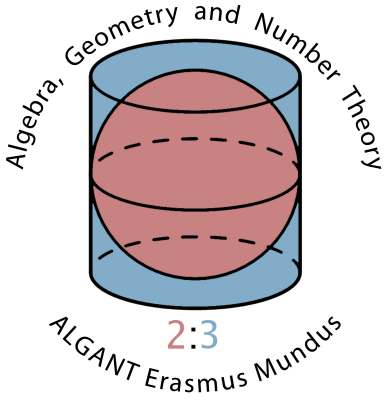
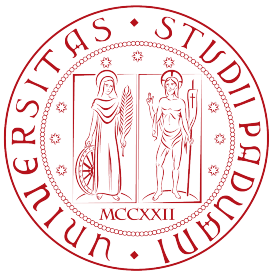


ALGANT Master Thesis in Mathematics

CYCLIC REDUCTION OF ELLIPTIC CURVES

Francesco Campagna

Advisor: Prof. Peter Stevenhagen



UNIVERSITÀ DEGLI STUDI
DI PADOVA

UNIVERSITEIT
LEIDEN

Academic year 2017/2018
25 June 2018

Acknowledgements

The first person that I want to thank is my supervisor Prof. Dr. Peter Stevenhagen: thank you for the beautiful topic that you allowed me to study, for all the patience you had with me and for all the enthusiasm that you were able to convey. Sorry for all the times you arrived late at lunch!
Then I would like to express my gratitude to my family who supported me (also financially) when I was abroad and without whom this experience wouldn't have been possible.
The Leideners: Angela, Matteo, Sergej, Sebastiano, Alessandra, Linda, Francesca, Ilaria, Giulio, Mansi, Laura, Nadine, Sara and all the others. Thank you for all the unforgettable days spent together (and thank you Matteo for fixing all my Latex problems, there is a piece of you in this thesis).
Finally to all the very italian people who supported me and are too many to be mentioned: thank you!

Introduction

An elliptic curve E defined over a number field K is the locus of an equation of the form

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

where $A, B \in \mathfrak{O}_K$ are such that $-16(4A^3 + 27B^2) \neq 0$, together with a point at infinity O given in projective coordinates by $[0 : 1 : 0]$. Given a prime ideal $\mathfrak{p}$ of K we can reduce the equation of E modulo $\mathfrak{p}$, obtaining in this way the equation of a new curve $\tilde{E}(k_\mathfrak{p})$ on the residue field $k_\mathfrak{p} := \mathfrak{O}_K/\mathfrak{p}$. Just for finitely many primes this curve will be singular: these are called primes of bad reduction. For all the other prime ideals (the primes of good reduction) the reduced curve $\tilde{E}(k_\mathfrak{p})$ is an elliptic curve and, as such, the set of points on it carries a natural structure of finite abelian group. It is a standard result in the theory of elliptic curves that this group is abelian on at most two generators i.e. it is either cyclic or isomorphic to the product of two cyclic groups of non-coprime order. The question that we address in this thesis is the following:

Question: for how many primes $\mathfrak{p}$ of K the elliptic curve E has good reduction and the reduction of E modulo $\mathfrak{p}$ is cyclic? Are they infinitely many? If so, does the set of primes of cyclic reduction for E have a density?

As we shall see, this question resembles a classical problem in number theory called Artin's primitive root conjecture. The problem is the following: given a a non-zero integer, for how many primes p is $a \bmod p$ a primitive root, that is a generator of the cyclic group $\mathbb{F}_p^*$? Using algebraic number theory one can see that whether a is a generator modulo p of $\mathbb{F}_p^*$ depends on the splitting behaviour of p in the extension $\mathbb{Q}(\sqrt[l]{a}, \zeta_l)$ where l is a prime number and ζ_l denotes a primitive l-th root of unity. In 1966 Cristopher Hooley proved, under the assumption of the Generalized Riemann Hypothesis, that the density of the set of primes for which a is a primitive root is

$$\delta(a) = \sum_{m=1}^{\infty} \frac{\mu(m)}{[\mathbb{Q}(\sqrt[m]{a}, \zeta_m) : \mathbb{Q}]}$$

where $\mu(m)$ denotes the Möbius μ-function on the integers. Following Hooley's proof, J. P. Serre was able, modulo GRH, to give an analogous formula for the density of the set of rational primes for which a given elliptic curve defined over $\mathbb{Q}$ has cyclic reduction (see [17]). In this thesis we generalize Serre's proof for an elliptic curve defined over an arbitrary number field.

In chapter 1 we introduce the cyclic reduction problem for an elliptic curve starting form Artin's primitive root problem. We recall here the basic definitions and results concerning natural densities and elliptic curves, and we will also provide some numerical computations. In chapter 2 we prove, under the Generalized Riemann Hypothesis, a formula for the density of the set of primes in a number field K for which a given elliptic curve E defined over K has cyclic reduction. The proof will make use of analytic number theory. In chapter 3 we are able to factor

the found density into a finite sum and an infinite product which never vanishes. This shows that the vanishing of the density depends only on a finite computation. As we will see, the fact that the base field contains the full l-torsion of an elliptic curve for some prime l causes the vanishing of the density. In chapter 4 we exhibit an infinite family of examples of elliptic curves for which the density is zero but their field of definition does not contain the full l-torsion for any prime l. Finally in chapter 5 we discuss some numerical examples.

Contents

Chapter 1

Primitive root problems

In this chapter we discuss a family of problems from which this thesis arises, the so called primitive root problems. First we talk about the classical Artin primitive root conjecture and then we move to similar conjectures for elliptic curves. In both cases the problems can be studied by analyzing the splitting of primes of a number field K in an infinite family of finite extensions of K.

1.1 The multiplicative primitive root problem

Let a be an integer and p a prime number not dividing a. It is known that the multiplicative group $\mathbb{F}_p^*$ of the finite field $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ is cyclic. For $a \in \mathbb{F}_p^*$ we denote by $\mathrm{ord}_{\mathbb{F}_p^*}(a)$ the multiplicative order of a in $\mathbb{F}_p^*$.

Definition 1.1.1. *We say that a is a primitive root modulo p if $a \bmod p$ generates $\mathbb{F}_p^*$, i.e. $\langle a \bmod p \rangle = \mathbb{F}_p^*$.*

Example. The integer 2 is a primitive root modulo 5 and modulo 13.

The problem of determining the prime numbers p for which a given integer a is a primitive root modulo p is already mentioned, for the particular case $a = 10$, by Gauss in his "Disquisitiones Arithmeticae" (see [2] art. 49). In his study of the periodical decimal expansions of fractions with denominator p, Gauss asked why the decimal expansion of $1/7$ has period length 6 ($1/7 = 0.\overline{142857}$) while $1/11$ has period lenght only 2 ($1/11 = 0.\overline{09}$). These questions have a formulation in terms of primitive roots.

Lemma 1.1.2. *Let p be a prime number different from $2, 5$ and let k be the (minimal) period of the decimal expansion of $\frac{1}{p}$. Then $k = \mathrm{ord}_{\mathbb{F}_p^*}(10)$.*

Proof. Since $p \neq 2, 5$, the reduction $10 \bmod p$ is in $\mathbb{F}_p^*$. Let $k := \mathrm{ord}_{\mathbb{F}_p^*}(10)$. Then there exists an integer b such that

$$\frac{1}{p} = \frac{b}{10^k - 1}.$$

Using the geometric series we can write

$$\frac{1}{p} = \frac{b}{10^k - 1} = \frac{b \cdot 10^{-k}}{1 - 10^{-k}} = \sum_{j=1}^{\infty} b 10^{-jk}$$

and this shows that k is a period of $1/p$. Conversely if there exists $k' \leq k$ such that $1/p$ is periodic of period k', then writing

$$\frac{1}{p} = 0.\overline{b_1 \dots b_{k'}} \qquad b_1, ..., b_{k'} \in \{0, ..., 9\}.$$

we deduce that $10^{k'} \equiv 1 \bmod p$, so $k \leq k'$. Hence $k = k'$ and this completes the proof.

□

The lemma above shows that for $p \neq 2, 5$, the length of the period in the decimal expansion of $1/p$ is precisely the multiplicative order of $10 \in \mathbb{F}_p^*$. In particular the decimal expansion of $1/p$ is the longest possible precisely when 10 is a primitive root $\bmod\ p$. Of course the same argument can be repeated by replacing 10 with a different base $B > 1$. In this case the result of lemma 1.1.2 can be restated as follows: let B be an integer and p a prime number not dividing B. If k is the (minimal) period of the base B expansion of $\frac{1}{p}$ then $k = \mathrm{ord}_{\mathbb{F}_p^*}(B)$.

We see that these simple observations give rise to a number of interesting questions: how often is 10 a primitive root $\bmod\ p$? Is it a primitive root for infinitely many primes? More generally, given an integer a, is it true that a is a primitive root modulo infinitely many primes? To understand better what the answer to these questions should be, we can do some numerical experiments for different integers and primes up to 10^6: for an integer a let

$$P(a) := \frac{\#\{p \leq 10^6 \text{ prime} : \langle a \bmod p \rangle = \mathbb{F}_p^*\}}{\#\{p \text{ prime} : p \leq 10^6\}} = \frac{\#\{p \leq 10^6 \text{ prime} : \langle a \bmod p \rangle = \mathbb{F}_p^*\}}{78498}.$$

$P(a)$ is the fraction of primes up to 10^6 for which a is a primitive root. We collect data for $P(a)$ in the following table; the values of $P(a)$ have been given rounded to four decimal digits.

a	**Number of primes for which a is a primitive root**	$P(a)$
-2	29438	0.3750
2	29341	0.3737
4	0	0
5	30885	0.3934
6	29348	0.3739
10	29500	0.3758
11	29433	0.3749

TABLE 1.1: How often a is a primitive root modulo p for $p < 10^6$ for some integers a.

What we notice immediately from the table above is that when $a \neq 4, 5$ all the values of $P(a)$ are approximatly 0.374. The integer 4 is never a primitive root modulo p for any prime $p \leq 10^6$: this is clear because 4 is a square so it is a square also modulo all the primes. But except for $p = 2$, the index $|\mathbb{F}_p^* : (\mathbb{F}_p^*)^2|$ is always 2, so squares can never (except possibly for $p = 2$) be primitive roots modulo p. This suggests that perfect powers may behave differently from the other numbers. We give some numerical data for cubes.

a	**Number of primes for which a is a primitive root**	$P(a)$
8	17623	0.2245
27	17621	0.2244
125	18537	0.2361
343	17674	0.2251

TABLE 1.2: How often a is a primitive root modulo p for $p < 10^6$ for some cubes a

When $a \neq 125$, all the values of $P(a)$ seem to be approximately 0.224. The integer 125, as 5 before, appears to behave differently. Notice that both of them are congruent to 1 modulo 4. We give some data for integers congruent to 1 modulo 4.

a	**Number of primes for which a is a primitive root**	$P(a)$
-7	30089	0.3833
-3	35324	0.4499
5	30885	0.3934
125	18537	0.2361

TABLE 1.3: How often a is a primitive root modulo p for $p < 10^6$ for some $a \equiv 1 \bmod 4$

As the table shows, there is no clear pattern for the values of $P(a)$ when the integer a is congruent to 1 modulo 4. These values seem to behave differently even from each other.

The value of $P(a)$ above is not completely satisfactory: it depends on the bound 10^6 that we have taken for our computation. Of course increasing the bound will give us a better picture of the situation. This suggests that the right quantity to consider is:

$$A(a) = \lim_{x \to \infty} \frac{\#\{p \leq x \text{ prime} : \langle a \bmod p \rangle = \mathbb{F}_p^*\}}{\#\{p \text{ prime} : p \leq x\}}$$

if the limit exists. The quantity $A(a)$ is the density of the primes for which the integer a is a primitive root. The tables above show that this density, if it exists, should depend on whether the integer a is a perfect power or it is congruent to 1 modulo 4.

1.2 Artin's Primitive Root Conjecture

As we already noticed in the previous section, if an integer a is a square then it is never a primitive root modulo p for every $p > 2$. Hence

$$a \text{ square } \Rightarrow A(a) = 0.$$

Of course the same happens if $a = \pm 1, 0$. What about the other cases? Tables 1.1-1.3 seem to show that at least there are infinitely many primes for which a is a primitive root. Emil Artin studied the problem for $a = 2$ and in 1927 proposed the following conjecture.

Conjecture 1.2.1 (Artin's Primitive Root Conjecture)**.** *Let $a \neq \pm 1$ be a non-zero integer that is not a square. Then there exist infinitely many primes p for which a is a primitive root modulo p. Moreover if we write $a = b^n$ with $b \in \mathbb{Z}$ not a perfect power*

then the density $A(a)$ exists and its value is

$$A(a) = \prod_{l \nmid n} \left(1 - \frac{1}{l(l-1)}\right) \prod_{l \mid n} \left(1 - \frac{1}{l-1}\right).$$

Before explaining how Artin conjectured the above value of the density we want to compare Artin's conjectured density with the numerical data given in the previous section. For $a = 2$ the expected value of the density according to the conjecture is:

$$A(2) = \prod_{l \text{ prime}} \left(1 - \frac{1}{l(l-1)}\right) \approx 0.373955838964330$$

which agrees with the value given in table 1.1. However if $a = -3$ or $a = 5$ then according to Artin conjecture we should have

$$A(-3) = A(5) = A(2) \approx 0.373955838964330$$

which does not agree with the data $P(-3) \approx 0.449998$ and $P(5) \approx 0.393449514$ given in table 1.3. Again integers congruent to 1 modulo 4 seem to behave differently. To explain this phenomenon we give Artin's heuristic argument that leads to the conjecture above.

Let $a, p \in \mathbb{Z}$ with p a prime number not dividing $2a$. We claim that a is a primitive root $\bmod\ p$ if and only if

$$a^{\frac{p-1}{l}} \not\equiv 1 \pmod{p}.$$

for every prime divisor l of $p-1$. The "only if" part is clear. Conversely if k is the order of $a \bmod\ p$ then $k \mid p-1$ and if $k \neq p-1$ then there exists a prime number l dividing $p-1$ such that $k \mid \frac{p-1}{l}$.

The claim above shows that a is a primitive root $\bmod\ p$ if and only if the two "events"

$$\begin{cases} p \equiv 1 \pmod{l} \\ a^{\frac{p-1}{l}} \equiv 1 \pmod{p} \end{cases} \tag{1.1}$$

do not occur simultaneously for any prime l. Artin realized that the two conditions of 1.1 can be stated in terms of the splitting behaviour of p in a finite extension of $\mathbb{Q}$. We need a lemma.

Lemma 1.2.2. *Let a be an integer and p, l primes such that $p \nmid 2a$. Then*

$$\begin{cases} p \equiv 1 \pmod{l} \\ a^{\frac{p-1}{l}} \equiv 1 \pmod{p} \end{cases} \Leftrightarrow \quad p \text{ splits completely in } F_l$$

where $F_l = \mathrm{Split}_{\mathbb{Q}}(x^l - a) = \mathbb{Q}(\zeta_l, \sqrt[l]{a})$ with ζ_l a primitive l-th root of unity.

Proof. The conditions $p \equiv 1 \bmod\ l$ and $a^{\frac{p-1}{l}} \equiv 1 \bmod\ p$ together are equivalent to the condition $l \mid |\mathbb{F}_p^* : \langle a \bmod\ p \rangle|$. This means precisely that the group $\mathbb{F}_p^*$ contains a primitive l-th root of unity as well as an l-th root of a. Since the condition $p \nmid 2a$ implies that p does not ramify in F_l, this is equivalent to p splitting completely in F_l. □

Corollary 1.2.3. *Let $a \in \mathbb{Z} \setminus \{\pm 1\}$ be a nonzero integer and let p be a prime number not dividing $2a$. Then a is a primitive root modulo p if and only if for every prime $l < p$, the prime p does not split completely in any extension $F_l = \mathbb{Q}(\zeta_l, \sqrt[l]{a})$ of $\mathbb{Q}$.*

The corollary above says that, apart from finitely many primes, finding the primes p for which a is a primitive root modulo p is equivalent to finding the primes p that do not split completely in any field F_l with $l < p$ prime. Checking this conditions for all the rational primes clearly involves an infinite number of verifications to be done.

Since adding or removing a finite number of primes to a set does not change the density of the set itself, we deduce the following.

Proposition 1.2.4. *Let $a \in \mathbb{Z} \setminus \{\pm 1\}$ be a non zero integer. The density of the set of primes p for which a is a primitive root modulo p is equal to the density of the set of primes that do not split completely in any extension $F_l/\mathbb{Q}$, for every l prime.*

We can now understand how Artin was able to conjecture the value of the density $A(a)$. If $K/\mathbb{Q}$ is a normal extension, then a theorem of Chebotarev (the so called Chebotarev Density Theorem, see for instance [21]) implies that the density of the set of primes p that split completely in K is $\frac{1}{[K:\mathbb{Q}]}$ (for a precise notion of density see the next paragraph). The fields F_l for l prime are all Galois extensions of $\mathbb{Q}$ because they are splitting fields of the polynomials $x^l - a$. Hence by the Chebotarev Density Theorem, the density of the set of primes that do not split completely in F_l is

$$1 - \frac{1}{[F_l : \mathbb{Q}]}.$$

Assuming the conditions "not splitting completely in F_l" independent for all l, we would then expect the density of the primes p for which $a \in \mathbb{Z}\setminus\{\pm 1, 0\}$ is a primitive root $\bmod\ p$ to be

$$\prod_{l \text{ prime}} \left(1 - \frac{1}{[F_l : \mathbb{Q}]}\right).$$

Since $[F_l : \mathbb{Q}] = l(l-1)$ if a is not an l-th power and $[F_l : \mathbb{Q}] = l - 1$ otherwise, writing $a = b^n$ with $b \in \mathbb{Z}$ not a perfect power, we obtain the formula that appears in 1.2.1:

$$A(a) = \prod_{l \nmid n} \left(1 - \frac{1}{l(l-1)}\right) \prod_{l \mid n} \left(1 - \frac{1}{l-1}\right). \tag{1.2}$$

The problem in this heuristic argument is that the conditions for a prime p to "not split completely in $\mathbb{F}_l$" are in general not independent for different primes l. We give two examples.

Example. Let $a = 5$: in this case $F_2 = \mathbb{Q}(\sqrt{5})$ and algebraic number theory implies that

$$F_2 \subseteq \mathbb{Q}(\zeta_5) \subseteq \mathbb{Q}(\zeta_5, \sqrt[5]{5}) = F_5.$$

So in this case if a prime does not split completely in F_2 then it would not split completely in F_5. This means that for a given prime p, verifying that it does not split completely in F_2 is sufficient to conclude that it does not split completely also in F_5. Then the factor

$$1 - \frac{1}{[F_5 : \mathbb{Q}]} = 1 - \frac{1}{20} = \frac{19}{20}$$

which appears in the infinite product for $A(5)$ as in 1.2 is redundant and should be removed. So a corrected density in this case is

$$\frac{20}{19} A(5) \approx 0.393637724$$

which agrees with the figure in table 1.3.

Example. When $a = -3$ the correction factor is even bigger than in the previous example. In this case we have

$$F_2 = \mathbb{Q}(\sqrt{-3}) \subseteq \mathbb{Q}(\zeta_3) \subseteq \mathbb{Q}(\zeta_3, \sqrt[3]{-3}) = F_3$$

so we have to remove the factor

$$1 - \frac{1}{[F_3 : \mathbb{Q}]} = 1 - \frac{1}{6} = \frac{5}{6}$$

from the infinite product for $A(-3)$ as in 1.2. So a corrected density in this case is

$$\frac{6}{5} A(-3) \approx 0.448747$$

which agrees with the figure in table 1.3.

The problem in Artin's heuristic argument is that the fields F_l may be related in some way, so that knowing the splitting of a prime in one of the fields can automatically give information on the splitting of the same prime in another field. This problem was first spotted in a correspondence between Artin and Lehmer between 1957-1958 (see [20] for more details). When $D := \operatorname{disc}(\mathbb{Q}(\sqrt{a})/\mathbb{Q}) \equiv 1 \bmod 4$ there is always a relation between the fields F_l, l prime: indeed, algebraic number theory tells us that in this case we have the inclusions

$$\begin{aligned} F_2 = \mathbb{Q}(\sqrt{a}) = \mathbb{Q}(\sqrt{D}) &\subseteq \mathbb{Q}(\zeta_{|D|}) \\ &\subseteq \operatorname{Compositum}(\mathbb{Q}(\zeta_l, \sqrt[l]{a}) : l \mid D) = \operatorname{Compositum}(F_l : l \mid D) \end{aligned}$$

where all the fields F_l with $l \mid D$ are different from $\mathbb{Q}(\sqrt{D})$ since $D \equiv 1 \bmod 4$. However it is possible to show that this is the only case in which these fields are related.

What prevents Artin's reasoning from being a proof is the fact that his argument involves a limit process: he considers the fraction of primes that do not split completely in F_l with l prime and, by multiplication, he obtains an infinite product which should represent the wanted density. Of course this limit process requires an argument. In 1966 Cristopher Hooley was able to prove Artin's primitive root conjecture with a corrected density under the assumption of Generalised Riemann Hypothesis. The Hypothesis is used to obtain sufficient control of the error terms in the density statements for the sets of primes that split completely in the fields F_l. An unconditional solution to Artin primitive root problem is still unknown.

In this thesis we study the cyclic reduction problem for elliptic curves: roughly speaking, given an elliptic curve defined over a number field K, we want to find the density of the set of primes in K for which the reduction of the elliptic curve is cyclic (more details are given in the following sections). Apparently this is very different from the multiplicative primitive root problem that we studied so far. However, as we shall see, the two problems can be tackled in the same way, by looking at the splitting of primes in certain finite extensions of K.

1.3 Preliminaries: Natural densities and Elliptic curves

Before going on with the elliptic curve analogues of the multiplicative primitive root conjectures, we want to briefly recall some basic facts and definitions concerning natural densities and elliptic curves which will be used later in the thesis. Most of the results about elliptic curves will not be proved: the standard reference for these is [19].

1.3.1 Natural densities

In this section we make precise the concept of natural density that was already introduced in the section on Artin's conjecture. In Number Theory the natural density is one of the tools which allow to measure "how large" a subset of the prime ideals in the ring of integers of a number field is. For instance, all prime numbers $p \neq 2$ are congruent to either 1 or 3 modulo 4. Intuitively, one expects half of the prime numbers to be congruent to $1 \bmod 4$ and half of them congruent to $3 \bmod 4$. The concept of natural density makes this intuition precise.

Definition 1.3.1. *Let K be a number field and S a subset of primes in $\mathfrak{O}_K$. If the limit*

$$\delta(S) := \lim_{x\to\infty} \frac{\#\{\mathfrak{p} \in S : N_{K/\mathbb{Q}}(\mathfrak{p}) \leq x\}}{\#\{\mathfrak{p} \subseteq \mathfrak{O}_K \text{ prime ideal} : N_{K/\mathbb{Q}}(\mathfrak{p}) \leq x\}}$$

exists, then we call $\delta(S)$ the natural density of S.

Notice that if $K = \mathbb{Q}$ and S is a set of rational primes, the natural density of the set S becomes

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

which is analogous to the formula that we provided in section 1.1.

In what follows we use the following notation: let $f, g : \mathbb{R} \to \mathbb{R}$ be two real-valued functions. We say that f is asymptotic to g as $x \to \infty$ if

$$\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1.$$

In this case we write $f \sim g$.

Theorem 1.3.2 (Prime number theorem for Number Fields)**.** *Let K be a number field and let $\pi_K(x)$ be the number of prime ideals in $\mathfrak{O}_K$ with norm $\leq x$. Then $\pi_K(x) \backsim \frac{x}{\log x}$ as $x \to \infty$.*

Thanks to the theorem above we can write the density of a set of primes S as

$$\delta(S) = \lim_{x\to\infty} \frac{\#\{\mathfrak{p} \in S : N_{K/\mathbb{Q}}(\mathfrak{p}) \leq x\}}{x/\log x}.$$

Lemma 1.3.3. *Let K be a number field. Then the set of primes in $\mathfrak{O}_K$ with norm p^f for some $f > 1$, has density 0.*

Proof. Let S be the set of primes in $\mathfrak{O}_K$ with norm p^f for some $f > 1$, and let

$$S_x := \{\mathfrak{p} \in S : N_{K/\mathbb{Q}}(\mathfrak{p}) \leq x\}.$$

If $\mathfrak{p} \in S_x$ then $N_{K/\mathbb{Q}}(\mathfrak{p}) = p^f \leq x$ for some rational prime p and some integer $f > 1$. This implies that $p \leq \sqrt[f]{x} \leq \sqrt{x}$.

So every prime in S_x must lie over a rational prime $\leq \sqrt{x}$ and over such a prime can lie at most n primes of $\mathfrak{O}_K$, with $n := [K : \mathbb{Q}]$ the degree of K. This implies that

$$\#S_x \leq n\sqrt{x}.$$

Hence

$$0 \leq \delta(S) = \lim_{x\to\infty} \frac{\#S_x}{x/\log x} \leq \lim_{x\to\infty} \frac{n\sqrt{x}}{x/\log x} = 0$$

and this proves the lemma. □

The lemma above shows that if a set S of primes in a number field K has a density, then this is equal to the density of the set of primes S' obtained from S by removing all the prime ideals of non-prime norm.

1.3.2 Elliptic curves: basic definitions and results

In this subsection let K be a perfect field and $\overline{K}$ an algebraic closure of K. There are several ways in which elliptic curves can be introduced. For practical purposes we suppose $\mathrm{char}(K) \neq 2, 3$ and we give the following definition.

Definition 1.3.4. *An elliptic curve E is a plane projective curve given by a homogeneous equation of the form*

$$Y^2Z = X^3 + AXZ^2 + BZ^3 \tag{1.3}$$

with $A, B \in \overline{K}$ satisfying $-16(4A^3+27B^2) \neq 0$ and the specified base point $[0 : 1 : 0]$. The quantity $\Delta_E := -16(4A^3 + 27B^2)$ is called the discriminant of the elliptic curve E. If $A, B \in K$ we say that the elliptic curve E is defined over K. We denote by $E(K)$ the set of K-rational points on E, that is, the points of E whose homogeneous coordinates can be chosen in K.

An equation of the form 1.3 is called a Weierstrass equation for the elliptic curve E. Notice that, given an elliptic curve with Weierstrass equation as above there is just one point on the line $Z = 0$, namely the base point $[0 : 1 : 0]$. This means that we can think of an elliptic curve as an affine curve given by the equation

$$y^2 = x^3 + Ax + B \tag{1.4}$$

with an additional point at infinity which we will call O. Notice that if E is defined over K and $\lambda \in K^\times$ then the map $(x, y) \mapsto (\lambda^{-2}x, \lambda^{-3}y)$ gives an isomorphism of varieties between E and the curve

$$y^2 = x^3 + \lambda^4 Ax + \lambda^6 B.$$

Hence using a change of coordinates we can always scale (A, B) to $(\lambda^4 A, \lambda^4 B)$.

The set of points of an elliptic curve E has a natural structure of abelian group with the point O as zero element (see [19] section 3.2). This means that an addition law is defined for the points of an elliptic curve. The abelian group structure can be expressed as follows: given $P, Q, R \in E$ then $P + Q + R = O$ if and only if P, Q, R are collinear. The set $E(K)$ is a subgroup of $E(\overline{K})$ with the induced group law. We denote by $[m] : E \to E$ the multiplication by m map, i.e.

$$[m]P = \underbrace{P + \cdots + P}_{m \text{ times}}.$$

Definition 1.3.5. *Let E_1 and E_2 be elliptic curves with base points O_1 and O_2 respectively. An isogeny between E_1 and E_2 is a morphism of varieties $\phi : E_1 \to E_2$ satisfying $\phi(O_1) = O_2$. We say that an isogeny is defined over K if it can be locally written using rational functions with coefficients in K.*

Example. If E is an elliptic curve then the multiplication by m map defined above is an isogeny defined over $\mathbb{Q}$ from E in itself.

Proposition 1.3.6. *Every isogeny $\phi : E_1 \to E_2$ is a group morphism.*

The first consequence of proposition 1.3.6 is that if E is an elliptic curve then

$$\mathrm{End}(E) := \{\text{isogenies defined over } \overline{K} \text{ from } E \text{ in itself}\}$$

becomes a ring: if $\phi, \psi \in \mathrm{End}(E)$ then $(\phi + \psi)(P) = \phi(P) + \psi(P)$ and $(\phi \circ \psi)(P) = \phi(\psi(P))$. We have an injection

$$\mathbb{Z} \hookrightarrow \mathrm{End}(E)$$

sending $m \mapsto [m]$. When this map is surjective we say that the elliptic curve does not have complex multiplication. Otherwise we say that the elliptic curve has complex multiplication (CM in short).

Since every morphism of curves has finite degree, proposition 1.3.6 also implies that the the kernel of a non-zero isogeny is always a finite abelian group. Let

$$E[m](\overline{K}) = \ker[m] = \{P \in E(\overline{K}) : mP = O\}.$$

The group $E[m]$ is the group of m-torsion points on E.

Example. Let $\mathrm{char}(K) \neq 2, 3$ and E/K be an elliptic curve given by a Weierstrass equation as in 1.4. In this case the addition formulas for the points on E imply that if $P = (x, y) \in E$ is an affine point then its inverse $-P$ has coordinates $-P = (x, -y)$. We want to find $E[2](\overline{K})$ i.e. the set of points $P \in E$ such that $2P = O$. Clearly $O \in E[2](\overline{K})$. For every affine point $P = (x, y) \in E[2](\overline{K})$ we have

$$2P = O \Leftrightarrow P = -P \Leftrightarrow y = 0.$$

Hence

$$E[2](\overline{K}) = \{O, (x_1, 0), (x_2, 0), (x_3, 0)\}$$

where x_i is a root of $x^3 + Ax + B$ for every $i = 1, 2, 3$. Since $E[2](\overline{K})$ is a group of order 4 and of exponent 2 it is necessarily isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Proposition 1.3.7. *Let E be an elliptic curve defined over $\overline{K}$ and let $m \in \mathbb{Z}$ with $m \neq 0$. If $m \neq 0$ in $\overline{K}$ then*

$$E[m](\overline{K}) \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$$

If $\mathrm{char}(\overline{K}) = p > 0$ then one of the following is true:

- *$E[p^e](\overline{K}) = \{O\}$ for all $e = 1, 2, 3, ...$*
- *$E[p^e](\overline{K}) \cong \mathbb{Z}/p^e\mathbb{Z}$ for all $e = 1, 2, 3, ...$*

1.3.3 Reduction of elliptic curves defined over a number field

In this subsection let K be a number field, $\mathfrak{p} \subseteq \mathfrak{O}_K$ a prime ideal and E/K an elliptic curve defined over K with Weierstrass equation $y^2 = x^3 + Ax + B$. Using the

change of coordinates illustrated in the previous section, we may always suppose that $A, B \in \mathfrak{O}_K$ (so also the discriminant Δ_E of E lies in $\mathfrak{O}_K$). Call $k_\mathfrak{p}$ the residue field $\mathfrak{O}_K/\mathfrak{p}$. We denote by $\tilde{E}(k_\mathfrak{p})$ the cubic curve in $\mathbb{P}^n(k_\mathfrak{p})$ with equation

$$y^2 = x^3 + \tilde{A}x + \tilde{B}$$

where $\tilde{A} = A \bmod \mathfrak{p}$ and $\tilde{B} = B \bmod \mathfrak{p}$. Hence the defining equation of $\tilde{E}(k_\mathfrak{p})$ is the reduction modulo $\mathfrak{p}$ of the defining equation of $E(K)$: in particular the discriminant of $\tilde{E}(k_\mathfrak{p})$ is the reduction modulo $\mathfrak{p}$ of the discriminant Δ_E of E. By definition 1.3.4 the curve $\tilde{E}(k_\mathfrak{p})$ is an elliptic curve if and only if $\mathfrak{p}$ does not divide Δ_E.

Definition 1.3.8. *A prime ideal $\mathfrak{p} \subseteq \mathfrak{O}_K$ is called a prime of bad reduction for E/K if $\mathfrak{p}$ divides the discriminant Δ_E. Otherwise $\mathfrak{p}$ is called a prime of good reduction for E/K.*

It is clear from the definition that there are only finitely many primes of bad reduction for E.

Proposition 1.3.9. *Let E/K be an elliptic curve and $\mathfrak{p}$ a prime of good reduction for E. Then the group of points of $\tilde{E}(k_\mathfrak{p})$ is either cyclic or isomorphic to the direct product of two cyclic groups.*

Proof. Let $\overline{k_\mathfrak{p}}$ be a fixed algebraic closure of $k_\mathfrak{p}$. Since $k_\mathfrak{p}$ is a finite field, also the group of points of $\tilde{E}(k_\mathfrak{p})$ is a finite group. Let $m := \#\tilde{E}(k_\mathfrak{p})$. Then for every $P \in \tilde{E}(k_\mathfrak{p})$, $[m]P = O$ so we have

$$\tilde{E}(k_\mathfrak{p}) \subseteq \tilde{E}(\overline{k_\mathfrak{p}})[m].$$

However by proposition 1.3.7 the latter group is finite, and either cyclic or isomorphic to the direct product of two cyclic groups. Hence also $\tilde{E}(k_\mathfrak{p})$ is either cyclic or isomorphic to the direct product of two cyclic groups. □

For every prime $\mathfrak{p} \subseteq \mathfrak{O}_K$ we can also define a reduction map

$$\mathrm{red} : \mathbb{P}^2(K) \to \mathbb{P}^2(k_\mathfrak{p})$$

as follows: for every point $[X : Y : Z] \in \mathbb{P}^2(K)$, we can scale its coordinates such that the new point obtained has all its coordinates in $\mathfrak{O}_K$ but not all in $\mathfrak{p}$. Hence, by reducing all the coordinates of the new point modulo $\mathfrak{p}$, we get a point in $\mathbb{P}^2(k_\mathfrak{p})$. This gives the reduction map above.

The restriction of this map to $E(K)$ has image contained in $\tilde{E}(k_\mathfrak{p})$. However the restriction map is not in general surjective.

1.3.4 Division fields

Let K be a number field, $\overline{K}$ a fixed algebraic closure of K and E/K an elliptic curve. The absolute Galois group $\mathrm{Gal}(\overline{K}/K)$ acts on the set of points $E(\overline{K})$ in the following way: if $P = [X : Y : Z] \in E(\overline{K})$ and $\sigma \in \mathrm{Gal}(\overline{K}/K)$, we define

$$\sigma(P) = [\sigma(X) : \sigma(Y) : \sigma(Z)].$$

In particular, we have $\sigma(O) = O$. The fact that the addition formulas for the points of E are rational functions with coefficients in K of their coordinates implies that

$$\sigma(P + Q) = \sigma(P) + \sigma(Q)$$

for every $P, Q \in E(\overline{K})$. So $\mathrm{Gal}(\overline{K}/K)$ fixes $E[m]$ and acts on it by group automorphisms. Thus for every $m \in \mathbb{N}$ we obtain a Galois representation

$$\mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}(E[m](\overline{K})).$$

By proposition 1.3.7 and the fact that K has characteristic 0, we know that $E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. So we actually have a map

$$\mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}(\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}) \cong \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}). \tag{1.5}$$

Definition 1.3.10. *Let K be a number field, E/K an elliptic curve and $m \in \mathbb{N}$ fixed. The m-division field over K is the field $K_m := K(E[m](\overline{K}))$, obtained by adjoining to K all the affine coordinates of the m-torsion points of E.*

Proposition 1.3.11. *For every $m \in \mathbb{N}$ the m-division field K_m is a finite Galois extension of K with Galois group isomorphic to a subgroup of $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$.*

Proof. Every field embedding $K_m \hookrightarrow \overline{K}$ sends m-torsion points to m-torsion points, so actually is a K-automorphism of K_m. Hence the extension K_m/K is Galois. The kernel of the map 1.5 is clearly $\mathrm{Gal}(\overline{K}/K_m)$, so by the first isomorphism theorem and by Galois theory we deduce that $\mathrm{Gal}(K_m/K)$ is isomorphic to a subgroup of $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$. □

In general $\mathrm{Gal}(K_m/K)$ can be isomorphic to a proper subgroup of $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$: for instance let $K = \mathbb{Q}$ and E/K be the elliptic curve defined by

$$E : y^2 = x(x-1)(x+1).$$

Then we know that $E[2] = \{O, (0,0), (1,0), (-1,0)\}$ so $K_2 = K(E[2]) = K$. In this case we have

$$\mathrm{Gal}(K_2/K) = \{1\} \subsetneq \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}).$$

We can then ask, given E as above, for how many natural numbers m the Galois group $\mathrm{Gal}(K_m/K)$ is isomorphic to the full $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$. For non-CM curves an answer is given by a well-known theorem of Serre called "open image theorem". This theorem can be formulated in several equivalent ways. We have chosen the most useful statement for the purposes of this thesis.

Theorem 1.3.12 (Serre's open image theorem)**.** *Let K be a number field and E/K an elliptic curve without CM. Then for all but finitely many prime numbers $p \in \mathbb{N}$ we have*

$$\mathrm{Gal}(K_p/K) \cong \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z}),$$

and the index of $\mathrm{Gal}(K_m/K) \subseteq \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ remains bounded for $m \to \infty$.

One of the consequences of Serre's theorem is that for every elliptic curve E defined over a number field K without CM, there exists a constant c_E such that

$$[K_m : K] \sim c_E \cdot m^4 \qquad \text{as } m \to \infty.$$

If E has CM instead then the endomorphism ring $\mathrm{End}(E)$ is strictly bigger than $\mathbb{Z}$. It is possible to prove that in this case $\mathrm{End}(E)$ is isomorphic to an order

$$\mathfrak{O}_D = \mathbb{Z}\left[\frac{D+\sqrt{D}}{2}\right], \qquad D < 0, D \equiv 0, 1 \bmod 4$$

in an imaginary quadratic field $\mathbb{Q}(\sqrt{D})$, and all the endomorphisms of E are defined over $F = K(\sqrt{D})$ (the field F is called the CM-field associated to E). By proposition 1.3.6 every endomorphism sends m-torsion points to m-torsion points for every $m \in \mathbb{N}$, so the group $E[m](\overline{K})$ has a natural structure of $\mathfrak{O}_D$-module for every natural m. Since all the endomorphisms of E are defined over F, for every $m \in \mathbb{N}$ we obtain a Galois representation

$$\mathrm{Gal}(\overline{K}/F) \to \mathrm{Aut}_{\mathfrak{O}_D}(E[m](\overline{K})).$$

Moreover the $\mathfrak{O}_D$-module $E[m](\overline{K})$ is cyclic and isomorphic to $\mathfrak{O}_D/m\mathfrak{O}_D$, so we have $\mathrm{Aut}_{\mathfrak{O}_D}(E[m](\overline{K})) \cong (\mathfrak{O}_D/m\mathfrak{O}_D)^*$. This fact implies that for every $m \in \mathbb{N}$ we have an injection

$$\mathrm{Gal}(F \cdot K_m/F) \hookrightarrow (\mathfrak{O}_D/m\mathfrak{O}_D)^*,$$

As in the non-CM case, the image of the representation above has bounded index in $(\mathfrak{O}_D/m\mathfrak{O}_D)^*$ for $m \to \infty$, so there exists a constant c_E such that

$$[K_m : K] \sim c_E \cdot m^2 \qquad \text{as } m \to \infty.$$

We conclude this subsection with a result on ramification in division fields (for the proof see [19] prop. 8.1.5).

Proposition 1.3.13. *Let K be a number field and E/K an elliptic curve. If $\mathfrak{p}$ is a prime ideal in $\mathfrak{O}_K$ and $\mathfrak{p}$ ramifies in K_m, then either $\mathfrak{p}$ divides m or $\mathfrak{p}$ is a prime of bad reduction for E.*

1.3.5 The Weil pairing

Let E/K be an elliptic curve and m an integer coprime with $\mathrm{char}(K)$. By proposition 1.3.7 $E[m]$ is a free $\mathbb{Z}/m\mathbb{Z}$-module of rank two. It is possible to define a pairing (see [19] section 3.8 for details)

$$e_m : E[m] \times E[m] \to \mu_m$$

where μ_m is the group of m-th roots of unity in K. This pairing satisfies the following properties

- It is bilinear

  $$e_m(S_1+S_2, T) = e_m(S_1, T)e_m(S_2, T) \quad \text{and} \quad e_m(S, T_1+T_2) = e_m(S, T_1)e_m(S, T_2).$$

  In particular $e_m(O, T) = e_m(S, O) = 1$ for every $S, T \in E[m]$.

- It is alternating

  $$e_m(T, T) = 1$$

  so in particular $e_m(S, T) = e_m(T, S)^{-1}$.

- It is non-degenerate i.e. if $e_m(S, T) = 1$ for all $S \in E[m]$ then $T = O$.

- It is Galois invariant

  $$\sigma(e_m(P, T)) = e_m(\sigma(P), \sigma(T)) \quad \text{for all } \sigma \in \mathrm{Gal}(\overline{K}/K)$$

- It is compatible i.e. $e_{mm'}(S, T) = e_m([m']S, T)$ for all $S \in E[mm']$ and $T \in E[m]$.

The pairing e_m is called the Weil e_m-pairing.

Proposition 1.3.14. *Let K be a number field and E/K an elliptic curve. Then for every $m \in \mathbb{N}$ the m-th division field K_m contains a primitive m-th root of unity.*

Proof. We first prove that the image of the Weil e_m-pairing is surjective. By the bilinearity of the pairing we see that the image of the Weil e_m-pairing is a subgroup of μ_m, hence it is of the form μ_d for $d \mid m$. So for every $S, T \in E[m]$ by bilinearity we have

$$1 = e_m(S,T)^d = e_m([d]S, T).$$

By the non-degeneracy of the pairing we deduce that $[d]S = O$ for all $S \in E[m]$. By proposition 1.3.7 the group $E[m]$ has exponent m so we deduce that $m \mid d$. Hence $m = d$ and the Weil e_m-pairing is surjective.

For every $\sigma \in \mathrm{Gal}(\overline{K}/K_m)$ the Galois invariance gives for all $S, T \in E[m]$

$$\sigma(e_m(S,T)) = e_m(\sigma(S), \sigma(T)) = e_m(S,T).$$

This implies that $e_m(S,T) \in K_m$ for every $S, T \in E[m]$. The surjectivity of the pairing implies that K_m contains a primitive m-th root of unity. □

Proposition 1.3.15. *Let E be an elliptic curve defined over a number field K, $m \in \mathbb{N}$ an integer and K_m the m-division field over K. Then, if ζ_m denotes a primitive m-th root of unity, $K(\zeta_m) \subseteq K_m$ and for every $\sigma \in \mathrm{Gal}(K_m/K)$*

$$\sigma(\zeta_m) = \zeta_m^{\det(\sigma)}.$$

Remark 1.3.16. *Notice that the formula above is well defined: indeed the automorphism σ can be written as 2×2 matrix with entries in $\mathbb{Z}/m\mathbb{Z}$, by choosing a basis of $E[m]$ as a free $\mathbb{Z}/m\mathbb{Z}$ module. The determinant is independent from the choice of the basis.*

Proof. The first part of the proposition was proved in 1.3.14. We know by the previous proposition that the Weil e_m-pairing is surjective: hence there exist $S, T \in E[m]$ such that

$$e_m(S,T) = \zeta_m.$$

We claim that $\{S, T\}$ is a basis of $E[m]$ as a free $\mathbb{Z}/m\mathbb{Z}$ module. First notice that both S and T have order m: suppose for example that S has order $d \mid m$. Then

$$1 = e_m([d]S, T) = e_m(S,T)^d = \zeta_m^d$$

and this implies $d = m$. Hence to conclude that $\{S, T\}$ is a basis it suffices to show that there don't exist $a, b \in \mathbb{Z}/m\mathbb{Z}$ such that $aS + bT = O$. Let $a, b \in \mathbb{Z}/m\mathbb{Z}$ be such that $aS + bT = O$: then

$$1 = e_m(aS + bT, T) = e_m(S,T)^a e_m(T,T)^b = \zeta_m^a$$

which implies that $a = 0 \in \mathbb{Z}/m\mathbb{Z}$. Similarly also $b = 0$ and this shows that $\{S, T\}$ is a basis.

Let now $\sigma \in \mathrm{Gal}(K_m/K)$: by the Galois invariance property of the Weil e_m-pairing we get

$$\sigma(\zeta_m) = \sigma(e_m(S,T)) = e_m(\sigma(S), \sigma(T)).$$

Now $\sigma(S), \sigma(T) \in E[m]$ and S, T form a basis of $E[m]$ as a free $\mathbb{Z}/m\mathbb{Z}$ module: hence there exist unique $a, b, c, d \in \mathbb{Z}/m\mathbb{Z}$ such that

$$\sigma(S) = aS + bT \qquad \sigma(T) = cS + dT.$$

Using the linearity of the Weil pairing we get

$$\begin{aligned}\sigma(\zeta_m) = e_m(aS + bT, cS + dT) &= e_m(S,S)^{ac} e_m(S,T)^{ad} e_m(T,S)^{bc} e_m(T,T)^{bd} \\ &= e_m(S,T)^{ad-bc} = \zeta_m^{\det(\sigma)}\end{aligned}$$

and this proves the proposition. □

1.4 Lang-Trotter conjecture and cyclic reduction problem

The immediate elliptic curve analogue of Artin's primitive root problem is the Lang-Trotter Conjecture. Let E be an elliptic curve defined over the rational numbers $\mathbb{Q}$ and let P be a rational point of infinite order. The problem is to determine, if it exists, the density of the set of primes p for which E has good reduction and $\tilde{E}(\mathbb{F}_p)$ is cyclic, generated by the reduction of P modulo p (cfr. section 1.2.2 in this thesis). Such a point P is called primitive for these primes.

Conjecture 1.4.1 (Lang-Trotter)**.** *The density of primes p for which P is a primitive point always exists.*

The way Lang and Trotter tried to deal with this problem is to study the splitting of primes in the field extensions $\mathbb{Q}(E[l], [l]^{-1}P)$ with l a prime number: these are analogous to the Kummer extensions that appeared in the multiplicative Artin conjecture and are actually called elliptic Kummer extensions. However the degree of the elliptic Kummer extensions is bigger than the degree of the corresponding multiplicative Kummer extensions and so is their Galois group. This causes the technique used by Hooley to fail in the study of this problem, even under the assumption of GRH (see [7] for more details).

The aim of this thesis is to study a simpler problem, first studied by Serre (see [17]): namely we want to find the density of the set of primes in a number field K for which a given elliptic curve E/K has a cyclic (good) reduction (hence we will not consider the generators of this cyclic group). As we did in the case of the multiplicative Artin problem, we first want to give some numerical examples of cyclic reduction of elliptic curves defined over $\mathbb{Q}$. To do the computations we used SAGE: we took several elliptic curves defined over the rationals and we reduced them modulo primes of good reduction up to 10^6. We will call $d(E)$ the quotient between the number of primes up to 10^6 for which the given elliptic curve has cyclic reduction and the total number of primes up to 10^6. The data have been collected in the following table.

Equation for E	**Primes up to** 10^6 **of cyclic reduction for** E	$d(E)$
$y^2 = x^3 - x$	0	0
$y^2 = x^3 - 3x + 1$	49024	0.6510
$y^2 = x^3 + 2x + 3$	38383	0.4889
$y^2 = x^3 - 12096x - 544752$	32652	0.4159
$y^2 = x^3 + x + 3$	63910	0.8141
$y^2 = x^3 - 1$	39265	0.5002

TABLE 1.4: How often E has cyclic reduction modulo p for $p < 10^6$ for some elliptic curves E.

Apparently the figures appearing in the table are very different form each other: the elliptic curves $E_3 : y^2 = x^3 + 2x + 3$ and $E_6 : y^2 = x^3 - 1$ seem to have cyclic reduction for approximately half of the primes while the elliptic curve $E_1 : y^2 = x^3 - x$ seems to not have any cyclic reduction. At the end of the thesis we will interpret these figures explaining why such different numbers appear. Essentially, as in the case of Artin's primitive root conjecture, the values appearing in the table are related to the splitting of rational primes in an infinite family of finite extensions of $\mathbb{Q}$. What we want to do in the following is to underline the similarities between the cyclic reduction problem for elliptic curves and Artin's primitive root problem. We need some basic lemmas:

Lemma 1.4.2. *Let G be a finite abelian group. Then G is cyclic if and only if it does not contain a subgroup isomorphic to $C_l \times C_l$ for every prime $l \in \mathbb{N}$ (here C_l denotes a cyclic group of order l).*

Proof. Immediate from the structure theorem of finite abelian groups. □

Corollary 1.4.3. *Let $m \in \mathbb{N}$ and let E be an elliptic curve defined over $\mathbb{F}_{p^m}$, p prime. Then $E(\mathbb{F}_{p^m})$ is cyclic if and only if it does not contain a subgroup isomorphic to $C_l \times C_l$ for every prime $l \neq p$. Equivalentely $E(\mathbb{F}_{p^m})$ is cyclic if and only if it does not contain the full l-torsion for every prime $l \neq p$.*

Lemma 1.4.4. *Let E be an elliptic curve defined over a number field K, let $l \in \mathbb{Z}$ be a prime number and $\mathfrak{p}$ be a prime of K such that $\mathfrak{p}$ does not lie over l and E has a good reduction at $\mathfrak{p}$. Then $\mathfrak{p}$ splits completely in K_l if and only if $\tilde{E}(k_\mathfrak{p})$ contains a subgroup isomorphic to $C_l \times C_l$.*

Proof. The result is clear: since $\mathfrak{p}$ is unramified in K_l by our assumptions, $\mathfrak{p}$ splits completely in K_l if and only if its residue degree is 1. Since for any prime $\mathfrak{q}$ lying over $\mathfrak{p}$ the reduction modulo $\mathfrak{q}$ gives an isomorphism between $E[l](\overline{K})$ and the l-torsion points on the reduced curve $\tilde{E}[l](k_\mathfrak{q}) = \tilde{E}[l](k_\mathfrak{p})$, this happens if and only if the field $k_\mathfrak{p}$ already contains the l-torsion points of E. Since E has good reduction at $\mathfrak{p}$ and $\mathfrak{p}$ does not lie over l, this happens if and only if $\tilde{E}(k_\mathfrak{p})$ contains a subgroup isomorphic to $C_l \times C_l$ (namely the l- torsion points of E). □

Corollary 1.4.5. *Let E be an elliptic curve defined over a number field K and let $\mathfrak{p}$ be a prime of K such that*

1. *$\mathfrak{p}$ is of good reduction for E/K.*
2. *$\mathfrak{p} \nmid \mathrm{disc}(K/\mathbb{Q})$.*

Then $\tilde{E}(k_{\mathfrak{p}})$ is cyclic if and only if $\mathfrak{p}$ does not split completely in any division field K_l for every l prime.

Proof. Let p be the unique prime number lying below $\mathfrak{p}$. Condition 1 implies that $p \neq 2$ (the integer 2 is never a prime of good reduction for our chosen model). The elliptic curve $\tilde{E}(k_{\mathfrak{p}})$ is cyclic if and only if it does not contain the full l-torsion for every $l \neq p$ by lemma 1.4.3. For all these l this happens if and only if $\mathfrak{p}$ does not split completely in K_l. If $l = p$, i.e. if $\mathfrak{p} \mid l$, we show that the field extension K_p/K has degree strictly greater than 1; by proposition 1.3.15 there is an inclusion of fields $K(\zeta_p) \subseteq K_p$ so $K_p = K$ woud imply that $\zeta_p \in K$. Since $p > 2$, p would ramify in K so that $p \mid \mathrm{disc}(K/\mathbb{Q})$. But this contradicts hypothesis 2.

Hence K_p/K has degree strictly greater than 1 and then $\mathfrak{p}$ ramifies in K_p because $K \subsetneq K(\zeta_p)$ and p is unramified in K. So $\mathfrak{p}$ does not split completely even in K_p and this proves the corollary. □

The corollary above says that checking if an elliptic curve over K has cyclic reduction at a prime ideal $\mathfrak{p}$ is, excluding a finite number of prime ideals, "the same" as checking if the prime $\mathfrak{p}$ does not split completely in any division field of prime index over K. Since the natural density of a set of primes does not change if we add finitely many primes to the set, we get that

$$\delta(\{\mathfrak{p} \subseteq \mathfrak{O}_K \text{ prime} : \mathfrak{p} \text{ does not split completely in any } K_l,\ l \text{ prime}\}) = \delta(\{\mathfrak{p} \subseteq \mathfrak{O}_K \text{ prime} : \tilde{E}(k_{\mathfrak{p}}) \text{ is cyclic}\})$$

where $\delta(\cdot)$ denotes the natural density. The similarity with Artin's primitive root conjecture is clear: also there the problem was tackled by studying the splitting of primes in an infinite family of number fields, namely the multiplicative Kummer extensions of the rationals $\mathbb{Q}(\zeta_l, \sqrt[l]{a})$ for l prime and a an integer. In the next chapter we are going to prove, under GRH, that the density above always exists and we will deduce an explicit formula for it.

Chapter 2

Cyclic reduction of Elliptic Curves

The main goal of this chapter is to prove the following

Theorem 2.0.1. *Let E be an elliptic curve defined over a number field K and let*

$$S = \{\mathfrak{p} \subseteq \mathfrak{O}_K \text{ prime} : \text{ the reduction } \tilde{E}(k_\mathfrak{p}) \text{ is cyclic}\}.$$

Then, subject to GRH, the density of S is given by

$$\sum_{m=1}^{\infty} \frac{\mu(m)}{[K_m : K]}$$

where μ is the usual Möbius μ function on the integers and for every natural m the field K_m is the m-division field over K.

Notice that the infinite sum appearing in the statement of the theorem always converges by what we discussed in section 1.3.4.

As we pointed out at the end of the previous chapter, the proof relies on the study of the splitting behaviour of the prime ideals of $\mathfrak{O}_K$ in the infinite family of division fields $\{K_m = K(E[m])(\overline{K}) : m \in \mathbb{N}\}$. Hence we begin by studying some properties of this family.

2.1 The family of division fields over a number field

In all this section let K be a number field and E/K an elliptic curve. Denote by K_m the m-division field over K (see definition 1.3.10). If $\mathfrak{p}$ is a prime ideal in $\mathfrak{O}_K$ we denote by $k_\mathfrak{p} := \mathfrak{O}_K/\mathfrak{p}$ its residue field and by $N_{K/\mathbb{Q}}(\mathfrak{p}) := \#k_\mathfrak{p}$ its norm. The symbol $\ll$ will replace the standard big-O notation.

Lemma 2.1.1. *Let $n, m \in \mathbb{N}$ and K_n, K_m respectively the n and the m-division fields over K. Then the compositum of K_n and K_m is $K_{\mathrm{lcm}(m,n)}$.*

Proof. Suppose first that m, n are coprime integers. Since $E[m], E[n] \subseteq E[mn]$ we have $K_m \cdot K_n \subseteq K_{mn}$. We want to prove the other inclusion. It is a general fact that if $(A, +)$ is an abelian group and $A[r]$ denotes the group of r-torsion points of A for every $r \in \mathbb{N}$, then the map

$$A[m] \times A[n] \to A[mn]$$

sending $(x, y) \mapsto x + y$ is an isomorphism whenever m and n are coprime integers. Applying this to the torsion points of the elliptic curve E we deduce that

$$E[mn](\overline{K}) = \{P + Q : P \in E[n](\overline{K}), Q \in E[m](\overline{K})\}.$$

Since the points $P+Q$ have coordinates which are K-rational functions of the coordinates of P, Q we get that $K_{mn} \subseteq K_m \cdot K_n$ and this shows that $K_{mn} = K_m \cdot K_n$.

If m, n are not coprime, let $l := \mathrm{lcm}(m,n)$. The fact that $K_m \cdot K_m = K_l$ follows from the previous case noticing that $l = \frac{mn}{\gcd(m,n)}$ and $E\left[\frac{m}{\gcd(m,n)}\right] \subseteq E[m]$ with $\gcd\left(\frac{m}{\gcd(m,n)}, n\right) = 1$. □

The lemma says that the family of division fields over K is closed under the operation of taking the compositum. In particular for every $m \in \mathbb{N}$ squarefree the field K_m is the compositum of all K_p with $p \in \mathbb{N}$ prime dividing m.

We now prove a technical lemma about the splitting of primes in the family of the division fields over K.

Lemma 2.1.2. *Every prime ideal $\mathfrak{p} \subseteq \mathfrak{O}_K$ splits completely in a finite number of K_l, with $l \in \mathbb{N}$ prime.*

Proof. By lemma 1.3.15 we know that the fields K_m contain the cyclotomic fields $K(\zeta_m)$ for every $m \in \mathbb{N}$. If $\mathfrak{p}$ splits completely in K_l for some prime l then it must split completely in $K(\zeta_l)$. Either l lies below $\mathfrak{p}$ or the residue field $k_\mathfrak{p}$ contains a primitive l-th root of unity and this implies that $N_{K/\mathbb{Q}}(\mathfrak{p}) \equiv 1 \mod l$. This gives a bound on l and proves the lemma. □

Corollary 2.1.3. *Every prime ideal $\mathfrak{p} \subseteq \mathfrak{O}_K$ splits completely in a finite number of K_m, with $m \in \mathbb{N}$ squarefree.*

The lemma above gives us a finitness condition which will be useful in a moment.

Let $\mathcal{F}$ be the family of division fields K_m with m squarefree integer. For every $x \in \mathbb{R}_{\geq 0}$ define the function

$$f(x,K) = \#\{\mathfrak{p} \subseteq \mathfrak{O}_K \text{ prime of good reduction for } E:\ N_{K/\mathbb{Q}}(\mathfrak{p}) \leq x, \\ \mathfrak{p} \text{ does not split completely in any } K_n \in \mathcal{F}, K_n \neq K\}.$$

For $K_m \in \mathcal{F}$ and $x \in \mathbb{R}_{\geq 0}$ define moreover

$$\pi_1(x,K_m) = \#\{\mathfrak{p} \subseteq \mathfrak{O}_K \text{ prime of good reduction for } E : N_{K/\mathbb{Q}}(\mathfrak{p}) \leq x, \\ \mathfrak{p} \text{ splits completely in } K_m\}.$$

These two functions are related by the following useful formula.

Lemma 2.1.4. *For every fixed $x \in \mathbb{R}$ we have*

$$f(x,K) = \sum_{m=1}^{\infty} \mu(m)\pi_1(x,K_m). \tag{2.1}$$

where μ is the usual Möbius function on the integers.

Proof. Recall that a prime ideal splits completely in the compositum of two fields if and only if it splits completely in each of the two given fields. This means that in order to compute $f(x,K)$ it suffices to consider the primes of norm less or equal to x that do not split completely in any of the fields K_l, l prime number. The counting technique for these primes relies on the so-called inclusion-exclusion principle. First we consider the total number of prime ideals whose norm is less or equal to x: this is by definition $\pi_1(x,K_1) = \pi_1(x,K)$. Then we have to subtract the number

of prime ideals of good reduction for E and of norm less or equal to x which split completely in either K_2 or K_3:

$$\pi_1(x, K_1) - \pi_1(x, K_2) - \pi_1(x, K_3).$$

In doing this however we have considered twice the primes which split completely in both K_2 and K_3. These are precisely the prime ideals of norm less or equal to x that split completely in their compositum which is K_6. We get then

$$\pi_1(x, K_1) - \pi_1(x, K_2) - \pi_1(x, K_3) + \pi_1(x, K_6).$$

We then repeat the argument considering now K_5, K_7, etc. This process terminates since, by corollary 2.1.3, $\pi_1(x, K_m) = 0$ if m squarefree is sufficientely large. Then in the resulting sum there will be just a finite number of terms of the form $\pm\pi_1(x, K_m)$ with m squarefree integer and the sign depending on whether m has an even or odd number of prime factors. Since $\mu(m) = 0$ if m is not squarefree we obtain formula 2.1. □

Our goal is to find the asymptotical behaviour of $f(x, K)$ as $x \to \infty$; formula 2.1 suggests that in order to do so we can estimate the quantity $\pi_1(x, K_m)$ for m large. The idea is that, in order to prove theorem 2.0.1, one wants to bound the right-hand side of formula 2.1. This motivates our next proposition.

Proposition 2.1.5. *We have*

$$\sum_{l > \frac{x^{1/2}}{\log^2 x},\ l \text{ prime}} \pi_1(x, K_l) = o\left(\frac{x}{\log x}\right).$$

as $x \to \infty$.

Proof. From now on l will denote a prime number. First we want to find a number k such that $\pi_1(x, K_l) = 0$ for $l > k$. We know that such a k exists because of lemma 2.1.3.

Let $\mathfrak{p} \subseteq \mathfrak{O}_K$ be a prime of good reduction for E such that $N_{K/\mathbb{Q}}(\mathfrak{p}) \leq x$, $\mathfrak{p}$ splits completely in K_l and $\mathfrak{p}$ does not lie over l. Then lemma 1.4.4 implies that $\tilde{E}(k_\mathfrak{p})$ contains a subgoup isomorphic to $C_l \times C_l$. Using the Hasse-Weil bound we get

$$l^2 \leq \#\tilde{E}(k_\mathfrak{p}) \leq (\sqrt{N_{K/\mathbb{Q}}(\mathfrak{p})} + 1)^2 \leq (\sqrt{x} + 1)^2 \leq 4x$$

and it follows that $l \leq 2\sqrt{x}$. On the other hand if $\mathfrak{p}$ lies over l then in order for $\mathfrak{p}$ to split completely in K_l it is necessary that $l \mid \mathrm{disc}(K/\mathbb{Q})$ by proposition 1.3.15. This implies that the number of primes $\mathfrak{p}$ as above is bounded by a constant which does not depend on x and so it does not change the asymptotic behaviour of the sum. Hence we need to estimate

$$\sum_{\frac{x^{1/2}}{\log^2 x} < l < 2\sqrt{x}} \pi_1(x, K_l).$$

By proposition 1.3.15 we know that for every prime l there is the inclusion $K_l \supseteq K(\zeta_l)$ with ζ_l a primitive l-th root of unity. In particular we have

$$\pi_1(x, K_l) \leq \pi_1(x, K(\zeta_l))$$

where $\pi_1(x, K(\zeta_l))$ is by definition the number of prime ideals with norm less or equal to x which split completely in $K(\zeta_l)$. Hence we want to estimate the number of primes in K which split completely in $K(\zeta_l)$ for every l prime.

Let $\mathfrak{p}$ be a prime ideal in K that does not divide l: then, as in lemma 2.1.2, $\mathfrak{p}$ splits completely in $K(\zeta_l)$ if and only if $N_{K/\mathbb{Q}}(\mathfrak{p}) \equiv 1 \mod l$. Since there are at most $[K:\mathbb{Q}]$ primes lying over l, we deduce that

$$\begin{aligned}\pi_1(x, K(\zeta_l)) &\leq [K:\mathbb{Q}] + \#\{\mathfrak{p} \subseteq \mathfrak{O}_K \text{ prime}: \ N_{K/\mathbb{Q}}(\mathfrak{p}) \leq x, N_{K/\mathbb{Q}}(\mathfrak{p}) \equiv 1 \mod l\} \\ &= [K:\mathbb{Q}] + A + B\end{aligned}$$

where

$$\begin{aligned}A &= \#\{\mathfrak{p} \subseteq \mathfrak{O}_K \text{ prime}: \ N_{K/\mathbb{Q}}(\mathfrak{p}) = p^f \leq x, \ p \text{ prime}, \ f > 1, \ p^f \equiv 1 \mod l\} \\ B &= \#\{\mathfrak{p} \subseteq \mathfrak{O}_K \text{ prime}: \ N_{K/\mathbb{Q}}(\mathfrak{p}) = p \leq x, \ p \text{ prime}, \ p \equiv 1 \mod l\}.\end{aligned}$$

By proposition 1.3.3 we know that $A = o\left(\frac{x}{\log x}\right)$ as $x \to \infty$. To estimate B instead we will use the following theorem.

Theorem 2.1.6 (Brun-Titchmarsh)**.** *For integers m, a, let $\pi(x,a,m)$ denote the number of primes not exceeding x which are congruent to $a \mod m$. Then*

$$\pi(x,a,m) \leq \frac{2x}{\varphi(m)\log(\frac{x}{m})}$$

where φ denotes the Euler φ function.

By theorem 2.1.6 we get

$$\#\{p \in \mathbb{Z} \text{ prime}: p \leq x, \ p \equiv 1 \mod l\} \leq \frac{2x}{(l-1)\log\left(\frac{x}{l}\right)}$$

and this implies that

$$\begin{aligned}B &\leq [K:\mathbb{Q}] \cdot \#\{p \in \mathbb{Z} \text{ prime}: p \leq x, \ p^f \equiv 1 \mod l \text{ for some } f \leq [K:\mathbb{Q}]\} \\ &\leq [K:\mathbb{Q}] \frac{2x}{(l-1)\log\left(\frac{x}{l}\right)}.\end{aligned}$$

Hence we have

$$\pi_1(x, K(\zeta_l)) \leq [K:\mathbb{Q}] + A + [K:\mathbb{Q}] \frac{2x}{(l-1)\log\left(\frac{x}{l}\right)} \ll \frac{x}{l\log\left(\frac{x}{l}\right)}.$$

We then get

$$\begin{aligned}\sum_{\frac{x^{1/2}}{\log^2 x} < l < 2\sqrt{x}} \pi_1(x, K_l) &\ll \sum_{\frac{x^{1/2}}{\log^2 x} < l < 2\sqrt{x}} \frac{x}{l\log\left(\frac{x}{l}\right)} \\ &\ll \frac{x}{\log x} \sum_{\frac{x^{1/2}}{\log^2 x} < l < 2\sqrt{x}} \frac{1}{l}.\end{aligned}$$

Using the well-known fact that

$$\sum_{p\leq x,\ p \text{ prime}} \frac{1}{p} = \log\log x + B + O\left(\frac{1}{\log x}\right)$$

for some positive constant B, we can write

$$\begin{aligned}
&\sum_{\frac{x^{1/2}}{\log^2 x}<l<2\sqrt{x}} \frac{1}{l} = \sum_{l<2\sqrt{x}} \frac{1}{l} - \sum_{l<\frac{x^{1/2}}{\log^2 x}} \frac{1}{l} \\
&= \log\log 2\sqrt{x} + B + O\left(\frac{1}{\log 2\sqrt{x}}\right) - \log\log\left(\frac{\sqrt{x}}{\log^2 x}\right) - B - O\left(\frac{1}{\log\left(\frac{\sqrt{x}}{\log^2 x}\right)}\right) \\
&= \log\left(\frac{\log 2 + \frac{1}{2}\log x}{\frac{1}{2}\log x - 2\log\log x}\right) + O\left(\frac{1}{\log x}\right) \\
&= \log\left(1 + \frac{\log 2 + \log\log x}{\frac{1}{2}\log x - 2\log\log x}\right) + O\left(\frac{1}{\log x}\right) = O\left(\frac{\log\log x}{\log x}\right).
\end{aligned}$$

So we get

$$\sum_{\frac{x^{1/2}}{\log^2 x}<l<2\sqrt{x}} \pi_1(x, K_l) \ll \frac{x\log\log x}{\log^2 x} = o\left(\frac{x}{\log x}\right).$$

□

We conclude this section with an estimate on the growth of discriminant of the division fields K_m compared to their degree. For every $m \in \mathbb{N}$ denote by $n(m) := [K_m : K]$ and by d_m the discriminant of K_m over $\mathbb{Q}$.

Proposition 2.1.7. *For every $m \in \mathbb{N}$*

$$\frac{1}{n(m)} \log|d_m| = O(\log m).$$

To prove the proposition we need the following theorem

Theorem 2.1.8. *Let L/K be a finite Galois extension of number fields and let $\delta_{L/K}$ be the relative discriminant of the extension. Denote by $P(L/K)$ the set of rational primes p for which there is a prime $\mathfrak{p}$ of F such that $\mathfrak{p} \mid p$ and $\mathfrak{p}$ is ramified in L. Then:*

$$\log N_{K/\mathbb{Q}}(\delta_{L/K}) \leq ([L:\mathbb{Q}] - [K:\mathbb{Q}]) \sum_{p\in P(L/K)} \log p + [L:\mathbb{Q}]\log([L:K]).$$

Proof. Let $\mathfrak{p}$ be a prime ideal in K and let $\mathfrak{p}_1, ..., \mathfrak{p}_{g_\mathfrak{p}}$ be the primes in L lying above $\mathfrak{p}$. Denote moreover by $e_\mathfrak{p}$ the ramification index of $\mathfrak{p}$ in L and by $f_\mathfrak{p}$ its residue degree. For every $i = 1, ..., g_\mathfrak{p}$ we want to estimate $\mathrm{ord}_{\mathfrak{p}_i}(\mathcal{D}_{L/K})$ where $\mathcal{D}_{L/K}$ is the different of the extension L/K. Let $L_{\mathfrak{p}_i}$ and $K_\mathfrak{p}$ be the completions of L and K at the primes $\mathfrak{p}_i$ and $\mathfrak{p}$ respectively. Then we have:

$$\mathrm{ord}_{\mathfrak{p}_i}(\mathcal{D}_{L/K}) = \mathrm{ord}_{\mathfrak{p}_i}(\mathcal{D}_{L_{\mathfrak{p}_i}/K_\mathfrak{p}}) \leq e_\mathfrak{p} - 1 + \mathrm{ord}_{\mathfrak{p}_i}(e_\mathfrak{p})$$

where in the last inequality we used Proposition 13 pag. 58 in [15].

So for every prime ideal $\mathfrak{p}$ in K we have:

$$\begin{aligned}\operatorname{ord}_{\mathfrak{p}}(\delta_{L/K}) = \operatorname{ord}_{\mathfrak{p}}(N_{L/K}(\mathcal{D}_{L/K})) &\leq f_{\mathfrak{p}}\left(\sum_{i=1}^{g_{\mathfrak{p}}} e_{\mathfrak{p}} - 1 + \operatorname{ord}_{\mathfrak{p}_i}(e_{\mathfrak{p}})\right) \\ &= [L:K] - f_{\mathfrak{p}}g_{\mathfrak{p}} + g_{\mathfrak{p}}f_{\mathfrak{p}}\operatorname{ord}_{\mathfrak{p}_i}(e_{\mathfrak{p}}) \leq [L:K] - f_{\mathfrak{p}}g_{\mathfrak{p}} + [L:K]\operatorname{ord}_{\mathfrak{p}}([L:K])\end{aligned}$$

where we used the fact that $e_{\mathfrak{p}}f_{\mathfrak{p}}g_{\mathfrak{p}} = [L:K]$. Now clearly we have

$$\delta_{L/K} = \prod_{\mathfrak{p}|\delta_{L/K}} \mathfrak{p}^{\operatorname{ord}_{\mathfrak{p}}(\delta_{L/K})} \;\Bigg|\; \prod_{\mathfrak{p}|\delta_{L/K}} \mathfrak{p}^{[L:K]-f_{\mathfrak{p}}g_{\mathfrak{p}}+[L:K]\operatorname{ord}_{\mathfrak{p}}([L:K])}$$

and the latter divides $n^n \prod_{\mathfrak{p}|\delta_{L/K}} \mathfrak{p}^{[L:K]-f_{\mathfrak{p}}g_{\mathfrak{p}}}$. Taking norms we get

$$\begin{aligned}N_{K/\mathbb{Q}}(\delta_{L/K}) &\leq [L:K]^{[L:\mathbb{Q}]} \prod_{\mathfrak{p}|\delta_{L/K}} N_{K/\mathbb{Q}}(\mathfrak{p})^{[L:K]-f_{\mathfrak{p}}g_{\mathfrak{p}}} \\ &= [L:K]^{[L:\mathbb{Q}]} \prod_{p\in P(L/K),\, \mathfrak{p}|\delta_{L/K}} p^{f(\mathfrak{p}/p)([L:K]-f_{\mathfrak{p}}g_{\mathfrak{p}})}\end{aligned}$$

where we $f(\mathfrak{p}/p)$ is the residue degree of $\mathfrak{p}$ over the rational prime p. Taking logarithms on both sides we obtain

$$\begin{aligned}\log N_{K/\mathbb{Q}}(\delta_{L/K}) &\leq \left(\sum_{p\in P(L/K),\, \mathfrak{p}|\delta_{L/K}} f(\mathfrak{p}/p)([L:K] - f_{\mathfrak{p}}g_{\mathfrak{p}})\log p\right) + [L:\mathbb{Q}]\log([L:K]) \\ &\leq ([L:K]-1)\left(\sum_{p\in P(L/K),\, \mathfrak{p}|\delta_{L/K}} f(\mathfrak{p}/p)\log p\right) + [L:\mathbb{Q}]\log([L:K]) \\ &\leq ([L:\mathbb{Q}] - [K:\mathbb{Q}]) \sum_{p\in P(L/K)} \log p + [L:\mathbb{Q}]\log([L:K])\end{aligned}$$

which gives the result. □

Proof of proposition 2.1.7. Applying the theorem to the extension K_m/K, which is Galois, we get

$$\log N_{K/\mathbb{Q}}(\delta_{K_m/K}) \leq ([K_m:\mathbb{Q}] - [K:\mathbb{Q}]) \sum_{p\in P(K_m/K)} \log p + [K_m:\mathbb{Q}]\log n(m). \quad (2.2)$$

Using the well-known formula for relative discriminants in tower of fields

$$d_m = N_{K/\mathbb{Q}}(\delta_{K_m/K}) d_{K/\mathbb{Q}}^{n(m)}$$

where $d_{K/\mathbb{Q}}$ is the absolute discriminant of the field K, we get

$$\log N_{K/\mathbb{Q}}(\delta_{K_m/K}) = \log|d_m| - n(m)\log|d_{K/\mathbb{Q}}|.$$

Hence , dividing both sides of the inequality 2.2 by $n(m)$ we get:

$$\begin{aligned}\frac{1}{n(m)}\log|d_m| - \log|d_{K/\mathbb{Q}}| &\leq \frac{[K_m:\mathbb{Q}]-[K:\mathbb{Q}]}{n(m)} \sum_{p\in P(K_m/K)} \log p + \frac{[K_m:\mathbb{Q}]}{n(m)}\log n(m) \\ &\leq [K:\mathbb{Q}]\left(\sum_{p\in P(K_m/K)} \log p + \log n(m)\right) \\ &\ll \sum_{p\in P(K_m/K)} \log p + \log n(m)\end{aligned}$$

Now by proposition 1.3.13 if $\mathfrak{p}\subseteq\mathfrak{O}_K$ ramifies in K_m then either $\mathfrak{p}$ divides m or $\mathfrak{p}$ is a prime of bad reduction for E. We know that there are just finitely many primes of bad reduction: call

$$C := \sum{}' \log p$$

where $\sum'$ is performed over primes lying under the primes in $\mathfrak{O}_K$ of bad reduction for E. Notice that C does not depend on m. Hence we have

$$\sum_{p\in P(K_m/K)} \log p \leq C + \sum_{p|m} \log p \leq C + \log m$$

and from this we get

$$\frac{1}{n(m)}\log|d_m| \ll \log|d_{K/\mathbb{Q}}| + C + \log m + \log n(m).$$

As we have $n(m) = O(m^4)$ (see section 1.3.4) and $\log|d_{K/\mathbb{Q}}| + C$ is a fixed number depending on the elliptic curve and on the base field K, we obtain

$$\frac{1}{n(m)}\log|d_m| = O(\log m)$$

as desired. □

2.2 The proof of the main theorem

In this section we are going to give a proof of theorem 2.0.1. We begin with some preliminary remarks. The notations are as in the previous section.
As we have shown in section 1.4 we have

$$\begin{gathered}\delta(\{\mathfrak{p}\subseteq\mathfrak{O}_K \text{ prime} : \mathfrak{p} \text{ does not split completely in any } K_l,\ l \text{ prime}\}) = \\ \delta(\{\mathfrak{p}\subseteq\mathfrak{O}_K \text{ prime} : \tilde{E}(k_\mathfrak{p}) \text{ is cyclic}\})\end{gathered}$$

Hence we are done if we compute the first density. By what we showed in section 1.3.1, this amounts to computing the limit

$$\lim_{x\to\infty} \frac{f(x,K)}{x/\log x}.$$

For this computation we will use the Generalized Riemann Hypothesis in the form given by Lagarias-Odlyzko in [6]: we have

$$\pi_1(x, K_m) = \frac{\operatorname{li} x}{n(m)} + O\left(\frac{x^{1/2}}{n(m)} \log(|d_m| x^{n(m)})\right)$$

for every $m \geq 1$ squarefree. Here $\operatorname{li} x$ is defined as

$$\operatorname{li} x = \int_0^x \frac{1}{\log t} dt \quad \forall x > 0,\ x \neq 1.$$

Proof of theorem 2.0.1. In this proof l will always denote a prime number. We know by 2.1 that

$$f(x, K) = \sum_{m=1}^{\infty} \mu(m) \pi_1(x, K_m).$$

Before going on with the proof we need to define some new quantities.
For every $x, y \in \mathbb{R}_{>0}$ define

$$N(x, y) := \#\{\mathfrak{p} \subseteq \mathfrak{O}_K \text{ prime}:\ N_{K/\mathbb{Q}}(\mathfrak{p}) \leq x, \\ \mathfrak{p} \text{ does not split completely in any } K_l, l \leq y\}.$$

By the inclusion-exclusion principle we have that

$$N(x, y) = {\sum}' \mu(m) \pi_1(u, K_m) \tag{2.3}$$

where ${\sum}'$ is performed over all the $m \in \mathbb{N}$ with all prime divisors less or equal to y (notice that all the sums we are dealing with are finite by corollary 2.1.3).

Take now $x \in \mathbb{R}$ and $y = y(x) \in \mathbb{R}$ to be fixed later. Clearly we have $f(x, K) \leq N(x, y)$. For every $\xi_1, \xi_2 \in \mathbb{R}$ let $M(x, \xi_1, \xi_2)$ be the number of prime ideals $\mathfrak{p}$ in K with $N_{K/\mathbb{Q}}(\mathfrak{p}) \leq x$ and $\mathfrak{p}$ splits completely in some K_l with $\xi_1 \leq l \leq \xi_2$. Let $g(x)$ denote the largest index m squarefree such that some prime $\mathfrak{p} \subseteq \mathfrak{O}_K$ with $N_{K/\mathbb{Q}}(\mathfrak{p}) \leq x$ splits completely in K_m. Such $g(x)$ exists because of lemma 2.1.3. Clearly we have

$$N(x, y) \geq f(x, K) \geq N(x, y) - M(x, y, g(x)). \tag{2.4}$$

We want to estimate $M(x, y, g(x))$. We have:

$$M(x, y, g(x)) \leq \sum_{y < l < \frac{x^{1/2}}{\log^2 x}} \pi_1(x, K_l) + \sum_{\frac{x^{1/2}}{\log^2 x} < l < g(x)} \pi_1(x, K_l).$$

By proposition 2.1.5

$$\sum_{\frac{x^{1/2}}{\log^2 x} < l < g(x)} \pi_1(x, K_l) = o\left(\frac{x}{\log x}\right).$$

We use proposition 2.1.7 and GRH to bound the first sum:

$$\sum_{y < l < \frac{x^{1/2}}{\log^2 x}} \pi_1(x, K_l) = \sum_{y < l < \frac{x^{1/2}}{\log^2 x}} \frac{\operatorname{li} x}{n(l)} + \sum_{y < l < \frac{x^{1/2}}{\log^2 x}} H(x, l)$$

where

$$H(x,l) := \left| \frac{\operatorname{li} x}{n(l)} - \pi_1(x, K_l) \right| = O\left(\frac{x^{1/2}}{n(l)} \log(|d_l| x^{n(l)}) \right).$$

We get (all the sums are over $y < l < \frac{x^{1/2}}{\log^2 x}$)

$$\sum H(x,l) \ll \sum x^{1/2} \left(\log x + \frac{\log |d_l|}{n(l)} \right) \ll \sum x^{1/2} (\log x + \log l)$$

where in the second inequality we used proposition 2.1.7. To estimate the latter sum we have to recall the following result due to Chebyshev:

Theorem 2.2.1. *There exist two positive constants A, B such that for every $x \in \mathbb{R}_{>0}$*

$$\frac{Ax}{\log x} \leq \pi(x) \leq \frac{Bx}{\log x}$$

where $\pi(x)$ is the number of rational primes less or equal to x.

Using the above theorem we obtain:

$$\begin{aligned}
\sum_{y<l<\frac{x^{1/2}}{\log^2 x}} x^{1/2} (\log x + \log l) &\leq \sum_{y<l<\frac{x^{1/2}}{\log^2 x}} x^{1/2} \left(\log x + \log \left(\frac{x^{1/2}}{\log^2 x} \right) \right) \\
&\ll \sum_{y<l<\frac{x^{1/2}}{\log^2 x}} x^{1/2} \log x \leq x^{1/2} \log x \pi \left(\frac{x^{1/2}}{\log^2 x} \right) \\
&\leq x^{1/2} \cdot \log x \cdot \frac{x^{1/2}}{\log^2 x} \cdot \frac{1}{\log \left(\frac{x^{1/2}}{\log^2 x} \right)} \\
&= \frac{x}{\log x} \cdot \frac{1}{\frac{1}{2} \log x - 2 \log \log x} \ll \frac{2}{\log^2 x} = o\left(\frac{x}{\log x} \right).
\end{aligned}$$

We deduce that

$$\sum_{y<l<\frac{x^{1/2}}{\log^2 x}} H(x,l) = o\left(\frac{x}{\log x} \right).$$

Now we also know that

$$\sum_{l \text{ prime}} \frac{1}{n(l)} \leq \sum_{m=1}^{\infty} \frac{1}{n(m)} < \infty$$

by what we remarked in chapter 1, so also

$$\sum_{y<l<\frac{x^{1/2}}{\log^2 x}} \frac{\operatorname{li} x}{n(l)} = o\left(\frac{x}{\log x} \right)$$

providing that $y = y(x) \to \infty$ as $x \to \infty$ (indeed recall that $\operatorname{li} x = O(x/\log x)$ as $x \to \infty$). Combining what we have obtained so far with the inequalities 2.4 we get

$$f(x,K) = N(x,y) + o\left(\frac{x}{\log x} \right). \tag{2.5}$$

Now we want to study $N(x,y)$. Using equation 2.3 and GRH we get

$$\begin{aligned} N(x,y) &= \sum{}' \mu(m) \left(\frac{\operatorname{li} x}{n(m)} + O\left(\frac{x^{1/2}}{n(m)} \log(|d_m| x^{n(m)}) \right) \right) \\ &= \sum{}' \mu(m) \left(\frac{\operatorname{li} x}{n(m)} + O\left(x^{1/2} \left[\frac{\log |d_m|}{n(m)} + \log x \right] \right) \right) \\ &= \sum{}' \mu(m) \left(\frac{\operatorname{li} x}{n(m)} + O\left(x^{1/2} \log mx \right) \right) \\ &= \sum{}' \mu(m) \frac{\operatorname{li} x}{n(m)} + O\left(\sum{}' \mu(m) x^{1/2} \log mx \right) \end{aligned}$$

where $\sum'$ is performed over all the $m \in \mathbb{N}$ whose prime divisors are $\leq y$.

We know that $\mu(m) = 0$ when m is not square-free. The square-free numbers whose prime divisors are all $\leq y$ are less or equal to

$$1 + \binom{\lfloor y \rfloor}{1} + \cdots + \binom{\lfloor y \rfloor}{\lfloor y \rfloor} = 2^{\lfloor y \rfloor} \leq 2^y.$$

Then we have

$$\begin{aligned} \sum{}' \mu(m) x^{1/2} \log mx &= \sum{}' \mu(m) x^{1/2} \log m + \sum{}' \mu(m) x^{1/2} \log x \\ &\leq \sum{}' \mu(m) x^{1/2} \log m + 2^y x^{1/2} \log x. \end{aligned}$$

Now, if m is square-free and all its prime factors $p_1, ..., p_n$ are $\leq y$, we have

$$\log m = \log(p_1 \cdots p_n) \leq \pi(y) \log y \leq \frac{Ay}{\log y} \cdot \log y = Ay = O(y)$$

where in the last inequality we used theorem 2.2.1. To sum up we obtain

$$N(x,y) = \left(\sum{}' \frac{\mu(m)}{n(m)} \right) \operatorname{li} x + O(x^{1/2} 2^y (y + \log x)).$$

Choose now $y = y(x)$ such that $2^{y(x)} \ll \frac{x^{1/2}}{\log^3 x}$ and $y(x) \to \infty$ as $x \to \infty$. Then necessarily

$$y(x) \ll \frac{1}{\log 2} \left(\frac{1}{2} \log x - 3 \log \log x \right) \ll \log x$$

and we deduce that

$$x^{1/2} 2^y y \ll x^{1/2} \cdot \frac{x^{1/2}}{\log^3 x} \cdot \log x = \frac{x}{\log^2 x} = o\left(\frac{x}{\log x} \right).$$

Hence $O((x^{1/2} 2^y (y + \log x)) = o\left(\frac{x}{\log x} \right)$ and using the fact that $\operatorname{li} x \sim \frac{x}{\log x}$ we get

$$\lim_{x \to \infty} \frac{N(x,y)}{x/\log x} = \sum_{m=1}^{\infty} \frac{\mu(m)}{n(m)}.$$

Equation 2.5 now implies

$$\lim_{x\to\infty} \frac{f(x,K)}{x/\log x} = \sum_{m=1}^{\infty} \frac{\mu(m)}{n(m)} = \sum_{m=1}^{\infty} \frac{\mu(m)}{[K_m : K]}.$$

This proves the theorem. □

Chapter 3

The factorization of the density in the non-CM case

In the previous chapter we were able, under GRH, to prove an explicit formula for the density of the set of prime ideals in a number field K for which a given elliptic curve E defined over K has cyclic reduction. The formula for the density was

$$\delta(E) = \sum_{m=1}^{\infty} \frac{\mu(m)}{[K_m : K]}.$$

In general the density of a set of primes, if exists, is a real number between 0 and 1. When the density is strictly positive it is clear that the given set is infinite. If the density is 0 the set could be either finite or infinite. Therefore it is an interesting problem to understand when the density that we computed in chapter 2 vanishes. However, looking at the formula above, it is by no means clear when the density becomes 0. The aim of this chapter is to factor the density into the product of a finite sum and an infinite product that never vanishes. Hence the vanishing of the density will become equivalent to the vanishing of a finite sum, which will be relatively easy to deal with. We will be able to do so in the case E does not have complex multiplication.

3.1 The general strategy

We want to reduce the problem of factoring the density found in chapter 2 to a problem concerning Galois groups. Let K be a number field and E an elliptic curve defined over K. As usual for every $m \in \mathbb{N}$, let K_m denote the m-division field over K. For every $n \in \mathbb{N}$ squarefree define

$$\delta_n(E) := \sum_{d|n} \frac{\mu(d)}{[K_d : K]}.$$

Clearly $\delta_n(E)$ is a partial sum of the infinite sum giving the density in theorem 2.0.1 in the sense that $\delta(E)$ is the limit, as n tends to infinity by divisibility, of $\delta_n(E)$. We are going to interpret these sums in terms of certain subsets of the Galois groups of the division fields over K. For n squarefree define

$$H_n := \{\sigma \in \mathrm{Gal}(K_n/K) : \sigma|_{K_l} \neq \mathrm{id}_{K_l} \text{ for every prime } l \mid n\}.$$

Notice that when n is squarefree the field K_n is the compositum of all the division fields K_l with l prime dividing n.

Lemma 3.1.1. *For every n squarefree*

$$\delta_n(E) = \frac{\#H_n}{[K_n : K]}$$

Proof. For every positive integer d dividing n define

$$D_d = \{\sigma \in \mathrm{Gal}(K_n/K) : \sigma|_{K_l} = \mathrm{id}_{K_l} \text{ for every prime } l \mid d\}.$$

Since n is squarefree, also d is so and then K_d is the compositum of all the division fields K_l with l prime dividing d. Hence $D_d := \mathrm{Gal}(K_n/K_d)$ so $\#D_d = [K_n : K_d]$. By inclusion-exclusion we have

$$\#H_n = \sum_{d|n} \mu(d)\#D_d = \sum_{d|n} \mu(d)[K_n : K_d].$$

We deduce that

$$\frac{\#H_n}{[K_n : K]} = \sum_{d|n} \frac{\mu(d)}{[K_d : K]} = \delta_n(E)$$

and this gives the result. □

The lemma 3.1.1 suggests that in order to study the behaviour of the density $\delta(E)$ (and therefore of the partial sums $\delta_n(E)$) we should study the subsets H_n for n squarefree. When n is squarefree we have an injective morphism

$$\mathrm{Gal}(K_n/K) \hookrightarrow \prod_{l|n,\ l \text{ prime}} \mathrm{Gal}(K_l/K).$$

Suppose for a moment that the fields K_l are linearly disjoint over K. This by definition means that the map above is an isomorphism (if this is not the case we say that the fields are entangled). Since the number of non-trivial automorphism in each Galois group $\mathrm{Gal}(K_l/K)$ is $[K_l : K] - 1$ we have that

$$\#H_n = \prod_{l|n, l \text{ prime}} ([K_l : K] - 1)$$

so

$$\delta_n(E) = \prod_{l|n, l \text{ prime}} \left(1 - \frac{1}{[K_l : K]}\right).$$

This suggests that in order to factor our density $\delta(E)$ we should find a finite set of primes such that for every prime outside this set the corresponding division fields over K are linearly disjoint. This is what we are going to do in what follows.

3.2 Group-theoretical preliminaries

In this section we want to recall some definitions and results from group theory. We will apply them to the study of the Galois groups of division field extensions of K.

3.2.1 Composition series

Let G be a fnite group. A subnormal sequence is a chain of subgroups

$$\{1\} = G_0 \lhd G_1 \lhd \cdots \lhd G_n = G$$

such that for every $i = 1, ..., n$, the subgroup G_{i-1} is normal in G_i. A subnormal sequence is called a composition series if for every $i = 1, ..., n$ the factor groups G_i/G_{i-1} are simple. In this case the quotients G_i/G_{i-1} are called composition factors of G. It is easy to see that every finite group G admits a composition series. All the composition series of a finite group G are "essentially the same" in the sense of the following theorem.

Theorem 3.2.1 (Jordan-Hölder)**.** *Let G be a finite group and let*

$$\{1\} = H_0 \lhd H_1 \lhd \cdots \lhd H_r = G \qquad \{1\} = K_0 \lhd K_1 \lhd \cdots \lhd K_t = G$$

be two composition series of G. Then $r = t$ and there exists $\sigma \in S_r$ such that for every $n = 1, ..., r$

$$H_n/H_{n-1} = K_{\sigma(n)}/K_{\sigma(n)-1}.$$

We now study how composition series behave under taking subgroups, quotients and direct products.

Let G be a finite group, $\{1\} = G_0 \lhd G_1 \lhd \cdots \lhd G_n = G$ a composition series for G. If $H \leqslant G$ then

$$\{1\} = H \cap G_0 \lhd H \cap G_1 \lhd \cdots \lhd H \cap G_n = H$$

is a subnormal sequence in H whose factors are isomorphic to subgroups of the composition factors of G: in particular we have for every $i = 1, ..., n$

$$(H \cap G_i)/(H \cap G_{i-1}) \hookrightarrow G_i/G_{i-1}.$$

In general the subnormal sequence above is not a composition series for H, but it can always be refined to a such a series.

Let now N be a normal subgroup of G. Then

$$\{1\} = \overline{G}_0 \lhd \overline{G}_1 \lhd \cdots \lhd \overline{G}_n = G/N$$

with $\overline{G}_i := G_iN/N$ for $i = 0, ...n$ is a subnormal series of G/N. The quotients $\overline{G}_i/\overline{G}_{i-1}$ are isomorphic to quotients of the factors G_i/G_{i-1}. Since by hypothesis the quotients G_i/G_{i-1} are composition factors, they cannot have non-trivial quotients. This implies that the quotients $\overline{G}_i/\overline{G}_{i-1}$ are either $\{1\}$ or isomorphic to G_i/G_{i-1}.

Finally let G_1, G_2 finite groups: then the composition factors of the direct product $G_1 \times G_2$ are precisely the union of the composition factors of G_1 and G_2 because the "concatenation" of two composition series of G_1 and G_2 will give a composition series of the product $G_1 \times G_2$.

3.2.2 The special linear group over a finite field

Let N be an integer and let $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ be the group of 2×2 invertible matrices with entries in $\mathbb{Z}/N\mathbb{Z}$. This is called the general linear group over $\mathbb{Z}/N\mathbb{Z}$. If $N = 0$ we have $\mathrm{GL}_2(\mathbb{Z})$, i.e. the group of invertible 2×2 matrices with integer coefficients.

Definition 3.2.2. *The special linear group* $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ *is the subgroup of* $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ *consisting of all the matrices with determinant 1.*

Lemma 3.2.3. *For every* $N \in \mathbb{N}_{>0}$ *the reduction modulo* N *induces a surjection*

$$\mathrm{SL}_2(\mathbb{Z}) \twoheadrightarrow \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}).$$

Proof. We just give a sketch of the proof. First we claim that if c, d, N are integers such that $\gcd(c, d, N) = 1$ then there exist two integers t, s such that $\gcd(c + tN, d + sN) = 1$. Let $c = c_1c_2$ with $c_2 = \gcd(c, N)$ so that $\gcd(c_1, N) = 1$. Hence there exist two integers u, v such that

$$c_1u + Nv = 1.$$

Putting $m := v(1 - d)$, we have that

$$d + mN \equiv 1 \mod c_1$$

and it is immediate to verify that c and $d + mN$ are coprime. This proves the claim. Let now $N > 0$ be an integer and

$$\begin{pmatrix} \overline{a} & \overline{b} \\ \overline{c} & \overline{d} \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$$

with $a, b, c, d \in \mathbb{Z}$. We want to lift this matrix to an element of $\mathrm{SL}_2(\mathbb{Z})$. The condition on the determinant implies that there exists $m \in \mathbb{Z}$ such that

$$ad - bc + mN = 1$$

so in particular $\gcd(d, c, N) = 1$. By the claim above there exists two integers c' and d' such that

$$c' \equiv \overline{c} \mod N,\ d' \equiv \overline{d} \mod N,\ \gcd(c', d') = 1.$$

We want to find $j, k \in \mathbb{Z}$ such that

$$\det \begin{pmatrix} a + jN & b + kN \\ c' & d' \end{pmatrix} = 1$$

By hypothesis there exist $h \in \mathbb{Z}$ such that $ad' - bc' = 1 + hN$ so the problem reduces to find $j, k \in \mathbb{Z}$ such that

$$h = kc' - jd'$$

This is possible using the Extended Euclidean Algorithm . □

If p is a prime number we use the usual notation $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ to denote the finite field with p elements.

Lemma 3.2.4. *The group* $\mathrm{SL}_2(\mathbb{F}_p)$ *is normal in* $\mathrm{GL}_2(\mathbb{F}_p)$ *and has order* $p(p^2 - 1)$.

Proof. We have a surjective morphism of groups

$$\det : \mathrm{GL}_2(\mathbb{F}_p) \to \mathbb{F}_p^\times$$

whose kernel is precisely $\mathrm{SL}_2(\mathbb{F}_p)$. This shows that $\mathrm{SL}_2(\mathbb{F}_p)$ is normal in $\mathrm{GL}_2(\mathbb{F}_p)$. It is immediate to see that the order of $\mathrm{GL}_2(\mathbb{F}_p)$ is $(p^2-1)(p^2-p)$. So the first isomorphism theorem gives

$$|\mathrm{SL}_2(\mathbb{F}_p)| = \frac{(p^2-1)(p^2-p)}{p-1} = p(p^2-1).$$

□

Inside $\mathrm{SL}_2(\mathbb{F}_p)$ there is the normal subgroup $\{\pm I\}$. The quotient group

$$\mathrm{PSL}_2(\mathbb{F}_p) := SL_2(\mathbb{F}_p)/\{\pm I\}$$

is called the projective special linear group over $\mathbb{F}_p$. It is well known (see for instance [5]) that if $p \geq 5$ then $\mathrm{PSL}_2(\mathbb{F}_p)$ is a simple group. Hence in $\mathrm{SL}_2(\mathbb{F}_p)$ there is the following composition series:

$$\{1\} \lhd \{\pm I\} \lhd \mathrm{SL}_2(\mathbb{F}_p). \tag{3.1}$$

We now want to prove that $\mathrm{SL}_2(\mathbb{F}_p)$ does not have subgroups of index 2 for p sufficently large. We need a lemma.

Lemma 3.2.5. *Let $p \geq 5$ be a prime number. Then $\mathrm{SL}_2(\mathbb{F}_p)^{ab}$ is trivial.*

Proof. In this proof if G is a group then G' denotes the derived subgroup and $G^{ab} := G/G'$ denotes the abelianized group.

Fix $p \geq 5$ a prime. It is well known that the group $\mathrm{PSL}_2(\mathbb{Z}) := \mathrm{SL}_2(\mathbb{Z})/\{\pm I\}$ has the following presentation (see for example [4] appendix A):

$$\mathrm{PSL}_2(\mathbb{Z}) = \langle A, B : A^2 = 1, B^3 = 1 \rangle.$$

Hence the abelianized can be presented as

$$\mathrm{PSL}_2(\mathbb{Z})^{ab} = \langle A, B : A^2 = 1, B^3 = 1, AB = BA \rangle \cong \mathbb{Z}/6\mathbb{Z}.$$

We deduce that $|\mathrm{PSL}_2(\mathbb{Z})^{ab}| = 6$ (in the notations above it contains the six elements $1, A, B, AB, B^2, AB^2$). Using the definitions it is easy to see that

$$\mathrm{PSL}_2(\mathbb{Z})^{ab} \cong \frac{\mathrm{SL}_2(\mathbb{Z})}{\{\pm I\}\,\mathrm{SL}_2(\mathbb{Z})'}$$

and using the multiplicativity of the indeces we have

$$\begin{aligned} |\mathrm{SL}_2(\mathbb{Z})^{ab}| = |\mathrm{SL}_2(\mathbb{Z}) : \mathrm{SL}_2(\mathbb{Z})'| &= |\mathrm{SL}_2(\mathbb{Z}) : \{\pm I\}\,\mathrm{SL}_2(\mathbb{Z})'||\{\pm I\}\,\mathrm{SL}_2(\mathbb{Z})' : \mathrm{SL}_2(\mathbb{Z})'| \\ &= 6 \cdot |\{\pm I\}\,\mathrm{SL}_2(\mathbb{Z})' : \mathrm{SL}_2(\mathbb{Z})'|. \end{aligned}$$

Since the latter index is clearly either 1 or 2 we deduce that the order of $\mathrm{SL}_2(\mathbb{Z})^{ab}$ is either 6 or 12.

Now by 3.2.3 for every $m \in \mathbb{N}$ the reduction modulo m gives a surjection $\mathrm{SL}_2(\mathbb{Z}) \twoheadrightarrow \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})$ which induces a surjection

$$\mathrm{SL}_2(\mathbb{Z})^{ab} \twoheadrightarrow \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})^{ab}.$$

It can be directly checked that $|\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})^{ab}| = 3$ and $|\mathrm{SL}_2(\mathbb{Z}/4\mathbb{Z})^{ab}| = 4$. This, along with the surjection above, in particular implies that $|\mathrm{SL}_2(\mathbb{Z})^{ab}| = 12$. Let

$n := 12p$: since $p \neq 2, 3$ by assumption, the Chinese Reminder Theorem gives

$$\mathrm{SL}_2(\mathbb{Z})^{ab} \twoheadrightarrow \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})^{ab} \cong \mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})^{ab} \times \mathrm{SL}_2(\mathbb{Z}/4\mathbb{Z})^{ab} \times \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})^{ab}$$

and, by counting the orders, this gives $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})^{ab} = \{1\}$ as wanted. □

Corollary 3.2.6. *For $p \geq 5$ prime the group $\mathrm{SL}_2(\mathbb{F}_p)$ does not have a subgroup of index two.*

Proof. Any index 2 subgroup of $\mathrm{SL}_2(\mathbb{F}_p)$ would be normal with cyclic quotient of order 2. This in particular implies that the given subgroup contains the derived subgroup, which contradicts the previous lemma. □

3.3 The factorization of the density

Let K be a number field and E an elliptic curve defined over K without complex multiplication. In this section we will prove that the density $\delta(E)$ found in chapter 2 can be factorized into a finite sum and an infinite product that never vanishes. In order to do this, we first need to prove a fundamental theorem; as usual for every $n \in \mathbb{N}$, K_n denotes the n-division field over K.

Theorem 3.3.1. *Let K be a number field and E an elliptic curve defined over K without complex multiplication. Let S be the set of all prime numbers p such that:*

- $p \mid 6\,\mathrm{disc}(K/\mathbb{Q})$.
- *p lies under one of the prime ideals in $\mathfrak{O}_K$ dividing the discriminant Δ_E of E.*
- $\mathrm{Gal}(K_p/K) \ncong \mathrm{GL}_2(\mathbb{F}_p)$.

For every $x > \max S$, let

$$N_x := \prod_{p \leq x} p.$$

Then $K_l \cap K_{N_x} = K$ for every prime $l > x$.

Remark 3.3.2. *Notice that S is a finite set because of theorem 1.3.12.*

Proof. We divide the proof in several steps. Let l be a prime number greater than N_x. Recall that by proposition 1.3.14 if ζ_l denotes a primitive l-th root of unity, then $K(\zeta_l) \subseteq K_l$.

Step 1. We have $[K(\zeta_l) : K] = l - 1$ and $\mathrm{Gal}(K(\zeta_l)/K) \cong \mathbb{F}_l^*$.

Proof. Notice that $\mathbb{Q}(\zeta_l) \cap K = \mathbb{Q}$ since K is unramified at l by the way we chose l whereas the cyclotomic field $\mathbb{Q}(\zeta_l)$ is totally ramified at l. Since both $K(\zeta_l)/K$ and $\mathbb{Q}(\zeta_l)/\mathbb{Q}$ are normal extensions, from Galois theory we have:

$$\mathrm{Gal}(K(\zeta_l)/K) \cong \mathrm{Gal}(\mathbb{Q}(\zeta_l)/\mathbb{Q}(\zeta_l) \cap K) \cong \mathrm{Gal}(\mathbb{Q}(\zeta_l)/\mathbb{Q}) \cong \mathbb{F}_l^*$$

and this gives the result. □

Step 2. We have $K(\zeta_l) \cap K_{N_x} = K$.

Proof. Suppose by contradiction that $K(\zeta_l) \cap K_{N_x} \neq K$. Consider a prime ideal $\mathfrak{p} \subseteq \mathfrak{O}_K$ which lies above l. By the way we have chosen l we know that l is totally ramified in $\mathbb{Q}(\zeta_l)$ while l does not ramify in K. This together with Step 1 implies that $\mathfrak{p}$ is totally ramified in $K(\zeta_l)$ and consequently $\mathfrak{p}$ ramifies in $K(\zeta_l) \cap K_{N_x}$. But then $\mathfrak{p}$ ramifies in K_{N_x} which, by proposition 1.3.13, implies that either $\mathfrak{p}$ divides N_x or $\mathfrak{p}$ divides Δ_E. None of these two cases is possible by the way we chose l. Hence $K(\zeta_l) \cap K_{N_x} = K$. □

Step 3. We have $\mathrm{Gal}(K_l/K(\zeta_l)) \cong \mathrm{SL}_2(\mathbb{F}_l)$.

Proof. There is a restriction map

$$\mathrm{Gal}(K_l/K) \to \mathrm{Gal}(K(\zeta_l)/K)$$

and the kernel is clearly $\mathrm{Gal}(K_l/K(\zeta_l))$. Moreover $\mathrm{GL}_2(\mathbb{F}_l) \cong \mathrm{Gal}(K_l/K)$ by the way we chose l. On the other hand, by proposition 1.3.15, the restriction is given by

$$\sigma \longmapsto (\zeta_l \mapsto \zeta_l^{\det(\sigma)})$$

and the kernel of this map is $\mathrm{SL}_2(\mathbb{F}_l)$. This gives the isomorphism above. □

Step 4. If $K_l \cap K_{N_x}(\zeta_l) = K(\zeta_l)$ then $K_l \cap K_{N_x} = K$.

Proof. This is immediate from the identity

$$K_l \cap K_{N_x} = K_l \cap K_{N_x}(\zeta_l) \cap K_{N_x} = K(\zeta_l) \cap K_{N_x} = K$$

where in the last passage we used Step 2. □

So we are reduced to prove that $K_l \cap K_{N_x}(\zeta_l) = K(\zeta_l)$. Suppose by contradiction that this is not true and call F the intersection. Hence $K(\zeta_l) \subsetneq F$. Notice that both $K_l/K(\zeta_l)$ and $K_{N_x}/K(\zeta_l)$ are Galois extensions: the first because of proposition 1.3.11, the second because K_{N_x} is the compositum of all K_p for $p \mid N_x$ (since N_x is squarefree) which are Galois extensions of K. Hence also $F/K(\zeta_l)$ is a Galois extension. We are going to study its Galois group $G := \mathrm{Gal}(F/K(\zeta_l))$ and to deduce a contradiction.

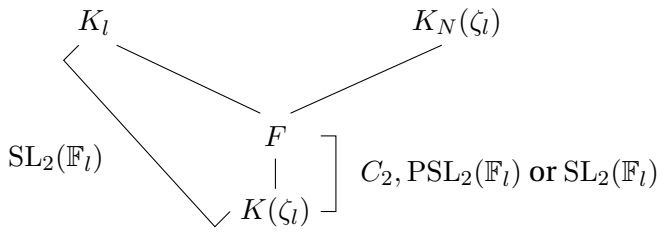


FIGURE 3.1: Possiblities for the Galois group of F over $K(\zeta_l)$.

By Step 3 we know that $\mathrm{Gal}(K_l/K(\zeta_l)) \cong \mathrm{SL}_2(\mathbb{F}_l)$. A composition series of $\mathrm{SL}_2(\mathbb{F}_l)$ is given by

$$\{1\} \lhd \{\pm I\} \lhd \mathrm{SL}_2(\mathbb{F}_l)$$

with composition factors C_2 (a cyclic group of order 2) and $\mathrm{PSL}_2(\mathbb{F}_l)$ (which is simple as we recalled in the previous paragraph). Since the Galois group G is isomorphic to a quotient of $\mathrm{Gal}(K_l/K(\zeta_l))$, the possible composition factors of G (which by theorem 3.2.1 are independent from the particular composition series) are

1. C_2.
2. $\mathrm{PSL}_2(\mathbb{F}_l)$.
3. C_2, $\mathrm{PSL}_2(\mathbb{F}_l)$.

We can immediately exclude the first case: if $G \cong C_2$ then $\mathrm{SL}_2(\mathbb{F}_l)$ would have a subgroup of index two, which is impossible by corollary 3.2.6, since $l \geq 5$ by assumption.

To exclude the other two cases we are going to analyze $\mathrm{Gal}(K_{N_x}(\zeta_l)/K(\zeta_l))$. We know that $K_{N_x}(\zeta_l)$ is the compositum of $K(\zeta_l)$ with all the division fields K_p, $p \mid N_x$. Hence we have the following inclusions:

$$\mathrm{Gal}(K_{N_x}(\zeta_l)/K(\zeta_l)) \leqslant \mathrm{Gal}(K_{N_x}(\zeta_l)/K) \hookrightarrow \mathbb{F}_l^* \times \prod_{p|N_x} \mathrm{Gal}(K_p/K) \leqslant \mathbb{F}_l^* \times \prod_{p|N_x} \mathrm{GL}_2(\mathbb{F}_p).$$

We deduce that a composition series for $\mathrm{Gal}(K_{N_x}(\zeta_l)/K(\zeta_l))$ can be obtained by refining the intersection of a composition series of the group on the right hand side with $\mathrm{Gal}(K_{N_x}(\zeta_l)/K(\zeta_l))$. The composition factors will be quotients of subgroups of the original composition factors. We know that the composition factors of a direct product of groups are just the union of the composition factors of the groups appearing in the product.
Suppose now that we are in case 2 or 3 above. Then $\mathrm{PSL}_2(\mathbb{F}_l)$ should appear as quotient of subgroups of the composition factors of either $\mathbb{F}_l^*$ or $\mathrm{GL}_2(\mathbb{F}_p)$ for some prime p dividing N_x. We can immediately exclude $\mathbb{F}_l^*$ because it is an abelian group and this property is preserved when taking subgroups and quotients. As far as $\mathrm{GL}_2(\mathbb{F}_p)$ is concerned we have the following subnormal sequence:

$$\{1\} \lhd \{\pm I\} \lhd \mathrm{SL}_2(\mathbb{F}_p) \lhd \mathrm{GL}_2(\mathbb{F}_p)$$

which can always be refined to a composition series. However $\mathrm{GL}_2(\mathbb{F}_p)/\mathrm{SL}_2(\mathbb{F}_p) \cong \mathbb{F}_p^*$ and $\{\pm I\} \cong C_2$ are abelian groups, so all the composition factors coming from here will be abelian too. The group $\mathrm{PSL}_2(\mathbb{F}_l)$ cannot appear as quotient of subgroups of them. The group $\mathrm{SL}_2(\mathbb{F}_p)/\{\pm I\} \cong \mathrm{PSL}_2(\mathbb{F}_p)$ is already simple, so it is a composition factor of $\mathrm{GL}_2(\mathbb{F}_p)$. Since $l > p$ by the way we chose l, $\mathrm{PSL}_2(\mathbb{F}_l)$ cannot appear as quotient of subgroups of $\mathrm{PSL}_2(\mathbb{F}_p)$.

The analysis allows us to exclude also cases 2 and 3. We deduce that $F = K(\zeta_l)$ and by Step 4 this proves the theorem. □

Using the theorem above we can finally prove the main theorem of this section about the factorization of the density.

Theorem 3.3.3. *Let K be a number field and E an elliptic curve defined over K without complex multiplication. Then, under GRH, the density of the set of primes of K for which E has a cyclic reduction is*

$$\delta(E) = \left(\sum_{d|N} \frac{\mu(d)}{[K_d : K]} \right) \prod_{l \nmid N,\ l \text{ prime}} \left(1 - \frac{1}{[K_l : K]} \right)$$

where

$$N := \prod_{p \leq \max S} p$$

with S as in theorem 3.3.1. Moreover the infinite product never vanishes.

Proof. As in section 1 for $n \in \mathbb{N}$ squarefree define

$$\delta_n(E) := \sum_{d|n} \frac{\mu(d)}{[K_d : K]}$$

and

$$H_n := \{\sigma \in \mathrm{Gal}(K_n/K) : \sigma|_{K_l} \neq \mathrm{id}_{K_l} \text{ for every prime } l \mid n\}.$$

Let l be the smallest prime which does not divide N; an element of H_{Nl} is obtained by extending an automorphism in H_N to an automorphism of K_{Nl} which is not the identity on K_l. This can be done in $[K_{Nl} : K_N] - 1$ ways. By theorem 3.3.1 we know that $[K_{Nl} : K_N] = [K_l : K]$: we deduce that

$$\#H_{Nl} = ([K_l : K] - 1)\#H_N.$$

Again by theorem 3.3.1 and by Galois theory we have $[K_{Nl} : K] = [K_N : K][K_l : K]$. Hence we get

$$\delta_{Nl}(E) = \frac{\#H_{Nl}}{[K_{Nl} : K]} = \frac{[K_l : K] - 1}{[K_l : K]} \cdot \frac{\#H_N}{[K_N : K]} = \delta_N(E)\left(1 - \frac{1}{[K_l : K]}\right).$$

For any increasing squarefree multiple N' of N, it follows by induction on the number of prime numbers dividing N'/N and 3.3.1 that

$$\delta_{N'}(E) = \delta_N(E) \prod_{l|N'/N,\, l \text{ prime}} \left(1 - \frac{1}{[K_l : K]}\right)$$

so taking the limit we get

$$\delta(E) = \delta_N(E) \prod_{l \nmid N,\, l \text{ prime}} \left(1 - \frac{1}{[K_l : K]}\right).$$

The product on the right is clearly never vanishing since for $l \nmid N$ the Galois group of K_l/K is the full $\mathrm{GL}_2(\mathbb{F}_l)$ so in particular $[K_l : K] = (l^2 - 1)(l^2 - l)$. □

Corollary 3.3.4. *Let K be a number field and E an elliptic curve defined over K without complex multiplication. Then, under GRH, the density of the set of primes of K for which E has a cyclic reduction is always a rational multiple of the full product*

$$A(E) = \prod_{l \text{ prime}} \left(1 - \frac{1}{[K_l : K]}\right)$$

The product $A(E)$ appearing in corollary 3.3.4 is called "naive density" because it represents the density of the primes for which an elliptic curve E has cyclic reduction under the hypothesis that all the division fields K_l for l prime are linearly disjoint over K. Clearly this is not always the case, and the corollary says that the real density is always the product of the naive density with a rational correction factor. Notice that when the $\mathrm{mod}\ l$ Galois representations associated to E have full

image $\mathrm{GL}_2(\mathbb{F}_l)$ for every l prime, then $[K_l : K] = (l^2-1)(l^2-l)$ for every prime l and the naive density has the value

$$A_\infty = \prod_{l \text{ prime}} \left(1 - \frac{1}{(l^2-1)(l^2-l)}\right) \approx 0.813751906106816.$$

The constant A_∞ is called the universal Artin constant for elliptic curves without CM. Since for a generic elliptic curve E without complex multiplication the $\mathrm{mod}\ l$ Galois representation is surjective for almost all the primes l, we deduce that the density $\delta(E)$ is always a rational multiple of the universal Artin constant.

We conclude by saying that in case the elliptic curve E has complex multipication the theory becomes more complicated and in general one cannot factor the density as we did in this chapter for non-CM curves. Indeed in the CM case the division fields K_l can be entangled for every prime l and this causes the strategy we used to factor the density for non-CM elliptic curves fail in this case: we will see an example of this phenomenon in the final chapter of this thesis.

Chapter 4

Non-trivial examples for the vanishing of the density

For an elliptic curve E defined over a number field K we denote by $\delta_K(E)$ the density of the set of prime ideals in K for which the reduction of E is good and cyclic. In this chapter we are concerned about finding examples of elliptic curves E and number fields K such that E is defined over K and $\delta_K(E) = 0$.

4.1 What "non-trivial" means

Given K a number field and E an elliptic curve defined over K, we know by chapter 1 that the density $\delta_K(E)$ is equal to the density of the set of primes in K that do not split completely in any division field K_l with l prime. The fact that a prime ideal $\mathfrak{p}$ splits completely in a division field K_l is equivalent to the residue field $k_\mathfrak{p} := \mathfrak{O}_K/\mathfrak{p}$ containing the full l-torsion of the reduced elliptic curve $\tilde{E}(k_\mathfrak{p})$. This implies that if the field K already contains the full l-torsion of E then every non-ramifying prime must split completely in K_l. This gives the following.

Lemma 4.1.1. *Let E be an elliptic curve defined over a number field K. If K contains the full l-torsion of E for some prime l then $\delta_K(E) = 0$.*

Definition 4.1.2. *Let E be an elliptic curve defined over a number field K. The pair (E, K) is called an example for the vanishing of the density if $\delta_K(E) = 0$. An example for the vanishing of the density (E, K) will be called trivial if K contains the full l-torsion of E for some rational prime l.*

It is easy to construct trivial examples: take E/K any elliptic curve. Then the pair (E, K_l) will always be a trivial example for the vanishing of the density for any prime l. The point here is that we can always enlarge the number field of definition of any elliptic curve E: if $K \subseteq L$ is a field extension and E is defined over K, then clearly E is also defined over L.

Fix now $K = \mathbb{Q}$: we want to characterize the trivial examples of the form $(E, \mathbb{Q})$.

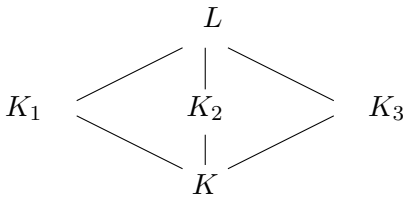
Lemma 4.1.3. *Let E be an elliptic curve defined over $\mathbb{Q}$. The pair $(E, \mathbb{Q})$ is a trivial example for the vanishing of $\delta_\mathbb{Q}(E)$ if and only if $\mathbb{Q}$ contains the full 2-torsion of E.*

Proof. If $\mathbb{Q}$ contains the full 2-torsion of E then the pair $(E, \mathbb{Q})$ is a trivial example by definition. On the other hand the field of rational numbers cannot contain the full l-torsion of E for any $l > 2$: indeed by proposition 1.3.15 the field $\mathbb{Q}(E[l](\overline{\mathbb{Q}}))$ always contains the cyclotomic extension $\mathbb{Q}(\zeta_l)$ which strictly contains $\mathbb{Q}$ if $l > 2$. This proves the lemma. □

On the other hand R. Murty and R. Gupta proved in [13] (theorem 1) that the only examples $(E, \mathbb{Q})$ for the vanishing of the density are the trivial ones. Hence over the rational numbers it is impossible to find non-trivial examples.

The aim of this chapter is to find non-trivial examples (E, K) with K a number field different from $\mathbb{Q}$. In order to do so we will make use of the following lemma.

Lemma 4.1.4. *Let L/K be a Galois extension of number fields with $\mathrm{Gal}(L/K) \cong V_4$ the Klein group and let $K \subseteq K_1, K_2, K_3 \subseteq L$ be the three intermediate fields of the extension. Then every prime ideal $\mathfrak{p}$ in K which does not ramify in L splits completely in at least one between K_1, K_2, K_3.*



Proof. Let $\mathfrak{p} \subseteq \mathfrak{O}_K$ be a prime ideal that does not ramify in L. The extension L/K is abelian, so there exists a unique Frobenius element $\mathrm{Frob}_\mathfrak{p} \in \mathrm{Gal}(L/K) \cong V_4$ associated to $\mathfrak{p}$. Since every automorphism of $\mathrm{Gal}(L/K)$ must be the identity on some K_i for $i = 1, 2, 3$, by restrcting the Frobenius element associated to $\mathfrak{p}$ we deduce that $\mathfrak{p}$ must split completely in at least one between K_1, K_2, K_3. □

Since there is just a finite number of prime ideals which ramify in L, the lemma above implies that the set of primes in K that do not split completely in any of the fields K_1, K_2, K_3 has zero density.

4.2 Non-trivial examples

Theorem 4.2.1. *Let E be an elliptic curve defined over a number field K without complex multiplication. Then there are infinitely many finite extensions F of K such that the pairs (E, F) are non-trivial examples for the vanishing of the density $\delta_F(E)$.*

Proof. Let S be the set of rational primes as in theorem 3.3.1 and choose three consecutive rational primes $p_1, p_2, p_3 > \max S$. By theorem 3.3.1 we know that the three division fields $K_{p_1}, K_{p_2}, K_{p_3}$ over K are all linearly disjoint over K and for $i = 1, 2, 3$ we have $\mathrm{Gal}(K_{p_i}/K) \cong \mathrm{GL}_2(\mathbb{F}_{p_i})$. This implies in particular that

$$\mathrm{Gal}(K_{p_1p_2p_3}/K) \cong \prod_{i=1}^{3} \mathrm{Gal}(K_{p_i}/K) \cong \mathrm{GL}_2(\mathbb{F}_{p_1}) \times \mathrm{GL}_2(\mathbb{F}_{p_2}) \times \mathrm{GL}_2(\mathbb{F}_{p_3})$$

where $K_{p_1p_2p_3} = \mathrm{Compositum}(K_{p_1}, K_{p_2}, K_{p_3})$. Let $I_j \in \mathrm{GL}_2(\mathbb{F}_{p_j})$ be the identity automorphism in the corresponding Galois group of K_{p_j} over K. Using the isomorphism above we have

$$H := \{\pm I_1\} \times \{\pm I_2\} \times \{\pm I_3\} \leqslant \mathrm{Gal}(K_{p_1p_2p_3}/K).$$

The group H is of order 8 since $p_i > \max S > 2$ for every $i = 1, 2, 3$. Define then the following subgroup of H:

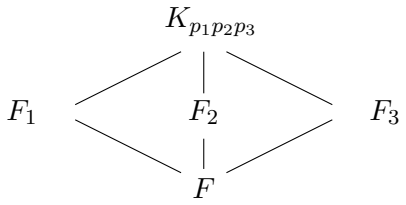
$$G := \{(A, B, C) \in H : \mathrm{sgn}(A)\,\mathrm{sgn}(B)\,\mathrm{sgn}(C) = 1\} \leqslant \mathrm{Gal}(K_{p_1p_2p_3}/K)$$

The subgroup G is of order 4 and exponent 2, hence $G \cong V_4$ the Klein group. Define $F := K_{p_1p_2p_3}^G$ (i.e. F is the subfield fixed by G in $K_{p_1p_2p_3}$) and let

$$G_1 := \langle (I_1, -I_2, -I_3) \rangle \qquad G_2 := \langle (-I_1, I_2, -I_3) \rangle \qquad G_3 := \langle (-I_1, -I_2, I_3) \rangle$$

be the three non-trivial subgroups of G. Put $F_i := \mathrm{Compositum}(F, K_{p_i})$ for $i = 1, 2, 3$: it is clear that for all such i's, F_i is the p_i-division field over F.

We claim that $K_{p_1p_2p_3}^{G_i} = F_i$ for every $i = 1, 2, 3$. Clearly $F_i \subseteq K_{p_1p_2p_3}^{G_i}$ because the group G_i fixes F (by definition of F) and K_{p_i} (by definition of the group G_i). If $F_i \neq K_{p_1p_2p_3}^{G_i}$ then $F_i \subseteq F$ since $[K_{p_1p_2p_3}^{G_i} : F] = 2$ so in particular we would have $K_{p_i} \subseteq F$. But this is impossible since K_{p_i} is not fixed by every automorphism of G. Hence $K_{p_1p_2p_3}^{G_i} = F_i$ for every $i = 1, 2, 3$ and this proves the claim.
We have managed to construct the following diagram of fields:



where $\mathrm{Gal}(K_{p_1p_2p_3}/F) \cong V_4$ and F_i is the p_i-th division field over F. By corollary 1.4.5 and lemma 4.1.4 we deduce that the pair (E, F) is an example for the vanishing of $\delta_F(E)$. Clearly for different choices of consecutive p_i's we obtain different fields F since they all have different degrees over K.

What is left to prove is that the examples (E, F) are non-trivial i.e. that F does not contain the full l-torsion of E for any prime l. We will just sketch the proof of this since it is very similar to the proof of theorem 3.3.1. Clearly F cannot contain the full p_i-torsion for $i = 1, 2, 3$ by construction. Moreover the field $K_{p_1p_2p_3}$ is linearly disjoint from all the fields K_l for $l > \max_{i=1,2,3}\{p_i\}$ by theorem 3.3.1. This implies that the field F cannot contain the full l-torsion for any $l > \max_{i=1,2,3}\{p_i\}$. It remains to prove that F does not contain the full l-torsion for every prime $l < \min_{i=1,2,3}\{p_i\}$. This can be done by showing that the field $K_{p_1p_2p_3}$ is linearly disjoint over K with the field

$$K_N := \mathrm{Compositum}(K_l : l < \min_{i=1,2,3}\{p_i\}).$$

We already know that $K_{p_1} \cap K_N = K$ by theorem 3.3.1. Imitating the same proof first with the field $K_{p_1p_2}$ and then with the field $K_{p_1p_2p_3}$ gives the result. □

Remark 4.2.2. *We notice that the proof of the above theorem can be weakened in two ways:*

1. *We do not really need the condition* $\mathrm{Gal}(K_{p_i}/K) \cong \mathrm{GL}_2(\mathbb{F}_{p_i})$*: it just suffices to have an element* $\sigma_i \in \mathrm{Gal}(K_{p_i}/K)$ *of order* 2.

2. *We do not really need the fact that* $\mathrm{Gal}(K_{p_1p_2p_3}/K) \cong \prod_{i=1}^3 \mathrm{Gal}(K_{p_i}/K)$*; we always have an injection* $\mathrm{Gal}(K_{p_1p_2p_3}/K) \hookrightarrow \prod_{i=1}^3 \mathrm{Gal}(K_{p_i}/K)$ *and we just need that the image of this map contains the subgroup* $\langle\sigma_1\rangle \times \langle\sigma_2\rangle \times \langle\sigma_3\rangle$.

The theorem above tells that for an elliptic curve without complex multiplication defined over a number field K we can find infinitely many extensions F/K for which the density $\delta_F(E)$ non-trivially vanishes. In principle one could compute

these extensions F/K but in practice their degree is too big to do so. This leaves out an open question: can we find an elliptic curve and a field F of "small degree" such that the pair (E,F) is a non trivial example for the vanishing of the density? One way to tackle this problem may be to find an elliptic curve defined over the rationals for which is possible to repeat the same construction seen in the proof of the theorem using the $2,3$ and 5-division fields over $\mathbb{Q}$.

Chapter 5

Conclusions: some numerical examples over the field of rationals

We want to conclude this thesis by discussing the numerical examples that we provided in table 1.4 since we have now all the necessary tools to understand the densities appearing. The notations used in the examples are as in chapter 1: if E is an elliptic curve defined over $\mathbb{Q}$ we will call $d(E)$ the quotient between the number of primes up to 10^6 for which E has cyclic reduction and the total number of primes up to 10^6. To get information about the Galois representations of the elliptic curves we used the online database LMFDB, http://www.lmfdb.org. As usual for every l prime K_l will denote the l-division field over $\mathbb{Q}$.
As we explained at the end of chapter 3, the density of the the set of primes of cyclic reduction for a given elliptic curve E is a rational multiple of the naive density

$$A(E) = \prod_{l \text{ prime}} \left(1 - \frac{1}{[K_l : \mathbb{Q}]}\right).$$

The correction factors for $A(E)$ are usually very close to 1 so the real density $\delta(E)$ is mostly determined by the splitting behaviour of primes in the 2-division field and in the 3-division field, since the degree of the division fields rapidly grows. Recall also that when E does not have complex multiplication then the density is actually a rational multiple of the universal Artin constant

$$A_\infty \approx 0.813751906106816$$

while in case E has CM the density is a rational multiple of an Artin constant $A_{\infty,D}$ depending on the ring of endomorphisms $\mathfrak{O}_D$ of E.

Example 1. Let E be the elliptic curve defined by

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

Then the computations show that for no prime of good reduction up to 10^6 the elliptic curve E has a cyclic reduction. In other words $d(E) = 0$. This is not a surprise: indeed the polynomial $x^3 - x$ splits completely over $\mathbb{Q}$, so all the 2-torsion points of E are defined over the rationals. As we explained in chapter 4 the pair $(E, \mathbb{Q})$ is a trivial example for the vanishing of the density.

Example 2. Let E be the elliptic curve defined by

$$E : y^2 = x^3 - 3x + 1.$$

The elliptic curve E does not have complex multiplication and computations show that $d(E) \approx 0.6510$. The polynomial $x^3 - 3x + 1$ is irreducible in this case but its discriminant is $D = 1296 = 2^4 \cdot 3^4$ which is a square in $\mathbb{Q}$. This means that the Galois group of $K_2/\mathbb{Q}$ is isomorphic to A_3 and so $[K_2 : \mathbb{Q}] = 3$. If $l \neq 2$, the $\bmod\ l$ Galois representation associated to E has maximal image $\mathrm{GL}_2(\mathbb{F}_l)$ for all primes l. In this case the density of the set of primes of cyclic reduction for E should be approximated by

$$\frac{6}{5} \cdot \frac{2}{3} \cdot A_\infty \approx 0.6510015$$

which agrees with our figure.

Example 3. Let E be the elliptic curve defined by:

$$E : y^2 = x^3 + 2x + 3.$$

The elliptic curve E does not have complex multiplication and computations here show that $d(E) \approx 0.4889$. Notice that E has precisely one rational 2-torsion point: indeed we can factor

$$x^3 + 2x + 3 = (x + 1)(x^2 - x + 3)$$

where all the factors are irreducible over $\mathbb{Q}$. This means that the 2-division field of E has degree 2 over $\mathbb{Q}$ and it is generated by the square root of the discriminant of the elliptic curve (hence by the square root of the discriminant of the polynomial $x^3 + 2x + 3$). Since we have that the discriminant $\Delta_E = -1 \cdot 2^4 \cdot 5^2 \cdot 11$, we deduce that $K_2 = \mathbb{Q}(\sqrt{-11})$. Since for every $m \in \mathbb{N}$ the m-division field over $\mathbb{Q}$ contains the m-th cyclotomic extension of the rationals, we have the inclusions

$$K_2 = \mathbb{Q}(\sqrt{-11}) \subseteq \mathbb{Q}(\zeta_{11}) \subseteq K_{11}.$$

Hence if a prime does not split completely in K_2 then automatically it does not split completely in K_{11}. This means that in the computation of the density we do not have to consider the factor $1 - 1/[K_{11} : \mathbb{Q}]$. Since E has surjective Galois representation for every prime $l \neq 2$, we need to multiply the naive density by the correction factor

$$\frac{[K_{11} : \mathbb{Q}]}{[K_{11} : \mathbb{Q}] - 1} = \frac{13200}{13199}.$$

Notice that this correction factor is very close to 1.
Hence we see that the expected density in this case is

$$\frac{13200}{13199} \cdot \frac{6}{5} \cdot \frac{1}{2} \cdot A_\infty \approx 0.4882881$$

which is consistent with our numerical computation.

Example 4. Let E be the elliptic curve defined by:

$$E : y^2 = x^3 - 12096x - 544752.$$

The elliptic curve does not have complex multiplication and numerical computations show that $d(E) \approx 0.4159$. For every prime $l \neq 3$, the $\bmod\ l$ Galois representation associated to E has maximal image $\mathrm{GL}_2(\mathbb{F}_l)$. The 3-division field instead is minimal i.e. $K_3 = \mathbb{Q}(\zeta_3)$ and so it has degree 2 over $\mathbb{Q}$. Notice that the discriminant $\Delta_E = -1 \cdot 2^{12} \cdot 3^{12} \cdot 19^3$ so the 2-division field K_2 contains the quadratic subfield $\mathbb{Q}(\sqrt{\Delta_E}) = \mathbb{Q}(\sqrt{-19})$. Since $\mathbb{Q}(\zeta_{19}) \subseteq K_{19}$ we see that the intersection $K_2 \cap K_{19}$ is non-trivial. Since $\mathrm{Gal}(K_{19}/\mathbb{Q}) \cong \mathrm{GL}_2(\mathbb{F}_{19})$ it is not difficult to see that we have the equality $K_2 \cap K_{19} = \mathbb{Q}(\sqrt{-19})$.

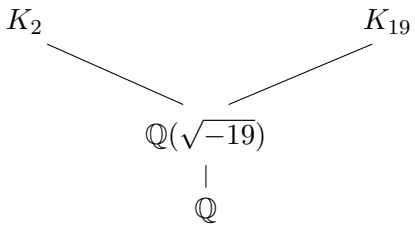


FIGURE 5.1: Entanglement between K_2 and K_{19}.

We want to compute the correction factor that arise from this entanglement between the division fields. Since $K_2 = \mathrm{Split}_{\mathbb{Q}}(x^3 - 12096x - 544752)$ and the latter polynomial is irreducible with a non-square discriminant, we have that $\mathrm{Gal}(K_2/\mathbb{Q}) \cong S_3$. By Chebotarev Density Theorem we know that:

1. For $1/6$ of the rational primes p the Frobenius element $\mathrm{Frob}_p \in \mathrm{Gal}(K_2/\mathbb{Q})$ is the identity.
2. For $1/2$ of the rational primes p the Frobenius element $\mathrm{Frob}_p \in \mathrm{Gal}(K_2/\mathbb{Q})$ has order 2.
3. For $1/3$ of the rational primes p the Frobenius element $\mathrm{Frob}_p \in \mathrm{Gal}(K_2/\mathbb{Q})$ has order 3.

Notice that the non-ramifying primes in (1) and (2) are precisely the primes p for which the Legendre symbol $\left(\frac{-19}{p}\right) = 1$ while the non-ramifying primes in (3) are those such that $\left(\frac{-19}{p}\right) = -1$. We know that $1/6$ of the rational primes p splits completely in K_2 and we have to disregard these in order to compute the density of the primes for which E has cyclic reduction. We want to compute the fraction of the remaining primes that split completely in K_{19}: among these primes, $3/5$ are such that $\left(\frac{-19}{p}\right) = -1$ and $2/5$ are such that $\left(\frac{-19}{p}\right) = 1$. Primes of the first type clearly cannot split completely in K_{19}. So we have to compute the fraction of primes of the second type that split compltely in K_{19}. Since the probability that a prime ideal $\mathfrak{p}$ of $\mathbb{Q}(\sqrt{-19})$ splits completely in K_{19} is $2/n_{19}$ by Chebotarev Density theorem, this fraction must be equal to

$$\frac{2}{n_{19}} \cdot \frac{2}{5} = \frac{4}{5n_{19}}.$$

This means that in the product corresponding to the naive density we have to substitute the factor $1-\frac{1}{n_{19}}$ with the factor $1-\frac{4}{5n_{19}}$. The correction factor is then

$$\frac{1-\frac{4}{5n_{19}}}{1-\frac{1}{n_{19}}}=\frac{5n_{19}-4}{5n_{19}}=\frac{615596}{615595}$$

which is very close to 1. The expected density is then

$$\frac{48}{47}\cdot\frac{1}{2}\cdot\frac{615596}{615595}\cdot A_\infty\approx 0.4155335$$

which is consistent with our figure.

We want to remark here that there is a more general technique that one could use to compute correction factors caused by the dependences between the 2-division field and the other dvision fields: it is called "character sum method" and it is due to Lenstra, Moree and Stevenhagen (see [9]). Using this technique one can prove that, for a given elliptic curve E with discriminant Δ_E, if $D:=\mathrm{disc}(\mathbb{Q}(\sqrt{\Delta_E})/\mathbb{Q})$ is congruent to 1 modulo 4 then the correction factor for the naive density is

$$c_E=1+\prod_{l|2D,\ l\text{ prime}}\frac{-1}{[K_l:\mathbb{Q}]-1}.$$

For instance in example 3 we have $D=-11$ and the entanglement correction factor given by the character sum formula is in this case

$$c=1+\frac{1}{([K_2:\mathbb{Q}]-1)([K_{11}:\mathbb{Q}]-1)}=\frac{[K_{11}:\mathbb{Q}]}{[K_{11}:\mathbb{Q}]-1}$$

This is the same number that we computed in example 3. Similarly in example 4 the character sum method gives

$$c=1+\frac{1}{([K_2:\mathbb{Q}]-1)([K_{19}:\mathbb{Q}]-1)}=\frac{5[K_{19}:\mathbb{Q}]-4}{5([K_{19}:\mathbb{Q}]-1)}$$

which is the same correction that we heuristically computed.

Example 5. Let E be the elliptic curve defined by

$$E: y^2=x^3+x+3.$$

The elliptic curve does not have complex multiplication and computations show that $d(E)\approx 0.8141$. The polynomial x^3+x+3 is irreducible but its discriminant $d=-247$ is not a square in $\mathbb{Q}$. This means that the Galois group of $K_2/\mathbb{Q}$ is isomorphic to S_3 so $[K_2:\mathbb{Q}]=6$. Moreover the $\bmod\ l$ Galois representation associated to E has maximal image $\mathrm{GL}_2(\mathbb{F}_l)$ for all primes l. Hence in this case the naive density A_∞ above should approximate well the numerical results, and actually it does. Notice however that $\mathrm{disc}(\mathbb{Q}(\sqrt{\Delta_E})/\mathbb{Q})=\mathrm{disc}(\mathbb{Q}(\sqrt{-247})/\mathbb{Q})=-247$ is congruent to 1 modulo 4. This means that we have an entanglement correction factor given by the character sum formula:

$$c_E=1+\prod_{l|2\cdot 247,\ l\text{ prime}}\frac{-1}{[K_l:\mathbb{Q}]-1}=1-\frac{1}{([K_2:\mathbb{Q}]-1)([K_{13}:\mathbb{Q}]-1)([K_{19}:\mathbb{Q}]-1)}$$

This factor is really close to 1 so it cannot be seen numerically.

In this thesis we mostly dealt with elliptic curves without complex multiplication, and we just mentioned few times CM elliptic curves. However in this last example we want to study an elliptic curve with complex multiplication: the first reason is that we want to underline the differences from non-CM case. The second reason is that this example will carry along some questions that can in principle be the starting point for a new topic.

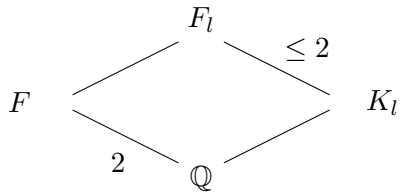
Example 6. Let E be the elliptic curve defined by

$$E : y^2 = x^3 - 1.$$

The elliptic curve E has complex multiplication by $(x, y) \mapsto (\zeta_3 x, y)$ where ζ_3 denotes a primitive third root of unity. In this case the endomorphism ring of E is isomorphic to $\mathbb{Z}[\zeta_3]$ and the CM-field is the third cyclotomic field $\mathbb{Q}(\zeta_3)$. In this case numerical computations show that $d(E) \approx 0.5002$. Notice that we can factor $x^3 - 1 = (x-1)(x^2 + x + 1)$ so we have

$$K_2 = \mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\zeta_3).$$

Hence in this case the 2-division field is precisely the CM-field of the elliptic curve. We want to show that this fact implies that K_2 is contained in K_l for every l prime. Since in this thesis we have not explained in detail the theory of Galois representations attached to CM elliptic curves we will show this using, without proof, some facts coming from that theory.
If $l = 2$ we already know that $K_2 = \mathbb{Q}(\zeta_3)$. For $l = 3$ we know by proposition 1.3.15 that $\mathbb{Q}(\zeta_3)$ is contained in K_3. Let then $l > 3$ be a prime number and let $F = \mathbb{Q}(\zeta_3)$ and $F_l = F(E[l](\overline{\mathbb{Q}}))$. We have the following diagram of fields:



Suppose by contradiction that $[F_l : K_l] = 2$. Then there exists an automorphism $\sigma \in G := \mathrm{Gal}(F_l/\mathbb{Q})$ of order 2 such that $F_l^\sigma = K_l$. Since the extension $K_l/\mathbb{Q}$ is Galois, the subgroup generated by σ is normal in G and this implies that $\sigma \in Z(G)$. Moreover $\sigma \notin \mathrm{Gal}(F_l/F)$ because it is a non trivial automorphism. We know from the first chapter that $\mathrm{Gal}(F_l/F) \cong (\mathfrak{O}/l\mathfrak{O})^*$ where $\mathfrak{O} = \mathbb{Z}[\zeta_3]$, and representation theory implies that we have

$$G \cong (\mathfrak{O}/l\mathfrak{O})^* \rtimes \langle\sigma\rangle$$

where the action of σ depends on the splitting of l in F.

1. If l splits completely in F, i.e. if $l \equiv 1 \bmod 3$, then $(\mathfrak{O}/l\mathfrak{O})^* \cong \mathbb{F}_l^* \times \mathbb{F}_l^*$ and σ acts by swapping the entries.
2. If l is inert in F, i.e. if $l \equiv 2 \bmod 3$, then $(\mathfrak{O}/l\mathfrak{O})^* \cong \mathbb{F}_{l^2}^*$ and σ acts as the Frobenius element $\mathrm{Frob}_l : x \mapsto x^l$.

It is not difficult to show, using the fact that σ has order 2 and is in the center og G, that none of the two cases are possible, and this leads to a contradiction. Hence

$K_l = F_l$ and this proves that K_l contains $F = K_2$ for every $l > 3$.
We remark that this situation is really different from the non-CM case; indeed in chapter 3 we proved that if the prime l is sufficiently large, then the division fields K_l of a non-CM elliptic curves are all linearly disjoint from each other. The situation above is completely different: all the division fields of prime index contain the 2-division field and so these fields are never linearly disjoint. This in particular implies that if a prime does not split completely in $K_2 = \mathbb{Q}(\zeta_3)$, then automatically it does not split completely in any K_l for l prime. Hence the primes of cyclic reduction are precisely the primes which are inert in $\mathbb{Q}(\zeta_3)$, i.e. the primes congruent to 1 modulo 3 (notice that 2 and 3 are primes of bad reduction for E). By the Chebotarev density theorem, the density of these primes is $1/2$, and this agrees with the numerical figure obtained.

The example above shows, en passant, that there is no hope to get a factorization theorem similar to theorem 3.3.3 in the CM-case, because the division fields in this case can all be entangled together. This means in particular that, even if we could in principle define an Artin constant associated to an elliptic curve with complex multiplication, the density of cyclic reduction is not necessarily a rational multiple of this constant (as in the previous example). For the elliptic curve $y^2 = x^3 - 1$ the problems arise from the fact that the 2-division field is also the CM-field. However this is not always the case: the elliptic curve of example 1 has clearly complex multiplication by the order $\mathbb{Z}[i]$, but its 2-division field is trivial. This discussion leads to a number of interesting questions that we will not answer here: when is the CM-field of an elliptic curve defined over the rationals and with complex multiplication contained in the 2-division field? Is it true that this happens if and only if the 2-division field is non-trivial? Is it true that the CM-field is contained in the l-division field for every $l \geq 3$? The answers to this questions can certainly shed some light on the entanglement of the division fields associated to an elliptic curve with complex multiplication.

Bibliography

[1] E. Artin, *Collected papers*, Addison-Wesley, 1965.

[2] C.F. Gauss, *Disquisitiones Arithmeticae*, 1801.

[3] C. Hooley, *On Artin's Conjecture*, J. Reine Angew. Math. **225**, 1967, 209-220.

[4] K. Conrad, $\mathrm{SL}_2(\mathbb{Z})$, expository notes, http://www.math.uconn.edu/ kconrad/blurbs/.

[5] K. Conrad, *Simplicity of* $\mathrm{PSL}_n(F)$, expository notes, http://www.math.uconn.edu/ kconrad/blurbs/.

[6] J. Lagarias, A. Odlyzko, *Effective versions of the Tchebotarev density theorem*, in "Algebraic Number Fields" (A. Fröhlich, Ed), Proceedings of the 1975 Durham Symposium, Academic Press, London/New York, 1977.

[7] S. Lang, H. Trotter, *Primitive Points on Elliptic Curves*, Bulletin of American Mathematical Society, Volume 83, n. 2, 1977.

[8] H.W. Lenstra Jr., *On Artin's conjecture and Euclid's algorithm in global fields*, Inventiones mathematicae, Volume 42, 1977.

[9] H.W. Lenstra Jr., P. Moree, P. Stevenhagen, *Character sums for primitive root densities*, Mathematical Proceedings of the Cambridge Philosophical Society, Volume 157 Issue 3, 2014.

[10] D. Marcus, *Number Fields*, Springer-Verlag New York, 1977.

[11] R. Murty, *On Artin's Conjecture*, Journal of Number Theory **16**, 1983, 147-168.

[12] R. Murty, K. Murty, *Non-vanishing of L-Functions and Applications*, Modern Birkhäuser Classics, 1997.

[13] R. Murty, R. Gupta, *Cyclicity and generation of points mod* p *on elliptic curves*, Inventiones mathematicae, Volume 101, pp 225-235, 1990.

[14] G. C. Rota, *On the foundation of combinatorial theory. 1. Theory of Möbius functions*, Z. Wahrsch. Verw. Gebiete **2**, 1964, 340-368.

[15] J.P. Serre, *Local fields*, Graduate Text in Mathematics, Springer, 1979.

[16] J.P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15**, 1972, 259-331.

[17] J.P. Serre, *Résumé des cours de 1977-1978*, Annuaire du Collége de France,1978, pp. 67-70.

[18] J.H. Silverman, J. Tate, *Rational Points on Elliptic Curves*, 2nd edition, Undergraduate Texts in Mathematics, Springer, 2015.

[19] J.H. Silverman, *The Arithmetic of Elliptic Curves*, 2nd edition, Springer-Verlag Graduate Texts in Mathematics 106, 2009.

[20] P. Stevenhagen, *The correction factor in Artin's primitive root conjecture*, Journal de Théorie des Nombres de Bordeaux, tome 15 no. 1, 2003.

[21] P. Stevenhagen, H.W. Lenstra Jr., *Chebotarev and his Density Theorem*, The Mathematical Intelligencer, Vol. 18 no. 2, 1996.