University of Groningen

BSc Thesis Mathematics

The Barreto-Naehrig method for elliptic curves with complex multiplication

Tysger Boelens

supervised by
prof. dr. Jaap Top and Max Kronberg, MSc

July 12, 2017

Contents

Preface **v**

Conventions **vii**

An informal introduction **ix**

Points on a quadratic curve ix

The group structure on cubic curves xi

1 Elliptic curves: an introduction **1**

1.1 General theory of elliptic curves 2

1.2 Elliptic curves over the rational numbers 13

1.3 Elliptic curves over finite fields 15

1.4 Elliptic curves over the complex numbers 18

2 The result of Barreto and Naehrig **25**

2.1 Determining the embedding degree 26

2.2 The parametrization 29

2.3 Making the curves 31

2.4 How often are $p(x)$ and $n(x)$ prime numbers? 34

3 Complex multiplication **37**

3.1 General theory 37

3.2 Complex multiplication with discriminant -3 and -11 43

3.3 The relation between the Frobenius and the 1- or 3-norm element 45
3.4 A family of curves with CM-discriminant −11 47

4 Extending the Barreto-Naehrig result 51

4.1 Testing curves with CM-discriminant −11 52
4.2 Testing curves with a small embedding degree 53
4.3 Testing curves with CM-discriminant −11 and small embedding degree 56
4.4 Recycling the $2x^2 + 1$-trace parametrization 59
4.5 Concluding remarks 60

A Just enough algebraic geometry 63

A.1 Affine varieties 63
A.2 Projective varieties 66

Bibliography 75

Index 77

Preface

In this thesis, we detail the reasoning of a paper ([1]) by Barreto and Naehrig. In this paper they describe an algorithm that generates without effort elliptic curves that are of interest to cryptographers. In this paper we will look at two quantities associated to these curves – the embedding degree 12 and the CM-discriminant -3 – and describe how one obtains curves with these values of these quantities, and how one can obtain curves with other embedding degrees or CM-discriminants. Then we use Magma and Sage to find curves with low embedding degree and CM-discriminant -11.

Before we start with Chapter 1, we give an informal introduction to elliptic curves and how one can define a group structure on them.

In Chapter 1 we go into the general theory of elliptic curves. We define concepts as the endomorphism ring and the j-invariant, and we mention results for curves over the rationals (such as the Mordell-Weil theorem), and the finite fields (here we discuss the Hasse bound and the trace of the Frobenius morphism). We finish the chapter with a discussion of the connection between lattices in $\mathbf{C}$ and elliptic curves, looking towards the theory of complex multiplication.

In Chapter 2 we discuss the calculations Barreto and Naehrig made in [1]. We define the embedding degree of a curve, and we give an easy way to determine it, given the size of a curve and the field it is defined over. Then we see how they used this result and a theorem from [2] to find a parametrization of the size of the curve and the size of the field. Finally we discuss their algorithm to generate elliptic curves with those properties.

Chapter 3 focuses on complex multiplication. First we describe the general theory, building further on Chapter 1. Then we describe a parametrization of sizes of curves and fields of elliptic curves with specific CM-discriminants (namely those of the curve Barreto and Naehrig used, and the CM-discriminant we want). We use this to find the j-invariant of the curves with CM-discriminant -11.

Chapter 4 contains all the code we used to find elliptic curves with a small

embedding degree and a small CM-discriminant. We list the code, the underlying theory and the results we found with the code. The chapter is concluded with a few remarks on the search efforts.

In Appendix A, at last, we give all the definitions from algebraic geometry we need in this thesis. The reader not familiar with concepts as projective varieties and rational maps is advised to read it (or skim it).

The last paragraph of this preface I'd like to use to thank a few people. First of all, I want to thank my supervisor Jaap Top for his patience and good advice, and for always finding some time to talk about the thesis. I also want to thank Max Kronberg for his efforts as secondary supervisor. I'm very grateful for all the support I received from my parents and my grandmother, even when the completion of the thesis seemed centuries away. I want to thank Ayla, Eline, Gerben, Joep and Matthijs for distracting me from my thesis once in a while, and most of all Yne, for the hours we spent writing and not writing.

Tysger Boelens,
11 juli 2017, Amstelveen

Conventions

In this thesis we will adopt the following conventions.

Z refers to the set of integers, **Q** to the set of rational numbers, **R** to the set of real numbers, **C** to the set of complex numbers and $\mathbf{F}_q$ to the finite field with q elements, q being a prime power (of p). $\mathbf{F}_p$ always refers to a prime field.

K will always be a field, and $\overline{K}$ the[1] algebraic closure of K.

Composition of functions will be denoted in the following way: $g \circ f$ is the function that sends x to $g(f(x))$.

Furthermore, results on elliptic curves do often not hold over fields of characteristic 2 or 3. Since this thesis is not concerned with curves over those fields, we will mostly ignore this issue: that is, results in the text may not be true over fields of characteristic 2 or 3! In [8], one can find all the details for what happens in that case.

[1] Actually, an algebraic closure of a field is not unique, but all algebraic closures of a given field are isomorphic, so we will ignore this point from now on and speak of 'the algebraic closure'.

An informal introduction

This chapter should be read as a very informal introduction to elliptic curves. Quite a number of technical points are ignored, for instance the issue of the multiplicity of intersection points. An interested reader can find all these details in for example [10].

Points on a quadratic curve

The question

> What are the rational solutions (x, y) of $x^2 + y^2 = 1$?

was asked and answered more than 2500 years ago: it appears as a Lemma to Propostion X.29 in Euclid's Elements.

Using more modern terms than Euclid had to his disposal, we can solve this with a geometric argument: find one rational solution (x_0, y_0), draw a line $y = \lambda x + c$ through (x_0, y_0) (so we set $c = y_0 - \lambda x_0$), and find the other intersection point of ℓ and the curve[2] $C : x^2 + y^2 = 1$.

For this we use a trick: suppose we have a quadratic equation $0 = x^2 + bx + c$ with a solution α and we want to find the other solution, say β. We can do this without using square roots, by noticing that the right hand side of the equation can be factored as $(x - \alpha)(x - \beta)$, i.e. $x^2 - (\alpha + \beta)x + \alpha\beta$: we see that $\beta = -b - \alpha$.
For future reference, we will prove this in general:

Lemma 0.1 *Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ be a polynomial defined over a field K, and suppose we have n roots $b_1, \ldots, b_n$ of this polynomial, where we list roots as often as their multiplicity. Then*

$$a_{n-1} = -(b_1 + \cdots + b_n),$$

[2] A curve is the set of all (x, y) in some field (in our case $\mathbf{Q}$) that satisfy $f(x, y) = 0$ for some polynomial f is two variables. A quadratic resp. cubic curve is a curve for which the degree of f in 2 resp. 3.

and if $b_1, \ldots, b_{n-1} \in K$*, then* $b_n \in K$ *too.*
Proof:
Since $b_1, \ldots, b_n$ are all the roots of f, we can write

$$f(x) = (x - b_1) \cdots (x - b_n).$$

If we work this out we get

$$f(x) = x^n - (b_1 + \cdots b_n)x^{n-1} + \cdots + (-1)^n b_1 b_2 \cdots b_n.$$

We know that coefficient of x^{n-1} is a_{n-1}, so the desired equality holds. Furthermore, we have

$$b_n = a_{n-1} + b_1 + \cdots + b_{n-1},$$

so b_n is the sum of elements in K and therefore in K too. □

We return to our line ℓ and curve C. The x-coordinate of any intersection point of those two needs to satisfy:

$$(\lambda x + (y_0 - \lambda x_0))^2 = y^2 = 1 - x^2.$$

We can rewrite this to

$$(\lambda^2 + 1)x^2 + 2\lambda(y_0 - \lambda x_0)x + (y_0 - \lambda x_0)^2 - 1 = 0.$$

This has the same solutions as

$$x^2 + \frac{2\lambda(y_0 - \lambda x_0)}{\lambda^2 + 1}x + \frac{(y_0 - \lambda x_0)^2 - 1}{\lambda^2 + 1} = 0.$$

Using our trick, we see that from our solution $x = x_0$ we can find the solution

$$x_1 = \frac{\lambda x_0 - y_0}{\lambda^2 + 1} - x_0,$$

which clearly is rational if λ is.

On the other hand, if (x_1, y_1) is a rational point (not equal to (x_0, y_0)), we have that the slope λ of the line connecting them is $\frac{y_1 - y_0}{x_1 - x_0}$: clearly a rational number. So all rational solutions are parametrized by λ: every choice of $\lambda \in \mathbf{Q}$ corresponds bijectively to a rational point on C.

Note that we ignore the case where $\lambda = \infty$, i.e. where the line is vertical. This case can be covered using projective coordinates. They are discussed in section A.2.

This example is characteristic: the rational points of all other quadratic curves with rational coefficients can be described in a similar way. The

natural next step would be to consider cubic curves. Clearly the method we used above breaks down: a line can intersect a cubic curve as many as three times: if we have one rational intersection point, we cannot just use the trick with coefficients to obtain another rational intersection point. We need to do something more complicated, namely use *two* rational points to get a third.

The group structure on cubic curves

The set of rational points on a cubic curve turns out to have a lot of structure: there is a natural way to make a group of it. We will now sketch how this is done.

The first step is to notice that every irreducible[3] smooth[4] cubic curve *with a rational point on it*, say

$$a_1x^3+a_2x^2y+a_3xy^2+a_4y^3+a_5x^2+a_6xy+a_7y^2+a_8x+a_9y+a_{10}=0, \quad (1)$$

is *birationally equivalent* to a smooth curve of the following form:

$$y'^2 = x'^3 + ax'^2 + bx' + c. \quad (2)$$

This form is called the *Weierstrass normal form*. 'Birationally equivalent' means that there are invertible rational maps (as defined in Definition A.27) that take almost every point of (1) to almost every point of (2). The exceptions are the points where the rational maps are not defined, i.e. the zeros of the polynomial in the denominator, but these points are generally easy to find.

We call a curve of the form (2) an *elliptic curve* if it is smooth. (We will formally define it in Definition 1.1) This happens precisely when the right hand side has no multiple roots, which is equivalent with the discriminant[5] of the polynomial on the right hand side being non-zero. (This discriminant is also referred to as the discriminant of the curve.) One can compute that the discriminant of the curve $y^2 = x^3+ax^2+bx+c$ is $-4a^3c+a^2b^2+18abc-4b^3-27c^3$.

We now adapt the method of the previous section. Suppose that we have *two* rational points P and Q on a elliptic curve E. The line ℓ through these points usually intersects the curve at a third point R. (The only exception

[3] An irreducible curve is a curve $f(x,y)=0$ such that there are no non-constant polynomials $g(x,y)$ and $h(x,y)$ such that $f(x,y)=g(x,y)h(x,y)$. [4] A smooth curve is a curve $f(x,y)=0$ with no points P on the curve such that $\frac{\mathrm{d}f}{\mathrm{d}x}=\frac{\mathrm{d}f}{\mathrm{d}y}=0$ in P. [5] The discriminant of a polynomial $f(x)$ is defined as $\prod_{i\neq j}(\alpha_i-\alpha_j)^2$ where $\alpha_1,\alpha_2,\ldots,\alpha_n$ is the list of roots of f counted with multiplicity. By definition, it vanishes exactly if two roots are equal.

is when ℓ is tangent to E in P or Q, or if ℓ is parallel to the y-axis.)
If two solutions of a monic cubic equation with rational coefficients are rational, then the third solution is also rational. This is true because the x^2-coefficient is the sum of the three solutions, by Lemma 0.1. It follows that the point R also has rational coordinates. We write $P*Q$ for R. Clearly $P * Q = Q * P$.

We now consider the 'exceptional cases'. In the case where $P = Q$, we take ℓ to be the tangent line (if it is not vertical) to E in P and proceed as above. If $P \neq Q$, but ℓ is tangent to the curve in P, we define $P * Q = P$.
In the remaining case, where ℓ is parallel to the y-axis, we use the following solution[6]: we define an extra point $\mathcal{O}$ that is not on the (x, y)-plane, but that we assume to be on every vertical line, and on E. With this definition, we have 3 intersection points of ℓ and E and we can define $P * Q = \mathcal{O}$.

However, since we added a new point, we need to define how it works with $*$. We want to define $P * \mathcal{O}$ for points P in the plane and $\mathcal{O} * \mathcal{O}$. There is an obvious way to define $P * \mathcal{O}$: we just draw the vertical line (since $\mathcal{O}$ lies per definition on this line) through P and look for the other intersection point with the curve E (or P itself, if the vertical line is a tangent line to E in P). Finally, we define $\mathcal{O} * \mathcal{O} = \mathcal{O}$ for technical reasons.

We have one problem: $*$ is not a group operation. For instance, there is no identity element. If there was a point I that is the identity element with respect to $*$, then any line ℓ through I must be tangent to the curve in the other intersection point of E and ℓ, which is not true in general. Fortunately, there is another way to define a group structure. We define, for any two points P and Q:

$$P + Q = \mathcal{O} * (P * Q).$$

We now consider if the group axioms are satisfied.
Existence of the identity. This is easy: $\mathcal{O}$ is the identity element. By definition we have

$$\mathcal{O} + P = \mathcal{O} * (\mathcal{O} * P).$$

If $Q = \mathcal{O} * P$ is the third point that lies on both E and the line ℓ through P and $\mathcal{O}$, then $R = \mathcal{O} * Q$ is the third point that lies both on E and the line m through $\mathcal{O}$ and Q. But both ℓ and m go through $\mathcal{O}$ and Q, so $\ell = m$. So R is the point on ℓ that is not $\mathcal{O}$ and not Q. So it has to be P. This proves $\mathcal{O} + P = P$. Likewise we have $P + \mathcal{O} = P$.
Existence of the inverse. We claim $-P = \mathcal{O} * P$. By definition we have

$$-P + P = \mathcal{O} * (-P * P) = \mathcal{O} * ((\mathcal{O} * P) * P).$$

[6] In fact, this is a special case of using projective coordinates, which will be discussed in appendix A.

In a similar fashion as above, we see that $\mathcal{O} * P$, P and $\mathcal{O}$ lie on a line and on E, so the point on that line not equal to $\mathcal{O} * P$ and P is $\mathcal{O}$. So $-P + P = \mathcal{O} * \mathcal{O} = \mathcal{O}$, by definition. Similarly we have $P + -P = \mathcal{O}$.
Associativity. This one is rather difficult to verify. It can be done directly if one derives the formulas for the addition, but this is not very insightful. One can also show it by a geometrical argument, however, this is quite involved. This is described extensively in section 2.4 of [11].
Commutativity. Since $*$ is commutative, it follows that $+$ is also commutative.

This makes the set of points on an elliptic curve with rational coordinates into an abelian group. We will denote this group with $E(\mathbf{Q})$. Since there is no special property of $\mathbf{Q}$ we did use except that it is a field, we can use the above to make a group out of the set of points with coordinates in any field K. This group is denoted by $E(K)$.

We will now start with a more formal approach to elliptic curves.

Chapter 1

Elliptic curves: an introduction

In the previous chapter we have given a informal definition of the elliptic curve and its group operation. In this chapter, the focus lies on the endomorphisms of these objects, and the properties elliptic curves have over specific fields such as $\mathbf{Q}$, $\mathbf{C}$ and the finite fields. It fungates as a basis for the theory of complex multiplication which will be discussed in Chapter 3. We will mainly follow the exposition in [11].

Contents

1.1 General theory of elliptic curves 2
1.1.1 Isogenies and endomorphisms 2
1.1.2 The dual isogeny 7
1.1.3 Torsion points 11
1.1.4 The j-invariant 12
1.1.5 Twists of curves 12
1.2 Elliptic curves over the rational numbers 13
1.2.1 The Lutz-Nagell theorem 13
1.2.2 The Mordell-Weil theorem 14
1.3 Elliptic curves over finite fields 15
1.3.1 The Hasse bound and the Frobenius trace 16
1.3.2 Reducing elliptic curves 17
1.3.3 The quadratic twist 17
1.4 Elliptic curves over the complex numbers 18
1.4.1 Lattices and the Weierstrass-$\wp$-function 18
1.4.2 Elliptic functions and curves 19
1.4.3 Maps between elliptic curves 21

§1.1 General theory of elliptic curves

We assume that the reader know what a projective variety is. (It is defined in Appendix A.) With that concept, we can define an elliptic curve formally.

Definition 1.1 *An* elliptic curve *over a field K is a projective variety of dimension 1 and genus*[1] *1, with a designated point $\mathcal{O}$ on it.*

If we write the curve in the Weierstrass form (as defined in equation (2) on page xi), we can make sure that there lies precisely one point at infinity, namely $(0 : 1 : 0)$. We will take that point to be the designated point $\mathcal{O}$. Thinking projectively, we see that there is nothing 'special' about the definition of the extra point $\mathcal{O}$ at page xii: it is just a point on the curve like any other where the elliptic curve happens to intersect its tangent line with multiplicity 3, so $\mathcal{O} * \mathcal{O} = \mathcal{O}$.

If one defines the group structure on elliptic curves more formally than we did, the choice of the basepoint does matter. From now on however, we will usually assume that the basepoint is the point at infinity on the curve, and that curves are given in the Weierstrass normal form.

§1.1.1. Isogenies and endomorphisms. Since we have elliptic curves equipped with a group in the first section, our natural next goal is to consider maps between elliptic curves that respect both the group structure and the variety structure.

Definition 1.2 *Suppose we have two elliptic curves, E_1 and E_2 defined over a field K. An* isogeny *from E_1 to E_2 is a map that is both a morphism from the variety E_1 to the variety E_2 and a group homomorphism from $E_1(K)$ to $E_2(K)$.*

If we assume the curves to be in Weierstrass normal form, it can be shown (see page 51 of [11]) that we can write any isogeny in the form $(x, y) \mapsto (r_1(x), r_2(x)y)$, for some rational functions r_1 and r_2, for all points except ∞. Since an isogeny is a group homomorphism, it is immediate that ∞ always maps to ∞. We make the following convention: if r_1 has a pole at $x = x_0$, then $(x_0, y_0) \mapsto \infty$. For future reference, we will prove the following property of this representation.

[1] The genus of a curve is a rather technical geometric notion, so we will not define it here. In the case $K = \mathbf{C}$ we have the following visualization: consider a curve E. Then we have a group $E(\mathbf{C})$, which can be considered as a complex manifold. Now ignore everything but the topology of this manifold. Then the genus is the number of 'handles' in this topological space. For instance, as a topological space, a sphere has genus 0, and a torus has genus 1. In section 1.4 we show that an elliptic curve over $\mathbf{C}$ is 'the same' as $\mathbf{C}$ modulo a lattice, i.e. a parallellogram with opposing sides glued together: that is, a torus.

Lemma 1.3 *Let $(x, y) \mapsto (r_1(x), r_2(x)y)$ be the representation of an isogeny α from an elliptic curve $E_1 : y^2 = x^3 + A_1x + B_1$ to an elliptic curve $E_2 : y^2 = x^3 + A_2x + B_2$, both defined over K. If $(x_0, y_0) \in E_1(K)$ is such that r_1 has no pole at x_0, then r_2 also has no pole at x_0.*

Proof:

Let us write $r_1(x) = p(x)/q(x)$ and $r_2(x) = s(x)/t(x)$ for polynomials $p(x)$, $q(x)$, $r(x)$ and $s(x)$. We assume $p(x)$ and $q(x)$ to be coprime, and $s(x)$ and $t(x)$ too. Suppose that (x_0, y_0) is such that r_2 has a pole at x_0. We want to show that r_1 also has a pole at x_0. In our notation: we want to show that $t(x_0) = 0$ implies $q(x_0) = 0$.

Since $(x, y) \in E_1(K)$ implies that $\alpha(x, y)$ is a point on E_2 we have

$$\frac{s(x)^2}{t(x)^2}y^2 = \frac{p(x)^3}{q(x)^3} + A_2\frac{p(x)}{q(x)} + B_2.$$

We clear denominators:

$$s(x)^2q(x)^3y^2 = p(x)^3t(x)^2 + A_2p(x)q(x)^2t(x)^2 + B_2q(x)^3t(x)^2.$$

Since (x, y) is a point on E_1, we also have

$$s(x)^2q(x)^3(x^3 + A_1x + B_1) = p(x)^3t(x)^2 + A_2p(x)q(x)^2t(x)^2 + B_2q(x)^3t(x)^2$$

Now we look at this equality in polynomials at the point $x = x_0$: suppose $t(x_0) = 0$, then at the right hand side we have a zero of order ≥ 2. $s(x_0) \neq 0$, because we assumed $s(x)$ and $t(x)$ to be coprime, and if $s(x_0) = 0$, then $(x - x_0)$ divides both $t(x)$ and $s(x)$. Because E_1 is an elliptic curve, $x^3 + A_1x + B$ cannot have multiple zeros (see also our discussion on page xi), so this means that the order of $x^3 + A_1x + B_1$ in x_0 can be at most 1. So $q(x_0)$ also needs to have a zero of order at least 1 in x_0: $q(x_0) = 0$, which is what we did want to prove. □

In the remainder, we will be mainly interested in isogenies from one curve to itself.

Definition 1.4 *An* endomorphism *of an elliptic curve E is an isogeny from E to itself.*

Theorem 1.5 *The set of endomorphisms (defined over $\overline{K}$) of an elliptic curve E (defined over K) is a ring of characteristic 0 without zero divisors, if we define $(\varphi + \psi)(P) = \varphi(P) + \psi(P)$ and $\varphi \cdot \psi(P) = \varphi(\psi(P))$ for any point P and endomorphisms φ and ψ. We denote this ring with* $\mathrm{End}(E)$. *Occasionally, we will talk about the subring* $\mathrm{End}_K(E)$ *of endomorphisms defined over K.*

We will postpone the proof a little, to introduce some concepts that are useful in proving this theorem.

Example 1.6 An important example of an endomorphism is the *multiplication-by-m* map, denoted by $[m]$. We define

$$[m](P) = \overbrace{P + \cdots + P}^{m \text{ times}} \quad (m > 0),$$

$[0](P) = \mathcal{O}$ (also known as the *zero endomorphism*) and

$$[m](P) = [-m](-P) \quad (m < 0).$$

This is a group homomorphism, because the set of points of an elliptic curve forms an abelian group. The map $\mathbf{Z} \to \mathrm{End}(E) : m \mapsto [m]$ embeds the integers injectively in the endomorphism ring of any curve. (That this happens injectively is the content of Proposition III.4.2.a in [8].) ◇

Example 1.7 Let E be an elliptic curve over the finite field $\mathbf{F}_q$. Then the *Frobenius map* F_q defined by

$$F_q(x, y) = (x^q, y^q)$$

is an endomorphism of E. ◇

As we mentioned above, any isogeny and therefore every endomorphism between curves written in the Weierstrass normal form can be written as $(x, y) \mapsto (r_1(x), r_2(x)y)$ for some rational functions r_1 and r_2. A lot of properties and quantities associated to endomorphisms can be defined either in terms of these rational functions, or, more abstractly, in terms of a certain field extension. We will first describe this field extension, and then define the concepts in terms of the polynomials while mentioning how these relate to properties the field extension.

In Definition A.26 we defined the function field $\overline{K}(V)$of an projective variety V defined over a field K. Now, if we have a morphism $\varphi : V_1 \to V_2$, we also get a map $\varphi^* : \overline{K}(V_2) \to \overline{K}(V_1)$, namely the map that sends the rational map $f : V_2 \to \mathbf{P}^1$ to the rational map $f \circ \varphi : V_1 \to \mathbf{P}^1$.
The field extension *associated* to a morphism φ is the extension $\overline{K}(V_1) \supseteq \varphi^*\overline{K}(V_2)$.

Definition 1.8 *Let $\alpha : E \to E : (x, y) \mapsto (p(x)/q(x), r_2(x)y)$ be a non-trivial endomorphism where $p(x)$ and $q(x)$ are polynomials with no common*

factors, and $r_2(x)$ is a rational function. The degree *of α is the maximum of* $\deg(p(x))$ *and* $\deg(q(x))$. [2] *The degree of the zero endomorphism is 0.*

The degree of an endomorphism is the same as the degree of the associated field extension.

We now prove Theorem 1.5:
Proof:
Since $E(\overline{K})$ is an abelian group, its set of endomorphisms can be assigned a ring structure, when we take $+$ and $\cdot$ to be the operations in the statement of the theorem.

Proposition III.4.2.a in [8] states that any endomorphism $[m]$ is non-trivial, for $m \neq 0$. Therefore, the ring has characteristic 0. Furthermore, if a product of two endomorphisms α and β is the zero endomorphism, then α or β should be constant too: by Theorem A.35, any morphism from an elliptic curve to another (so *a fortiori* any isogeny) is either surjective or constant: the composition of two surjective maps cannot be constant, since $E(\overline{K})$ is an infinite group, so either α or β must be constant, i.e. the zero endomorphism. □

EXAMPLE 1.9 The degree of the multiplication-by-m-map $[m]$ is m^2, for any $m \in \mathbf{Z}$. One way to see this is to determine inductively the degree of the rational maps that give this endomorphism, as is done in section 3.2 of [11]. ◇

We also make the following definition. Again we have the close connection with the field extension: an endomorphism is (in)separable if the associated field extension is (in)separable.

Definition 1.10 *Let $\alpha : E_1 \to E_2 : (x, y) \mapsto (r_1(x), r_2(x)y)$ be a isogeny where $r_1(x)$ and $r_2(x)$ are rational functions. α is said to be* separable *if $r_1'(x)$ is not the zero polynomial. If it is not separable, it is called* inseparable.

It is immediate that all non-zero endomorphisms are separable if they are defined over a field of characteristic 0. In fact, the only non-constant polynomials with zero derivative are of the form $g(x^p)$, if we are working over a field of characteristic p. The Frobenius endomorphism is therefore always inseparable, and of degree q.

[2] It falls outside the scope of this thesis, but one can show that in fact $\deg(p(x)) > \deg(q(x))$, so $\deg(\alpha) = \deg(p(x))$. A heuristic for this is: ∞ is always mapped to ∞, so if $x = \infty$, then $p(x)/q(x)$ should also be infinity. This happens precisely if the order of q at infinity is larger than the order of p at infinity, and the order of a polynomial at infinity is minus its degree, so the degree of q is smaller than the degree p. Of course this is not rigourous at all.

Intuitively, the size of the kernel of a map is related to the degree of the polynomial that defines it. We have the following theorem:

Theorem 1.11 *Let $\alpha : E_1 \to E_2$ be a non-zero isogeny between elliptic curves E_1 and E_2. If α is separable we have*

$$\deg(\alpha) = \#\ker\alpha$$

and if α is inseparable we have

$$\deg(\alpha) > \#\ker\alpha$$

where $\ker\alpha$ is the kernel of the map α in $E_1(\overline{K})$.
Proof:
First, we fix notation: we know that we can write α as

$$\alpha : (x, y) \mapsto \left(\frac{p(x)}{q(x)}, r(x)y\right),$$

where we take p and q to be coprime polynomials and r a rational function in x.

We first prove $\deg(\alpha) = \#\ker\alpha$ for separable α.

Now, we define

$$S = \{x \in \overline{K} : p(x)q'(x) - p'(x)q(x) = 0\}.$$

Note that this is a finite set: since we take α to be separable, we have $(\frac{p(x)}{q(x)})' \neq 0$, so $pq' - p'q$ is not the zero polynomial.

We choose an element (a, b) of $\alpha(E_1(\overline{K}))\backslash\{\mathcal{O}\}$ that satisfies the following conditions: $a \neq 0$, $b \neq 0$ and $a \notin r(S)$. Such an element can always be found, because $\alpha(E_1(\overline{K}))$ is an infinite set, and all conditions only rule out a finite number of its elements: S is a finite set and so $r(S)$ is also a finite set.

Now we will count the number of elements of $E_1(\overline{K})$ that are mapped to (a, b) by α. Suppose (z, w) maps to (a, b). Then $(a, b) = (\frac{p(z)}{q(z)}, r(z)w)$ (note that a, b is not the point at infinity), so $x = z$ is a solution of the equation $p(x) - aq(x) = 0$. Since r has no pole at z since $q(z) \neq 0$ (by Lemma 1.3) and no zero (since we assumed $b \neq 0$), we see that $w = \frac{b}{r(z)}$. So if we have a z that satisfies $p(z) - aq(z) = 0$, there is exactly one w such that $\alpha(z, w) = (a, b)$.
If we show that $p(x) - aq(x) = 0$ has no solutions with multiplicity larger than 1, we know (see the footnote in Definition 1.8) that there are exactly $\deg(p(x) - aq(x)) = \deg(p(x)) = \deg(\alpha)$ points that map to (a, b). Suppose there is a solution z_0 that has multiplicity ≥ 2. Then $p(z_0) - aq(z_0) = 0$

and $p'(z_0) - aq'(z_0) = 0$. Multiplication of these equations with suitable constants gives

$$p(z_0)p'(z_0) - ap'(z_0)q(z_0) = 0 = p(z_0)p'(z_0) - ap(z_0)q'(z_0),$$

so

$$ap'(z_0)q(z_0) = ap(z_0)q'(z_0).$$

Since we took $a \neq 0$, this implies $z_0 \in S$, but then $a = r(z_0) \in r(S)$. This also contradicts with our assumptions.
So $p(x) - aq(x) = 0$ has exactly $\deg(\alpha)$ solutions, and the preimage of (a, b) consists of $\deg(\alpha)$ points.

Since an endomorphism is a group homomorphism, the preimage of any point in the image has the same size, so the size of the kernel is also $\deg(\alpha)$.

If α is not separable on the other hand, we have $(p/q)'(x)$ is the zero polynomial. In that case, p' and q' are both the zero polynomial. We can again look at the preimage of an arbitrary point that is not infinity, say (a, b), with $a, b \neq 0$. This consists of exactly the points (z, w) with $p(z) - aq(z) = 0$ and $w = \frac{b}{r(z)}$. However, since $p'(z) - aq'(z) = 0$ (since p' and q' are the zero polynomial), any root of $p(x) - aq(x)$ will be a multiple root. So the preimage of any point satisfying the above conditions will be smaller than $\deg(p(x) - aq(x))$, which is $\deg(\alpha)$. So in this case the preimage of a point (and hence of all points) will be smaller than $\deg(\alpha)$. So the size of the kernel is smaller than $\deg(\alpha)$. □

From this theorem it follows that the kernel of any non-zero isogeny $E_1 \to E_2$ must be a finite subgroup of $E_1(\overline{K})$. This also works the other way round:

Theorem 1.12 *Let E be an elliptic curve. For any finite subgroup Φ of $E(\overline{K})$, there is a unique elliptic curve E' such that there is an isogeny $\varphi : E \to E'$ with kernel Φ.*
Proof:
This is Proposition III.4.12 in [8]. □

§1.1.2. The dual isogeny. When we will study the theory of complex multiplication, there will be a very useful property of the endomorphism ring: namely that we can define an *anti-involution*[3] on it, the *dual isogeny*. It bears this name, since this phenomenon is not limited to endomorphisms: it works for all isogenies.

Since we need some machinery outside of the scope of this thesis, we will not prove the following statement here:

[3] An *anti-involution* on a ring R is a map $\hat{\cdot} : x \mapsto \hat{x}$ satisfying $\widehat{a+b} = \hat{a} + \hat{b}$, $\widehat{ab} = \hat{b}\hat{a}$, $\hat{\hat{a}} = a$ for all $a, b \in R$ and $\hat{n} = n$ for all $n \in \mathbf{Z} \subseteq R$.

Theorem 1.13 *Let $\varphi : E_1 \to E_2$ be a non-zero isogeny of degree m. Then there exists an isogeny $\psi : E_2 \to E_1$ such that*

$$\psi \circ \varphi = [m]$$

Proof:
This is Theorem III.6.1.a in [8]. □

We now prove it makes sense to speak of *the* dual isogeny.

Corollary 1.14 *The isogeny ψ in Theorem 1.13 is unique with this property.*
Proof:
Suppose there are two isomorphisms ψ and ψ' from E_2 to E_1 satisfying $\psi \circ \varphi = [m] = \psi' \circ \varphi$. Then

$$(\psi - \psi') \circ \varphi = [m] - [m] = [0].$$

Using Theorem A.35 (just like in the proof of Theorem 1.5 on page 5), we see that either $\psi - \psi' = [0]$ or $\varphi = [0]$. Since we assumed φ to be non-zero, it follows that $\psi = \psi'$. □

Definition 1.15 *Let $\varphi : E_1 \to E_2$ be a non-zero isogeny. We call the unique isogeny specified in Theorem 1.13 the* dual isogeny *and denote it with $\hat{\varphi}$. Furthermore, we define $\hat{[0]} = [0]$.*

We now list some properties of the dual isogeny:

Theorem 1.16 *Suppose E_i is an elliptic curve for $i \in \{1, 2, 3\}$. Let $\varphi : E_1 \to E_2$ be an isogeny and $\hat{\varphi}$ its dual isogeny, and let $\psi : E_2 \to E_3$ also be an isogeny with dual $\hat{\psi}$. Then*

1. $\varphi \circ \hat{\varphi} = [\deg \varphi]$ *and* $\hat{\varphi} \circ \varphi = [\deg \varphi]$.
2. $\widehat{\varphi + \psi} = \hat{\varphi} + \hat{\psi}$.
3. $\widehat{\psi \circ \varphi} = \hat{\varphi} \circ \hat{\psi}$.
4. $\widehat{[m]} = [m]$ *for all* $m \in \mathbf{Z}$.
5. $\hat{\hat{\varphi}} = \varphi$.
6. $\deg(\varphi) = \deg(\hat{\varphi})$.

Proof:
All properties hold trivially if $\varphi = [0]$ or $\psi = [0]$, so we will ignore that case.

1. The first property follows from Theorem 1.13. For the second property, consider the equation

$$[\deg\varphi]\circ\varphi = \varphi\circ[\deg\varphi] = \varphi\circ\hat{\varphi}\circ\varphi.$$

The first equality follows here from the fact that $[m]\varphi = \varphi[m]$ for all isogenies: since an isogeny is a group homomorphism, we have

$$[m]\varphi(P) = \overbrace{\varphi(P)+\cdots+\varphi(P)}^{m \text{ times}} = \varphi(\overbrace{P+\cdots+P}^{m \text{ times}}) = \varphi[m](P).$$

Since φ is surjective by Theorem A.35, we see that $[\deg\varphi] = \varphi\circ\hat{\varphi}$.

2. This is Theorem III.6.2.(c) in [8].

3. We know that the degree of $\psi\circ\varphi$ is $\deg\psi\cdot\deg\varphi$. Since

$$\begin{aligned}\psi\circ\varphi\circ\hat{\varphi}\circ\hat{\psi} = \psi\circ[\deg\varphi]\circ\hat{\psi} = \psi\circ\hat{\psi}\circ[\deg\varphi] = \\ = [\deg\varphi]\circ[\deg\psi] = [\deg\varphi\cdot\deg\psi],\end{aligned}$$

we see by the uniqueness of the dual that $\hat{\varphi}\circ\hat{\psi}$ must be the dual of $\psi\circ\varphi$.

4. By Example 1.9, the degree of $[m]$ is m^2 for all $m\in\mathbf{Z}$. Since $[m]\circ[m] = [m^2]$, by the uniqueness of the dual we see that $[m]$ is its own dual.

5. Note that, with use of (1) and the multiplicity of the degree:

$$\begin{aligned}[\deg\varphi]^2 = [(\deg\varphi)^2] = [\deg[\deg\varphi]] = [\deg(\varphi\circ\hat{\varphi})] = \\ = [\deg\varphi\cdot\deg\hat{\varphi}] = [\deg\varphi][\deg\hat{\varphi}]\end{aligned}$$

so $\deg\varphi = \deg\hat{\varphi}$.

6. With [4] we see

$$[\deg\varphi] = \widehat{[\deg\varphi]},$$

then with (1) and (3) it follows that

$$\varphi\circ\hat{\varphi} = \widehat{\varphi\circ\hat{\varphi}} = \hat{\hat{\varphi}}\circ\hat{\varphi}.$$

Since $\hat{\varphi}$ is surjective (by Theorem A.35), we see $\varphi = \hat{\hat{\varphi}}$.

□

Analogous to the degree of an endomorphism (which can be seen as a norm), we can define the trace of an endomorphism. We will first demonstrate that – just like the degree – this is always a member of $\mathbf{Z}$.

Proposition 1.17 *Let φ be an endomorphism of an elliptic curve E. Then $\varphi + \hat{\varphi} \in \mathbf{Z}$.*

Proof:
If φ is an endomorphism, then so is $\varphi - [1]$. The degrees of these maps are integers. Now we employ the Theorems 1.13 and 1.16: we get

$$[\deg \varphi] = \varphi\hat{\varphi},$$

and

$$[\deg \varphi - [1]] = (\varphi - [1])(\widehat{\varphi - [1]}) = \varphi\hat{\varphi} - \varphi - \hat{\varphi} + [1].$$

Since the degrees of φ and $\varphi - [1]$ are integers, so is their difference:

$$[\deg \varphi - \deg(\varphi - [1])] = \varphi + \hat{\varphi} - [1]. \tag{1.1}$$

Clearly $\varphi + \hat{\varphi} = [\deg \varphi - \deg(\varphi - [1]) + 1]$, so $[\varphi + \hat{\varphi}]$ is in the image of $\mathbf{Z}$ in $\mathrm{End}(E)$. □

Definition 1.18 *We define the trace* $\mathrm{tr}(\varphi)$ *of an endomorphism $\varphi \in \mathrm{End}(E)$ to be the endomorphism $\varphi + \hat{\varphi}$, which is an integer.*

Corollary 1.19 *Let φ be an endomorphism of an elliptic curve E. Then*

$$\mathrm{tr}(\varphi) = \deg(\varphi) - \deg(\varphi - [1]) + 1.$$

Proof:
This follows from (1.1) and the definition of the trace. □

Finally, we have the following equality:

Lemma 1.20 *Let φ be an endomorphism of an elliptic curve E. Then*

$$\varphi^2 - \mathrm{tr}(\varphi) \cdot \varphi + [\deg \varphi] = [0].$$

Proof:
Clearly

$$\varphi^2 - \varphi^2 - \hat{\varphi}\varphi + \hat{\varphi}\varphi = [0]$$

holds. We have $\hat{\varphi}\varphi = [\deg \varphi]$ and $\varphi + \hat{\varphi} = \mathrm{tr}(\varphi)$, so taking φ out of the brackets gives

$$\varphi^2 - \mathrm{tr}(\varphi) \cdot \varphi + [\deg \varphi] = [0]..$$

□

§1.1.3. Torsion points. We are often interested in points of finite order, i.e. points in the kernel of $[m]$, for some $m \in \mathbf{Z}$. We write

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

and we have the following theorem:

Theorem 1.21 *Let E be an elliptic curve defined over K, and n be a positive integer such that either* $\operatorname{char} K \nmid n$ *or* $\operatorname{char} K = 0$. *Then*

$$E[n] \cong \mathbf{Z}/n\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}.$$

Proof:
This is Theorem 3.2 in [11]. □

In fact, this shows that $[m]$ is separable precisely when $\operatorname{char} K = 0$ or $\operatorname{char} K \nmid m$, by Theorem 1.11 and Example 1.9.

In this case, i.e. when $\operatorname{char} K = 0$ or $\operatorname{char} K \nmid n$, we can see $E[n]$ as a free $\mathbf{Z}/n\mathbf{Z}$-module of dimension 2. Now, let $\alpha : E \to E$ be an endomorphism. Clearly, α sends points of order dividing n to points of order dividing n: so α restricted to $E[n]$ is a module homomorphism.

Theorem 1.22 *If we have an elliptic curve E defined over K, and n a positive integer such that either* $\operatorname{char} K \nmid$ *or* $\operatorname{char} K = 0$. *Let $\alpha : E \to E$ be an endomorphism, and write α_n for the $\mathbf{Z}/n\mathbf{Z}$-module homomorphism from $E[n]$ to itself. Then*

$$\det(\alpha_n) \equiv \deg(\alpha) \bmod n.$$

Proof:
This is Theorem 3.15 in [11]. □

Theorem 1.23 *Let the notation be as in Theorem 1.22. Then*

$$\operatorname{tr}(\alpha_n) \equiv \operatorname{tr}(\alpha) \bmod n.$$

Proof:
Note that we have, for any 2×2-matrix $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$:

$$\begin{aligned} &\operatorname{tr}(M) = a + d = ad - bc - ad + a + d - 1 + bc + 1 = \\ &= (ad - bc) - ((a-1)(d-1) - bc) + 1 = \det(M) - \det(M - 1) + 1. \end{aligned} \quad (1.2)$$

Furthermore, by Corollary 1.19, we have for any endomorphism φ

$$\operatorname{tr}(\varphi) = \deg(\varphi) - \deg(\varphi - 1) + 1 \quad (1.3)$$

If we substitute α_n for M in (1.2) and α for φ in (1.3) and use Theorem 1.22, we get

$$\mathrm{tr}(\alpha_n) = \det(\alpha_n) - \det((\alpha-1)_n) + 1 \equiv \deg(\alpha) - \deg(\alpha-1) + 1 = \mathrm{tr}(\alpha) \bmod n.$$

□

§1.1.4. The j-invariant. Now that we have defined isomorphisms of curves, we could ask if there are invariants that determine if certain curves are isomorphic or not. It turns out that there is a very interesting function that has this property:

Definition 1.24 *The* j-invariant *of the elliptic curve* $E : y^2 = x^3 + ax + b$ *is*

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

We have the following:

Theorem 1.25 *Two elliptic curves defined over* K *are isomorphic over* $\overline{K}$ *iff their* j*-invariants are equal.*
Proof:
This is Theorem III.1.4.b in [8]. □

and

Theorem 1.26 *Let* K *be a field, and* $j_0 \in \overline{K}$*. Then there exists an elliptic curve defined over* $K(j_0)$ *with* j*-invariant* j_0*.*
Proof:
If j_0 is not equal to 0 or 1728, a straightforward calculation reveals that

$$E : y^2 = x^3 + \frac{-27j_0}{j_0 - 1728}x + \frac{54j_0}{j_0 - 1728},$$

has j-invariant j_0. Furthermore, $y^2 = x^3 + x$ has j-invariant 1728 and $y^2 = x^3 + 1$ has j-invariant 0. □

§1.1.5. Twists of curves. In this subsection we discuss an interesting relationship between curves that is similar to what happens in Example A.34. This example is about varieties defined over K that are isomorphic over the algebraic closure of K.

Definition 1.27 *Two elliptic curves* E_1 *and* E_2 *defined over a field* K *are* twists *of each other if they are isomorphic over* $\overline{K}$*.*

In Theorem 1.25, we saw that two curves are twists from each other if they have the same j-invariant. We will now discuss an example:

EXAMPLE 1.28 Consider an elliptic curve $E : y^2 = x^3 + ax + b$ over K. Then, for every $d \in K$, we can define the *twist by d*:

$$E^{(d)} : y^2 = x^3 + ad^2x + bd^3.$$

Indeed,

$$j(E) = 1728\frac{4a^3}{4a^3 + 27b^2} = 1728\frac{4a^3d^6}{4a^3d^6 + 27b^2d^6} = \\ = 1728\frac{4(ad^2)^3}{4(ad^2)^3 + 27(bd^3)^2} = j(E^{(d)}).$$

These two curves are isomorphic over $K(\sqrt{d})$, namely by the change of coordinates $E \to E^{(d)} : x \mapsto dx, y \mapsto d^{\frac{3}{2}}y$. ◇

We will discuss the special case of twists of curves over finite field on page 17.

§1.2 ELLIPTIC CURVES OVER THE RATIONAL NUMBERS

We now return to the case we considered in the introduction: that of rational points on an elliptic curve. Two important theorems exist about the structure of $E(\mathbf{Q})$: the Lutz-Nagell theorem, which gives a complete finite list of possible points with finite order, and the Mordell-Weil theorem, which states that $E(\mathbf{Q})$ is finitely generated.

§1.2.1. The Lutz-Nagell theorem. We start with stating the theorem. Note that this works for curves that can be put in the form $y^2 = x^3 + ax + b$, however, this is always possible in fields of characteristic 0 such as $\mathbf{Q}$.

Theorem 1.29 *(Lutz-Nagell) Let $P = (x, y) \in E(\mathbf{Q})$ be a point of finite order on the elliptic curve $E : y^2 = x^3 + ax + b$ with a and b integers. Then $x, y \in \mathbf{Z}$, and $y = 0$ or $y^2 \mid 4a^3 + 27b^2$.*
Proof:
This is Theorem 8.7 in [11]. □

The proof of this theorem goes along these lines: if P is a point of finite order with non-integral coordinates, then there is a prime p that divides the denominator of one of the coordinates. Using the relation between the

coordinates, we can show that p also divides the denominator of the other coordinate. From there on, we can, with the use of a coordinate transformation and the fact that P is of finite order, show that there higher and higher powers of p that divide the denominator, eventually reaching a contradiction.

The condition on y in Theorem 1.29 makes it an effective way to find all points of finite order: it follows from the fact that both P and $2P$ have integral coordinates (since they are both of finite order). This allows us to use the duplication formula (which gives the coordinates of $2P$ in terms of P) to show that y divides the discriminant of the curve, i.e. $4a^3 + 27b^2$. We can strenghten the result to y^2 dividing the discriminant.

§1.2.2. The Mordell-Weil theorem. We first state the theorem:

Theorem 1.30 *(Mordell-Weil) Let E be an elliptic curve defined over $\mathbf{Q}$. The abelian group $E(\mathbf{Q})$ is finitely generated.*
Proof:
This is Theorem 8.17 in [11]. □

In the proof of the Mordell-Weil theorem, the *descent method* is used. We will discuss parts of the proof.

We will take for granted that the group $E(\mathbf{Q})/2E(\mathbf{Q})$ is finite. The proof of this uses a lot of algebraic number theory, at least in the general case, so we will not discuss it here. (If we assume $E(\mathbf{Q})$ has a point of order 2, an easier proof can be given, like in chapter 3 of [10].)

The name 'descent method' implies that we want to look at some decreasing quantity. This quantity is the *height*, which for a point $(\frac{m_1}{n_1}, \frac{m_2}{n_2})$ is defined as $\log(\max(|m_1|, |n_1|))$, with $\gcd(m_i, n_i) = 1$. From a number-theoretic perspective, this is a useful way of looking at points, because we have the following inequalities for points in $E(\mathbf{Q})$:

> For every P_0 there is a κ_0 such that for all P we have $h(P+P_0) \leq 2h(P) + \kappa_0$.

and

> There is a κ such that for all P we have $h(2P) \geq 4h(P) - \kappa$.

These equalities follow from analyzing the formules for addition and duplication of points, and checking that the amount of cancellation between the numerator and the denominator is not too large.

Now we can prove $E(\mathbf{Q})$ is finitely generated. If we take a set of representatives for $E(\mathbf{Q})/2E(\mathbf{Q})$, say $\{Q_1, \ldots, Q_n\}$, we can write any $P \in E(\mathbf{Q})$ as $P \in 2E(\mathbf{Q}) + Q_{i_1}$ for some $1 \leq i_1 \leq n$, so there is a P_1 such that $P = 2P_1 + Q_{i_1}$. Analogously, there are a Q_{i_2} and a P_2 such that $P_1 = 2P_2 + Q_{i_2}$, etcetera. So, we can write

$$P = Q_{i_1} + 2Q_{i_2} + 4Q_{i_3} + \cdots + 2^{m-1}Q_{i_m} + 2^m P_m$$

for m as large as we want. Using the inequalities for the height above, one can show that the P_i's are of decreasing height, as long as their height is larger than a certain constant, say c_0. So if we make m large enough, we can write P as the sum of points in $\{Q_1, \ldots, Q_m\}$ and a point of height less than c_0. The first set is finite, and the second set is too: there are only a finite number of rational numbers with numerator and denominator bounded by $\exp(c_0)$, and there are at most 2 points with the same x-coordinate. So we can write every point of $E(\mathbf{Q})$ as the sum of points from a finite set. So it is finitely generated.

Now that we know that $E(\mathbf{Q})$ is finitely generated, by elementary abelian group theory it follows that it can be written as

$$E(\mathbf{Q}) \cong \mathbf{Z}^r \times T,$$

where $r \geq 0$ is the *rank* and T the *torsion group*: the points of finite order. The group T can easily be determined with Theorem 1.29. Determining the rank is a harder task; for some types of curves there is an algorithm, but not for all of them. The question 'Is there an upper bound for the rank of $E(\mathbf{Q})$?' is still an unanswered one.

§1.3 Elliptic curves over finite fields

Closely related to elliptic curves over $\mathbf{Q}$ are elliptic curves defined over the finite fields. As we said on page vii, $\mathbf{F}_p$ will refer to the field with p elements with p a prime number, and $\mathbf{F}_q$ to the field with $q = p^k$ elements, where $k \geq 1$.

A first question is: what is the structure of $E(\mathbf{F}_q)$, for any elliptic curve E? Since there are only finitely many pairs of elements (x, y) in $\mathbf{F}_q$, this is a finite group. A finite abelian group must be isomorphic to

$$\mathbf{Z}/n_1\mathbf{Z} \times \cdots \times \mathbf{Z}/n_k\mathbf{Z} \tag{1.4}$$

for $1 < n_1 \mid n_2 \mid \cdots \mid n_k$. Let us now consider $E[n_1]$, the set of points of order dividing n_1, in $E(\overline{\mathbf{F}_p})$, i.e. over the algebraic closure of $\mathbf{F}_q$. By Theorem 1.21, this is isomorphic to $\mathbf{Z}/n_1 \times \mathbf{Z}/n_1\mathbf{Z}$, i.e. we can not find 3

points that are independent of each other. If $k \geq 3$ in the representation of 1.4, then the first three factors would all contain a point of order n_1 that is independent of the others, which is a contradiction. So only $0 \leq k \leq 2$ can occur. We conclude:

Proposition 1.31 *Let E be an elliptic curve defined over $\mathbf{F}_q$. Then there exist integers $n_1, n_2 > 0$ such that $E(\mathbf{F}_q) \cong \mathbf{Z}/n_1\mathbf{Z} \times \mathbf{Z}/n_2\mathbf{Z}$, for $n_1 \mid n_2$.*

We can say even more about $E(\mathbf{F}_q)$: namely about its size. The classical heuristic reasoning:

> The elliptic curve $y^2 = f(x)$ has two points with first coordinate x for every non-zero square value of $f(x)$, one point with that first coordinate if $f(x) = 0$ and zero points for every non-square value. Half of $\mathbf{F}_q^\times$ is a non-zero square, so there are $\frac{1}{2} \cdot 2 \cdot (q-1)+1+1 = q+1$ points in $E(\mathbf{F}_q)$. (The first $+1$ is for the point for which $f(x) = 0$, the second one is for the point at infinity.)

turns out to be a good estimate. One can prove a bound on the error of the estimate, called the *Hasse bound.*

§1.3.1. The Hasse bound and the Frobenius trace. In the '30s, Hasse proved this result about the size of $E(\mathbf{F}_q)$, which was first conjectured by Artin. Later, Weil generalized the bound to other types of curves.

Theorem 1.32 *Let E be an elliptic curve over $\mathbf{F}_q$. Then*

$$|q + 1 - \#E(\mathbf{F}_q)| \leq 2\sqrt{q}.$$

Proof:
This is Theorem 3.5 in [11]. □

The standard proof of this theorem (see for example [8]) makes heavy use of the endomorphism defined in 1.7, the Frobenius map F that sends (x, y) to (x^q, y^q). We can define this map over the algebraic closure $\overline{\mathbf{F}_p}$ of $\mathbf{F}_q$. This endomorphism fixes exactly the points (x, y) for which both x and y are inside $\mathbf{F}_q$, since $\mathbf{F}_q$ is the set of zeroes of the polynomial $x^q - x$ in $\overline{\mathbf{F}_p}$. So $E(\mathbf{F}_q) = \ker(F - 1)$. In fact, one can show that $F - 1$ is separable, so $\deg(F - 1) = \#(E(\mathbf{F}_q))$.

A quantity that will play an important role in this thesis is that of the *trace of the Frobenius morphism F*. As we saw in Theorem 1.23, we have

$$\mathrm{tr}(F) = \deg(F) - \deg(F - 1) + 1 = q - \#E(\mathbf{F}_q) + 1.$$

Note that this is precisely the quantity that is bounded by the Hasse bound in Theorem 1.32. Often we will denote it with t.

From Lemma 1.20 it follows that F satisfies the following equation:

$$F^2 - tF + q = 0. \tag{1.5}$$

§1.3.2. Reducing elliptic curves. The central problem of this thesis is based upon the concept of 'reducing curves': if we have a curve defined over $\mathbf{Z}$[4] and some map $\mathbf{Q} \to \mathbf{F}_p$, we can try to say something about the 'image' of the curve and its points. This turns out to work rather well.

The map from $\mathbf{Q} \to \mathbf{F}_p$ is not very surprising: take $\frac{a}{b} \mapsto ab^{-1} \bmod p$ where $a, b \in \mathbf{Z}$. One restriction applies: it is not defined if $p \mid b$, so we have to take care of this case separately.

Furthermore, to ensure the 'reduced' curve is still an elliptic curve, we need to know if the polynomial $f(x)$ is not mapped to a polynomial with multiple roots. We have the following definition:

Definition 1.33 *Let E be a curve defined over $\mathbf{Q}$ with discriminant Δ, and p a prime number. We say E has* good reduction *modulo p, if $p \nmid \Delta$. Otherwise, E has* bad reduction *modulo p.*

Now we can formulate the reduction theorem:

Theorem 1.34 *Suppose we have an elliptic curve E with coefficients in $\mathbf{Z}$ which is of good reduction modulo p. We reduce E modulo p (by taking the coefficients modulo p) and we obtain a curve $\tilde{E}$ over $\mathbf{F}_p$. Consider the map defined by*

$$\rho : E(\mathbf{Q}) \to \tilde{E}(\mathbf{F}_p) : \left(\frac{a}{b}, \frac{c}{d}\right) \mapsto (ab^{-1} \bmod p, cd^{-1} \bmod p)$$

if $p \mid b$ and $p \mid d$, and defined by $\rho(P) = \mathcal{O}$ otherwise.

This map is a group homomorphism. Furthermore, if $\gcd(n, p) = 1$, then $E[n] \cap E(\mathbf{Q})$ is injectively mapped into $\tilde{E}(\mathbf{F}_p)$.

Proof:
This is Proposition VII.2.1 and Theorem VII.3.1 in [8]. □

§1.3.3. The quadratic twist. For curves over finite fields, the twists are easy to describe. Furthermore, there is a connection with the trace of the Frobenius that will be useful later on.

[4] If we have a curve defined over $\mathbf{Q}$ we can with a simple change of coordinates make sure that the coefficients are integral, so this is not a restriction.

Theorem 1.35 *Let E be an elliptic curve over $\mathbf{F}_q$. Then there are – modulo $\mathbf{F}_q$-isomorphisms – two twists of E, if $j(E) \notin \{0, 1728\}$. (If $j(E) = 1728$ there are four twists, and if $j(E) = 0$ there are six.)*
Proof:
This is Theorem X.5.4 in [8]. □

For curves with j-invariant not equal to 0 and 1728, we write E^{tw} for the elliptic curve that is a twist of E and not $\mathbf{F}_q$-isomorphic to E. This is called the quadratic twist of E.

Theorem 1.36 *Let E be a curve over $\mathbf{F}_q$ with j-invariant not equal to 0 or 1728. We write $E^{(d)}$ for the twist of E by d, as in Example 1.28. Then $E = E^{(d)}$ if d is a square in $\mathbf{F}_q^\times$ and $E^{\mathrm{tw}} = E^{(d)}$ if d is a non-square.*
The Frobenius trace of E^{tw} is the opposite of the Frobenius trace of E.
Proof:
This is Proposition 13.1.10 in [4]. □

§1.4 Elliptic curves over the complex numbers

After all the number theory above, we now look from an analytic perspective. As it turns out, the points of an elliptic curve defined over the complex numbers form a torus. The central tool we need to show this is the Weierstrass-$\wp$-function.

§1.4.1. Lattices and the Weierstrass-$\wp$-function. The focus of this subsection is on complex-valued functions that are defined on a torus. Since a torus is basically a parallellogram with opposing sides glued together, it is natural to look at functions with as domain a parallellogram in $\mathbf{C}$. In order to garantuee that the function is analytical 'around the seam', we consider meromorphic functions that are defined on the whole of $\mathbf{C}$ and periodic along both axes of the parallellogram.

Definition 1.37 *A* lattice *is a discrete subgroup of $\mathbf{C}^+$ generated by two elements of $\mathbf{C}$ that are $\mathbf{R}$-independent.*
An elliptic function *for a lattice Λ is a meromorphic function such that*

$$f(z) = f(z + \omega) \text{ for all } \omega \in \Lambda$$

for all z where f is defined.

Usually we denote a set of two generates for a lattice with ω_1 and ω_2. The set

$$\{\lambda\omega_1 + \mu\omega_2 : 0 \leq \lambda, \mu \leq 1\}$$

is called a *fundamental parallellogram* for Λ.

A very important example of an elliptic function is the Weierstrass-$\wp$-function:

EXAMPLE 1.38 Let Λ be the lattice generated by ω_1 and ω_2. The Weierstrass-$\wp$-function is defined as

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega \in \Lambda \setminus \{0\}} \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}$$

Of course, this function depends on Λ. If it is unclear to which lattice Λ the Weierstrass-$\wp$-function is associated, we write $\wp(z, \Lambda)$. One can show that this series defines indeed an even meromorphic function on $\mathbf{C}$: it has a double pole at every point of Λ. The periodicity follows from Example 1.39. $\diamond$

EXAMPLE 1.39 Another example of an elliptic function is the derivative of the Weierstrass function:

$$\wp'(z) = -2 \sum_{\omega \in \Lambda} \frac{1}{(z-\omega)^3}.$$

This function is odd, and clearly periodic with respect to Λ. In fact, since this function is periodic, there must be a constant c only depending on ω such that $\wp(z) = \wp(z+\omega) + c$. However, since $\wp(-\omega/2) = \wp(\omega/2)$ (by its evenness), we see that $c = 0$, so $\wp$ is also periodic. $\diamond$

We now have seen two examples of elliptic functions. As it happens, this is 'all there is':

Theorem 1.40 *Every elliptic function on a lattice Λ can be written as a rational function of $\wp$ and $\wp'$.*
Proof:
This is Theorem VI.3.2 in [8]. $\square$

§1.4.2. Elliptic functions and curves. Now that we have established the importance of the function $\wp$, we want to connect it to the theory of elliptic curves. First, we need a lemma:

Lemma 1.41 *Every holomorphic elliptic function is constant.*
Proof:
Suppose we have an holomorphic elliptic function f. We look at the values of f on the fundamental parallellogram. Since this is a compact subset of $\mathbf{C}$, the function takes a minimum and a maximum here, so $|f|$ is also bounded on the fundamental parallellogram. But all the values that f assumes in $\mathbf{C}$

are already assumed on the fundamental parallellogram, so $|f|$ is bounded everywhere. By Liouville's theorem, it follows that f is constant. □

The use of this lemma is that, if we have two Laurent series of elliptic functions, say of f and g, around a point z_0 and we can show that the Laurent series of $f-g$ has no terms of negative degree, it follows that $f-g$ is holomorphic around z_0. If f and g can be written as polynomials in $\wp$ and $\wp'$ this is especially interesting, because these functions have only poles in points of Λ. So, if we take the Laurent series around 0, show that $f-g$ is holomorphic around 0, it follows that $f-g$ is holomorphic everywhere by the periodicity. But then $f-g$ is a holomorphic elliptic function and hence constant.
So: if we can show that f and g have the same coefficients for terms of negative degree in the Laurent expansions, we get $f = g +$ a constant. And that is exactly how one shows

Theorem 1.42 *There are exist constants g_2 and g_3 in $\mathbf{C}$ such that*

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

for all $z \in \mathbf{C}$ where $\wp$ and $\wp'$ are defined (i.e. in $\mathbf{C}\backslash\Lambda$)
Proof:
This is Theorem VI.3.5 in [8]. □

In the theorem above, g_2 and g_3 are some constants depending on the lattice. It is not hard to show that the polynomial $4x^3 - g_2x - g_3$ always has distinct roots. So if we map a point z in $\mathbf{C}$ to a point $(\wp(z), \wp'(z))$, it is a point on the elliptic curve $y^2 = 4x^3 - g_2x - g_3$.

Theorem 1.43 *There is a isomorphism between $\mathbf{C}/\Lambda$ and the elliptic curve $E : y^2 = 4x^3 - g_2x - g_3$ over $\mathbf{C}$, given by*

$$z \mapsto (\wp(z), \wp'(z)).$$

Proof:
This is Theorem VI.3.6 in [8]. □

This also works the other way round:

Theorem 1.44 *(Uniformization theorem) Let E be an elliptic curve of the form $y^2 = 4x^3 - g_2x - g_3$. Then there is a lattice Λ in $\mathbf{C}$ such that $\mathbf{C}/\Lambda$ is isomorphic to $E(\mathbf{C})$, and Λ is unique up to multiplication with a constant $\alpha \in \mathbf{C}$.*
Proof:

This is Theorem VI.5.1 in [8]. □

The equivalence between lattices and elliptic curves gives us directly insight into the group structure of $E(\mathbf{C})$. A simple observation such as 'the points z in $\mathbf{C}$ for which $mz \in \Lambda = \langle \omega_1, \omega_2 \rangle$ are precisely the points $\frac{i}{m}\omega_1 + \frac{j}{m}\omega_2$ for integers i, j' implies that there are m^2 points z in $\mathbf{C}/\Lambda$ such that $mz \in \Lambda$. It is not hard to determine the group structure of this set of points of order m and we obtain:

Proposition 1.45 *For any $m \geq 1$ and any elliptic curve defined over $\mathbf{C}$ we have*

$$E[m] \cong \mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/m\mathbf{Z}.$$

§1.4.3. Maps between elliptic curves. As we have seen that elliptic curves are essentially the same thing as complex tori, we can study maps between elliptic curves via maps between tori, which are much easier to understand. We will first give an example of a map between two tori, i.e. $\mathbf{C}/\Lambda_1 \to \mathbf{C}/\Lambda_2$: suppose we have an $\alpha \in \mathbf{C}$ such that $\alpha\Lambda_1 \subseteq \Lambda_2$. Then

$$f_\alpha : \mathbf{C}/\Lambda_1 \to \mathbf{C}/\Lambda_2 : z + \Lambda_1 \mapsto \alpha z + \Lambda_2$$

is a well-defined holomorphic map, that sends 0 to itself.
We will now show that this exhausts all possible maps with these properties.

Theorem 1.46 *There is a bijection between $\alpha \in \mathbf{C}$ such that $\alpha\Lambda_1 \subseteq \Lambda_2$ and holomorphic maps $f_\alpha : \mathbf{C}/\Lambda_1 \to \mathbf{C}/\Lambda_2$ that send $0 + \Lambda_1$ to $0 + \Lambda_2$.*
Proof:
We will show that the map $\alpha \mapsto f_\alpha$ is surjective and injective.

Suppose $f_\alpha = f_\beta$ for α and β both in the set $\{\gamma : \gamma\Lambda_1 \subseteq \Lambda_2\}$. We compose f_α and f_β from the left with the canonical map $\mathbf{C} \to \mathbf{C}/\Lambda_1$, so that we can assume the input to be in $\mathbf{C}$. Then $\alpha z = \beta z \bmod \Lambda_2$ for all $z \in \mathbf{C}$. So $(\alpha - \beta)z \in \Lambda_2$ for all z. Since the map $g : z \mapsto (\alpha - \beta)z$ is a continuous function, and Λ_2 is a discrete set in $\mathbf{C}$, the image of g consists of a single point. The only way in which $(\alpha - \beta)z = (\alpha - \beta)w$ can be true for $z \neq w$, is when $\alpha - \beta = 0$. So $\alpha = \beta$. This proves the injectivity.

Let f be a holomorphic map $\mathbf{C}/\Lambda_1 \to \mathbf{C}/\Lambda_2$ that sends $0 + \Lambda_1$ to $0 + \Lambda_2$. Using that $\mathbf{C}$ is simply connected, we can lift this map to $\bar{f} : \mathbf{C}/\Lambda_1 \to \mathbf{C}$. If we compose this with the canonical map $\mathbf{C} \to \mathbf{C}/\Lambda_1$, we get a map $g : \mathbf{C} \to \mathbf{C}$ that satisfies

$$g(z) = g(z + \omega) \bmod \Lambda_2,$$

for any $z \in \mathbf{C}$ and $\omega \in \Lambda_1$. So $g(z) - g(z+\omega) \in \Lambda_2$. Since $z \mapsto g(z) - g(z+\omega)$ is a continous function, and Λ_2 is a discrete set, we conclude that $g(z) - g(z+\omega)$ must be some constant (dependent on ω):

$$g(z) = g(z+\omega) + c_\omega.$$

g is holomorphic, so we can differentiate this equation:

$$g'(z) = g'(z+\omega)$$

This relation holds for any $\omega \in \Lambda_2$, so g' is a elliptic function! However, by Lemma 1.41, then g' is a constant function. So $g(z) = cz + d$. By our assumption, 0 is mapped to 0, so $d = g(0) = 0$. So $g(z) = cz$, and that implies that $f(z) = cz + \Lambda_2$. So $f = f_c$, which proves the surjectivity. □

Using the periodicity of the Weierstrass-$\wp$-function, one can show that

Theorem 1.47 *Let Λ_i be the lattice associated to the elliptic curve E_i, for $i = 1, 2$. There is a bijection between isogenies $E_1 \to E_2$ over $\mathbf{C}$ and holomorphic maps $\mathbf{C}/\Lambda_1 \to \mathbf{C}/\Lambda_2$ that send $0 + \Lambda_1$ to $0 + \Lambda_2$.*
Proof:
Since isogenies are given by rational functions that are locally everywhere defined, any isogeny $E_1 \to E_2$ corresponds to a holomorphic map $\mathbf{C}/\Lambda_1 \to \mathbf{C}/\Lambda_2$. That 0 maps to 0 follows from the fact that isogenies are group homomorphisms. So the map from the set of isogenies to the set of holomorphic maps is well-defined, and clearly injective.

It is also surjective. One can see this in the following way. Take a holomorphic map $\mathbf{C}/\Lambda_1 \to \mathbf{C}/\Lambda_2$ that sends $0 + \Lambda_1$ to $0 + \Lambda_2$. By the previous lemma, this map is of the form $z \mapsto \alpha z + \Lambda_2$ for some α satisfying $\alpha\Lambda_1 \subseteq \Lambda_2$. By Theorem 1.43, this corresponds to a map

$$E_1 \to E_2 : (\wp(z, \Lambda_1), \wp'(z, \Lambda_1)) \mapsto (\wp(\alpha z, \Lambda_2), \wp'(\alpha z, \Lambda_2).$$

This is an isogeny if we can write the expression to the right of $\mapsto$ as a rational function of $\wp(z, \Lambda_1)$ and $\wp'(z, \Lambda_1)$. (It is already a group homomorphism, since 0 maps to 0. However, for any $\omega \in \Lambda_1$,

$$\wp(\alpha(z+\omega), \Lambda_2) = \wp(\alpha z + \alpha\omega, \Lambda_2) = \wp(\alpha z, \Lambda_2)$$

since $\alpha\omega \in \alpha\Lambda_1 \subseteq \Lambda_2$. Similarly, $\wp'(\alpha z, \Lambda_2)$ is periodic with respect to Λ_1. So, by Theorem 1.40, we can write $\wp(\alpha z, \Lambda_2)$ and $\wp'(\alpha z, \Lambda_2)$ as rational functions of $\wp(z, \Lambda_1)$ and $\wp'(z, \Lambda_1)$. This proves that the map is an isogeny, and hence the desired surjectivity holds. □

From the Theorems 1.46 and 1.47 we can conclude directly

Corollary 1.48 *Let Λ_i be the lattice associated to the elliptic curve E_i, for $i = 1, 2$. Two elliptic curves E_1 and E_2 are isomorphic over $\mathbf{C}$ iff there exists an $\alpha \neq 0$ such that $\alpha\Lambda_1 = \Lambda_2$.*

For future reference, we will give lattices that differ by a factor a name:

Definition 1.49 *Let Λ_1 and Λ_2 be lattices in $\mathbf{C}$. They are* homothetic *if there is an $\alpha \in \mathbf{C}\backslash\{0\}$ such that $\alpha\Lambda_1 = \Lambda_2$.*

Chapter 2

The result of Barreto and Naehrig

In this chapter I will detail the reasoning of Barreto and Naehrig in their paper 'Paring-Friendly Curves of Prime Order' [1], for the following result:

> The polynomials $p(x) = 36x^4 + 36x^3 + 24x^2 + 6x + 1$ and $n(x) = 36x^4 + 36x^3 + 18x^2 + 6x + 1$ have the following property: if x_0 is such that $p = p(x_0)$ and $n = n(x_0)$ are prime, we can find an elliptic curve E of the form $y^2 = x^3 + b$ over $\mathbf{F}_p$ that has exactly n points with embedding degree 12. This means that the coordinates of the points in $E[n]$ generate $\mathbf{F}_{p^{12}}$.

Their strategy is to use the relation $n(x) \mid \Phi_{12}(t(x) - 1)$, where $t(x)$ is defined as $p(x) + 1 - n(x)$ and Φ_{12} the twelfth cyclotomic polynomial. By the definition on page 16, it follows that if x_0 is chosen such that $p(x_0)$ and $n(x_0)$ are prime, then $t(x_0)$ is the trace of the Frobenius map of $\mathbf{F}_{p(x_0)}$. First, we will show where this relation comes from. Then we will demonstrate how they did find polynomials that satisfy this relation and finally we will describe how one can find elliptic curves of the form $y^2 = x^3 + b$ (with $b \in \mathbf{F}_p$) that have n points over $\mathbf{F}_p$.

Contents

2.1 Determining the embedding degree 26
2.1.1 Some definitions 26
2.1.2 The relation $n \mid \Phi_k(t-1)$ 27
2.2 The parametrization 29
2.2.1 Galbraith's lemma 29
2.2.2 The application of the lemma 30

2.3 Making the curves 31
2.4 How often are $p(x)$ and $n(x)$ prime numbers? . . 34

§2.1 Determining the embedding degree

A essential part of [1] is that the embedding degree of the generated elliptic curves is equal to 12. This section discusses the connection between the embedding degree of a curve over a prime field, and the number of points and the size of the field. For convenience, we restrict our attention to a certain group of curves.

§2.1.1. Some definitions.

Definition 2.1 *Let E be an elliptic curve defined over $\mathbf{F}_p$, such that $\#E(\mathbf{F}_p)$ is a prime number, say n, and $p \neq n$. Then E is said to be a* good curve *of size n over $\mathbf{F}_p$.*

Note that saying that E is a good curve states two things: $\#E(\mathbf{F}_p)$ is prime, and it is not equal to p.

For these curves, we can now define the embedding degree.

Definition 2.2 *Let E be a good curve of size n over $\mathbf{F}_p$. Then the* embedding degree *of E is the smallest integer $k \geq 1$ such that $E[n] \subseteq E(\mathbf{F}_{p^k})$.*

Barreto and Naehrig show that $n(x) \mid \Phi_{12}(t(x)-1)$ iff the embedding degree is 12. They are only interested in the special case where the embedding degree k is equal to 12. However, it is no more work to prove that this relation holds in general: that is, for suitable x_0, the embedding degree of the curve with $n(x_0)$ points over $\mathbf{F}_{p(x_0)}$ is equal to k if the k-th cyclotomic polynomial modulo $n(x_0)$ has a zero in $t(x_0) - 1$.

We prove a straightforward lemma that will be of use in proving the relation this section is about.

Lemma 2.3 *Let E be a good curve of size n over $\mathbf{F}_p$. Then the embedding degree is equal to the smallest k such that the k-th power of the Frobenius morphism is the identity on $E[n]$. (Formulated in group-theoretic terms: the embedding degree of a good curve with n points is equal to the order of the Frobenius map restricted to $E[n]$.)*

Proof:

Suppose k is the embedding degree of E. Then $E[n] \subseteq E(\mathbf{F}_{p^k})$, and $E[n] \not\subseteq E(\mathbf{F}_{p^\ell})$ for any $\ell < k$. Let F be the Frobenius morphism $E(\overline{\mathbf{F}_p}) \to E(\overline{\mathbf{F}_p}) : (x, y) \mapsto (x^p, y^p)$. In the algebraic closure of $\mathbf{F}_p$, the map $z \mapsto z^{p^m}$ fixes precisely the points in $\mathbf{F}_{p^m}$. Since $F^m : (x, y) \mapsto (x^{p^m}, y^{p^m})$, the map F^m

fixes precisely the points (x, y) with x and y both in $\mathbf{F}_{p^m}$. So the set of fixpoints of F^m is $E(\mathbf{F}_{p^m})$. So F^ℓ (for $\ell < k$) does not send all points of $E[n]$ to itself, but F^k does. This proves what we want. □

§2.1.2. The relation $n \mid \Phi_k(t-1)$. The largest part of the reasoning is contained in the following proposition. We prove it by showing that the action of the Frobenius morphism on $E[n]$ can be represented as a matrix, after which we will determine the order of this matrix.

Proposition 2.4 *Let E be a good curve of size n over $\mathbf{F}_p$. We assume $n \geq 5$. Then E has embedding degree k precisely when $n \mid \Phi_k(p)$.*
Proof:
We consider again the Frobenius endomorphim F on E. As we have seen on page 11, $E[n]$ is a free $\mathbf{Z}/n\mathbf{Z}$-module of rank 2. In fact, since n is prime, $E[n]$ is a $\mathbf{F}_n$-vector space of dimension 2.

The Frobenius morphism sends, like any endomorphism, the points of $E[n]$ to itself. Since it is a linear map, we can represent it with a 2×2-matrix, once we fix a basis of $E[n]$. Let P be a non-trivial point of $E(\mathbf{F}_p)$, and Q a point of $E(\mathbf{F}_{p^k})$ that is not a multiple of P. Then (P, Q) clearly is a basis of $E[n]$.

Since the Frobenius morphism F acts like the identity on $E(\mathbf{F}_p)$, it follows that $FP = P$. So the matrix looks like

$$\begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix}. \tag{2.1}$$

As we have seen on page 17, the trace of the matrix representing the Frobenius endomorphism on $E[m]$ is equal to $p + 1 - \#E(\mathbf{F}_p)$, modulo m. In our case, this means that the trace of the matrix in (2.1) is equal to $p + 1 - n$, modulo n. It follows that the matrix looks like

$$\begin{pmatrix} 1 & * \\ 0 & p \end{pmatrix}. \tag{2.2}$$

We now invoke Lemma 2.3. The embedding degree of E is equal to the smallest k such that F^k is the identity on $E[n]$, i.e. the smallest k such that the matrix M in (2.2) satisfies $M^k = I$.

There are a few possible cases, depending on the Jordan normal form of the matrix.

If $p \not\equiv 1 \bmod n$, we can diagonalize the matrix to $\left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right)$. Since $\left(\begin{smallmatrix} a_1 & 0 \\ 0 & a_2 \end{smallmatrix}\right)^m = \left(\begin{smallmatrix} a_1^m & 0 \\ 0 & a_2^m \end{smallmatrix}\right)$, it follows that the order of the matrix is equal to the order of p as an element of $\mathbf{F}_n^\times$.

If $p \equiv 1 \bmod n$, the matrix is similar to either the identity matrix or to $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. In the first case F is the identity on P and Q which means that F is the identity on all elements of $E[n]$, so $E[n] \subseteq E(\mathbf{F}_p)$. However, $E[n]$ has n^2 elements and $E(\mathbf{F}_p)$ only n, so this is not possible.
In the second case the order of the matrix is of course n. We will now show why F cannot have order n, if $p \equiv 1 \bmod n$.

We will argue by contradiction. Suppose $n \geq 5$ and $p = \ell n + 1$, with $\ell \geq 2$. By the Hasse bound (Theorem 1.32) $p + 1$ and n have to be close together (within $2\sqrt{p}$ of each other).:

$$2\sqrt{p} > |p + 1 - n|.$$

We substitute our expression for p:

$$2\sqrt{\ell n + 1} > |(\ell - 1)n + 2|.$$

We square both sides to get

$$4\ell n + 4 > (\ell - 1)^2 n^2 + 4(\ell - 1)n + 4.$$

This is equivalent to:

$$0 > (\ell - 1)^2 n^2 - 4n = n((\ell - 1)^2 n - 4)$$

Of course, a product of two numbers is negative if one of the factors is positive and the other negative. However, since $n \geq 5$, we see that

$$(\ell - 1)^2 n < 4$$

Since we did assume $\ell \geq 2$, we have $(\ell - 1)^2 \geq 1$, so $n < 4$. But we did assume $n \geq 5$. Contradiction.

So $p \equiv 1 \bmod n$ implies $p = n+1$, under the assumption that $n \geq 5$. However, since we require p and n to be both prime we can never have $p = n + 1$ for $n \neq 2$, so this situation does not occur.

So k is the order of $p \bmod n$. This is equivalent to $n \mid p^k - 1$, and $n \nmid p^\ell - 1$ for all $\ell < k$. By definition of the cyclotomic polynomial, this is equivalent to $n \mid \Phi_k(p)$. □

Of course, since we have defined the trace of the Frobenius to be $t = p+1-n$, the relation $n \mid \Phi_k(p)$ is equivalent to $n \mid \Phi_k(t - 1)$, which is the form we used in the introduction of this chapter.

§2.2 The parametrization

We now want to use the relation $n \mid \Phi_k(t-1)$. Barreto and Naehrig do this in the following way: they choose $t(x)$ to be a quadratic polynomial in x such that $\Phi_{12}(t(x)-1)$ decomposes into two quartic factors, one of which is chosen to be $n(x)$. Then $p(x)$ can be calculated using the relation $n = p - t + 1$.

§2.2.1. Galbraith's lemma. The possible choices for a $t(x)$ such that there is a decomposition in two factors are a result of Galbraith *et al.* in [2]. We will describe in detail how they found these polynomials.

The basis of their result is the following lemma:
Lemma 2.5 *Let $q(x)$ be a quadratic polynomial over $\mathbf{Q}$, and ζ_k a complex k-th root of unity. Then $\Phi_k(q(x))$ is over $\mathbf{Q}$ either irreducible, or splits into two irreducible polynomials of degree $\varphi(k)$. The latter happens iff $q(z) = \zeta_k$ has a solution in $\mathbf{Q}(\zeta_k)$.*
Proof:
Let θ be a root of $\Phi_k(q(x))$. Since $q(\theta)$ is a root of the k-th cyclotomic polynomial, it must be a primitive k-th root of unity, say ω_k. We see $\omega_k \in \mathbf{Q}(\theta)$, so $\mathbf{Q}(\omega_k) \subseteq \mathbf{Q}(\theta)$, and so $\varphi(k) = [\mathbf{Q}(\omega_k) : \mathbf{Q}]$ which divides $[\mathbf{Q}(\theta) : \mathbf{Q}]$.

If we have $\theta \in \mathbf{Q}(\omega_k)$, then $\mathbf{Q}(\theta) = \mathbf{Q}(\omega_k)$, and then we see that θ has degree $\varphi(k)$ over $\mathbf{Q}$. The minimum polynomial $f(x)$ of θ divides $\Phi_k(q(x))$. $f(x)$ is one irreducible factor (of degree $\varphi(k)$), and since we did assume nothing about θ except that it is a root of $\Phi_k(q(x))$, it follows by analogy that the minimum polynomial of any root of $\Phi_k(q(x))$ has to be an irreducible factor of $\Phi_k(q(x))$ of degree $\varphi(k)$. So $\Phi_k(q(x))$ splits into two irreducible factors of degree $\varphi(k)$.

If on the other hand $\theta \notin \mathbf{Q}(\omega_k)$, $[\mathbf{Q}(\theta) : \mathbf{Q}]$ must be strictly larger than $\varphi(k)$. However, it has to be a multiple of $\varphi(k)$ and we know that it is the root of a polynomial of degree $2\varphi(k)$. So then θ has degree $2\varphi(k)$ over $\mathbf{Q}$, and $\Phi_k(q(x))$ is irreducible over $\mathbf{Q}$.

Finally, we will prove the last claim in the lemma, namely that $q(z) = \zeta_k$ has a solution in $\mathbf{Q}(\zeta_k)$ iff $\theta \in \mathbf{Q}(\omega_k)$.
If $\theta \in \mathbf{Q}(\omega_k)$, then clearly $q(z) = \omega_k$ has a solution in $\mathbf{Q}(\omega_k)$, since $q(\theta) = \omega_k$). By Galois conjugation, it follows that $q(z) = \zeta_k$ also is solvable in this field, and this field is of course equal to $\mathbf{Q}(\zeta_k)$.
Suppose that $q(z) = \zeta_k$ has a solution in $\mathbf{Q}(\zeta_k)$. Again by Galois conjugation, this implies that $q(z) = \omega_k$ has a solution in the field $\mathbf{Q}(\zeta_k) = \mathbf{Q}(\omega_k)$. But if the quadratic polynomial $q(z) - \omega_k$ has one root in $\mathbf{Q}(\omega_k)$, the other root must also be in $\mathbf{Q}(\omega_k)$. So all roots of $q(z) - \omega_k$ are in $\mathbf{Q}(\omega_k)$, and therefore $\theta \in \mathbf{Q}(\omega_k)$ because $q(\theta) - \omega_k = 0$ by definition. □

§2.2.2. The application of the lemma. In our case, we are interested in the case $k = 12$, so then $\varphi(k) = 4$ (in fact, $\zeta_{12}^4 = \zeta_{12}^2 - 1$ for any root of unity ζ_{12} of order 12). We want $\Phi_{12}(q(x))$ to split, so we are interested in polynomials $q(z)$ assume the value ζ_{12} when z ranges over $\mathbf{Q}(\zeta_{12})$.

A particular example (in section 6 of [2] it is shown that this is the only solution up to translation and scaling) forms the polynomial:

$$q(z) = \frac{1}{a}z^2 - \frac{b}{a},$$

with $a, b \in \mathbf{Q}$. If we can find an $x \in \mathbf{Q}(\zeta_{12})$ such that

$$x^2 = a\zeta_{12} + b,$$

we are done, since $q(x) = \zeta_{12}$.

One could say that this only a trivial reformulation of the problem, but it gives a way to find such x's in a clean way. Since $\mathbf{Q}(\zeta_{12})$ is a quartic extension of $\mathbf{Q}$, $(1, \zeta_{12}, \zeta_{12}^2, \zeta_{12}^3)$ is a $\mathbf{Q}$-basis of $\mathbf{Q}(\zeta_{12})$. If we express x in this basis, we can easily do the same for x^2 (using the relation $\zeta_{12}^4 = \zeta_{12}^2 - 1$), and simply require the ζ_{12}^2 and ζ_{12}^3 coefficient to be 0.

We get to work: write $x = A + B\zeta_{12} + C\zeta_{12}^2 + D\zeta_{12}^3$ with $A, B, C, D \in \mathbf{Q}$ and compute the ζ_{12}^2 and ζ_{12}^3 coefficients of x^2. A little computation gives us $2AC + B^2 + 2BD + C^2$ resp. $2AD + 2BC + 2CD$. So if we have

$$2AC + B^2 + 2BD + C^2 = 0 \tag{2.3}$$

and

$$2AD + 2BC + 2CD = 0 \tag{2.4}$$

we see that we then have $x^2 = (2AB - 2CD)\zeta_{12} + (A^2 - 2BD - C^2 - D^2)$, so that

$$q(z) = \frac{1}{2AB - 2CD}z^2 - \frac{A^2 - 2BD - C^2 - D^2}{2AB - 2CD} \tag{2.5}$$

is such that $\Phi_{12}(q(z))$ is the product of two quartic factors.

Since D appears in both (2.3) and (2.4) with degree 1, we can eliminate this variable with little effort. If we multiply (2.3) with $A + C$ we get

$$2A^2C + AB^2 + 2ABD + AC^2 + 2AC^2 + B^2C + 2BCD + C^3 = 0,$$

and if we multiply (2.4) with B we obtain:

$$2ABD + 2B^2C + 2BCD = 0.$$

The difference of these two equation is a homogeneous equation in three variables.

$$2A^2C + AB^2 + 3AC^2 - B^2C + C^3 = 0.$$

We can rewrite this to

$$-C^3 - 3AC^2 - 2A^2C = (A - C)B^2$$

After a change of variables (namely $X = -6C$, $Y = 6B$ and $Z = A - C$), this becomes

$$ZY^2 = X^3 - 7X^2Z + 12XZ^2. \tag{2.6}$$

Of course, this is an elliptic curve, which we can dehomogenize to

$$E : y^2 = x^3 - 7x^2 + 12x.$$

As it turns out, $E(\mathbf{Q})$ is of rank 0: we have $E(\mathbf{Q}) = \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$. A pair of generators is $(0, 0)$ and $(6, 6)$.

One can show that most rational points on this curve E do not lead back to a quadratic polynomial. The only points that do are $(6, \pm 6)$ and $(2, \pm 2)$. We will now work this out for one of these points: $(6, 6)$ corresponds to the point $(6 : 6 : 1)$ on (2.6). Using the formulae for the change of variables, we see that this corresponds to $A = 0$, $B = 1$ and $C = -1$. Using (2.4), we see that $D = -1$, so $x = \zeta_{12} - \zeta_{12}^2 - \zeta_{13}^3$ and the polynomial $q(z)$ is – using (2.5) –

$$q(z) = \frac{1}{-2}z^2 + 0.$$

Of course, using a change of variables, we also get the polynomial $q(z) = 2z^2$. (More generally, all polynomials of the form $q(z) = 2(\alpha z + \beta)^2$ for $\alpha, \beta \in \mathbf{Q}$ can be obtained by a linear change of variables.)

We can verify that this really works:

$$\begin{aligned}\Phi_{12}(2z^2) &= 16z^8 - 4z^4 + 1 = \\ &= \left(4z^4 - 4z^3 + 2z^2 - 2z + 1\right)\left(4z^4 + 4z^3 + 2z^2 + 2z + 1\right).\end{aligned} \tag{2.7}$$

Similarly, the point $(2, 2)$ leads to a family of polynomials that differ by a linear change of variables. An example is $q(z) = 6z^2$.

Unfortunately, all other points on the curve do lead to either the same polynomial, or to linear polynomials. So there are only two options for a quadratic polynomial $q(z)$ for which $\Phi_{12}(q(z))$ splits into two factors of degree 4.

§2.3 Making the curves

Now we use the relation $n(x) \mid \Phi_{12}(t(x) - 1)$ to find suitable $n(x)$, and $p(x)$.

We first work out $q(x) = 2x^2$. We set $t(x) - 1 = 2x^2$, so $t(x) = 2x^2 + 1$. From (2.7), we see that we have two choices for $n(x)$. We try

$$n(x) = 4x^4 - 4x^3 + 2x^2 - 2x + 1.$$

Using the relation $t(x) = p(x) + 1 - n(x)$, we have to set

$$p(x) = 4x^4 - 4x^3 + 2x^2 - 2x + 1 - 1 + 2x^2 + 1 = 4x^4 - 4x^3 + 4x^2 - 2x + 1.$$

The other choice for $n(x)$ (and $p(x)$) is found by changing the two minuses into plusses.

In the other case we have $q(x) = 6x^2$. It follows that $t(x) = 6x^2 + 1$. Since

$$\begin{aligned}\Phi_{12}(6x^2) &= 1298x^8 - 36x^4 + 1 = \\ &= (36x^4 - x^3 + 18x^2 - 6x + 1)(36x^4 + x^3 + 18x^2 + 6x + 1),\end{aligned}$$

we have to set

$$n(x) = 36x^4 \pm x^3 + 18x^2 \pm 6x + 1.$$

We can now compute

$$\begin{aligned}p(x) = n(x) - 1 + t(x) = 36x^4 \pm x^3 + 18x^2 \pm 6x + 1 - 1 + 6x^2 + 1 = \\ = 36x^4 \pm x^3 + 24x^2 \pm 6x + 1. \quad (2.8)\end{aligned}$$

When we have found a value x_0 for which $p = p(x_0)$ and $n = n(x_0)$ are both prime, we want to construct elliptic curves over $\mathbf{F}_p$ with n points. This can be done with the CM-method, as described in [7]. This method which generates a curve of n points over $\mathbf{F}_p$[1] has the following steps:

1. Compute $t = p + 1 - n$ and the CM-discriminant $D = 4p - t^2$.
2. Compute the Hilbert class polynomial $H_D(x)$ of D.
3. Find a root j_0 of H_D modulo p.
4. Produce[2] a curve of j-invariant j_0 and check if this curve or its twist has n points.

We will not go further into how one can compute the Hilbert class polynomial. An alternative way to get the j-invariant of a curve with a certain CM-discriminant is demonstrated in section 3.4. Furthermore, the method above is implemented in MAGMA (Listing 4.4) in section 4.2.

[1] That is, if p and n satisfy the Hasse bound (Theorem 1.32). [2] This can be done by Theorem 1.26.

The CM-discriminant D mentioned above is defined in section 3.1. It is the discriminant of the quadratic equation that the Frobenius endomorphism satisfies, as discussed on page 17. In chapter 3, we will see that a curve E with Frobenius trace t over $\mathbf{F}_p$ has complex multiplication by the ring of integers of $\mathbf{Q}(\sqrt{t^2-4p})$. Since $\mathbf{Q}(\sqrt{m^2 n}) = \mathbf{Q}(\sqrt{n})$, we might as well ignore the square part of the discriminant.

A practical consideration is that the Hilbert class polynomial get extremely large for large CM-discriminants, so if we want to generate lots of curves with a certain CM-discriminant D, we want D to be very small.

With MAGMA, we can easily compute the factorization of the associated CM-discriminant in the four cases mentioned above. The results are summarized in Table 2.1.

Table 2.1 CM-discriminants for values of $p(x)$ and $t(x)$ associated to curves with embedding degree 12

field size $p(x)$	trace $t(x)$	factorized CM-discr. D
$4x^4 - 4x^3 + 4x^2 - 2x + 1$	$2x^2 + 1$	$-(2x^2+1)(6x^2-8x+3)$
$4x^4 + 4x^3 + 4x^2 + 2x + 1$	$2x^2 + 1$	$-(2x^2+1)(6x^2+8x+3)$
$36x^4 - 36x^3 + 24x^2 - 6x + 1$	$6x^2 + 1$	$-3(6x^2-4x+1)^2$
$36x^4 + 36x^3 + 24x^2 + 6x + 1$	$6x^2 + 1$	$-3(6x^2+4x+1)^2$

We can now see two things: the curves with trace $2x^2 + 1$ will have a very large CM-discriminant with no square part immediately visible, and the curves with trace $6x^2 + 1$ will always have CM-discriminant -3 times a square: so complex multiplication in the ring of integers of $\mathbf{Q}(\sqrt{3})$.

As it turns out, complex multiplication with discriminant -3 happens precisely for the curves with j-invariant 0. By Definition 1.24, in Weierstrass form those are the curves with no linear term, i.e. of the form $y^2 = x^3 + b$. The only thing we have to do is to find a b in $\mathbf{F}_p$ such that this curve has n points. Barreto and Naehrig describe in [1] a very easy algorithm for this: they just look for a b such that $1 + b$ is a square in $\mathbf{F}_p^\times$ (for half of the b's this is true). Then $(1, \sqrt{1+b})$ is on the curve. They then check the order of this point: if it is n, they are done. We will not go into detail here, but since there are six twists of a curve with j-invariant (by Theorem 1.35), one out of six curves does have the right number of points. So, on average, they need to test 12 choices of b before finding a curve with n points.

So if we choose the trace $t(x)$ to be $6x^2 + 1$, there is a very fast way to find a curve over $p(x_0)$ with $n(x_0)$ points for any choice of x_0 that makes $p(x_0)$ and $n(x_0)$ prime.

§2.4 How often are $p(x)$ and $n(x)$ prime numbers?

In section 2.1, we operate under the hypothesis that we have chosen x_0 such that $p = p(x_0)$ and $n = n(x_0)$ are prime numbers. We have to, because the argument uses the fact that there exist prime fields of size p and n. The method would not be very interesting if there would be only a finite number of values such that this occurs, so the following question comes to mind: are there infinitely many values of x such that $p(x)$ and $n(x)$ are prime?

This question is not yet answered, but the generalized Bunyakovsky conjecture states that any finite family $\mathcal{F}$ of polynomials satisfying the following rather obvious conditions:

- The leading coefficients of all polynomials in $\mathcal{F}$ should be positive.
- All polynomials should be irreducible over $\mathbf{Z}$.
- The set $\{f(n) : n \in \mathbf{Z}\}$ should not have a common prime divisor for any polynomial f in $\mathcal{F}$.
- For any prime p, there has to be an $x \in \mathbf{Z}$ such that $p \nmid f(x)$ for all f in $\mathcal{F}$.

has the following property:

> There are infinitely many $x \in \mathbf{Z}$ such that $f(x)$ is prime for all polynomials f in the family $\mathcal{F}$.

If this conjecture is true and we have verified the above conditions, there are infinitely many values of x such that $p(x)$ and $n(x)$ are prime.

It is clear that $p(x) = 36x^4 + 36x^3 + 24x^2 + 6x + 1$ and $n(x) = 36x^4 + 36x^3 + 18x^2 + 6x + 1$ satisfy the first condition. By Lemma 2.5, $n(x)$ is irreducible. Below we prove that $p(x) \bmod 5$ does not have linear factors and no quadratic factors, so $p(x)$ must be irreducible over $\mathbf{F}_5$ and therefore over $\mathbf{Z}$.

Lemma 2.6 *The polynomial* $p(x) = 36x^4+36x^3+24x^2+6x+1$ *is irreducible over* $\mathbf{F}_5$ *and therefore over* $\mathbf{Q}$.

Proof:

We will show that the reduction $\bar{p}(x) = x^4 + x^3 - x^2 + x + 1$ of $p(x)$ in $\mathbf{F}_5$ is irreducible. The quickest way to prove this is by checking for factors of degree 1 and 2. A linear factor corresponds to a root of $\bar{p}(x)$ in $\mathbf{F}_5$. However, a simple calculation show that $\bar{p}(0) = 1$, $\bar{p}(1) = 3$, $\bar{p}(2) = 3$, $\bar{p}(3) = 3$ and $\bar{p}(4) = 4$, so $\bar{p}(x)$ has no roots in $\mathbf{F}_5$.

So if $\bar{p}(x)$ is reducible, it has two quadratic factors, say $x^2 + ax + b$ and $x^2 + cx + d$. Then

$$x^4 + x^3 - x^2 + x + 1 = x^4 + (a + c)x^3 + (ac + b + d)x^2 + (ad + bc)x + bd.$$

This gives us a system of four equations over $\mathbf{F}_5$ which we will show has no solution, by checking all values of b.

Suppose $b = 0$. Then bd can never be 1. So this cannot be the case.
Suppose $b = 1$. By $bd = 1$, we have $d = 1$. So $ac + b + d = -1$ implies $ac = 2$. We also have $a + c = 1$. But these things cannot be true at the same time, because $ac = 2$ implies $\{a, c\} = \{1, 2\}$ or $\{a, c\} = \{3, 4\}$.
Suppose $b = 2$. From $bd = 1$ it follows that $d = 3$. $1 = ad + bc = 3a + 2c$. If we subtract $a + c = 1$ twice, we get $a = 4$. Now, $a + c = 1$ gives $c = 2$, but then $4 = ac + b + d = 3 + 2 + 3 = 3$. Contradiction.
Suppose $b = 3$. We see $d = 2$, and similarly as above, $1 = 2a + 3c$, so $c = 4$. $a + c = 1$ gives $a = 2$ and then $4 = ac + b + d = 3 + 3 + 2 = 3$ which is also a contradiction.
Suppose $b = 4$. By $bd = 1$, we see $d = 4$. So $1 = ad + bc = -a - c$ and $a + c = 1$ at the same time. But $a + c$ cannot be both 1 and -1.

We see that $\bar{p}(x)$ is irreducible. If $p(x)$ was reducible, its reduction modulo 5 would also be reducible, because the degree of $\bar{p}(x)$ is equal to that of $p(x)$. So $p(x)$ is irreducible over $\mathbf{Z}$. □

Since $p(0) = n(0) = 1$, there can be no common prime divisor for the set of all values of $p(x)$ resp. $n(x)$ for integer inputs x, and this also makes sure the fourth condition is satisfied: for all primes we can take $x = 0$.

Chapter 3

Complex multiplication

In this chapter, we discuss the theory of complex multiplication. First we will cover the general theory and the basic results. After that we will consider two cases: that of CM-discriminant -3 and -11. We will compute parametrizations for p and n for these cases, and we will describe how to find a curve over $\mathbf{Q}$ with CM-discriminant -11, using the relation between kernels and isogenies from Theorem 1.12.

Contents

3.1 General theory 37
3.1.1 Algebraic number theory 38
3.1.2 Complex multiplication over $\mathbf{C}$ 40
3.1.3 Complex multiplication over finite fields and $\mathbf{Q}$ . . 42
3.2 Complex multiplication with discriminant -3 and -11 43
3.3 The relation between the Frobenius and the 1- or 3-norm element 45
3.4 A family of curves with CM-discriminant -11 . 47
3.4.1 The other elliptic curve 48

§3.1 General theory

In this section we will give a short introduction of complex multiplication, expanding on the exposition in Chapter 1. Coarsely said, complex multiplication is about the size of the endomorphism ring of a curve. As it turns out, this depends heavily on the field the curve is defined over. As we have seen in Example 1.6, every endomorphism ring contains a copy of $\mathbf{Z}$. With this in mind, we define

Definition 3.1 *A elliptic curve E defined over K has* complex multiplication *if its endomorphism ring is strictly larger than* $\mathbf{Z}$.

§3.1.1. Algebraic number theory. In order to formulate the theory of complex multiplication, we need a few bits of algebraic number theory. In algebraic number theory one studies subrings of finite extensions of $\mathbf{Q}$ that have properties similar to that of $\mathbf{Z}$ with respect to $\mathbf{Q}$. Since finite extensions of $\mathbf{Q}$ are a central object of study, they have their own name: *number fields*.

The analogon of $\mathbf{Z}$ in these number fields is called *the ring of integers*:

Definition 3.2 *Let K be a number field. We define the* ring of integers $\mathcal{O}_K$ *to be the set of roots in K of all monic polynomials with coefficients in* $\mathbf{Z}$.

As it turns out, this is indeed a ring.

EXAMPLE 3.3 Consider $K = \mathbf{Q}(\sqrt{d})$ with d squarefree (i.e. there is no $n > 1$ such that $n^2 \mid d$). Then $\mathcal{O}_K = \{\frac{a}{2} + \frac{b}{2}\sqrt{d} : a, b \in \mathbf{Z}, 2 \mid a - b\}$ if $d \equiv 1 \bmod 4$ and $\mathcal{O}_K = \{a + b\sqrt{d} : a, b \in \mathbf{Z}\}$ if $d \equiv 2, 3 \bmod 4$. ◇

Often enough we are also interested in certain subrings of rings of integers:

Definition 3.4 *Let K be a number field. An* order *in K is a ring R such that $\mathbf{Z} \subset R \subseteq \mathcal{O}_K$ and the field of fractions of R is K.*

EXAMPLE 3.5 The orders in the ring of integers of $\mathbf{Q}(\sqrt{d})$ with d squarefree have the following form:

$$\mathbf{Z} + f\mathbf{Z} \cdot \delta$$

where $f \geq 1$ is an integer and $\delta = \sqrt{d}$ if $d \equiv 2, 3 \bmod 4$, and $\delta = \frac{1+\sqrt{d}}{2}$ if $d \equiv 1 \bmod 4$. ◇

For future reference, we define, with the notation as in the above examples:

Definition 3.6 *The number f is called the* conductor *of the order $\mathbf{Z} + f\mathbf{Z} \cdot \delta$. f is also the index of the order in the ring of integers.*
We define the discriminant *of this order to be the number $f^2 d$ if $d \equiv 1 \bmod 4$, and otherwise, we let $-4f^2 d$ be the discriminant.*

An important property of $\mathbf{Z}$ is that numbers factor into primes *uniquely*.[1] Unfortunately, this is not always the case in rings of integers in number

[1] To be more explicit, unique factorization in a ring R means the following: Suppose we write an element of R as a product of irreducible elements in two ways. Then the factors of the products are the same, but possibly in a different order, and up to multiplication by a unit in R. *Example*: $10 = 2 \cdot 5 = (-5) \cdot (-2)$ is one factorization.

fields. For instance, we have

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}) \tag{3.1}$$

in $\mathbf{Z}[\sqrt{-5}]$, and one can show that these factorizations are really different in the sense of the previous footnote

However, it turns out that we do have some form of unique factorization in number rings.

Proposition 3.7 *Let R be a ring of integers of a number field. Then every non-zero ideal of R can be written as the product of prime ideals in a unique way, up to order.*
Proof:
This is Theorem 3.7 in [6]. □

Indeed, we see that we can decompose the prime elements in (3.1) further into prime ideals:

$$\begin{aligned}(2) &= (2, 1 + \sqrt{-5})^2 \\ (3) &= (3, 1 + \sqrt{-5})(3, 1 - \sqrt{-5}) \\ (1 + \sqrt{-5}) &= (2, 1 + \sqrt{-5})(3, 1 + \sqrt{-5}) \\ (1 - \sqrt{-5}) &= (2, 1 + \sqrt{-5})(3, 1 - \sqrt{-5})\end{aligned}$$

Now we see that the two factorizations in (3.1) are in fact the same.

There is a way to measure how much unique factorization fails in a ring of integers. We do this by defining an equivalence relation:

Definition 3.8 *Let R be a ring of integers. We say that two ideals $\mathfrak{a}$ and $\mathfrak{b}$ are equivalent if there are $x, y \in R$ such that $x\mathfrak{a} = y\mathfrak{b}$. The* ideal class group *$\mathcal{C}\ell(R)$ of R is the set of equivalence classes in the set of ideals with respect to the above equivalence relation.*
It is a group under the operation $[\mathfrak{a}][\mathfrak{b}] = [\mathfrak{a}\mathfrak{b}]$.

It is not easy, but one can prove that:

Theorem 3.9 *Let $\mathcal{O}_K$ be the ring of integers of a number field K. Then the ideal class group of K is finite.*
Proof:
This is Theorem 4.4 in [6]. □

§3.1.2. Complex multiplication over C. First we study complex multiplication over $\mathbf{C}$. It is this case that motivates the name 'complex multiplication'. Luckily, it is not hard to describe the endomorphism ring of a curve over $\mathbf{C}$, since we already derived a description of the set of isogenies from one curve to another, in the Theorems 1.46 and 1.47.

Corollary 3.10 *The ring of endomorphisms of an elliptic curve E defined over $\mathbf{C}$ is in a canonical bijection with the set*

$$\{\alpha \in \mathbf{C} : \alpha\Lambda \subseteq \Lambda\}$$

where Λ is any lattice that is corresponding to E.

We will write $[\alpha]$ for the endomorphism corresponding to $\alpha \in \mathbf{C}$ via this bijection.

This severely limits the possibilities for the endomorphism ring:

Proposition 3.11 *Let E be an elliptic curve over $\mathbf{C}$ with complex multiplication, with associated lattice Λ. If $\alpha\Lambda \subseteq \Lambda$, then α is in the ring of integers of an imaginary quadratic field K, depending only on Λ.*

Proof:
Let $\Lambda = \mathbf{Z}\omega_1 + \mathbf{Z}\omega_2$. If $\alpha\Lambda \subseteq \Lambda$, then $\alpha\omega_1 = a\omega_1 + b\omega_2$ and $\alpha\omega_2 = c\omega_1 + d\omega_2$, for some $a, b, c, d \in \mathbf{Z}$. So we have

$$\alpha \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix}. \tag{3.2}$$

Since $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ is a 2×2-matrix, by Cayley-Hamilton it satisfies its own characteristic polynomial, i.e.

$$M^2 - (a+d)M + (ad - bc) = 0$$

If we multiply this from the right with the vector $(\omega_1\, \omega_2)^\top$ and use (3.2), we get

$$\alpha^2 \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} - (a+d)\alpha \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} + (ad - bc) \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} = 0.$$

Clearly this equation can only hold if

$$\alpha^2 - (a+d)\alpha + (ad - bc) = 0.$$

So α is the ring of integers of a quadratic number field K.

Consider another endormorphism $\beta \notin \mathbf{Z}$. By the reasoning above, β lies in the ring of integers of a quadratic number field K'. Say $K = \mathbf{Q}(\sqrt{d})$ and $K' = \mathbf{Q}(\sqrt{d'})$. Then the smallest field containing $\alpha+\beta$ over $\mathbf{Q}$ is $\mathbf{Q}(\sqrt{d}, \sqrt{d'})$. $\alpha + \beta$ lies – again by the reasoning above – in a quadratic number field. So $\mathbf{Q}(\sqrt{d}, \sqrt{d'})$ is a quadratic number field, but that can only be true if $K = K'$.

This proves that all endomorphism lie in the ring of integers of the same quadratic number field.

We will now show why this field is imaginary. Suppose $\alpha \in \mathbf{R}$. Then $\alpha\omega_1$ lies in the subspace of $\mathbf{C}$ spanned by $\{\omega_1\}$ since $\{\omega_1, \omega_2\}$ is a $\mathbf{R}$-basis of $\mathbf{C}$. Analogously $\alpha\omega_2$ lies in the subspace of $\mathbf{C}$ spanned by $\{\omega_2\}$. This means that in the matrix M defined above, we have $a = d = \alpha$ and $b = c = 0$. Since $a, d \in \mathbf{Z}$, we conclude $M = \left(\begin{smallmatrix} n & 0 \\ 0 & n \end{smallmatrix}\right)$ for some $n \in \mathbf{Z}$. So then $[\alpha]$ is just the multiplication-by-n-map. So if $\alpha \notin \mathbf{Z}$, then α is not real. Since E has complex multiplication, there are elements in $\mathrm{End}(E)$ that are not multiplication-by-an-integer maps, so K is imaginary. □

Proposition 3.12 *Let E be an elliptic curve over $\mathbf{C}$, and consider $\mathrm{End}(E)$ as a subring of $\mathbf{C}$, as in Corollary 3.10. Let $\alpha \in \mathrm{End}(E)$. Then the dual endomorphism of α is the complex conjugate of α.*
Proof:
In Lemma 1.20 we saw that α satisfies a quadratic equation with coefficients in $\mathbf{Z}$:

$$\alpha^2 - (\alpha + \hat{\alpha})\alpha + (\alpha\hat{\alpha}) = 0.$$

Since this equation has a non-real solution (namely α, per Proposition 3.11), it follows that the other solution must be the complex conjugate of α. Furthermore, we know that the constant term of a polynomial is the product of its roots (in the algebraic closure). So if α is one solution of the equation, $\hat{\alpha}$ must be the other. So $\hat{\alpha} = \bar{\alpha}$.

For $n \in \mathbf{Z}$, we have that $\widehat{[n]} = n$ by Theorem 1.16, so then the conjugate of n is the same as its dual too. □

Corollary 3.13 *Let E be an elliptic curve over $\mathbf{C}$, and consider $\mathrm{End}(E)$ as a subring of $\mathbf{C}$. Then $\deg(\alpha) = \alpha\bar{\alpha}$.*
Proof:
By Theorem 1.13, $[\deg(\alpha)] = \alpha\hat{\alpha}$, and by Proposition 3.12 $\hat{\alpha} = \bar{\alpha}$. From this the above follows immediate. □

We can summarize this to:

Corollary 3.14 *Let E be an elliptic curve over $\mathbf{C}$. Then $\mathrm{End}(E) \cong \mathbf{Z}$ or $\mathrm{End}(E)$ is an order in an quadratic imaginary number field.*

In fact, there is more algebraic number theory going on.

Proposition 3.15 *Let R be an order in a quadratic imaginary number field. Then there is a bijection between*

- *homothety classes of lattices Λ such that $R\Lambda \subseteq \Lambda$, and*

- *ideal equivalence classes in R.*

Proof:
This is Proposition 10.3 in [11]. □

Furthermore, we have the following way to determine what type of complex multiplication is going on.

Proposition 3.16 *The elliptic curve over $\mathbf{C}$ corresponding to the lattice $\mathbf{Z}\omega_1 + \mathbf{Z}\omega_2$ has complex multiplication by an order in an imaginary quadratic number field K iff $\omega_2/\omega_1 \in K$.*
Proof:
This is Corollary 10.5 in [11]. □

§3.1.3. Complex multiplication over finite fields and Q. Complex multiplication over finite fields is rather different than over $\mathbf{C}$. The most striking difference is that every curve has complex multiplication.

Let us consider the finite field $\mathbf{F}_p$. We repeat (1.5): for the Frobenius morphism F we have:

$$F^2 - tF + p = 0.$$

The Hasse bound (Theorem 1.32) states that $|t| \leq 2\sqrt{p}$, so $t^2 \leq 4p$ and in fact $t^2 < 4p$ since t is an integer so equality cannot be reached. Since the discriminant of the polynomial is $t^2 - 4p$, we see that F cannot be in $\mathbf{Z}$. However, in finite fields not of prime order, we may have that $F \in \mathbf{Z}$. We will now only discuss fields of prime size (although the classification below holds for all finite fields):

Theorem 3.17 *Let E be an elliptic curve over $\mathbf{F}_p$. There are two possible situations:*

- *E* is ordinary. *In this case $\#E[p] = p$.* $\mathrm{End}(E)$ *is an order in a quadratic imaginary field.*
- *E* is supersingular. *In this case $\#E[p] = 1$.* $\mathrm{End}(E)$ *is an order in a quaternion algebra.*

A curve over $\mathbf{F}_p$ is supersingular precisely when $\#E(\mathbf{F}_p) = p + 1$.
Proof:
This is Theorem V.3.1 in [8], and the last claim is Proposition 13.3.9 in [4].
□

We will not discuss supersingular curves, since we will be interested in the cases where $\#E(\mathbf{F}_p)$ is a prime number, and $p+1$ cannot be prime if p is prime and $p > 2$.

Definition 3.18 *Let E be an elliptic curve over $\mathbf{F}_p$ with ordinary complex multiplication, and t the trace of the Frobenius. We call $t^2 - 4p$ the* CM-discriminant*. It is the discriminant of the equation $F^2 - tF + p = 0$ that the Frobenius endomorphism satisfies.*

One can show that the CM-discriminant is – up to a square – equal to the discriminant of the endomorphism ring, as defined in Definition 3.6.

As we have seen in Theorem 1.34, we can reduce curves defined over $\mathbf{Q}$ to curves defined over $\mathbf{F}_p$, for p prime. Let us write $E \bmod p$ for the reduction of E to $\mathbf{F}_p$.

Theorem 3.19 *Let E be an elliptic curve defined over $\mathbf{Q}$. Suppose E is of good reduction over a prime p.*

- $\mathrm{End}(E)$ *maps injectively into* $\mathrm{End}(E \bmod p)$.
- *If* $\mathrm{End}(E)$ *is an order in $\mathbf{Q}(\sqrt{-D})$, then E is ordinary precisely when $-D$ is a non-zero square modulo p.*

Proof:
This is Theorem 13.12 in [5]. □

§3.2 Complex multiplication with discriminant -3 and -11

In this section, we will discuss elliptic curves with a CM-discriminant -3 resp. -11. That is, the endomorphism ring of these curves is $\mathbf{Z}[\frac{1+\sqrt{-3}}{2}]$ resp. $\mathbf{Z}[\frac{1+\sqrt{-11}}{2}]$. The first of these is the sort of complex multiplication that appears in the curves Barreto and Naehrig describe. We will now describe this more explicitly.

We will show that the CM-discriminant is -3 iff there is a endomorphism satisfying a certain quadratic polynomial:

Theorem 3.20 *Let E be an elliptic curve defined over $\mathbf{Q}$.* $\mathrm{End}(E) = \mathbf{Z}[\frac{1+\sqrt{-3}}{2}]$ *if and only if there exists an endomorphism α for which*

$$\alpha^2 + \alpha + [1] = [0].$$

Proof:

We start with the easy half. Suppose $\mathrm{End}(E) = \mathbf{Z}[\frac{1+\sqrt{-3}}{2}]$. Then there is an endomorphism $\alpha = \frac{-1+\sqrt{-3}}{2}$. This α satisfies

$$\alpha^2 + \alpha + 1 = \frac{1}{4} - \frac{\sqrt{-3}}{2} + \frac{-3}{4} + \frac{-1}{2} + \frac{\sqrt{-3}}{2} + 1 = 0.$$

Suppose on the other hand that we have an elliptic curve E for which there exists an endomorphism α that satisfies $\alpha^2 + \alpha + 1 = 0$. Clearly, the only α satisfying this equation is $\alpha = \frac{-1\pm\sqrt{1^2-4\cdot1\cdot1}}{2} = \frac{-1\pm\sqrt{-3}}{2}$. So the ring of endomorphisms contains at least $\mathbf{Z}[\frac{-1+\sqrt{-3}}{2}]$. Since this is the ring of integers of $\mathbf{Q}(\sqrt{-3})$ (see Example 3.3), and because every endomorphism ring of a curve defined over the rationals is an order in a ring of integers (Corollary 3.14), we know that $\mathbf{Z}[\frac{-1+\sqrt{-3}}{2}]$ is the entire endomorphism ring. □

We can make this more concrete. The curves with CM-discriminant -3 are precisely those with j-invariant 0, and those are the elliptic curves that can be written as $E_b : y^2 = x^3 + b$ (for some $b \in K$). But for these curves, we can give α such that $\alpha^2 + \alpha + 1 = 0$ explicitly. Take

$$\alpha : E_b \to E_b : (x, y) \mapsto (\omega x, y),$$

where ω is a primitive third root of unity. Clearly this is an endomorphism, since, if (x, y) is a point on E_b, then

$$(\omega x)^3 + b = \omega^3 x^3 + b = x^3 + b = y^2$$

so $\alpha(x, y)$ is too. Furthermore, since $\alpha^2(x, y) = (\omega^2 x, y)$, the points $P = (x_0, y_0) \in E_b$, αP and $\alpha^2 P$ always have the same y-coordinates, so they are the three intersection points of the line $y = y_0$ and the curve E_b. By the way we did define the group structure on an elliptic curve, way back in the introduction, it follows that $P + \alpha P + \alpha^2 P = \mathcal{O}$ for all P, so $\alpha^2 + \alpha + 1 = 0$ as endomorphisms.

If we have such an elliptic curve over $\mathbf{Q}$ with complex multiplication with discriminant -3, we can look at the reductions of this curve modulo p for various primes p, as described in Theorem 1.34. (Of course we want the curve to be of good reduction modulo p.) We will be interested in cases where the reduced curve $E \bmod p$ is ordinary, and not supersingular, as described in Theorem 3.17. By Theorem 3.19 happens precisely when 3 is a non-zero square modulo p, i.e. when $(\frac{-3}{p}) = 1$. By quadratic reciprocity, if p is ≥ 5,

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right) = \left(\frac{p}{3}\right).$$

So $E \bmod p$ is ordinary, if p is a square modulo 3. This is the case for $p \equiv 1 \bmod 3$. Finally, -3 is also a square modulo 2, so $E \bmod 2$ is also ordinary. For $p = 3$, we have supersingularity, because $3 = 0$ there.

For our specific curve $E_b : y^2 = x^3 + b$, we can see this phenomenon illustrated. Let us reduce E_b modulo p (we assume this is good reduction, i.e. $p \nmid b$). Then we have the two endomorphisms: $\alpha(x, y) = (\omega x, y)$ (if $\mathbf{F}_p$ does not contain third roots of unity, α is defined over the larger field $\mathbf{F}_{p^2}$) and the Frobenius morphism $F(x, y) = (x^p, y^p)$. If these do not commute, then $\mathrm{End}(E \bmod p)$ has to be an order in a quaternion algebra, and hence $E \bmod p$ is supersingular.

We have

$$F\alpha(x, y) = F(\omega x, y) = (\omega^p x^p, y^p),$$

and

$$\alpha F(x, y) = \alpha(x^p, y^p) = (\omega x^p, y^p).$$

So: α and F commute iff $\omega^p = \omega$, so iff $\omega^{p-1} = 1$. Since ω is a third root of unity, this happens iff $3 \mid p - 1$, that is, if $p \equiv 1 \bmod 3$. This is precisely what we have shown above: if $E \bmod p$ is supersingular, then indeed we can find non-commuting endomorphisms.

Similarly, for the curves with complex multiplication with discriminant -11, we can show that this is equivalent with the existence of an endomorphism w for which $w^2 + w + [3] = [0]$.

If we have an elliptic curve over $\mathbf{Q}$ with complex multiplication with discriminant -11, we can look again at the reductions of this curve modulo p for various primes p, as described in Theorem 1.34. We will be interested in cases where the reduced curve $E \bmod p$ is ordinary, and not supersingular, as described in Theorem 3.17. By Theorem 3.19 happens precisely when 11 is a non-zero square modulo p, i.e. when $(\frac{-11}{p}) = 1$. By quadratic reciprocity, if p is odd,

$$\left(\frac{-11}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{11}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{11}\right) = \left(\frac{p}{11}\right).$$

So $E \bmod p$ is ordinary, if p is a square modulo 11. This is the case for $p \in \{1, 3, 4, 5, 9\} \bmod 11$. Finally, -11 is also a square modulo 2, so $E \bmod 2$ is also ordinary.

§3.3 The relation between the Frobenius and the 1- or 3-norm element

Suppose that we are working with a elliptic curve E with complex multiplication with discriminant -3 or -11 over $\mathbf{Q}$. Now we look at the reduction

of this curve modulo some prime p, such that $E \bmod p$ is ordinary, as specified in the previous section. Since $\mathrm{End}(E)$ injects into $\mathrm{End}(E \bmod p)$ by Theorem 3.19, we also have in $\mathrm{End}(E \bmod p)$ an endomorphism α such that $\alpha^2 + \alpha + 1 = 0$ resp. an endomorphism w that satisfies $w^2 + w + 3 = 0$.

Again, we will first discuss the case where the discriminant is -3.

Since $\overline{E} = E \bmod p$ is an elliptic curve over $\mathbf{F}_p$, the endomorphism ring contains the Frobenius morphism $F : (x, y) \mapsto (x^p, y^p)$. Let us write $F = a + b\alpha$, for some $a, b \in \mathbf{Z}$. We now calculate the degree of this map, using that the degree of the Frobenius is p, and that we have the properties in Theorem 1.16:

$$p = \deg(F) = \deg(a+b\alpha) = (a+b\alpha)\widehat{(a+b\alpha)} = a^2+ab(\alpha+\hat{\alpha})+b^2\alpha\hat{\alpha}. \quad (3.3)$$

By Lemma 1.20, we know that α satisfies the following equation in $\mathbf{Z}[x]$:

$$x^2 - (\alpha + \hat{\alpha})x + (\alpha\hat{\alpha}) = 0. \quad (3.4)$$

Since α is not in $\mathbf{Z}$ (since no integer x satisfies $x^2 + x + 1 = 0$), the minimal polynomial of α is $x^2 + x + 1$. Since the minimal polynomial is unique, it must be equal to (3.4). So $\mathrm{tr}(\alpha) = -1$ and $\deg(\alpha) = 1$. If we substitute this in (3.3), we get

$$p = a^2 - ab + b^2. \quad (3.5)$$

Since the Frobenius morphism F fixes precisely the points in $\overline{E}(\overline{\mathbf{F}_p})$ with coordinates in $\mathbf{F}_p$, the kernel of the map $F - 1$ is $\overline{E}(\mathbf{F}_p)$. So

$$\begin{aligned}\#\overline{E}(\mathbf{F}_p) &= \#\ker(F-1) = \deg(F-1) = \\ &= \deg((a-1)+b\alpha) = (a-1)^2 - (a-1)b + b^2 = \\ &= a^2 - 2a + 1 - ab + b + b^2 = p - 2a + b + 1.\end{aligned}$$

Note that we did use that $F - 1$ is separable (this is Corollary III.5.5 in [8]).

Furthermore,

$$\begin{aligned}\mathrm{tr}(F) = F + \hat{F} &= a + b\alpha + \widehat{a + b\alpha} = \\ &= a + b\alpha + a + b\hat{\alpha} = 2a + b\,\mathrm{tr}(\alpha) = 2a - b.\end{aligned}$$

Note that this confirms the equality $\mathrm{tr}(F) = p - \#\overline{E}(\mathbf{F}_p) + 1$ from page 17.

Again, we can do the same for the curves with CM-discriminant -11: from the equation $w^2 + w + 3 = 0$, we derive with Lemma 1.20 that the trace is -1 and the degree 3. We have

$$p = \deg(F) = \deg(a+bw) = (a+bw)\widehat{(a+bw)} = a^2+ab(w+\hat{w})+b^2w\hat{w}. \quad (3.6)$$

and hence

$$p = a^2 - ab + 3b^2. \tag{3.7}$$

The number of points on E with coordinates in $\mathbf{F}_p$ is given by

$$\begin{aligned}\#\overline{E}(\mathbf{F}_p) &= \#\ker(F-1) = \deg(F-1) = \\ &= \deg((a-1)+b\alpha) = (a-1)^2 - (a-1)b + 3b^2 = \\ &= a^2 - 2a + 1 - ab + b + 3b^2 = p - 2a + b + 1.\end{aligned}$$

so the trace of the Frobenius is again

$$\mathrm{tr}(F) = F + \hat{F} = a + bw + a + b\hat{w} = 2a + b\mathrm{tr}(w) = 2a - b.$$

§3.4 A family of curves with CM-discriminant -11

In this section we will use Theorem 1.12 to construct an explicit example of a curve over $\mathbf{C}$ with CM-discriminant -11.

The content of the theorem is that the existence of a degree 3 isogeny from a curve E to another curve E' corresponds with the existence of a subgroup of $E(\mathbf{C})$ of order 3. This subgroup must be generated by a point P of order 3. If E is written in Weierstrass form (we will assume this from now on), then the y-coordinate of a point with order 3 cannot be 0, so we can rescale the curve so that $P = (0,1)$. Let us write $E : y^2 = x^3 + ax^2 + bx + 1$. If $3P = \mathcal{O}$, then $P * P = P$, that is, the tangent line to E in P has multiplicity 3 there.

We will now do the calculation. First we will compute the coefficient of the tangent line. We write $\ell : y = tx + 1$, for some $t \in \mathbf{C}$. We have $t = \frac{\mathrm{d}y}{\mathrm{d}x}|_{(0,1)}$. Since we have for points on the curve

$$\mathrm{d}y^2 = \mathrm{d}(x^3 + ax^2 + bx + 1),$$

so

$$2y\mathrm{d}y = (3x^2 + 2ax + b)\mathrm{d}x,$$

it follows that

$$t = \frac{\mathrm{d}y}{\mathrm{d}x}|_{(0,1)} = \frac{3x^2 + 2ax + b}{2y}|_{(0,1)} = \frac{b}{2}$$

We will now determine when the intersection multiplicity in P is 3. This happens if the third intersection point of the line ℓ and the curve E has x-coordinate 0. For any intersection point (x, y) we have that they satisfy

$$y^2 = x^3 + ax^2 + bx + 1,$$

and

$$y = \frac{b}{2}x + 1.$$

If we square this second equation and combine it with the first, we obtain:

$$\frac{b^2}{4}x^2 + bx + 1 = y^2 = x^3 + ax^2 + bx + 1.$$

Clearly

$$\frac{b^2}{4}x^2 = x^3 + ax^2.$$

The three roots of this equation are the x-coordinates of the intersection points. Obviously $x = 0$ is a double solution: the line ℓ is tangent to E there. If we divide by x^2, we get

$$\frac{b^2}{4} = x + a.$$

So the last intersection point has x-coordinate $\frac{b^2}{4} - a$.

So the third intersection point is also P exactly when $a = \frac{b^2}{4}$.

So the curve E has a subgroup of order 3 in $E(\overline{K})$ generated by $(0, 1)$ precisely when it can be written as

$$E : y^2 = x^3 + \frac{b^2}{4}x^2 + bx + 1 \tag{3.8}$$

For technical purposes, it is easier to look at a curve that is isomorphic to this one, namely

$$y'^2 = x'^3 + \frac{1}{4}x'^2 + \frac{1}{b^3}x' + \frac{1}{b^6}.$$

E and this curve are indeed isomorphic: consider the change of coordinates $y' = \frac{y}{b^2}$ and $x' = \frac{x}{b^3}$. (Under this change of coordinates, P is mapped to $(0, b^{-3})$. From now on we will call this curve E.

§3.4.1. The other elliptic curve. Now we have the general form of a curve E with a subgroup of size 3. As mentioned above, this implies that there is a unique elliptic curve E' and a separable isogeny φ such that $\varphi : E \to E'$ is an isogeny of degree 3. We can give this curve E' explicitly with *Vélu's formula's*. This is described in for instance Theorem 12.16 in [11]. We will not do the calculation by hand, but instead let MAGMA do the dirty work. This gives that E' has the formula

$$E' : y^2 = x^3 + \frac{1}{4}x^2 - \frac{9}{b^3}x + \frac{-2b^3 - 27}{b^6}.$$

Furthermore, the isogeny $E \to E'$ is given by

$$f : (x, y) \mapsto \left(\frac{x^3 + \frac{1}{54}x^2 + \frac{1}{2916}}{x^2}, \frac{x^3 + \frac{1}{54}x^2 + \frac{1}{1458}}{x^3} y \right)$$

In the previous section, we have constructed an elliptic curve with an isogeny of degree 3. However, we are not interested in isogenies of degree 3, but in *endomorphisms* of degree 3. Since an endomorphism is just an isogeny from a curve to itself, this happens precisely when E' is isomorphic to E. A simple way to test this is by calculating the j-invariants of both curves (by Theorem 1.25). With the help of MAGMA, we see that

$$j(E) = \frac{\frac{1}{8}b^{12} - 18b^9 + 864b^6 - 13824b^3}{b^3 - 54}$$

and

$$j(E') = \frac{\frac{1}{2}b^{12} + 648b^9 + 279936b^6 + 40310784b^3}{b^9 - 162b^6 + 8748b^3 - 157464}$$

After a short calculation, we see that

$$j(E) - j(E') = \frac{\frac{1}{8}b^{18} - \frac{63}{2}b^{15} + 3172b^{12} - 160272b^9 + 3732480b^6 - 80621568b^3}{b^9 - 162b^6 + 8748b^3 - 157464}$$

We can factor the numerator of this expression:

$$\frac{1}{8}b^{18} - \frac{63}{2}b^{15} + 3172b^{12} - 160272b^9 + 3732480b^6 - 80621568b^3 = \\ = \frac{1}{8}b^3(b^3 - 108)(b^6 - 128b^3 + 6912)(b^6 - 16b + 864)$$

So we have a couple of options for b^3 that cause the j-invariant of $E = E_b$ and E' to be equal: 0, 108, $64 \pm 16\sqrt{-11}$ and $8 \pm 20\sqrt{-2}$. In MAGMA, it is easy to compute the j-invariants and the corresponding complex multiplication. If $b^3 = 0$, we cannot use our 'new' curve, so we have to use the 'old' curve E in (3.8) (i.e. before we did our change of coordinates). It turns out that the curve E_0 is $y^2 = x^3 + 1$, with j-invariant 0 and CM-discriminant -3.
If $b^3 = 108$, we get the j-invariant 54000, and CM-discriminant -12.
If $b^3 = 64 \pm 16\sqrt{-11}$, we get the j-invariant -32768 and CM-discriminant -11.
And the last option is $b^3 = 8 \pm 20\sqrt{-2}$, and in this case the curve has j-invariant 8000, and CM-discriminant -8.

It turns out that the only elliptic curve (up to isomorphism) with complex multiplication by $\mathbf{Z}[\frac{1+\sqrt{-11}}{2}]$ has j-invariant $-32768 = -2^{15}$. In subsection 4.1.1, we give an elliptic curve defined over $\mathbf{Q}$ with j-invariant -32768.

Chapter 4

Extending the Barreto-Naehrig result

In this chapter we discuss our attempts to extend the result of Barreto and Naehrig. These attempts consisted of writing SAGE and MAGMA code, executed in the online free SAGE environment respectively in the online MAGMA calculator. A version of the code in section 4.3 was run on the licensed version of MAGMA. Due to restrictions on the runtime (most notably in MAGMA), we were not able to find examples with large numbers (that is, with $p, n > 10^7$). In this chapter a number of code fragments are discussed, after which we examine some examples more closely. The chapter finishes with a description of yet another way to generate curves with CM-discriminant -11 and a summary of the efforts and a general conclusion.

Contents

4.1 Testing curves with CM-discriminant -11 52
4.1.1 The theory 52
4.1.2 The code 52
4.1.3 The results 53
4.2 Testing curves with a small embedding degree . 53
4.2.1 The theory 53
4.2.2 The code 54
4.2.3 The results 56
4.3 Testing curves with CM-discriminant -11 and small embedding degree 56
4.3.1 The theory 56
4.3.2 The code 58
4.3.3 The results 58
4.4 Recycling the $2x^2 + 1$-trace parametrization . . . 59

```
1  repeat
2    p := RandomPrime(30);
3    if p ge 7 then
4      ok,E := IsEllipticCurve([GF(p)|0,0,0,-264,1694]);
5      if ok then
6        if IsPrime(#E) and p ne #E then
7        n := #E;
8          if Order(GF(n)!p) le 50 then
9            k:=Order(GF(n)!p);
10           print "Curve found with low embedding degree:", E;
11           print "p =", p, "n =", n, "k =", k;
12         end if;
13       end if;
14     end if;
15   end if;
16 until false;
```

Listing 4.1 MAGMA code, testing reductions of a curve over $\mathbf{Q}$ with CM-discriminant -11.

4.5 Concluding remarks 60

§4.1 TESTING CURVES WITH CM-DISCRIMINANT -11

§4.1.1. The theory. The first attempt we did was testing a family of curves we know has CM-discriminant -11. In section 3.4 we saw that the only elliptic curves with this type of complex multiplication are those with j-invariant -32768. After a small calculation (performed with MAGMA) we see that one of those curves is

$$E : y^2 = x^3 - 264x + 1694,$$

as one can verify with the formula in Definition 1.24.

If reduce that curve modulo p, and E is of good reduction modulo p, then $E \bmod p$ is curve with CM by $\mathbf{Z}[\frac{1+\sqrt{-11}}{2}]$. If E is a good curve, we can determine its embedding degree by finding the order of p in $\mathbf{F}_n^\times$.

§4.1.2. The code. In the Listing 4.1, the code performing this procedure is listed. We will now discuss the code line by line.
The code tests random primes below a certain bound until the program is terminated. In this program, the bound is 2^{30}. The bound can be set to any 2^m by changing 30 into m on line 2.
The if-statement in line 3 makes sure we can apply Proposition 2.4, and the if-statement in line 5 makes sure the discriminant of the reduced curve is

not zero.
In line 6 we test if the curve is good, and then we test in line 8 if the embedding degree is ≤ 50. Any curve satisfying that condition is printed.

After running the program[1] once in the free version of Magma, we see that in 120 seconds, approximately 1430000 random primes were selected in line 2. 16460 of those primes (about 1.2%) turned out to have good reduction and resulted in a good curve. Of those primes, 0 turned out to have a lower embedding degree than 50. (The smallest embedding degree found was 1655.) Of course this is just one trial of the program, but this indicates that good curves are relatively rare, and that a small embedding degree is extremely rare.

§4.1.3. The results. The only interesting example (that is, with $p > 100$) found with this code is the following:

Example 4.1 The elliptic curve

$$E : y^2 = x^3 + 202337x + 47913$$

defined over $\mathbf{F}_p$ with $p = 452587$ has $n = 453601$ points. The endomorphism ring of this curve is $\mathbf{Z}[\frac{1+\sqrt{-11}}{2}]$, as it is ordinary and the reduction of a curve over $\mathbf{Q}$ with that endomorphism ring. As it turns out, the order of p in $\mathbf{F}_n$ is 40, so this curve has embedding degree 40, by Proposition 2.4. ◇

§4.2 Testing curves with a small embedding degree

§4.2.1. The theory. In this section we first discuss an attempt to use Proposition 2.4 like Barreto and Naehrig do: namely by picking a quadratic polynomial $t(x)$, after which they take $n(x)$ to do a factor of $\Phi_k(t(x) - 1)$, where k is the desired embedding degree. From the relation $p = t - 1 - n$, we can derive $p(x)$, and we can compute the form of complex multiplication by looking at the squarefree part of $t^2 - 4p$.

There are two pieces of code for this. In the code in Listing 4.2, we look at the polynomials $q(z)$ for which $\Phi_k(q(z))$ decomposes in factors. In Listing 4.3, we look at the cases where this polynomial is irreducible. Both pieces of code turn out to produce examples with a small CM-discriminant.

To avoid that we repeatedly check the same case, we do not check all quadratic polynomials: after a translation one can ensure the polynomial has no linear term. Furthermore we do not check the cases where a and c share a factor, if they are both non-zero. Finally, we take a to be positive.

[1] The program was somewhat adapted to be able to count the number of primes used.

```
1  R, x = ZZ['x'].objgen()
2  for k in [12..50]:
3    f = R.cyclotomic_polynomial(k)
4    for a in [1..100]:
5      for c in [-100..100]:
6        if (gcd(a,c)!=1 and c!=0):
7          continue
8        q = a*x^2+c
9        F=factor(f(x=q))
10       length = len(list(F))
11       if length != 1:
12         maxfact = list(F)[length - 1][0]
13         if maxfact.degree() != 2*f.degree():
14           t = q + 1
15           n = maxfact
16           p = n + t - 1
17           D = t^2 - 4*p
18           y = 0
19           while y < 100:
20             if is_prime(p(x=y)) and is_prime(n(x=y)) and
     squarefree_part(D(x=y)) >= -1000:
21               print "k =",k,"y =",y,"n =",n(x=y),"p =",p(x=y),"
     sq.free CM-disc. =",squarefree_part(D(x=y))
22             if is_prime(p(x=-y)) and is_prime(n(x=-y)) and
     squarefree_part(D(x=-y)) >= -1000:
23               print "k =",k,"y =",-y,"n =",n(x=-y),"p =",p(x=-y
     ),"sq.free CM-disc. =",squarefree_part(D(x=-y))
24             y = y + 1
```

Listing 4.2 SAGE code, looking for factors of $\Phi_k(q(x))$ for quadratic polynomials $q(x)$.

Once we have found a p, an n and a CM-discriminant D, we have to find a curve over $\mathbf{F}_p$ with n points. We do this based on the CM-method described in [7]. We ask MAGMA for the Hilbert class polynomial corresponding to the CM-discriminant. The roots of that polynomial over $\mathbf{F}_p$ are the j-invariants of the curves with that type of complex multiplication. After that, we let MAGMA generate those curves and test if their number of points is n.

§4.2.2. The code. We start with the case where we look for factors of the composition of the cyclotomic and the quadratic polynomial.
In line 1, we specify that we are working in $\mathbf{Z}[X]$, after which we define `f` to be the k-th cyclotomic polynomial. In the lines 4 – 7 we let f be a quadratic polynomial of the form specified in the previous subsection.
Then we factor $\Phi_k(q(x))$. If there is more than one factor, we look at the factor with the highest degree (`maxfact`). If the degree of this factor is not equal to the degree of $\Phi_k(q(x))$, that is, if the other factors are not constants, we let $n(x)$ be this factor and $t(x) = q(x) + 1$. Now we can compute $p(x)$,

```
1  R, x = ZZ['x'].objgen()
2  for k in [12..50]:
3    f = R.cyclotomic_polynomial(k)
4    for a in [1..100]:
5      for c in [-100..100]:
6        if (gcd(a,c)!=1 and c!=0):
7          continue
8        q = a*x^2+c
9        F=factor(f(x=q))
10       length = len(list(F))
11       if length == 1:
12           t = q + 1
13           n = f(x=q)
14           p = n + t - 1
15           D = t^2 - 4*p
16           y = 0
17           while y < 100:
18             if is_prime(p(x=y)) and is_prime(n(x=y)) and
     squarefree_part(D(x=y)) >= -1000:
19               print "k =",k,"y =",y,"n =",n(x=y),"p =",p(x=y),"
     sq.free CM-disc. =",squarefree_part(D(x=y))
20             if is_prime(p(x=-y)) and is_prime(n(x=-y)) and
     squarefree_part(D(x=-y)) >= -1000:
21               print "k =",k,"y =",-y,"n =",n(x=y),"p =",p(x=y)
     ,"sq.free CM-disc. =",squarefree_part(D(x=-y))
22           y = y + 1
```

Listing 4.3 Sage code, looking for cases where $\Phi_k(q(x))$ is irreducible for quadratic polynomials $q(x)$.

and then the CM-discriminant.
In the while-loop starting on line 19, we test for $y \in \{-100, \ldots, 100\}$ if there is a y such that $p(y)$ and $n(y)$ are prime and if the CM-discriminant has a small squarefree part (here we look for squarefree parts > -1000).
If we find such a y, we print k, y, $n(y)$, $p(y)$ and the squarefree part of the CM-discriminant.

The code for the case where the composition of the cyclotomic and the quadratic polynomial is irreducible is basically the same. The only difference is that we require the list of factors to be of length 1, in line 10.

In the first two lines, one has to fill in the prime field and the curve size for which elliptic curves should be sought. Then the CM-discriminant and the Hilbert polynomial is computed, and the roots of that polynomial in $\mathbf{F}_p$ are listed in `rootslist`.
Then Magma makes an elliptic curve for every j-invariant, which is successively reduced to $\mathbf{F}_p$, and it tests for that curve (and its quadratic twist[2]) if

[2] We also test the twist of the generated curve, since this curve has the same CM-discriminant (for $t^2 - 4p = (-t)^2 - 4p$).

```
p:= ; //the field size
n:= ; //the size of the curve
t:= p + 1 - n;
D:= t^2 - 4*p;
H := HilbertClassPolynomial(D);
Q<y> := PolynomialRing(GF(p));
len := #Roots(Q!H);
rootslist:=Roots(Q!H);
for j in [1..len] do
  E:=EllipticCurveFromjInvariant(rootslist[j][1]);
  E1:=ChangeRing(E,GF(p));
  E2:=QuadraticTwist(E1);
  if #E1 eq n then
    print E1, "satisfies";
  end if;
  if #E2 eq n then
    print E2, "satisfies.";
  end if;
end for;
```

Listing 4.4 Magma code, looking for curves over $\mathbf{F}_p$ with n points and CM-discriminant D.

the number of points is n. If that is the case, the curve is printed.

§4.2.3. The results. With these pieces of code, no large examples were found. We discuss the two interesting curves.

Example 4.2 The curve

$$E : y^2 = x^3 + 1440x + 834$$

turns out to have $n = 1657$ points over $\mathbf{F}_p$ with $p = 1669$. Its embedding degree is 18, and it has CM-discriminant -723. ◇

Example 4.3 The curve

$$E : y^2 = x^3 + 209x + 60$$

has $n = 241$ points over $\mathbf{F}_p$ with $p = 239$. The embedding degree is 24, and it has CM-discriminant -955. ◇

§4.3 Testing curves with CM-discriminant -11 and small embedding degree

§4.3.1. The theory. The third attempt was to use the theory of Chapter 3: we start with a curve with CM-discriminant -11, and then we

look for values of p and n such that the embedding degree is low, and p and n are prime.

If the CM-discriminant is -11, for the Frobenius trace t and p the following holds:

$$t^2 - 4p = -11s^2$$

for some integer s. Consequently,

$$4p = t^2 + 11s^2. \tag{4.1}$$

n is now determined by $n = p + 1 - t$:

$$4n = 4p + 4 - 4t = t^2 - 4t + 4 + 11s^2 = (t-2)^2 + 11s^2. \tag{4.2}$$

If we look at (4.1) modulo 4, we see that $0 \equiv t^2 - s^2 \bmod 4$, so $t^2 \equiv s^2 \bmod 4$. It follows that t and s have the same parity. Furthermore, since the cases we consider have $p, n > 2$ both these numbers are odd. It follows that $4(p-n)$ is divisible by 8. Since the difference of (4.1) and (4.2) is $4t - 4$, we now have $8 \mid 4t - 4$, so $2 \mid t - 1$. So t is odd, and so is s. We write $t = 2a + 1$ and $s = 2b + 1$.

We can also analyze (4.1) and (4.2) modulo 3. Then we get $p \equiv t^2 + 2s^2 \bmod 3$ and $n \equiv (t-2)^2 + 2s^2 \bmod 3$. Let us assume $p, n > 3$. Then $p, n \not\equiv 0 \bmod 3$. Since squares are 0 or 1 modulo 3, it follows that $t^2 + 2s^2 \equiv t^2 - s^2$ is not $0 \bmod 3$ only if exactly one of t and s is divisible by 3. Similarly, we see that only one of the numbers $t - 2$ and s is divisible by 3. If s is not divisible by 3, then both t and $t - 2$ are, which is impossible. So $3 \mid s$, and both $3 \nmid t$ and $3 \nmid t - 2$ hold, so $t \equiv 1 \bmod 3$. This happens precisely if $a \equiv 0$ and $b \equiv 1$ modulo 3.

One can express p and n in a and b:

$$p = \frac{t^2 + 11s^2}{4} = \frac{4a^2 + 4a + 1 + 44b^2 + 44b + 11}{4} = a^2 + a + 3 + 11b^2 + 11b,$$

and

$$n = p + 1 - t = a^2 + a + 3 + 11b^2 + 11b + 1 - 2a - 1 = a^2 - a + 3 + 11b^2 + 11b.$$

The divisibility relation $n \mid \Phi_k(t-1)$ of Proposition 2.4 can also be expressed in a and b:

$$a^2 - a + 3 + 11b^2 + 11b \mid \Phi_k(2a). \tag{4.3}$$

So if we find an a and a b such that p and n are prime and the above condition is satified, we have found a curve with CM-discriminant -11 and an embedding degree of k.

```
1  R, x = ZZ['x'].objgen()
2  for k in [12..50]:
3    f = R.cyclotomic_polynomial(k)
4    for c in [-1000..1000]:
5      for d in [1..1000]:
6        a = 3*c
7        b = 3*d+1
8        m = a^2 - a + 3 + 11*b^2 + 11*b
9        n = f(x=2*a)
10       if m.divides(n):
11         t = 2*a + 1
12         s = 2*b + 1
13         p = (t^2 + 11*s^2)/4
14         n = p + 1 - t
15         if is_prime(ZZ(p)) and is_prime(ZZ(n)):
16           print "k =",k,"p =",p,"n =",n
```

Listing 4.5 SAGE code, looking for p and n such that the CM-discriminant is -11 and the embedding degree low.

§4.3.2. The code. This code is relatively simple: again we define the cyclotomic polynomial, in line 3, and then we test for a number of a's and b's if the relation (4.3) holds. Since we only need to test $a \equiv 0 \bmod 3$ and $b \equiv 1 \bmod 3$, we parametrize a and b by c and d. If the divisibility relation holds, the corresponding p and n are computed, and if they are indeed primes, they are printed.

§4.3.3. The results. Using this code, we found the following examples:

EXAMPLE 4.4 Over $\mathbf{F}_{2347}$, we have the elliptic curve

$$y^2 = x^3 + 160x + 672$$

with $n = 2311$ points. It has embedding degree 35 and CM-discriminant -11. ◇

EXAMPLE 4.5 Over $\mathbf{F}_{9277}$, we have the elliptic curve

$$y^2 = x^3 + 7899x + 5591$$

with $n = 9241$ points. It has also embedding degree 35 and CM-discriminant -11. ◇

We also found the curve from Example 4.1: for this curve we have $p = 452587$ and $n = 453601$, and

$$4p = (-1013)^2 + 11 \cdot 267^2,$$

and

$$4n = (-1015)^2 + 11 \cdot 267^2,$$

so the corresponding values of a and b are

$$a = -507, b = 133.$$

Indeed:

$$n = 453601 \mid 124912896785573731630041840143356256743896541848 1 = \Phi_{40}(2a)$$

so the divisibility relation for $k = 40$ is satisfied.

A version of this code was run on the full version of Magma by Jaap Top. Not bounded by time limits, he was able to find the following two examples:

Example 4.6 The elliptic curve

$$y^2 = x^3 + 192480115x + 263727633$$

has $n = 1571812201$ points over $\mathbf{F}_p$, where $p = 1571795437$. The embedding degree is 24, and the CM-discriminant -11. ◇

We finish with the largest example we found:

Example 4.7 The elliptic curve

$$y^2 = x^3 + 15445874592x + 26923017614$$

has $n = 28907447911$ points over $\mathbf{F}_p$ with $p = 28907383399$. The embedding degree of this curve is 30, and it has CM-discriminant -11. ◇

§4.4 Recycling the $2x^2 + 1$-trace parametrization

Another possible avenue of investigation is the following: consider the parametrizations Barreto and Naehrig found (as described in section 2.3). These parametrization lead to four different CM-discriminants. For the curves with trace $2x^2 + 1$ this discriminant is given by $-(2x^2 + 1)(6x^2 \pm 8x + 3)$, for the curves with trace $6x^2 + 1$ it is given by $-3(6x^2 \pm 4x + 1)^2$. Since we are interested in the squarefree part of this expression, the curves with trace $6x^2 + 1$ are not interesting (they always have CM-discriminant -3).

We can look at the curves with trace $2x^2 + 1$. In that case, we need to find $(x, y) \in \mathbf{Z}$ such that

$$-(2x^2 + 1)(6x^2 \pm 8x + 3) = -11y^2. \tag{4.4}$$

For any point (x_0, y_0) satisfying this, we have that the CM-discriminant is -11 times a square, so if $p(x_0)$ and $n(x_0)$ are primes, this gives a curve with embedding degree 12 and CM-discriminant -11.

Since it can be shown that the curve (4.4) is an elliptic curve, by Siegel's theorem (see section IX.3 in [8]) there are only a finite number of points with integral coordinates, so this method can never give us infinitely many curves with CM-discriminant -11.

In fact, one can find all the integral points using MAGMA with the command `IntegralQuarticPoints`. To use this command, we need to give a point on the curve, and write it in the $z^2 = f(x)$ for a quartic polynomial $f(x)$. The first of these is easy: $(2, 3)$ lies on $-(2x^2 + 1)(6x^2 - 8x + 3) = -11y^2$ and $(-2, 3)$ lies on $-(2x^2+1)(6x^2+8x+3) = -11y^2$. For the second requirement we multiply (4.4) with -11:

$$11(2x^2 + 1)(6x^2 \pm 8x + 3) = (11y)^2.$$

If we take $z = 11y$, we see that this becomes

$$132x^4 \pm 176x^3 + 132x^2 \pm 88x + 33 = z^2.$$

The point $(x, y) = (\pm 2, 3)$ becomes $(x, z) = (\pm 2, 33)$. According to MAGMA, $(2, 33)$ resp. $(-2, 33)$ are the only integral points on these curves.

As it turns out, for both the parametrizations with trace $2x^2 + 1$, the value of $p(2)$ is a composite number. If we take $p(x) = 4x^4 - 4x^3 + 2x^2 - 2x + 1$, we get $p(2) = 45$ and $n(2) = 29$, and if we take $p(x) = 4x^4 + 4x^3 + 2x^2 + 2x + 1$, we get $p(2) = 117$ and $n(2) = 109$.
So this method cannot be used to generate curves with embedding degree 12 and CM-discriminant -11.

§4.5 CONCLUDING REMARKS

Using the programs above, some examples were found. However, we did find only five remarkable examples, where remarkable means that $k \ll p, n$. However, since we did not search with much computation power (a few hours in MAGMA and SAGE), it seems not unlikely that more examples can be found using the code in this chapter.

The meagre harvest illustrates how remarkable the result of Barreto and Naehrig is: whereas we struggle to find a handful of examples, they give a method to produce without effort infinitely many curves.

We could not find another coincidence like Barreto and Naehrig did, namely the appearance of a factor that appears twice in the CM-discriminant given

$n(x)$ and $p(x)$, which is essential for generating a whole family of curves like they did. Asking for this coincidence to happen for CM-discriminant -11 is even more hard to come by.

Appendix A

Just enough algebraic geometry

To be able to define elliptic curves and the maps between them, we need some concepts from algebraic geometry. In this appendix we discuss the theory from the subject we need. We will not go into every detail. The interested reader is referred to any introduction on algebraic geometry, for instance [3].

Contents

A.1 Affine varieties 63
A.1.1 Ideals and algebraic sets 63
A.1.2 Maps between affine varieties 65
A.2 Projective varieties 66
A.2.1 Projective coordinates 66
A.2.2 Ideals and algebraic sets 67
A.2.3 The connection between projective and affine . . . 68
A.2.4 Maps between projective varieties 70

§A.1 Affine varieties

§A.1.1. Ideals and algebraic sets. We start with the study of subsets of K^n.

Definition A.1 Affine n-space *over* K *is defined as the set of points*

$$\mathbf{A}^n = \mathbf{A}^n(\overline{K}) = \{(x_1, \ldots, x_n) : x_i \in \overline{K}\}.$$

The set of K-rational points *is defined as*

$$\mathbf{A}^n(K) = \{(x_1, \ldots, x_n) : x_i \in K\}.$$

Within this space, we want to study the set of points where a certain (family of) polynomial(s) vanishes. Let $S \subseteq \overline{K}[X_1, \ldots, X_n]$ be a subset of the polynomials over $\overline{K}$. We then look at the set of all the points where all polynomials in S vanish. Of course, any linear combination of vanishing polynomials also vanishes, so we don't lose anything if we look just at the ideal generated by S.

Definition A.2 *Let I be an ideal in $\overline{K}[X_1, \ldots, X_n]$. Then we define*

$$\mathcal{V}(I) = \{(x_1, \ldots, x_n) \in \mathbf{A}^n : f(x_1, \ldots, x_n) = 0 \text{ for all } f \in I\}$$

Any subset of $\mathbf{A}^n$ of this form is called an algebraic subset.

Note that we have $\mathcal{V}(I) \cup \mathcal{V}(J) = \mathcal{V}(I + J)$ and $\mathcal{V}(I) \cap \mathcal{V}(J) = \mathcal{V}(IJ)$, for any ideals I, J in $\overline{K}[X_1, \ldots, X_n]$

Since any finite union of algebraic sets is an algebraic set itself, we don't lose much if we restrict ourselves to sets that cannot be written as a union:

Definition A.3 *If an algebraic set cannot be written as the union of two strictly smaller algebraic sets, it is called an* irreducible *algebraic set, or a* affine variety.

We have defined the set corresponding to an ideal, but we can also define the ideal corresponding to an algebraic set:

Definition A.4 *Let V be an algebraic subset of $\mathbf{A}^n$. Then we define*

$$\mathcal{I}(V) = \{f \in \overline{K}[X_1, \ldots, X_n] : f(x_1, \ldots, x_n) = 0 \text{ for all } (x_1, \ldots, x_n) \in V\}.$$

We will not prove the following statement: it can be found in any introductory text on the subject.

Proposition A.5 *An algebraic set $V \subseteq \mathbf{A}^n$ is a variety precisely when $\mathcal{I}(V)$ is a prime ideal in $\overline{K}[X_1, \ldots, X_n]$.*

In fact, the operations $\mathcal{I}(\cdot)$ and $\mathcal{V}(\cdot)$ are almost each other's inverse. This is the content of Hilbert's famous *Nullstellensatz*. We will not go further into this.

Definition A.6 *We say that an affine variety $V \subseteq \mathbf{A}^n$ is* defined over K *if $\mathcal{I}(V)$ can be generated by polynomials in $K[X_1, \ldots, X_n]$.*

If an affine variety V is defined over K, we write $V(K) = V \cap \mathbf{A}^n(K)$, and $\mathcal{I}_K(V) = \mathcal{I}(V) \cap K[X_1, \ldots, X_n]$.

Let V be an affine variety defined over K. Every element f of $K[X_1, \ldots, X_N]$ defines a polynomial function from the variety to K: simply by sending $(x_1, \ldots, x_n)$ to $f(x_1, \ldots, x_n)$. This gives a surjective map

$$K[X_1, \ldots, X_n] \to \{\text{polynomial functions from } V \text{ to } K\}$$

Of course, the kernel of this map is $\mathcal{I}_K(V)$. This means that there is a bijection between a quotient of the polynomial ring and the set of polynomial functions from V to K. The former object is an important object called the coordinate ring.

Definition A.7 *Let V be an affine variety defined over K. Then the* coordinate ring *of V is defined as*

$$K[V] = K[X_1, \ldots, X_n]/\mathcal{I}_K(V).$$

The function field *$K(V)$ of V is defined as the field of fractions of $K[V]$.*

Finally, we will formally define the dimension of a variety.

Definition A.8 *Let V be an affine variety. We define the* dimension of V *to be the transcendence degree*[1] *of $\overline{K}(V)$ over $\overline{K}$.*

§A.1.2. Maps between affine varieties. Now we want to define maps from one variety to another. Since we are working with sets defined by polynomials in some sense, the logical thing to do is to look at maps defined by polynomials:

Definition A.9 *A* morphism *between two affine varieties $V \subseteq \mathbf{A}^n$ and $W \subseteq \mathbf{A}^m$ is a map:*

$$f : V \to W : (x_1, \ldots, x_n) \mapsto (f_1(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n))$$

with $f_i \in \overline{K}[X_1, \ldots, X_n]$, such that the image of f lies inside W.

EXAMPLE A.10 On every affine variety $V \subseteq \mathbf{A}^n$ we can define the identity morphism id_V that is given by

$$(x_1, \ldots, x_n) \mapsto (x_1, \ldots, x_n).$$

◇

[1] The *transcendence degree* of a field extension L over K is defined as the size of the smallest subset S of L such that L is algebraic over $K(S)$.

EXAMPLE A.11 Consider the varieties $V = \mathbf{A}^1$ and $W = \mathcal{V}(y - x^2) \subseteq \mathbf{A}^2$. Then

$$f : V \to W : x \mapsto (x^2, x)$$

is a morphism from V to W. ◇

Just like many other mathematical structures, the idea of a structure-preserving map (a morphism) allows us to say that two structures are 'essentially the same' (isomorphic).

Definition A.12 *Two affine varieties V and W are said to be* isomorphic *if there exists an morphism $\varphi : V \to W$ and an isomorphism $\psi : W \to V$ such that $\psi \circ \varphi = \mathrm{id}_V$ and $\varphi \circ \psi = \mathrm{id}_W$.*

EXAMPLE A.13 The two varieties V and W from Example A.11 are isomorphic. The map

$$g : W \to V : (x, y) \mapsto y$$

is the inverse of the map f. ◇

One says that two varieties are *isomorphic over K* if we can define morphisms over K between them that are each other's inverse.

§A.2 PROJECTIVE VARIETIES

On page x we encountered the following phenomenon: we wanted to describe straight lines in the plane. These are of the form $y = ax + b$ with a, b in some field K. However, this is not entirely true. One group of lines in the plane cannot be written in this way: the line $x = c$ for any $c \in K$. Intuitively, this corresponds to the case '$a = \infty$'. This is inconvenient: everytime we want to prove something for all straight lines we need to take this 'exceptional case' in account, so we would like to find some way to describe all lines at once.

§A.2.1. Projective coordinates. A way to solve this problem is with *projective coordinates*. We add some points to the affine space, and we extend the definition of any variety defined on the affine part to the new space. We will first define projective space.

Definition A.14 Projective n-space *over K is defined as the set of points $(x_0 : x_1 : \cdots : x_n)$ where all x_i are in $\overline{K}$ and not all x_i are zero, modulo the following equivalence relation:*
$(x_0 : \cdots : x_n) \sim (y_0 : \cdots y_n)$ if there exists a $\lambda \in \overline{K} \backslash \{0\}$ such that for all i

we have $x_i = \lambda y_i$.
We write $\mathbf{P}^n$ *or* $\mathbf{P}^n(\overline{K})$.

As we can see, a point P in projective space has many different representations of the form $(x_0 : \ldots : x_n)$. We will call such a representation homogeneous coordinates for P.

EXAMPLE A.15 Let $K = \mathbf{Q}$. Typical points of $\mathbf{P}^2$ look like $(0 : 0 : 1)$ or $(3 : 4 : 5)$. We have for instance $(2 : 0 : 4) = (-1 : 0 : -2)$. ◇

We can embed $\mathbf{A}^n$ in many ways in $\mathbf{P}^n$: take for instance the map $(x, y) \mapsto (x : y : 1)$.

Just like with affine space, we want to define the K-rational points of the space. We cannot simply demand that all coordinates are in K, since every point can be written with coordinates not in K. Instead, we define:

Definition A.16 *The* K-rational points *of* $\mathbf{P}^n$ *are points* $(x_0 : \cdots : x_n)$ *such that there is a* $\lambda \in \overline{K}\backslash\{0\}$ *with* $\lambda x_i \in K$ *for all* i.

§A.2.2. Ideals and algebraic sets. Again, we want to study zero sets of polynomials in a space. However, we have a problem: a point has many coordinates, and we do not want the answer to the question 'does this point lie in the zero set?' to be dependent of the particular choice of coordinates. We therefore have to restrict our focus to polynomials $f \in \overline{K}[X_0, \ldots, X_n]$ with the following property:

$$f(\lambda X_0, \ldots, \lambda X_n) = \lambda^d f(X_0, \ldots, X_n)$$

for some $d \in \mathbf{Z}$. Such a polynomial is said to be *homogeneous* of degree d.

We also define homogeneous ideals:

Definition A.17 *A* homogeneous ideal *of* $\overline{K}[X_0, \ldots, X_n]$ *is an ideal that is generated*[2] *by homogeneous polynomials.*

Now we can define the operations $\mathcal{V}(\cdot)$ and $\mathcal{I}(\cdot)$ for projective spaces.

Definition A.18 *Let* I *be a homogeneous ideal of* $\overline{K}[X_0, \ldots, X_n]$. *Then we define*

$$\mathcal{V}(I) = \{P \in \mathbf{P}^n : f(P) = 0 \text{ for all homogeneous } f \text{ in } I\}.$$

Any set of this form is called an algebraic subset *of* $\mathbf{P}^n$.

Definition A.19 *Let* V *be an algebraic set in* $\mathbf{P}^n$. *Then we define* $\mathcal{I}(V)$ *to be the ideal generated by all homogeneous polynomials* f *in* $\overline{K}[X_0, \ldots, X_n]$

[2] Be warned, a homogeneous ideal will usually contain lots of non-homogeneous polynomials.

such that $f(P) = 0$ for all points P in V. We say V is defined over K *if $\mathcal{I}(V)$ can be generated by homogeneous polynomials in $K[X_0, \ldots, X_n]$.*

With Proposition A.5 in mind, we define:

Definition A.20 *Let V be an algebraic set in $\mathbf{P}^n$. V is said to be a* projective variety *if $\mathcal{I}(V)$ is a prime ideal in $\overline{K}[X_0, \ldots, X_n]$.*

§A.2.3. The connection between projective and affine. Of course, the reason for defining all these things is that we wanted to make the study of affine varieties more natural. Certainly we need a way to make projective varieties out of affine varieties and vice versa.

We already have seen a map from affine space to projective space. In fact we can define for any i between 0 and n the function $\varphi_i : \mathbf{A}^n \to \mathbf{P}^n : (x_1, \ldots, x_n) \mapsto (x_1 : \cdots : x_i : 1 : x_{i+1} : \cdots : x_n)$ which is a bijection between $\mathbf{A}^n$ and the set U_i of points in $\mathbf{P}^n$ with non-zero $i+1$-th coordinate, since we can write down its inverse:

$$\varphi_i^{-1} : U_i \to \mathbf{A}^n : (y_0 : \cdots : y_n) \mapsto \left(\frac{y_0}{y_i}, \ldots, \frac{y_{i-1}}{y_i}, \frac{y_{i+1}}{y_i}, \ldots, \frac{y_n}{y_i} \right).$$

So, $\mathbf{P}^n$ is covered by $n+1$ copies of $\mathbf{A}^n$.

Another ingredient for this process is that we can *homogenize* and *dehomogenize* polynomials with respect to a variable.

Definition A.21 *Suppose we have a polynomial $f(X_1, \ldots X_n)$. We define the* homogenization *of f with respect to Z to be*

$$f^\sharp(X_1, \ldots, X_n, Z) = Z^d f\left(\frac{X_1}{Z}, \ldots, \frac{X_n}{Z} \right)$$

where d is the smallest integer such that $f^\sharp$ is a polynomial.
Suppose we have a homogeneous polynomial $f(X_0, \ldots, X_n)$. We define the dehomogenization *of f with respect to the $i+1$-th coordinate to be*

$$f^\flat(X_0, \ldots, X_{i-1}, X_{i+1}, \ldots, X_n) = f(X_0, \ldots, X_{i-1}, 1, X_{i+1}, \ldots, X_n).$$

We interrupt ourselves for a short view back to the problem we discussed on page 66. We looked at lines of the form $y = ax + b$, and the 'exceptional case' $x = c$. If we homogenize the first equation, we get $y = ax + bz$, which can also be written as $0 = \alpha x + \beta y + \gamma z$. Now the exceptional case is also covered by this formula: take $\beta = 0$ and we get $0 = \alpha x + \gamma z$ which is $x = c$ after dehomogenization.

Now we return to the connection between the two flavors of varieties and how to switch between them.

Definition A.22 *(From projective to affine.) Let V be a projective algebraic set, in $\mathbf{P}^n$. Let $I = \mathcal{I}(V)$ be the homogeneous ideal corresponding to V. Then for any X_i (with $0 \leq i \leq n$) we define an[3] affine algebraic set $V^\flat = V \cap \mathbf{A}^n = \varphi_i^{-1}(V \cap U_i)$ with ideal*

$$I' = \{f(X_0, \ldots, X_{i-1}, 1, X_{i+1}, \ldots, X_n) : f(X_0, \ldots, X_n) \in I\}.$$

That is, I' consists of the dehomogenized elements of I with respect tot $i+1$-th coordinate.

Definition A.23 *(From affine to projective.) Let V be an affine algebraic set, in $\mathbf{A}^n$. Let $I = \mathcal{I}(V)$ be the ideal corresponding to V. We define $V^\sharp$ (often called the* projective closure *of V) to be the[4] projective algebraic set corresponding to the homogeneous ideal generated by all homogenized elements of I.*

Of course, this is only useful if we can show that these operations are in some way each other's inverse:

Proposition A.24 *Let V be an affine variety defined over K. Then $V^\sharp$ is a projective variety defined over K.*
Let W be a projective variety defined over K. Then $W^\flat$ is an affine variety defined over K.
We have $V = (V^\sharp)^\flat$, and if $W^\flat \neq \emptyset$ then $(W^\flat)^\sharp = W$.

Given a affine variety V, and its projective closure $V^\sharp$, we can identify the points on V with a subset of $V^\sharp$. The points *outside* this subset are called, slightly informally, the *points at infinity*.

We will now demonstrate this process with an elliptic curve.

EXAMPLE A.25 Suppose we have the elliptic curve $y^2 = x^3 + x + 2$, say over $\mathbf{Q}$. Formally, this is the affine variety, say V, corresponding to the ideal $I = (Y^2 - X^3 - X - 2) \subseteq \overline{\mathbf{Q}}[X, Y]$. This ideal is clearly generated by one polynomial $f = Y^2 - X^3 - X - 2$. We want to find $V^\sharp$, with respect to Z, so we homogenize this polynomial. We get

$$f^\sharp = Z^d(Y^2Z^{-2} - X^3Z^{-3} - XZ^{-1} - 2).$$

for some d. The smallest d for which this a polynomial is 3, so we conclude $f^\sharp = Y^2Z - X^3 - XZ^2 - 2Z^3$. So $V^\sharp$ is the projective variety generated by the homogeneous ideal $(Y^2Z - X^3 - XZ^2 - 2Z^3)$ in $\overline{\mathbf{Q}}[X, Y, Z]$.

The points at infinity are the points of $V^\sharp$ that do not lie in $\varphi_3(\mathbf{A}^n)$, i.e. the points of $V^\sharp$ for which $Z = 0$. It is not hard to find these: these are the

[3] For any projective set we have usually different affine set. However, since by Proposition A.24 these all have the same homogenization, we do not distinguish between them in the notation. [4] From Propostion A.24 we know that $V^\sharp$ is essentially independent of the choice of the variable we homogenize with.

points $(x : y : z)$ for which $z = 0$ and $y^2z - x^3 - xz^2 - 2z^3 = 0$ hold, i.e. $x^3 = 0$ so $x = 0$. The only point in $\mathbf{P}^2$ that satisfies this has coordinates $(0 : 1 : 0)$. So this is the only point of infinity of V. Let us keep this point, say Q, a moment in our thoughts.

We also can go the other way round. Take $W = V^\sharp$ as defined above. Suppose we want to dehomogenize by Y: now $W^\flat$ corresponds to the ideal consisting of the dehomogenized elements of $(Y^2Z - X^3 - XZ^2 - 2Z^3)$. If we dehomogenize (w.r.t. Y) the generator $Y^2Z - X^3 - XZ^2 - 2Z^3$ of this ideal, we get $Z - X^3 - XZ^2 - 2Z^3$. So

$$W^\flat = \mathcal{V}(Z - X^3 - XZ^2 - 2Z^3),$$

or, more informally, the variety $x^3 = -2z^3 - xz^2 + z$.

Since we have dehomogenized with respect to a variable where Q has a non-zero coordinate, the point Q is no longer at infinity. Indeed, it corresponds to the point $(x, z) = (0, 0)$ on this variety. ◇

Finally, we extend the scope of the definition of some concepts we already defined for affine varieties.

Definition A.26 *Let V be a projective variety defined over K.*
The dimension *of V is defined to be the same as that of $V^\flat$ (where we choose the dehomogenization variable such that $V^\flat \neq \emptyset$).*
We say that V is smooth *in a point P if it it is smooth in $V^\flat$ if P does not lie at infinity.*
The function field $\overline{K}(V)$ *of V is the field of rational functions f/g such that f and g are homogeneous elements of $\overline{K}[X_0, \ldots, X_n]$ of the same degree and $g \notin \mathcal{I}(V)$, modulo the follow equivalence relation: $f/g \sim f'/g'$ if $fg' - f'g \in \mathcal{I}(V)$.*

A *curve* is a projective variety of dimension 1.

§A.2.4. Maps between projective varieties. Our last task is to define maps between projective varieties. We do not only define morphisms, but also rational maps.

Definition A.27 *A* rational map $\varphi : V_1(\subseteq \mathbf{P}^m) \to V_2(\subseteq \mathbf{P}^n)$ *is a map*

$$(x_0 : \cdots : x_m) \mapsto (\varphi_0(x_0, \ldots, x_m) : \cdots : \varphi_n(x_0, \ldots, x_m)),$$

where

- *every φ_i is a homogeneous polynomial in $\overline{K}[X_0, \ldots, X_m]$ of the same degree. We require that not all φ_i's are in $\mathcal{I}(V_1)$.*

- *for all* $f \in \mathcal{I}(V_2)$ *we have that*

$$f(\varphi_0(X_0, \ldots, X_m), \ldots, \varphi_n(X_0, \ldots, X_m)) \in \mathcal{I}(V_1).$$

If $\varphi_i(P) = 0$ *for all* i *for some point* $P \in V_1$*, we set, instead of the definition above,*

$$\varphi(P) = (\psi_0(P) : \cdots \psi_n(P)),$$

for any choice of homogeneous polynomials $\psi_0, \ldots, \psi_n$ *of the same degree in* $\overline{K}[X_0, \ldots, X_m]$ *that satisfy for all* i *and* j*:*

$$\varphi_i\psi_j - \varphi_j\psi_i \in \mathcal{I}(V_1)$$

and $\psi_i(P) \neq 0$ *for some* i*.*

Note that there might be points where a rational map is not defined, even with the provision in the second part of the definition. We call all points where we can define $\varphi(P)$ *regular*.

Definition A.28 *A rational map* $V_1 \to V_2$ *that is regular everywhere on* V_1 *is called a* morphism.

Definition A.29 *A rational map* $\varphi = (\varphi_0, \ldots, \varphi_n)$ *between projective varieties* $V_1 \subseteq \mathbf{P}^m$ *and* $V_2 \subseteq \mathbf{P}^n$ *is* defined over K *if there is a* $\lambda \in \overline{K}$ *such that* $\lambda\varphi \in K[X_1, \ldots, X_m]$

We now give a couple of examples:

EXAMPLE A.30 Let $V \subseteq \mathbf{P}^n$ be a projective variety. We can now define the *identity morphism*:

$$\mathrm{id}_V : V \to V : (x_0 : \cdots : x_n) \mapsto (x_0 : \cdots : x_n)$$

◇

EXAMPLE A.31 Let K be a finite field of size q, and $V \subseteq \mathbf{P}^n$ a variety defined over K. Then

$$F_q : (x_0 : \cdots : x_n) \mapsto (x_0^q : \cdots : x_n^q)$$

is a morphism, since it is defined everywhere and the map $x \mapsto x^q$ is an automorphism of K. ◇

Isomorphisms of projective varieties are exactly in the same way defined as with affine varieties:

Definition A.32 *Two projective varieties V and W are said to be* isomorphic *if there exists an morphism $\varphi : V \to W$ and a morphism $\psi : W \to V$ such that $\psi \circ \varphi = \mathrm{id}_V$ and $\varphi \circ \psi = \mathrm{id}_W$.*
If V and W are defined over K we say that they are isomorphic over K *if there maps as mentioned above that are defined over K.*

EXAMPLE A.33 Consider the variety $V : Y^2Z = X^3$. Then

$$\varphi : \mathbf{P}^1 \to V : (s : t) \mapsto (s^2t : s^3 : t^3)$$

is a morphism. To see this, we need to check that $y^2z = x^3$ if we substitute $x = s^2t$, $y = s^3$ and $z = t^3$, and that $\varphi(P)$ is well-defined for all $P \in \mathbf{P}^1$. The former is clear, and the latter follows from the fact that $s^2t = s^3 = t^3 = 0$ implies that $s = t = 0$: there are no points for which all coordinate functions are zero.

It is easily checked that the map

$$\psi : V \to \mathbf{P}^1 : (x : y : z) \mapsto (y : x)$$

is a rational map. One can show that

$$\varphi \circ \psi : V \to V : (x : y : z) \mapsto (y^2x : y^3 : x^3) = (y^2x : y^3 : y^2z) = (x : y : z)$$

and

$$\psi \circ \varphi : \mathbf{P}^1 \to \mathbf{P}^1 : (s : t) \mapsto (s^3 : s^2t) = (s : t)$$

are the identity morphism *where they are defined.*

However, since ψ is not defined at $(0 : 0 : 1) \in V$, ψ is not an isomorphism. $\diamond$

EXAMPLE A.34 Consider the varieties $V : Y^2Z = X^3 - 5XZ^2$ and $W : Y^2Z = X^3 - XZ^2$. We can easily show that they are isomorphic over $\overline{\mathbf{Q}}$. Take

$$\varphi : V \to W : (x : y : z) \mapsto \left(x : \frac{y}{\sqrt[4]{5}} : \sqrt{5}z\right).$$

clearly if $y^2z = x^3 - 5xz^2$, then $(\frac{y}{\sqrt[4]{5}})^2\sqrt{5}z = x^3 - x(\sqrt{5}z)^2$. However, V has infinitely many rational points and W has only 4, so they can't be isomorphic over $\mathbf{Q}$, since then this $\mathbf{Q}$-isomorphism would send rational points bijectively to rational points. (The sizes of $V(\mathbf{Q})$ and $W(\mathbf{Q})$ are computed in section III.6 of [10], using the Mordell-Weil-theorem.) $\diamond$

A fact we will often need is the following:

Theorem A.35 *Let $\varphi : C_1 \to C_2$ be a morphism from a curve C_1 to a curve C_2. Then φ is either surjective or constant.*

Proof:
This is Theorem II.6.8 in [3]. □

Bibliography

[1] P.S.L.M. Barreto and M. Naehrig. *Pairing-Friendly Elliptic Curves of Prime Order.* Selected areas in cryptography, 319-331, Lecture Notes in Comput. Sci., vol. 3897. Springer, 2006.

[2] S.D. Galbraith, J.F. McKee, and P.C. Valença. *Ordinary abelian varieties having small embedding degree.* Finite Fields Appl. 13, no. 4, 800-814. Elsevier, 2007.

[3] R. Hartshorne. *Algebraic Geometry.* Graduate Texts in Mathematics, vol. 52. Springer, 1977.

[4] D. Husemöller. *Elliptic Curves.* Graduate Texts in Mathematics, vol. 111, 2nd ed. Springer, 2004.

[5] S. Lang. *Elliptic functions.* Graduate Texts in Mathematics, vol. 112, 2nd ed. Springer, 1986.

[6] J.S. Milne. *Algebraic Number Theory.* Lecture notes, v. 3.07. Available on `http://www.jmilne.org/math/`, 2017.

[7] F. Morain. *Building Cyclic Elliptic Curves Modulo Large Primes.* Advances in Cryptology – Eurocrypt'1991, vol. 547 of Lecture Notes in Computer Science, pp. 335 – 353. Springer, 2002.

[8] J.H. Silverman. *Arithmetic of Elliptic Curves.* Graduate Texts in Mathematics, vol. 106. Springer, 1986.

[9] J.H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves.* Graduate Texts in Mathematics, vol. 151. Springer, 1994.

[10] J.H. Silverman and J. Tate. *Rational Points on Elliptic Curves.* Undergraduate Texts in Mathematics, vol. 69. Springer, 1992.

[11] L.C. Washington. *Elliptic Curves: Number Theory and Cryptography.* 2nd ed. Chapman & Hall/CRC, 2008.

Index

affine n-space, 63
    rational points, 63
affine variety, 64
algebraic subset
    in projective n-space, 67
    over affine n-space, 64

bad reduction, 17
Barreto-Naehrig algorithm, 33
Bunyakovsky conjecture, 34

CM-discriminant, 33, 43
CM-method, 32
complex multiplication, 38
    ordinary, 42
    singular, 42
conductor, 38
coordinate ring, 65
curve, 70

degree, 4
dehomogenization, 68
dimension
    of a projective variety, 70
    of an affine variety, 65
dual isogeny, 8

elliptic curve, xi, 2
    group operation, xii
    reduction, 17
        complex multiplication, 43
elliptic function, 18
embedding degree, 26
endomorphism, 3
    field extension, 4
    Frobenius morphism, 4
    inseparable, 5
    multiplication-by-m-map, 4
    on the n-torsion, 11
    separable, 5
    trace, 10
endomorphism ring, 3

function field, 65
    of a projective variety, 70
fundamental parallellogram, 19

Galbraith's lemma, 29, 53
good curve, 26
good reduction, 17

Hasse bound, 16
Hilbert class polynomial, 32, 54
homogeneous ideal, 67
homogeneous polynomial, 67
homogenization, 68
homothetic, 23

ideal class group, 39
irreducible curve, xi
isogeny, 2
isomorphism
    between affine varieties, 66
    between projective varieties, 72
    over K, 66, 72

j-invariant, 12

lattice, 18

morphism
    between affine varieties, 65
    between projective varieties, 71

number fields, 38

order, 38
    discriminant, 38

parametrization of CM-curves, 46, 57
projective n-space, 66
    rational points, 67
projective closure, 69
projective coordinates, 66
projective variety, 68

quadratic curve, ix
quadratic twist, 18

rational map, 70
ring of integers, 38

smooth
    curve, xi
    projective variety, 70

torsion points, 11
    complete list, 13
    over $\mathbf{C}$, 21
trace of the Frobenius, 16
transcendence degree, 65
twist, 12
    by d, 13

uniformization theorem, 20

Vélu's formula's, 48

Weierstrass normal form, xi
Weierstrass-$\wp$-function, 19