd case, which is especially useful to compare to the plots in the previous section. We will also show some more average plots to see that $N(\alpha)$ even or odd makes a big difference.

What is immediately apparent when comparing Figure 4.6 to Figure 4.3 and 4.2 is that the values $K_{\alpha,p}$ get much closer to 1 in the even case. We further see that, for $N(\alpha)$ odd, it is likely that $K_{\alpha,p} \leq 1/8$, while for $N(\alpha)$ even, $K_{\alpha,p} > 1/8$ occurs more often. To compare, see Figure 4.7 and 4.8 portraying the average instance of $N(I_c) \leq 1/8$ for the odd and even cases. For an endomorphism with an odd norm, the graph has more connected components as opposed to longer cycles, while in contrast, when an endomorphism has an even norm, is is also possible to have longer cycles. For the odd case, we also plot when $K_{\alpha,p}$ is even smaller in Figure 4.9.

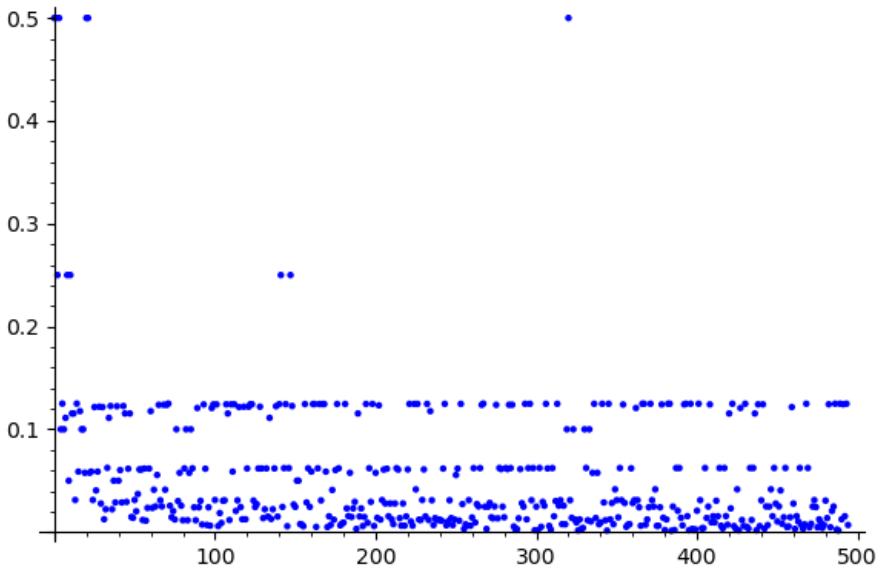


Figure 4.6: $K_{\alpha,p}$ plotted against prime numbers for $\alpha = i + 2$. We see that $K_{\alpha,p} = 1/2, 1/4$ is rare. This is true in general for all 80 studied cases. Another thing to notice, which holds for any checked endomorphism, is that the only points between $1/2$ and $1/8$ are at $1/4$.

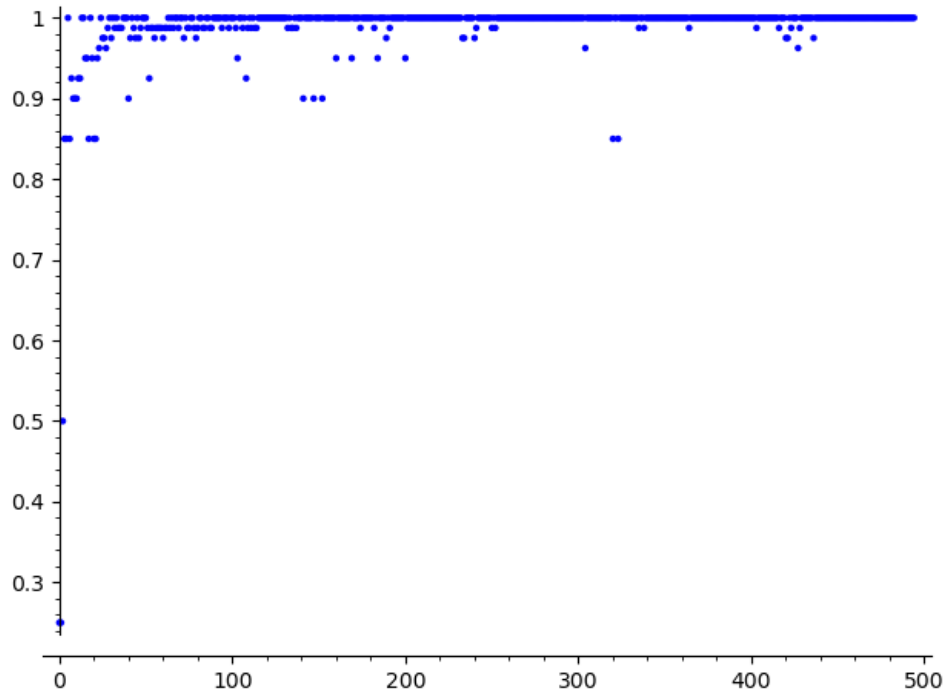


Figure 4.7: For every prime number p with index ≤ 495 on the x-axis, the average number of instances of $K_{\alpha,p} \leq 1/8$ among all computed endomorphisms, $\alpha = a + bi$ with $1 \leq a, b \leq 9$ and $N(\alpha)$ odd, is portrayed.

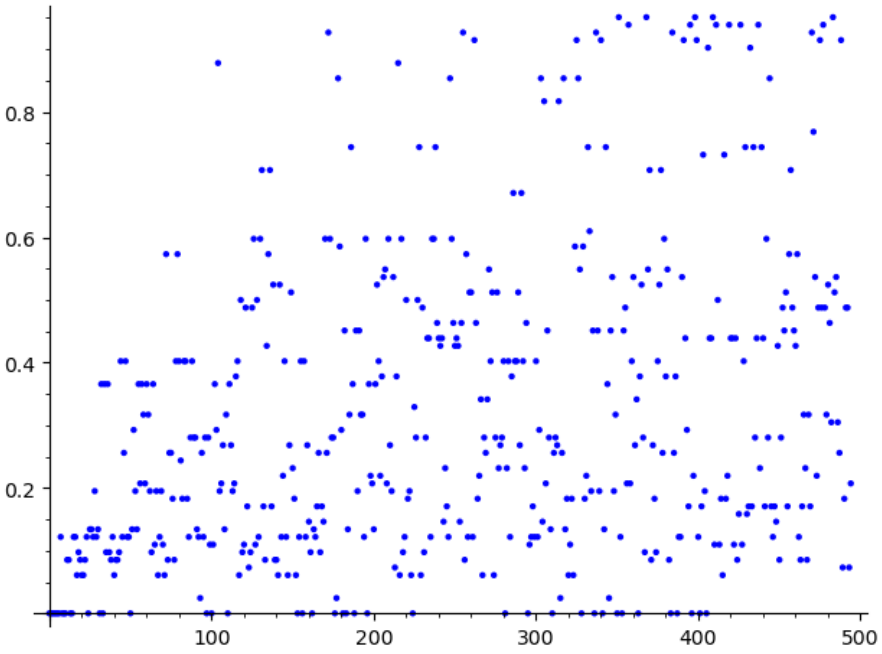


Figure 4.8: For every ordinary prime number p with index ≤ 495 on the x-axis, the average number of instances of $K_{\alpha,p} \leq 1/8$ among all computed endomorphisms, $\alpha = a + bi$ with $1 \leq a, b \leq 9$ and $N(\alpha)$ even, is portrayed.

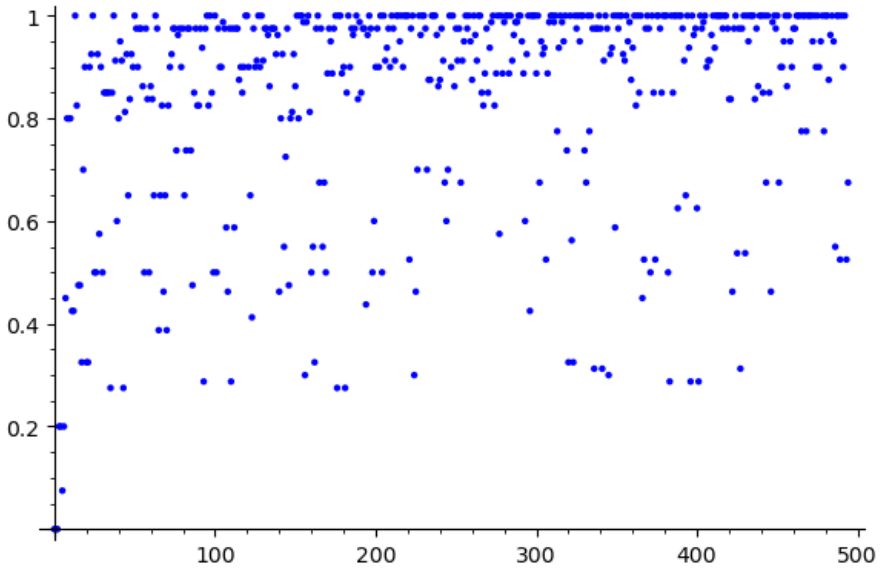


Figure 4.9: For every prime number p with index ≤ 495 on the x-axis, the average number of instances of $K_{\alpha,p} < 1/16$ among all computed endomorphisms, $\alpha = a + bi$ with $1 \leq a, b \leq 9$ and $N(\alpha)$ odd, is portrayed.

Conclusion and discussion

In this thesis we have given a description of the cycles and trees of graphs of endomorphisms of ordinary elliptic curves over finite fields $\mathbb{F}_q$. We have built on previous results on rational maps from Ugolini and Qureshi & Reis. We described the group of points $E(\mathbb{F}_{q^n})$ on an elliptic curve as a module over the endomorphism ring. Assuming that the endomorphism ring is the ring of integers, we did calculations in an algebraic number theoretic setting. Next, we wanted to analyse different invariants while varying the finite field. We looked at the specific curve $y^2 = x^3 - x$ and the invariants the number of points in cycles and the maximal cycle length. To analyse how the invariants change relative to the size of points increasing, we looked at the proportion of total points in cycles and the proportion of periodic points in the maximal cycle. Besides certain exact results, we have some experimental results for 162 endomorphisms looking at the first 495 ordinary primes.

One exact result is regarding the proportion of points in cycles. We looked at $|E(\mathbb{F}_p)| \bmod q$ for q dividing the norm of α. When the norm of α is not divisible by a split prime, we gave a lower bound for the lower density (infimum limit) of ordinary primes where the proportion of points in cycles is maximal. Next, we analysed the split case experimentally, where we found that our lower bound is a suprisingly good approximate when α is not divisble by a rational prime number $p \neq 2$. One could look into answering the Question 4.2.1; does the density of primes where the proportion of points in cycles is maximal exist? Can we prove Conjecture 4.2.1, which gives a probable answer for the case when α is not divisble by a full prime $p \neq 2$?

For the proportion of periodic points in cycles, we can prove something with regard to when the proportion is maximal. When the norm of α is even, we know that the maximal equals 1. Else, we theorize that it is always 1/2, 1/4 or 1/8. What we can prove, is that when there are exactly 8 points in cycles, indeed we find a proportion of 1/2, 1/4 or 1/8. In Conjecture 4.3.1 we gave this experimental value for the maximal proportion of cyclic points in the maximal cycle for a fixed endomorphism.

There are plenty of directions to take from here. First of all, it would be interesting to look at the plots for different curves. There are congruence results for when the cardinality of $E : y^2 = x^3 - cx$ and $E : y^2 = x^3 + b^3$ equals 0 modulo $16, 24$ for a general c, see [PKL03], [İna+07] and [JK13]. There are also some results for more general curves, see [KKP08] for a discussion curves of the shape $E : y^2 = x^3 + f(k)x + g(k)$ and in particular a result when for a specific $f(k), g(k)$ gives $|E(\mathbb{F}_p)| \equiv 0 \bmod 3$. This can give a start to deriving theorems such as Theorem 4.2.5 for more general curves as well.

Another aspect to look into is proving density statements by using the Ugolini approach with Galois rings to describe cycles, as we saw in Appendix A. This could work because Theorem A.2.1 still holds in the split and inert case. We can use this perhaps for density statements relating to cycles, such as the proportion of points in cycles.

There are other directions we did not look into but could be interesting to study. One could be to fix p, and vary over the endomorphism. This means that the points $E(\mathbb{F}_p)$ are fixed, and a question is: how many possible graphs are there when varying α? How many isomorphisms classes do we find? Note that the trees are determined exactly by f_i, e_i and $N(\mathfrak{D}_i)$ from Theorem 3.3.1. Each α will correspond to a different number of points in the pre-image: there will be $\prod_i e_i$ options for the size of the pre-image as per Theorem

3.3.1 by letting each f_i range $0 \leq i \leq e_i - 1$. Letting $f_i \geq e_i$ does not give a new graph, so there are at most $\prod_i e_i$ isomorphism classes. If each prime ideal $\mathfrak{B}_i$ of $\pi_p - 1$ lies above a ramified or inert rational prime, or if the rational prime is split but $\mathfrak{B}_i$'s conjugate does not divide $\pi_p - 1$, then there is a one-one relation between the choice for the f_i's and the number of points in the pre-image (and thus $\prod_i e_i$ gives the number of isomorphism classes). If $\mathfrak{B}_i$ lies above a split prime, we can have that the pre-image sizes are equal and in fact the trees are isomorphic (as they only depend on norms), but α is different. In that case, it is not clear how many isomorphism classes there are. This depends on the cycles. The one factor which is not given by norms is the cycle length, which we can check by analysing $\alpha^v - 1$. To find out more about exact number of isomorphism classes, we will need to know more about this.

We noted that there are some symmetries in the trees of the graphs. In general, points at level h in a tree do not have the same pre-image size; the size of the pre-image is either $k > 0$ or 0 for some constant k. One can get extra symmetry if $|T_h| = k \cdot |T_{h-1}|$ for each level of the tree $h > 1$. This holds for example when $N(I_t)$ is a power of 2. If one is interested in graphs which have this symmetry in the vertices, this could be a good starting point.

Another direction which could be interesting for experiments as well, is to check what happens when the endomorphism ring R is not equal to the maximal order. However, analysing this would require a completely different approach.

Appendix A

Alternative proof for cycles theorem

Here I present an alternative approach from [Ugo18] for the theory of cycles in the graphs. This gives a proof for the split and inert cases, but does not work in the ramified case. In the end it is not really necessary to distinguish the split, inert and ramified cases which is why the presentation in the thesis was different and in fact simpler. I believe the original approach is still an interesting idea, which works in many cases, and therefore deserves discussion and so I include it here. We will first need to discuss Galois rings.

A.1 Galois rings

Back in Chapter 1, we reduced the problem of understanding finite graphs of elliptic curve endomorphisms to a number theoretic problem. We now present a way to understand the graph of the action of an element of the order R of a number field on $R/(\pi_q^n - 1)$. Let us assume that R is a maximal order and thus a Dedekind domain. Therefore we have unique factorisation of ideals. Let us thus write

$$R/(\pi_q^n - 1) = \prod_{i=1}^{k} R/\mathfrak{B}_i^{e_i}$$

with each $\mathfrak{B}_i$ a prime ideal and $e_i > 0$. In this section we will describe the structure of these rings. They are in fact Galois rings. We will describe some basic results on Galois rings and the rings $R/\mathfrak{B}_i^{e_i}$.

The main reference for this section is chapter 14 of [Wan03], which gives a very detailed exposition of the material.

Definition A.1.1. A Galois ring is a finite ring with identity 1 so that the set of its zero divisors with 0 forms a principal ideal $(p \cdot 1)$ for some prime number p.

An example of a Galois ring is $\mathbb{Z}/p^s\mathbb{Z}$. It turns out that Galois rings can be determined up to isomorphism by their characteristic and prime power cardinality [Wan03][Section 14.2]. Let R be a Galois ring. It is not hard to show that $R/(p) \cong \mathbb{F}_{p^m}$ and $|R| = p^{sm}$ for an integer m. It turns out that a Galois ring R with zero divisors in (p) can be determined up to isomorphism by the integers m and s for which the ring has characteristic p^s and cardinality p^{sm}. We will denote such a Galois ring by $GR(p^s, p^{sm})$. For example $\mathbb{Z}/p^s\mathbb{Z} \cong GR\,(p^s, p^s)$.

We are interested in Galois rings because the followings holds. This theorem is section 2.3 of [Ugo18].

Theorem A.1.1. *(1) Let p_i be inert. There is an isomorphism*

$$R/\mathfrak{B}_i^{e_i} \cong \mathbb{Z}/p_i^{e_i}\mathbb{Z} = GR\left(p_i^{e_i}, p_i^{e_i}\right).$$

(2) Let p_i be split. There is an isomorphism

$$R/\mathfrak{B}_i^{e_i} \cong GR\left(p_i^{e_i}, p_i^{2e_i}\right).$$

(3) Let p_i be ramified. There are three cases. Let $x+c$ be a factor in $\mathbb{Q}(\sqrt{-d})[x]$ of the minimal polynomial of $\sqrt{-d}$ over $\mathbb{Q}$.
- If $e_i = 1$, then the additive group of $R/\mathfrak{B}_i^{e_i}$ is isomorphic to a cyclic group of order p_i.
- If e_i is even, then the additive group of $R/\mathfrak{B}_i^{e_i}$ is isomorphic to the direct sum of two cyclic groups and its elements can be represented as

$$z_0 + z_1(c-d),$$

where $(c-d)$ is a principal ideal in $\mathbb{Z}[\omega_d]$ and $z_0, z_1 \in \mathbb{Z}/p_i^{e_i/2}\mathbb{Z}$.
- If e_i is odd and $e_i \geq 3$, then the additive group of $R/\mathfrak{B}_i^{e_i}$ is isomorphic to the direct sum of two cyclic groups and its elements can be represented as

$$x_0 + z_0(c-d),$$

where $x_0 \in \mathbb{Z}/p_i^{(e_i+1)/2}\mathbb{Z}$ and $z_0 \in \mathbb{Z}/p_i^{(e_i-1)/2}\mathbb{Z}$.

The remainder of this section will be dedicated to some theorems that we will need later on. We will use the terminology basic primitive or irreducible to denote a polynomial in $\mathbb{Z}/p^s\mathbb{Z}[x]$ which is primitive or irreducible in $\mathbb{Z}/p\mathbb{Z}[x]$ after reducing the coefficients modulo p. If f is some polynomial, we will denote by $\bar{f}$ the the polynomial resulting from reducing the coefficients of f modulo p.

Lemma A.1.1. *Let R be a Galois ring of characteristic p^s and cardinality p^{sm}, where p is a prime number and s and m are positive integers. Let $f(x)$ be a polynomial over $\mathbb{Z}_{p^s}$ and assume that $\bar{f}(x)$ has a root $\bar{\beta}$ in $R/(p) \simeq \mathbb{F}_{p^m}$ and that $\bar{f}'(\bar{\beta}) \neq 0$. Then there exists a (unique) root $\xi \in R$ of the polynomial $f(x)$ such that $\bar{\xi} = \bar{\beta}$.*

Proof. Let $\xi_0 \coloneqq \beta$ and consider a sequence $\xi_{i+1} \coloneqq \xi_i - f'(\xi_i)^{-1}f(\xi_i) \in R$. We can show with induction that $\bar{\xi_i} = \bar{\beta}$ and $f(\xi_i) \in (p^{i+1})$ for all non-negative integers i. Note that $\overline{f'(\xi_i)} = \bar{f}'(\bar{\xi}) = \bar{f}'(\bar{\beta}) \neq 0$, so that p does not divide $f'(\xi_i)$. Therefore $f'(\xi_i)$ it is a unit of R. It is clear that $\bar{\xi_{i+1}} = \bar{\xi_i}$. We can prove that $f(\xi_{i+1}) = f(\xi_i - f'(\xi_i)^{-1}f(\xi_i)) \in (p^{i+2})$ by applying Taylor's formula. Then we get for $\xi \coloneqq \xi_{s-1}$, $\bar{\xi} = \bar{\beta}$ and $f(\xi) = f(\xi_{s-1}) \in (p^s) = (0)$, so $f(\xi) = 0$. □

One can use the above lemma to show that any Galois ring is isomorphic to the ring $\mathbb{Z}/p\mathbb{Z}[x]/(h(x))$ for any monic basic irreducible polynomial $h(x)$ of degree m over $\mathbb{Z}/p^s\mathbb{Z}$. This is because if $\bar{h}$ is irreducible and $\zeta \in \mathbb{F}_{p^m} \cong R/(p)$ is a root of $\bar{h}$, then $\bar{h}$ is the minimal polynomial of ζ and thus we have $\bar{h}'(\zeta) \neq 0$. Then h has a unique root ξ with $\bar{\xi} = \bar{\zeta}$. Now it is not hard to show that the map

$$\begin{aligned} \mathbb{Z}/p^s\mathbb{Z}[x]/(h(x)) &\longrightarrow R \\ a_0 + a_1 + \cdots + a_{m-1}x^{m-1} + (h(x)) &\longmapsto a_0 + a_1\xi \cdots + a_{m-1}\xi^{m-1} \end{aligned}$$

where $a_0, \ldots, a_{m-1} \in \mathbb{Z}/p^s\mathbb{Z}$ gives a well-defined ring isomorphism [Wan03][Theorem 14.6].

Theorem A.1.2. *In the Galois ring $GR\left(p^s, p^{sm}\right)$ there exists a nonzero element ξ of order $p^m - 1$, which is a root of a monic basic primitive polynomial $h(x)$ of degree m over $\mathbb{Z}/p^s\mathbb{Z}$ and dividing $x^{p^m-1}-1$ in $\mathbb{Z}/p^s\mathbb{Z}[x]$.*

Proof. Let h_p be a primitive polynomial of degree m with coefficients in $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Such a polynomial always exists (see [Wan03][Corollary 6.13]). First we will prove that it divides $x^{p^m-1}-1$ which is Lemma 6.9 from [Wan03]. Since $\mathbb{F}_p[x]/(h_p(x))$ is a finite field with p^m elements, it follows that any $r \in \mathbb{F}_p[x]/(h_p(x))$ satisfies $r^{p^m-1}-1=0$. So $x^{p^m}-x \equiv 0 \bmod h_p(x)$ and thus $h_p(x)|x^{p^m-1}-1$.

We will now show that there exists a monic basic primitive polynomial in $\mathbb{Z}/p^s\mathbb{Z}$ of degree m that divides $x^{p^m-1}-1$. Write $x^{p^m-1}-1 = h_p(x)g_p(x)$ in $\mathbb{F}_p[x]$. Since h_p, g_p are coprime ($x^{p^m-1}-1$ has no multiple roots), we can apply Hensel's lemma [Ste02, p. 15] and get $x^{p^m-1}-1 = h(x)g(x)$ in $\mathbb{F}_{p^s}[x]$ with $\bar{h}=h_p$ and $\bar{g}=g_p$ and $\deg h = m$. Also h is monic and basic primitive.

Since $\bar{h}$ is primitive, it has a nonzero root $\xi_p \in \mathbb{F}_{p^m}$ of order p^m-1. Now as $\bar{h}$ is the minimal polynomial of ξ_p, we have that $\bar{h}'(\xi_p) \neq 0$. So applying Lemma A.1.1 gives a unique nonzero root $\xi \in GR(p^s, p^{sm})$ of h with $\bar{\xi} = \xi_p$. Clearly $\xi^{p^m-1}-1=0$. Further, because $\bar{\xi}$ has order p^m-1 we have $x^i-1 \neq 0$ for integers $0 < i < p^m-1$. So we found a nonzero element ξ of order p^m-1 in the Galois ring. □

The following is a straightforward but important corollary of the above theorem.

Corollary A.1.1. *(1) Any element $c \in GR(p^s, p^{sm})$ can be written uniquely as*

$$c = c_0 + c_1 p + \cdots + c_{s-1}p^{s-1},$$

where $c_0, c_1, \ldots, c_{s-1} \in \{0, 1, \xi, \xi^2, \ldots, \xi^{p^m-2}\}$.
(2) Every nonzero element $c \in GR(p^s, p^{sm})$ can be expressed uniquely in the form $c = up^r$, where u is a unit and $0 \leq r < s$.

To determine the cycles of the graph, we can study I_c. Let its factorisation into prime ideals be given by

$$R/I_c \cong \left(\prod_{i=1}^{l} R/\mathfrak{B}_i^{e_i} \right)$$

where $\mathfrak{B}_i$ is a prime ideal lying above a rational prime p_i. We have seen that the rings $R/\mathfrak{B}_i^{e_i}$ are Galois rings and that the structure depends on if the rational prime p_i above $\mathfrak{B}_i$ is inert, ramified or split.

A.2 Proof for inert and split cases

We will make use of the fact that it turns out that all points of the same additive order, are a part of cycles of the same length. So we determine first how many points of a same order there are, and then what the length of the corresponding cycles is, to find out how many cycles of this certain length there are. Here we use exactly the terminology and theorems from [Ugo18], which we adapt to apply to endomorphisms.

For each prime factor, so for each i, consider intervals $H_i = [0, e_i]$ or $H_i = [0, (e_i+1)/2]$ depending if the corresponding rational prime p_i is ramified or not. Then for $P = (P_i)_i \in R/I_c$, each P_i has additive order $p_i^{h_i}$ in $R/\mathfrak{B}_i^{e_i}$ for some $h_i \in H_i$. We need the following terminology:
(1) If p_i is split, then

$$n_{h_i} := \begin{cases} 1 & \text{if } h_i = 0 \\ p_i^{h_i} - p_i^{h_i-1} & \text{otherwise.} \end{cases}$$

(2) If p_i is inert, or if p_i is ramified and e_i is even, then

$$n_{h_i} := \begin{cases} 1 & \text{if } h_i = 0 \\ {p_i}^{2h_i} - {p_i}^{2(h_i-1)} & \text{otherwise.} \end{cases}$$

(3) If p_i is ramified and e_i is odd, then

$$n_{h_i} := \begin{cases} 1 & \text{if } h_i = 0 \\ {p_i}^{2h_i} - {p_i}^{2(h_i-1)} & \text{if } 1 \leq h_i \leq (e_i-1)/2 \\ {p_i}^{2h_i-1} - p_i^{2(h_i-1)} & \text{if } h_i = (e_i+1)/2. \end{cases}$$

Lastly we define

$$s_{h_i} := \min\left\{ v \in \mathbb{N}\backslash\{0\} : \alpha^v - 1 \in \mathfrak{B}_i^{h_i} \right\}.$$

The following theorem is Lemma 3.7 from [Ugo18]. The proofs are expanded and a proof of the ramified case in (1) has been added. The ramified case of (2) is missing, as this is where we could not complete the proof unfortunately.

Theorem A.2.1. *(1) Let $i \in [1,l]$. Then in $R/\mathfrak{B}_i^{e_i}$ there are n_{h_i} points of additive order $p_i^{h_i}$ for any $h_i \in H_i$. (2) Let P_i be a point of order $p_i^{h_i}$ in $R/\mathfrak{B}_i^{e_i}$ for p_i inert or split. Then the smallest of the positive integers v such that $[\alpha]^v P_i = P_i$ is s_{h_i}.*

Proof. (1) If $h_i = 0$, it is clear that $n_{h_i} = 1$, because only the point zero $[0] \in R/\mathfrak{B}_i^{e_i}$ has order 1. Now assume $h_i > 0$ and let P_i be a point of order $p_i^{h_i}$. We will first do the case that p_i is inert or split in R so that by Theorem A.1.1 $R/\mathfrak{B}_i^{e_i} \cong GR\left(p_i^{e_i}, p_i^{ne_i}\right)$ with $n = 1$ and $n = 2$ respectively. Now we can represent P_i as an element c in the Galois ring, and Corollary A.1.1(1) tells us what c looks like. Now because of the isomorphism it also follows that P_i has order $p_i^{h_i}$ if and only if we can write the representative as

$$c_{e_i-h_i} p_i^{e_i-h_i} + \cdots + c_{e_i-1} p_i^{e_i-1} \tag{A.1}$$

for some coefficients $c_{e_i-h_i}, \ldots, c_{e_i-1} \in \left\{0, 1, \ldots, \xi^{p_i^m-2}\right\}$ with $c_{e_i-h_i} \neq 0$. Therefore there are $p_i^m - 1$ choices for the first coefficient and p_i^m for the other $h_i - 1$ coefficients. We conclude there are

$$(p_i^m - 1) \cdot p_i^{m(h_i-1)} = p_i^{mh_i} - p_i^{m(h_i-1)}$$

points of additive order $p_i^{h_i}$ in $R/\mathfrak{B}_i^{e_i}$. Now consider p_i ramified. Let P_i be a point in $R/\mathfrak{B}_i^{e_i}$ with additive order $p_i^{h_i} > 1$. If $e_i = 1$, then the proof is the one above with $e_i = m = 1$, because $\mathbb{Z}/p_i\mathbb{Z} \cong GR(p_i, p_i)$. Now assume e_i is even. Then we can write $P_i = z_0 + z_1(c+d)$ as in Theorem A.1.1, where $z_0, z_1 \in \mathbb{Z}/p_i^{e_i/2}\mathbb{Z} \cong GR\left(p_i^{e_i/2}, p_i^{e_i/2}\right)$. Then z_0, z_1 can be represented as A.1, but only one of the first coefficients has to be nonzero and we should replace e_i with $e_i/2$. Therefore we can calculate separately the elements with exactly one of the initial coefficients nonzero and those with both initial coefficients nonzero. We get the following:

$$2(p_i - 1)p_i^{2(h_i-1)} + (p_i-1)^2 p_i^{2(h_i-1)} = p_i^{2h_i} - p_i^{2h_i-2}.$$

The case that e_i is odd goes in the same way. Consider an element $P_i = x_0 + x_1(c+d)$ as in Theorem A.1.1, where $x_0 \in \mathbb{Z}/p_i^{(e_i+1)/2}\mathbb{Z} \cong GR\left(p_i^{(e_i+1)/2}, p_i^{(e_i+1)/2}\right)$ and $x_1 \in GR\left(p_i^{(e_i-1)/2}, p_i^{(e_i-1)/2}\right)$. The main difference with the even case is that we have to look carefully when $h_i = \frac{e_i+1}{2}$. That is because in this case, we have for any choice of z_0 that $p_i^{h_i} z_0 = 0 \in GR\left(p_i^{(e_i-1)/2}, p_i^{(e_i-1)/2}\right)$. Therefore we need that the initial coefficient of z_1 is nonzero. We get the following number of elements

$$(p_i - 1)p_i^{h_i-1} p_i^{h_i-1}$$

because there are $p_i - 1$ choices for the initial coefficient of z_1 and p_i choices for the remaining coefficients of z_1 and all $\frac{e_i-1}{2} = h_i - 1$ coefficients of z_0.

(2) Suppose that p_i inert or split. We want the equality of sets

$$\left\{v \in \mathbb{N}\backslash\{0\} : \alpha^v - 1 \in \mathfrak{B}_i^{h_i}\right\} = \{v \in \mathbb{N}\backslash\{0\} : [\alpha^v - 1]P_i \in \mathfrak{B}_i^{e_i}\}$$

or for any $v \in \mathbb{N}$

$$\alpha^v - 1 \in \mathfrak{B}_i^{h_i} \iff [\alpha^v - 1]P_i \in \mathfrak{B}_i^{e_i}.$$

First let v be a positive integer such that $\alpha^v - 1 \in \mathfrak{B}_i^{h_i}$. As P_i is a point of order $p_i^{h_i}$ in $R/\mathfrak{B}_i^{e_i}$, and p_i is split or inert, it follows that $[\alpha^v - 1]P_i = [0]$ in $R/\mathfrak{B}_i^{e_i}$. (Note that this does not work if $p_i = \mathfrak{B}_i^2$ is ramified.)

Now let v be a positive integer such that $[\alpha^v - 1]P_i \in \mathfrak{B}_i^{e_i}$ or $[\alpha^v - 1]P_i = [0]$ in $R/\mathfrak{B}_i^{e_i}$. Again we can represent P_i as an element in $GR\,(p_i^{e_i}, p_i^{ne_i})$ ($n \in \{1, 2\}$) that can be written as A.1. Thus $[\alpha^v - 1] = [0]$ or else we get with Corollary A.1.1(2) that $[\alpha^v - 1]$ can be written in $GR\,(p_i^{e_i}, p_i^{ne_i})$ as

$$up_i^{h_i}$$

for some unit u. It follows that $[\alpha^v - 1] = [0]$ in $R/\mathfrak{B}_i^{h_i}$, so indeed $\alpha^v - 1 \in \mathfrak{B}_i^{h_i}$. □

We define

$$s_h \coloneqq \operatorname{lcm}(s_{h_1}, \ldots, s_{h_l})$$
$$n_h \coloneqq \prod_{i=1}^{l} n_{h_i}.$$

To determine the cycles of the graph, we need to consider all tuples $(h_i)_i \in \prod_i H_i$ and the corresponding points $P = (P_i)_i \in R/I_c$ so that each P_i has additive order $p_i^{h_i}$. We know there are n_{h_i} points P_i of additive order $p_i^{h_i}$ in $R/\mathfrak{B}_i^{e_i}$ and that s_{h_i} is the smallest positive integer so that $[\alpha]^{s_{h_i}} P_i = P_i$ for such a point P_i. As s_h is defined as the least common multiple of these s_{h_i}, we get that it is the smallest integer so that

$$\alpha^{s_h} P = (\alpha^{s_h} P_1, \alpha^{s_h} P_2, \ldots, \alpha^{s_h} P_k) = P$$

by pointwise calculation. So s_h is the order of P and there are $n_h = \prod_{i=1}^{l} n_{h_i}$ points of that same order. Now we have

$$C_h \coloneqq \frac{n_h}{s_h}$$

cycles of length s_h.

Note: The main difference with [Ugo18] in this paragraph is that we have replaced $\pm$ by either $+$ or $-$ in certain places, for example in the definition of s_{h_i}. The reason is that because Ugolini considers the graph of the projection onto the x-coordinate, $\alpha(P) = P$ and $\alpha(P) = -P$ give the same result. For the same reason we write $\frac{1}{s_h}$ instead of $\frac{1}{2s_h}$ when calculating C_h. The result is that either a cycle doubles in length or the number of cycles is doubled.

Appendix B

Full table for δ

α	$\mathrm{N}(\alpha)$	δ
$i+1$	2	1.31
$-i+1$	2	1.31
$3i+1$	$2\cdot 5$	1.29
$-3i+1$	$2\cdot 5$	0.480
$5i+1$	$2\cdot 13$	1.04
$-5i+1$	$2\cdot 13$	1.04
$7i+1$	$2\cdot 5^2$	0.480
$-7i+1$	$2\cdot 5^2$	1.29
$9i+1$	$2\cdot 41$	1.55
$-9i+1$	$2\cdot 41$	1.55
$2i+2$	2^3	1.31
$-2i+2$	2^3	1.31
$4i+2$	$2^2\cdot 5$	0.480
$-4i+2$	$2^2\cdot 5$	1.29
$6i+2$	$2^3\cdot 5$	1.29
$-6i+2$	$2^3\cdot 5$	0.480
$8i+2$	$2^2\cdot 17$	2.22
$-8i+2$	$2^2\cdot 17$	1.00
$i+3$	$2\cdot 5$	0.480
$-i+3$	$2\cdot 5$	1.29
$3i+3$	$2\cdot 3^2$	20.9
$-3i+3$	$2\cdot 3^2$	20.9
$5i+3$	$2\cdot 17$	1.00
$-5i+3$	$2\cdot 17$	2.22
$7i+3$	$2\cdot 29$	1.28
$-7i+3$	$2\cdot 29$	1.48
$9i+3$	$2\cdot 3^2\cdot 5$	16.2
$-9i+3$	$2\cdot 3^2\cdot 5$	15.2
$2i+4$	$2^2\cdot 5$	1.29
$-2i+4$	$2^2\cdot 5$	0.480
$4i+4$	2^5	1.31
$-4i+4$	2^5	1.31
$6i+4$	$2^2\cdot 13$	1.04
$-6i+4$	$2^2\cdot 13$	1.04
$8i+4$	$2^4\cdot 5$	0.480
$-8i+4$	$2^4\cdot 5$	1.29
$i+5$	$2\cdot 13$	1.04
$-i+5$	$2\cdot 13$	1.04
$3i+5$	$2\cdot 17$	2.22
$-3i+5$	$2\cdot 17$	1.00
$5i+5$	$2\cdot 5^2$	-9.01
$-5i+5$	$2\cdot 5^2$	-9.01
$7i+5$	$2\cdot 37$	1.29
$-7i+5$	$2\cdot 37$	1.49
$9i+5$	$2\cdot 53$	0.860
$-9i+5$	$2\cdot 53$	1.26
$2i+6$	$2^3\cdot 5$	0.480
$-2i+6$	$2^3\cdot 5$	1.29
$4i+6$	$2^2\cdot 13$	1.04
$-4i+6$	$2^2\cdot 13$	1.04
$6i+6$	$2^3\cdot 3^2$	20.9
$-6i+6$	$2^3\cdot 3^2$	20.9
$8i+6$	$2^2\cdot 5^2$	1.29
$-8i+6$	$2^2\cdot 5^2$	0.480
$i+7$	$2\cdot 5^2$	1.29
$-i+7$	$2\cdot 5^2$	0.480
$3i+7$	$2\cdot 29$	1.48
$-3i+7$	$2\cdot 29$	1.28
$5i+7$	$2\cdot 37$	1.49
$-5i+7$	$2\cdot 37$	1.29
$7i+7$	$2\cdot 7^2$	8.23
$-7i+7$	$2\cdot 7^2$	8.23
$9i+7$	$2\cdot 5\cdot 13$	0.170
$-9i+7$	$2\cdot 5\cdot 13$	0.574
$2i+8$	$2^2\cdot 17$	1.00
$-2i+8$	$2^2\cdot 17$	2.22
$4i+8$	$2^4\cdot 5$	1.29
$-4i+8$	$2^4\cdot 5$	0.480
$6i+8$	$2^2\cdot 5^2$	0.480
$-6i+8$	$2^2\cdot 5^2$	1.29
$8i+8$	2^7	1.31
$-8i+8$	2^7	1.31
$i+9$	$2\cdot 41$	1.55
$-i+9$	$2\cdot 41$	1.55
$3i+9$	$2\cdot 3^2\cdot 5$	15.2
$-3i+9$	$2\cdot 3^2\cdot 5$	16.2
$5i+9$	$2\cdot 53$	1.26
$-5i+9$	$2\cdot 53$	0.860
$7i+9$	$2\cdot 5\cdot 13$	0.574
$-7i+9$	$2\cdot 5\cdot 13$	0.170
$9i+9$	$2\cdot 3^4$	20.9
$-9i+9$	$2\cdot 3^4$	20.9
$2i+1$	5	0.152
$-2i+1$	5	0.960
$4i+1$	17	1.40
$-4i+1$	17	-0.215
$6i+1$	37	0.354
$-6i+1$	37	-0.455
$8i+1$	$5\cdot 13$	0.543
$-8i+1$	$5\cdot 13$	0.341
$i+2$	5	0.960
$-i+2$	5	0.152
$3i+2$	13	-0.354
$-3i+2$	13	0.657
$5i+2$	29	0.339
$-5i+2$	29	0.339
$7i+2$	53	0.307
$-7i+2$	53	-0.0971
$9i+2$	$5\cdot 17$	0.597
$-9i+2$	$5\cdot 17$	2.01
$2i+3$	13	0.657
$-2i+3$	13	-0.354
$4i+3$	5^2	0.960
$-4i+3$	5^2	0.152
$6i+3$	$3^2\cdot 5$	29.4
$-6i+3$	$3^2\cdot 5$	30.4
$8i+3$	73	-0.227
$-8i+3$	73	-0.0253
$i+4$	17	-0.215
$-i+4$	17	1.40
$3i+4$	5^2	0.152
$-3i+4$	5^2	0.960
$5i+4$	41	0.278
$-5i+4$	41	0.884
$7i+4$	$5\cdot 13$	1.15
$-7i+4$	$5\cdot 13$	-0.265
$9i+4$	97	-0.170
$-9i+4$	97	-0.170
$2i+5$	29	0.339
$-2i+5$	29	0.339
$4i+5$	41	0.884
$-4i+5$	41	0.278
$6i+5$	61	0.253
$-6i+5$	61	0.253
$8i+5$	89	0.126
$-8i+5$	89	-0.278
$i+6$	37	-0.455
$-i+6$	37	0.354
$3i+6$	$3^2\cdot 5$	30.4
$-3i+6$	$3^2\cdot 5$	29.4
$5i+6$	61	0.253
$-5i+6$	61	0.253
$7i+6$	$5\cdot 17$	1.40
$-7i+6$	$5\cdot 17$	0.597
$9i+6$	$3^2\cdot 13$	35.6
$-9i+6$	$3^2\cdot 13$	36.4
$2i+7$	53	-0.0971
$-2i+7$	53	0.307
$4i+7$	$5\cdot 13$	-0.265
$-4i+7$	$5\cdot 13$	1.15
$6i+7$	$5\cdot 17$	0.597
$-6i+7$	$5\cdot 17$	1.40
$8i+7$	113	0.489
$-8i+7$	113	0.287
$i+8$	$5\cdot 13$	0.341
$-i+8$	$5\cdot 13$	0.543
$3i+8$	73	-0.0253
$-3i+8$	73	-0.227
$5i+8$	89	-0.278
$-5i+8$	89	0.126
$7i+8$	113	0.287
$-7i+8$	113	0.489
$9i+8$	$5\cdot 29$	0.810
$-9i+8$	$5\cdot 29$	0.608
$2i+9$	$5\cdot 17$	2.01
$-2i+9$	$5\cdot 17$	0.597
$4i+9$	97	-0.170
$-4i+9$	97	-0.170
$6i+9$	$3^2\cdot 13$	36.4
$-6i+9$	$3^2\cdot 13$	35.6
$8i+9$	$5\cdot 29$	0.608
$-8i+9$	$5\cdot 29$	0.810
2	2^2	1.31
$2i$	4	1.31
3	3^2	39.1
$3i$	9	39.1
4	2^4	1.31
$4i$	16	1.31
5	5^2	-18.2
$5i$	25	-18.2
6	$2^2\cdot 3^2$	20.9
$6i$	36	20.9
7	7^2	14.6
$7i$	49	14.6
8	2^6	1.31
$8i$	64	1.31
9	3^4	39.1
$9i$	81	39.1

Appendix C

Code

C.1 Sagemath for generating the dynamics of finite elliptic curve endomorphisms

C.1.1 Functions: trees, cycles and lists

p-Frobenius element

```
def frob(E,q):
    m = E.cardinality();
    d=(q+1-m)^2-4*q
    frob = (q+1-m+sqrt(d))/2;
    return frob
```

α-decomposition of $\pi_p - 1$

```
def decomp(I,alpha): #the alpha-decomposition of I=frob_p - 1
    K.<a> = NumberField(x^2+1) #make flexible?
    f = K.factor(alpha)

    Ic = K.ideal(1)
    It = K.ideal(1)

    l = len(f)

    for k in range(l):
        while f[k][0].divides(I):
            I = I/f[k][0]
            It = It*f[k][0]

    Ic = I
    return It,Ic
```

Generating cycles

```
def cyclesQ(Ic,alpha): #cycles without ramification distinction
    K.<a> = NumberField(x^2+1)
    H = []
    fact = K.factor(Ic)
    for k in range(len(fact)):
            H.append(range(fact[k][1]+1))
    H = list(itertools.product(*H)) #reorganizing H: all combinations (h_i)_i
    data = []
    for k in range(len(H)):
        lstn = []
        lsts = []

        for i in range(len(H[k])):
            B_i = fact[i][0]
            p_i = B_i.smallest_integer()
            e_i = fact[i][1]

            h_i = H[k][i]

            if h_i==0:
                n_h_i=1
            else:
                n_h_i = norm(B_i)^(h_i)-norm(B_i)^(h_i-1)

            lstn.append(n_h_i)

            v=1
            while not (B_i^(h_i)).divides(K.ideal(alpha^v-1)):
                v += 1
            s_h_i = v
            lsts.append(s_h_i)




        n_h = prod(lstn)
        s_h = LCM_list(lsts) #order of alpha mod B^h


        data.append([s_h,n_h,n_h/s_h])
    return data
```

Generating reduced cycles

```
def cyclesQreduced(Ic,alpha): #cycles but reduced
    lst = cyclesQ(Ic,alpha)
    lst2 = []
    data2= []

    lst2.append([x[0] for x in lst])
    lst2=lst2[0]
```

```
    from collections import OrderedDict
    data = list(OrderedDict.fromkeys(lst2))

    data2.append([[x] for x in data])
    data2=data2[0]

    for l in data2:
        nh = 0
        for k in lst:
            if l[0]==k[0]:
                nh += k[1]
        l.append(nh/l[0])
    return data2
```

Generating trees

```
def trees(It,alpha):
    K.<a> = NumberField(x^2+1)
    lst = []
    fact = K.factor(Ic)
    alpha = K.factor(alpha)
    for k in range(len(alpha)):
        B = alpha[k][0]
        f = alpha[k][1]
        e=0
        I=It
        while B.divides(I):
            I = I/B
            e += 1
        lst.append(ceil(e/f))
    d = max(lst)


    klist = []
    for k in range(len(alpha)):
        B = alpha[k][0]
        f = alpha[k][1]
        e=0
        while B.divides(It):
            It = It/B
            e += 1


        prod1 =[]
        prod2 = []
        preim = []

        for h in range(1,d+1):
            mh = min(f*h,e)
            mh2 = min(f*(h-1),e)

            nh1 = norm(B^mh)
```

```
            nh2 = norm(B^(mh2))

            preimh = norm(B^min(f,mh))

            prod1.append(nh1)
            prod2.append(nh2)
            preim.append(preimh)

        klist.append([prod1,prod2,preim])

    preim = []
    vh = []

    for h in range(1,d+1):
        preimx = []
        prd1=[]
        prd2=[]
        for i in range(len(klist)):
            prd1.append(klist[i][0][h-1])
            prd2.append(klist[i][1][h-1])
        vh.append(prod(prd1) - prod(prd2))

        for i in range(len(klist)):
            preimx.append(klist[i][2][h-1])
        preim.append(prod(preimx))


    return d,vh,preim
```

Creating lists for various plots

```
def create_list(alpha):


    K.<a> = NumberField(x^2+1)


    rows = []


    for k in range(1,1000):

        q = Primes().unrank(k)
        lst = []
        E1 = EllipticCurve(GF(q),[-1,0])
        if E1.is_ordinary():
                    lst.append(q)

                    P = K.ideal(frob(E1,q)-1)
                    It,Ic = decomp(P,alpha)

                    lst.append(It)
```

```
                    lst.append(Ic)
                    lst.append(norm(It))
                    lst.append(norm(Ic))


                    cycQr = cyclesQreduced(Ic,alpha)

                    cycle_lengths = []
                    number_of_cycles = 0
                    for cycle in cycQr:
                        cycle_lengths.append(cycle[0])
                        number_of_cycles += cycle[1]
                    max_cycle_lenght = max(cycle_lengths)

                    lst.append(cycQr)

    #lst.append(numerical_approx(max_cycle_lenght/sqrt(q),digits=2))
    #lst.append(numerical_approx(sum(cycle_lengths)/
        #(float(len(cycle_lengths))*sqrt(q)),digits=2))
    #lst.append(numerical_approx(number_of_cycles/sqrt(q),digits=2))

                    lst.append(simplify(max_cycle_lenght/norm(Ic)))

    #lst.append(numerical_approx(max_cycle_lenght/norm(Ic),digits=2))

    #st.append(simplify(sum(cycle_lengths)/(float(len(cycle_lengths))*norm(Ic))))
    #lst.append(numerical_approx(sum(cycle_lengths)/
        #(float(len(cycle_lengths))*norm(Ic)),digits=2))


    #lst.append(numerical_approx(number_of_cycles/norm(Ic),digits=2))

    #lst.append(numerical_approx(norm(Ic)/number_of_cycles,digits=2))
    #av number of points in cycles
    #lst.append(numerical_approx(norm(Ic)/(number_of_cycles*sqrt(q)),digits=2))

    #lst.append(simplify(1/number_of_cycles))
     #...av number of points in cycles, normalised
    #lst.append(numerical_approx(1/number_of_cycles,digits=2))


                    rows.append(lst)
                    save(rows,str(alpha)+'-listR')
```

C.1.2 δ table

Example for odd case

```
#congruences 1/N(It) testing, odd case

lst_odd = []
```

```
for k in range(1,10):
    for l in range(1,10):
        T=0
        alpha = k+l*i
        if int(norm(alpha)) %2 == 1:

            n = int(norm(alpha))
            x = prime_factors(n)
            prod1 = 1
            prod2 = 1
            for w in range(len(x)):
                if x[w] != 2:
                    prod1 = prod1*(x[w]-2)
                    prod2 = prod2*(x[w]-1)
            x = prod1/(prod2)

            rows=load(str(alpha)+'-listR')

            for j in range(495):
                if rows[j][3]==1:
                    T += 1
            lst_odd.append([alpha,x,numerical_approx(x, digits=3),T,T/495,numerical_approx(T


            T = 0
            alpha = k-l*i

            n = int(norm(alpha))
            x = prime_factors(n)
            prod1 = 1
            prod2 = 1

            for w in range(len(x)):
                if x[w] != 2:
                    prod1 = prod1*(x[w]-2)
                    prod2 = prod2*(x[w]-1)
            x = prod1/(prod2)
            rows=load(str(alpha)+'-listR')

            for j in range(495):
                if rows[j][3]==1:
                    T += 1
            lst_odd.append([alpha,x,numerical_approx(x, digits=3),T,T/495,numerical_approx(T

lst_odd
```

C.1.3 Plots

Plot example

```
rows = load('2*I + 6-listR') ### plotting
```

```
lst = []
for k in range(len(rows)):
    q = rows[k][0]
    lst.append([k,rows[k][6]])

list_plot(lst)
```

Average plot example

```
lst = [] ### plot for average instances of l/N(I_c) <=1/8 in p, odd case


for j in range(495):
    T=0
    for k in range(1,10):
        for l in range(1,10):
            alpha = k+l*i
            if int(norm(alpha)) %2 == 1:

                rows=load(str(alpha)+'-listR')

                if rows[j][6]<=1/8:
                    T += 1

                alpha = k-l*i


                rows=load(str(alpha)+'-listR')

                if rows[j][6] <= 1/8:
                    T += 1

    lst.append([j,T/80])

list_plot(lst)
```

C.1.4 Graphs

```
def quad(q):
    var('x')
    return solve_mod(x^2==-1,q)[1][0]


def create_graph(E):
    G = Graph(loops = True,multiedges=True);

    for P in E.points():
        G.add_vertex(name = P);

    for P in E.points():
        if P[2]!= 0:
```

```
            x=P[0]
            y=P[1]
            V=E(-x,quad(q)*y)
            R=(P+2*V) #function part, can make flexible
            G.add_edge(P,R)
        else:
            G.add_edge(P,P)
    return G
```

Getting string for Graphviz

```
q=17          ### creating graph pictures
K.<a> = NumberField(x^2+1)
E = EllipticCurve(GF(q),[1,0])

G=create_graph(E)

str = G.graphviz_string()

str = str.replace('\n', '')
str.replace('graph {', 'graph {layout = neato; node [shape="point"];')
```

C.2 Mathematica: $\mathbb{F}_{83}$ picture

```
<< FiniteFields`

t = TimeUsed[];
For[r = 1, r <= 1, r++,
  p = 83;
  fld = GF[p, {-2, 1}];
  PowerListQ[fld] = True;
  PowerListQ[GF[p, {-2, 1}]] = True;
  p1 = FieldExp[fld, 1];


  p1list = {};

  ellist = Table[p1^i, {i, 1, p^r - 1}];
  squarelist = ellist^2;

  For[i = 0, i <= p^r - 1, i++,
   If[i == 0, x = 0;, x = p1^i];
    If[ x^3 + 56*x + 34 == 0, AppendTo[p1list, {x, 0}]];
    If[MemberQ[squarelist, x^3 + 56*x + 34] == True ,
     AppendTo[
       p1list, {x,
        p1^Position[squarelist, x^3 + 56*x + 34][[1, 1]]}] &&
      AppendTo[
       p1list, {x, -p1^(Position[squarelist, x^3 + 10*x + 19][[1,
            1]]) }]];
    ;
```

```
 ];
Print[Length[p1list]];


g[x_] :=
 4*x^17 + 38*x^16 - 31*x^15 - 35*x^14 - 4*x^13 + 38*x^12 -
  38*x^11 - 40*x^10 + 32*x^9 + 8*x^8 - 32*x^7 - 4*x^6 + 4*x^5 -
  26*x^4 - 2*x^3 - 39*x^2 + 33*x + 5;
h[x_] :=
 x^16 - 32*x^15 - 39*x^14 + 19*x^13 + 36*x^12 + 8*x^11 + 41*x^10 -
  8*x^9 - 32*x^8 - 16*x^7 - 41*x^6 - 13*x^5 - 3*x^4 + 5*x^3 +
  3*x^2 - 10*x + 23;

v[x_, y_] :=
 y*(8*x^24 + 31*x^23 + 30*x^22 - 40*x^21 - 33*x^20 - 24*x^19 +
    5*x^18 - 30*x^17 - 20*x^16 + 40*x^15 + 39*x^14 - 9*x^13 -
    3*x^12 + 20*x^11 + 19*x^10 - 29*x^9 + 15*x^8 + 17*x^7 -
    19*x^6 - 13*x^5 - 7*x^4 - 24*x^3 + 38*x^2 + 5*x - 28);
u[x_, y_] :=
 x^24 + 35*x^23 + 35*x^22 - 17*x^21 + 18*x^20 + 25*x^19 + 27*x^18 -
  34*x^17 + 2*x^16 - 17*x^15 + 9*x^14 + 7*x^12 - 8*x^11 + 4*x^10 -
  36*x^9 + 37*x^8 - 41*x^7 + 23*x^5 + 18*x^4 + 14*x^3 + 11*x^2 +
  19*x - 7;


glist = {};
For[i = 1, i <= Length[p1list], i++,
 s = p1list[[i, 1]] ;
 t = p1list[[i, 2]];
 Print[s, t];

 a = g[s];
 b = h[s];
 c = v[s, t];
 d = u[s, t];

 Print[a/b, c/d];

 If[TrueQ[Or[b == 0, d == 0]], j = \[Infinity],
  j = Position[p1list, {a/b, c/d}][[1, 1]]];

 AppendTo[glist, i -> j];
 ];



AppendTo[glist, \[Infinity] -> \[Infinity]];
Print[{p, r}];
glist = Sort[glist, #1[[2]] < #2[[2]] &];
graph =
 GraphPlot[glist, VertexLabeling -> False, DirectedEdges -> False,
  PlotStyle -> {Black, Thickness[0.004]}, ImageSize -> 1024,
```

```
  BaselinePosition -> Top,
  PackingMethod -> "ClosestPackingCenter"];
Print[graph];
Export[
 "Elliptic" <> "_" <> ToString[p] <> "_" <> ToString[r] <> ".pdf",
 graph];
Print[TimeUsed[] - t];

];
```

References

[AM69] M. F. Atiyah and I. G. Macdonald. *Introduction to commutative algebra*. Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969, pp. ix+128.

[Bol01] Béla Bollobás. *Random graphs*. Second. Vol. 73. Cambridge Studies in Advanced Mathematics. Cambridge University Press, Cambridge, 2001, pp. xviii+498.

[BCH20] Jakub Byszewski, Gunther Cornelissen, and Marc Houben. "Dynamically affine maps in positive characteristic". In: *Dynamics: topology and numbers*. Vol. 744. Contemp. Math. With Appendix B by the authors and Lois van der Meijden. Amer. Math. Soc., Providence, RI, 2020, pp. 125–156.

[İna+07] İlker İnam, Gökhan Soydan, Musa Demirci, Osman BiZim, and İsmail Naci Cangül. "Corrigendum on: "The number of points on elliptic curves $E\colon y^2 = x^3 + cx$ over $\mathbb{F}_p$ mod 8" [Commun. Korean Math. Soc. **18** (2003), no. 1, 31–37; MR1959227] by H. Park, D. Kim and E. Lee". In: *Commun. Korean Math. Soc.* 22.2 (2007), pp. 207–208.

[JK13] Wonju Jeon and Daeyeoul Kim. "The number of points on elliptic curves $y^2 = x^3 + Ax$ and $y^2 = x^3 + B^3$ mod 24". In: *Commun. Korean Math. Soc.* 28.3 (2013), pp. 433–447.

[KKP08] Daeyeoul Kim, Ja Kyung Koo, and Yoon Kyung Park. "On the elliptic curves modulo p". In: *J. Number Theory* 128.4 (2008), pp. 945–953.

[Len96] H. W. Lenstra Jr. "Complex multiplication structure of elliptic curves". In: *J. Number Theory* 56.2 (1996), pp. 227–241.

[PKL03] Hwasin Park, Daeyeoul Kim, and Eunhee Lee. "The number of points on elliptic curves $E\colon y^2 = x^3 + cx$ over $\mathbb{F}_p$ mod 8". In: *Commun. Korean Math. Soc.* 18.1 (2003), pp. 31–37.

[QR19] Claudio Qureshi and Lucas Reis. "Dynamics of the a-map over residually finite Dedekind domains and applications". In: *J. Number Theory* 204 (2019), pp. 134–154.

[Sil94] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*. Vol. 151. Graduate Texts in Mathematics. Springer-Verlag, New York, 1994, pp. xiv+525.

[Sil09] Joseph H. Silverman. *The arithmetic of elliptic curves*. Second. Vol. 106. Graduate Texts in Mathematics. Springer, Dordrecht, 2009, pp. xx+513.

[Ste02] Peter Stevenhagen. *Voortgezette Getaltheorie*. 2002. URL: `https://www.math.leidenuniv.nl/~psh/VGT.pdf`.

[Ugo18] S. Ugolini. "Functional graphs of rational maps induced by endomorphisms of ordinary elliptic curves over finite fields". In: *Period. Math. Hungar.* 77.2 (2018), pp. 237–260.

[Wan03] Zhe-Xian Wan. *Lectures on finite fields and Galois rings*. World Scientific Publishing Co., Inc., River Edge, NJ, 2003, pp. x+342.

[Wit01] Christian Wittmann. "Group structure of elliptic curves over finite fields". In: *J. Number Theory* 88.2 (2001), pp. 335–344.