NTNU – Trondheim
Norwegian University of
Science and Technology

Number Theoretic Properties of Elliptic Curves

Marius Blomlie

Master of Science in Physics and Mathematics
Submission date: June 2014
Supervisor: Sverre Olaf Smalø, MATH

Norwegian University of Science and Technology
Department of Mathematical Sciences

NUMBER THEORETIC PROPERTIES OF ELLIPTIC CURVES

Marius Blomlie

Spring 2014

NTNU

Department of Mathematical Sciences
Norwegian University of Science and Technology

Abstract

In this thesis we will look at some of the theory of elliptic curves. We will use this for some number theoretical examples, use methods to determine the number of points on an elliptic curve over finite fields, and also discuss primality testing. We will also have a look at the Riemann hypothesis and see how it is related to elliptic curves.

The primary source of literature for this thesis is [1], which we loosely follow in our presentation of the theory.

Sammendrag

I denne tesen vil vi se på noe av teorien til elliptiske kurver. Vi vil bruke dette på noen tallteoretiske eksempler, bruke metoder for å angi antallet punkter på en elliptisk kurve over endelige kropper, og også diskutere primtallstesting. Vi vil også se på Riemannhypotesen og se hvordan den er relatert til elliptiske kurver.

Den primære litteraturkilden for denne tesen er [1], som vi løst følger i vår presentasjon av teorien.

Preface

This master thesis marks the end of my 5 years at the Norwegian University of Science and Technology. The work was carried out at the Department of Mathematical Sciences during the spring of 2014.

I would like to thank my supervisor Professor Sverre O. Smalø for all the help during this work and for excellent guidance throughout the semester.

I would also like to thank all my family and friends who have supported me during my studies at NTNU.

Lastly I want to thank my closest family, Kelly, Bridget and Lucia, for your invaluable support during all this time. Without you, this work would not have been done. This thesis is dedicated to you.

Contents

Index of notations

$a \mid b$	a divides b
$a \nmid b$	a does not divide b
$\in$	membership
$\subseteq$	set inclusion
$\cup$	union of sets
$\cap$	intersection of sets
$\simeq$	isomorphism
$\forall$	for all
$\mathbb{N}$	natural numbers
$\mathbb{Z}$	integers
$\mathbb{Q}$	rational numbers
$\mathbb{R}$	real numbers
$\mathbb{C}$	complex numbers
$\mathbb{Z}_p$	integers modulo $p\mathbb{Z}$ for a prime p
$\mathbb{F}_{p^n}$	a finite field of p^n elements, p prime
$\mathbb{RP}^2$	the real projective plane
$\mathbb{CP}^2$	the complex projective plane
gcd	greatest common divisor
Δ	the elliptic discriminant
$K^\star$	the multiplicative group of a field K
$\overline{K}$	the algebraic closure of a field K
$K[x]$	polynomial with coefficients in a field K
$\mathrm{char}(K)$	characteristic of the field K
$K(\eta)$	the smallest field containing K and $\eta \in L$, where L is a field extension of K.
$E(L)$	elliptic curve with coordinates in a field L
$\det(A)$	determinant of a matrix A
$\mathrm{tr}(A)$	trace of a matrix A
$\mathrm{adj}(A)$	the adjugate matrix of a matrix A
$\deg(\alpha)$	degree of an endomorphism α
$\mathrm{Ker}(\alpha)$	kernel of an endomorphism α
(x/p)	the Legendre symbol for an odd prime p with x and p coprime

Chapter 1

Introduction to elliptic curves

A very important concept in modern number theory and algebraic geometry is that of *elliptic curves*. They are a major area of research today and have applications in integer factorization of large numbers and the so-called Elliptic Curve Cryptography. Elliptic curves were, as most mathematical theories, originally studied for their own sake without any concern regarding eventual applicabilities. It was only lately that the aforementioned applications were discovered. Elliptic curves were also used in Sir Andrew Wiles' proof of Fermat's Last Theorem, which helped to spur the growing interest in the field.

In this text we will present some of the rich theory of elliptic curves, a broad subject which, in Serge Lang's words, it is "*possible to write endlessly about*".

1.1 Weierstrass normal form

Definition 1.1. An *elliptic curve* E over a field K is a nonsingular (it has no cusps or self-intersections) cubic curve in two variables (a smooth curve of genus one), which contains a specified point O, often taken to be a point at "infinity" relative to the chosen coordinate system. □

A general cubic curve over a field K is given as the set of $(x, y) \in K^2$ which satisfies an equation

$$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0, \tag{1.1}$$

where $a, b, c, \ldots$ are in K. Throughout this text, unless otherwise stated, an elliptic curve will be denoted by E, where K will be a field (which usually is either the complex numbers $\mathbb{C}$, the real numbers $\mathbb{R}$, the rational numbers $\mathbb{Q}$, or the finite fields with p^n elements $\mathbb{F}_{p^n}$). It can be shown that the equation (1.1) can be reduced, by appropriate transformations, to an equation of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{1.2}$$

where $a_1, a_2, \dots a_6$ are constants. This is called the *generalized Weierstrass equation*. When $\text{char}(K) = 2$ or 3, this is the most general form an equation for an elliptic curve takes. However, we will usually be working in fields with characteristic different from 2 and 3, and in these cases it is possible to reduce (1.2) into a more simple form.

If the field characteristic is not 2, we can add $(\frac{a_1x}{2} + \frac{a_3}{2})^2$ on both sides of (1.2) to complete the square:

$$y^2 + a_1xy + a_3y + \left(\frac{a_1x}{2} + \frac{a_3}{2}\right)^2 = x^3 + a_2x^2 + a_4x + a_6 + \left(\frac{a_1x}{2} + \frac{a_3}{2}\right)^2. \tag{1.3}$$

Then we get that

$$y^2 + a_1xy + a_3y + \frac{a_1^2x^2}{4} + \frac{a_1a_3x}{2} + \frac{a_3^2}{4} = x^3 + a_2x^2 + a_4x + a_6 + \frac{a_1^2x^2}{4} + \frac{a_1a_3x}{2} + \frac{a_3^2}{4}, \tag{1.4}$$

and so we obtain

$$\left(y + \frac{a_1x}{2} + \frac{a_3}{2}\right)^2 = x^3 + \left(a_2 + \frac{a_1^2}{4}\right)x^2 + \left(a_4 + \frac{a_1a_3}{2}\right)x + \left(\frac{a_3^2}{4} + a_6\right). \tag{1.5}$$

Thus we have

$$y_1^2 = x^3 + a_2'x^2 + a_4'x + a_6', \tag{1.6}$$

where $y_1 = y + \frac{a_1x}{2} + \frac{a_3}{2}$. We will discuss elliptic curves in characteristic 2 in chapter 3.2. Now if the field characteristic is also different from 3, we can simplify further by letting $x = x_1 - \frac{a_2'}{3}$. Then we get

$$y_1^2 = x_1^3 - a_2'x_1^2 + \frac{1}{3}(a_2')^2x_1 - \frac{(a_2')^3}{27} + a_2'x_1^2 - \frac{2}{3}(a_2')^2x_1 + \frac{(a_2')^3}{9} + a_4'x_1 - \frac{a_2'a_4'}{3} + a_6'. \tag{1.7}$$

We restructure the equation to obtain

$$y_1^2 = x_1^3 + \left(a_4' - \frac{1}{3}(a_2')^2\right)x_1 + \left(\frac{2(a_2')^3}{27} - \frac{a_2'a_4'}{3} + a_6'\right), \tag{1.8}$$

so that we have (1.6) of the form

$$y_1^2 = x_1^3 + Ax_1 + B. \tag{1.9}$$

This equation for an elliptic curve when the field characteristic is different from 2 and 3 is called the *Weierstrass normal form*, or just the *Weierstrass equation* for an elliptic curve. From now on, unless otherwise mentioned, when we speak of elliptic curves we mean elliptic curves

given by an equation in Weierstrass normal form..

The coordinates of the elliptic curve can be in a field L which is larger than K. We define $E(L) = \{\infty\} \cup \{(x, y) \in L \times L \mid y^2 = x^3 + Ax + B\}$, where $K \subseteq L$. For technical reasons, which will be described in greater detail later, we add this point at "infinity". This point is regarded as a formal symbol which follows certain computational rules. Visually, if the elliptic curve is over $\mathbb{R}$, it is easiest to regard this point as sitting on top and at the bottom of the y-axis in the xy-plane (as if the y-axis was wrapped around to bite itself in the tail). A line is said to pass through ∞ when the line is vertical, i.e. $x =$ constant. Two vertical lines meet at ∞, so by symmetry, if they meet at the top they should also meet at the bottom. But two distinct lines can only intersect in one point, and so the point at infinity on top of the y-axis and the point at infinity on bottom of the y-axis is the same point.

Elliptic curves over the real numbers have two basic forms, one with one real root of $x_1^3 + Ax_1 + B$, and one with three distinct real roots. It is important to note that we don't allow multiple roots. If the roots of the cubic $x^3 + Ax + B = 0$ are $\alpha_1, \alpha_2, \alpha_3$, then the elliptic dicriminant is given by

$$\Delta = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3) = -16(4A^3 + 27B^2). \tag{1.10}$$

Thus, for the roots to be distinct, we must assume that $(4A^3 + 27B^2) \neq 0$.

Later we will look at other types of equations that can be transformed to Weierstrass normal form. Before we move on, it is worth mentioning why these curves are called *elliptic* curves, when the curves are obviously not ellipses. In the computation of the arc-length of ellipses there arise some so-called elliptic integrals, which is given by

$$\int_{x_1}^{x_2} \frac{\mathrm{d}x}{\sqrt{x^3 + ax + b}}. \tag{1.11}$$

We notice the form $x^3 + ax + b$, which clearly resembles the Weierstrass normal form of elliptic curves.

In general it is not possible to draw meaningful graphs of elliptic curves (since the fields can be arbitrary), but for elliptic curves over the real numbers we can visualize by the familiar graphs. See Figure 1.1 for examples.

1.2 GROUP STRUCTURE

It turns out that the points on an elliptic curve form an abelian group, with a peculiar binary operation. Let P and Q be two points on the curve. Let L be the "straight" line through P and

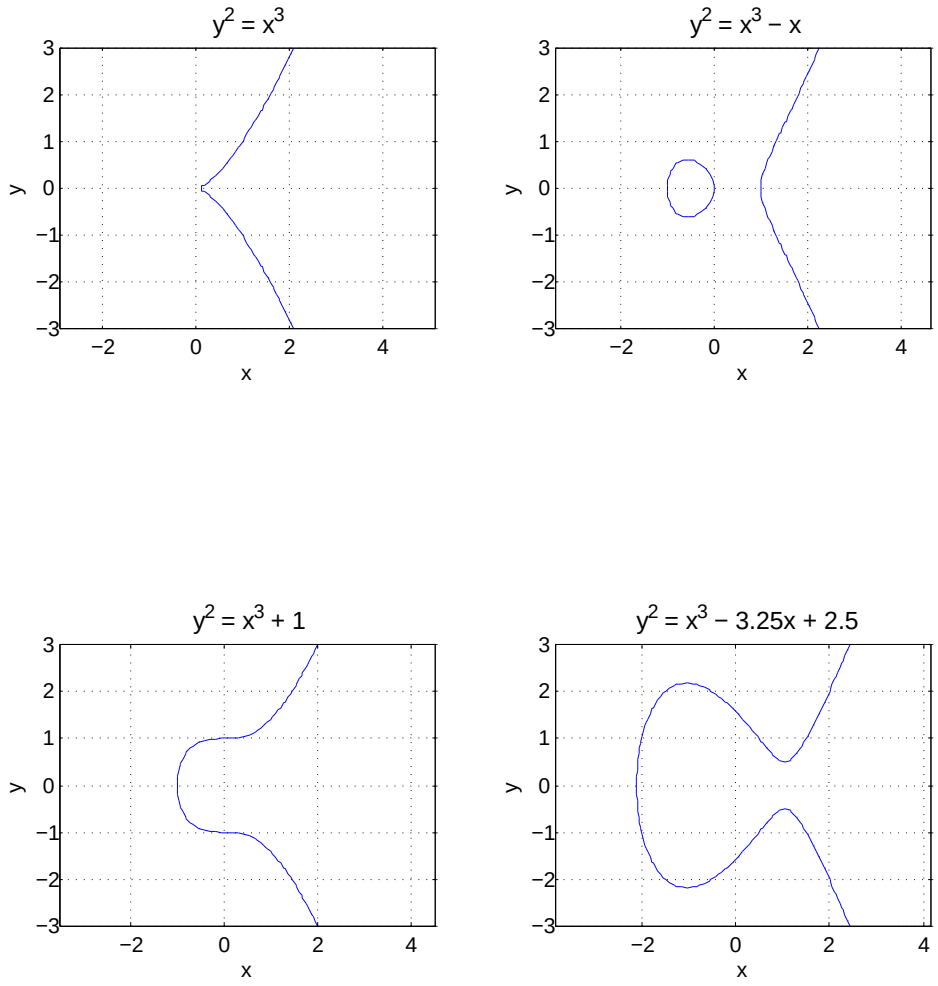

Figure 1.1: The figure shows four examples of cubic curves with equations in Weierstrass normal form. The first one is *not* an elliptic curve, as the discriminant of the curve is 0 and has a singular point at $(0, 0)$. The other three curves are elliptic curves over $\mathbb{R}$.

Q. We define $P * Q$ on an elliptic curve E to be the third point where the line L through P and Q intersects with E. We choose a fixed point ∞, which we call the origin (which is the point at infinity, a notion which we will make more precise in the next section). Let G be the set of points on E. Then we define the binary operation $+$ on G by $P + Q = (P * Q) * \infty$. This means that we reflect the intersection point between L and E in the x-axis to obtain the third point R. See Figure 1.2.

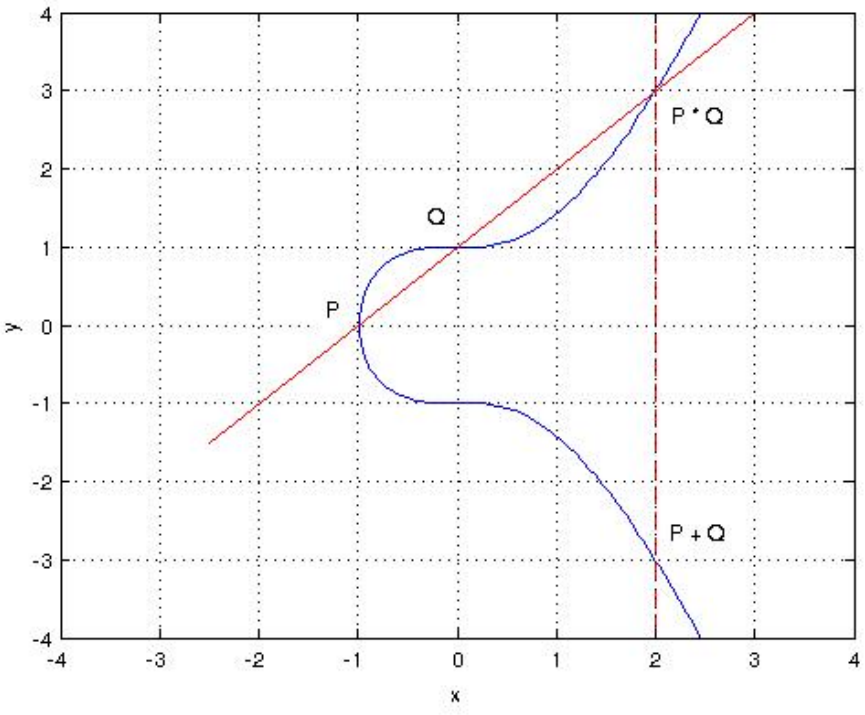

Figure 1.2: The figure shows the binary operation of the abelian group. The red line going through $P = (-1, 0)$ and $Q = (0, 1)$ intersects the curve in $P * Q = (2, 3)$. Reflection across the x-axis (the red dashed line) gives $P + Q = (2, -3)$.

Theorem 1.1. *The set G then forms an abelian group under this binary operation, where the identity element is ∞.*

Proof. The identity element is ∞, which holds by the definition of addition. For each point P there is an inverse point P' which is the reflection of P in the x-axis. The line through P and Q is obviously the same as the line through Q and P and so commutativity follows trivially. Associativity can be checked by calculation with the formulas, but since there are many different cases which needs to be considered, the proof becomes messy. For a geometric visualization of the proof, see I. Stewart and D. Tall, *Algebraic Number Theory and Fermat's Last Theorem* [6], pp. 228 – 229. For a full overview, see L. C. Washington, *Elliptic Curves - Number Theory and Cryptography* [1], pp. 20-32. □

We will derive the formulas for calculating the new point $P + Q = R = (x_3, y_3)$, given $P = (x_1, y_1)$ and $Q = (x_2, y_2)$. First we assume that $P \neq Q$ and that neither of the points are

∞. The slope of the line L through P and Q is given by $m = \dfrac{y_2 - y_1}{x_2 - x_1}$.

Assume now first that $x_1 \neq x_2$ (so that L is not vertical). Then L is given by the equation

$$y = m(x - x_1) + y_1. \tag{1.12}$$

We want to find the point where L intersects our elliptic curve E, i.e.

$$y^2 = (m(x - x_1) + y_1)^2 = x^3 + Ax + B. \tag{1.13}$$

Observe that for any numbers a, b, c, we have that

$$(x - a)(x - b)(x - c) = x^3 - (a + b + c)x^2 + (ab + ac + bc)x - abc. \tag{1.14}$$

So when the coefficient of x^3 is 1, the negative of the coefficient of x^2 is the sum of the roots. Now eq. (1.12) can be rearranged to the form

$$x^3 - m^2x^2 + \ldots = 0. \tag{1.15}$$

The three points of intersection of L with E correspond to the three roots of this cubic. We already know the two points $P = (x_1, y_1)$ and $Q = (x_2, y_2)$, so we can get the third one by seeing that for eq. (1.13) the negative of the coefficient of x^2 is m^2. This must thus be equal to the sum of the roots, so we obtain that our new point $R = (x_3, y_3)$ is given by

$$x_3 = m^2 - x_1 - x_2, \tag{1.16}$$

and, after we reflect in the x-axis;

$$y_3 = m(x_1 - x_3) - y_1. \tag{1.17}$$

Secondly, if $x_1 = x_2$ but $y_1 \neq y_2$, the line through P and Q will be vertical, and thus intersects E at ∞. Now reflecting across the x-axis gives the same point ∞. Therefore it follows that in this case $P + Q = \infty$.

Next, we consider the case where $P = Q = (x_1, y_1)$. When the two points are the same, the line L through them will be the "tangent line". When the two points coincide, we write $P + P = 2P$, and call it a *doubling* of the point P.

We use implicit differentiation of $y^2 = x^3 + Ax + B$ to get

$$2\,y\,\frac{dy}{dx} = 3x^2 + A, \tag{1.18}$$

so that

$$m = \frac{dy}{dx} = \frac{3x_1^2 + A}{2y_1}. \tag{1.19}$$

Now if $y_1 = 0$, then L is vertical, and so $P + Q = \infty$ as before, so we assume that $y_1 \neq 0$. The equation for the line L is still the same as earlier, namely

$$y = m(x - x_1) + y_1, \tag{1.20}$$

and the cubic equation is given by

$$x^3 - m^2x^2 + \ldots = 0. \tag{1.21}$$

Earlier we knew the two roots x_1 and x_2, but this time we only know one root, x_1. Since the line L is tangent to the elliptic curve E at the point P, we have that x_1 is a double root of the equation. Proceeding as before, we then obtain that

$$x_3 = m^2 - 2x_1 \tag{1.22}$$

and

$$y_3 = m(x_1 - x_3). \tag{1.23}$$

Finally we consider the case where $Q = \infty$. Now the line through P and ∞ will be a vertical line that intersects E in the point P', the reflection of the point P in the x-axis. When P' is reflected in the x-axis, we get back to P. Therefore we have

$$P + \infty = P \tag{1.24}$$

for all points P on E, which agrees with the fact that ∞ is the identity element in our abelian group. This obviously extends to include $\infty + \infty = \infty$.

We can now summarize the discussion above:

Theorem 1.2. *Let E be an elliptic curve defined by $y^2 = x^3 + Ax + B$ over $\mathbb{R}$.*
Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be points on E with $P, Q \neq \infty$. We then define $P + Q = R = (x_3, y_3)$ as follows:

Case 1. *If $x_1 \neq x_2$, then*

$$x_3 = m^2 - x_1 - x_2, \qquad y_3 = m(x_1 - x_3) - y_1, \qquad \text{where } m = \frac{y_2 - y_1}{x_2 - x_1}.$$

Case 2. *If $x_1 = x_2$, but $y_1 \neq y_2$, then $P + Q = \infty$.*

Case 3. *If $P = Q$ and $y_1 \neq 0$, then*

$$x_3 = m^2 - 2x_1, \qquad y_3 = m(x_1 - x_3) - y_1, \qquad \text{where } m = \frac{3x_1^2 + A}{2y_1}.$$

Case 4. *If $P = Q$ and $y_1 = 0$, then $P + Q = \infty$.*

Furthermore, we define $P + \infty = P$ for all points P on E.

Example 1.1. We consider the elliptic curve $y^2 = x^3 + 1$ over $\mathbb{R}$, as shown in Figure 1.1. Given the two points $P = (x_1, y_1) = (0, 1)$ and $Q = (x_2, y_2) = (2, 3)$, we want to find the third point $R = (x_3, y_3)$. Here $x_1 \neq x_2$, so we have the situation in Case 1. We first calculate to find

$$m = \frac{y_2 - y_1}{x_2 - x_1} = \frac{3 - 1}{2 - 0} = 1. \tag{1.25}$$

Then we get that

$$x_3 = m^2 - x_1 - x_2 = 1 - 0 - 2 = -1, \tag{1.26}$$

and

$$y_3 = m(x_1 - x_3) - y_1 = 1\,(0 + 1) - 1 = 0, \tag{1.27}$$

□

so our point is $R = (x_3, y_3) = (-1, 0)$.

Example 1.2. Let E be given by $y^2 = x^3 - 2$, where E is defined over $\mathbb{Q}$. We are given the point $P = (3, 5)$ and want to find a point (not ∞) with rational coordinates. In this case we double to find the new point $2P = R = (x_3, y_3)$. This corresponds to Case 3 in Theorem 1.1. We start by calculating m:

$$m = \frac{3x_1^2 + A}{2y_1} = \frac{3 \cdot 3^2 + 0}{2 \cdot 5} = \frac{27}{10}. \tag{1.28}$$

Then we obtain

$$x_3 = m^2 - 2x_1 = \left(\frac{27}{10}\right)^2 - 2 \cdot 3 = \frac{729}{100} - \frac{600}{100} = \frac{129}{100}. \tag{1.29}$$

Furthermore, we have

$$y_3 = m(x_1 - x_3) - y_1 = \frac{27}{10} \cdot \left(\frac{300}{100} - \frac{129}{100}\right) - 5 = \frac{27 \cdot 171}{1000} - \frac{5000}{1000} = -\frac{383}{1000}. \tag{1.30}$$

□

Doubling the point P thus give $2P = R = (x_3, y_3) = \left(\frac{129}{100}, -\frac{383}{1000}\right)$. This point can easily be checked to satisfy the equation $y^2 = x^3 - 2$.

This doubling procedure can be generalized further, as for any abelian group; if P is a point on E and k is a positive integer, we let kP denote $P + P + \ldots + P$ (with k summands). If $k < 0$, then we let $kP = (-P) + (-P) + \cdots + (-P)$ (with $|k|$ summands). Sometimes we will need to compute kP for a large integer k, say 37. Instead of adding P to itself 37 times, we can use a method called *successive doubling*: to compute $37P$, we first compute $2P = P + P$, $4P = 2P + 2P$, $8P = 4P + 4P$, $16P = 8P + 8P$, $32P = 16P + 16P$, so that $37P = 32P + 4P + P$.

In this way the computations are much more effective.

Turning it around, given two points P and kP, it will in general be very difficult to determine the value of k (specially when working over a large field). This is called the *discrete logarithm problem* for elliptic curves.

Finding kP goes relatively fast when k is known, but finding k when P and kP is known is a very slow computational procedure. Today there does not exist any efficient algorithm to compute the discrete logarithm, which makes it well suited for cryptographical applications.

1.3 Projective space

In the familiar Euclidean plane, two lines typically intersect at a single point. Exceptions are when the two lines are parallel to each other. A *projective* plane can be thought of as an extension of the Euclidean plane, in which two parallel lines intersect at a "point at infinity". See Figure 1.3 for an illustration. Then there exists a unique intersection point for any two given lines and there exist a unique line which can be drawn through any two given points. A projective plane is a somewhat more general notion than that of the Euclidean plane, and has some properties which allows certain statements (most notably Bézout's and Mordell's) to be true, which are not true in the Euclidean plane.

Bézout's theorem says that if X and Y are two plane projective curves over a field K that do not have a common component, where m is the degree of X and n is the degree of Y, then the number of intersection points (counting multiplicities) of X and Y with coordinates in an algebraically closed field L containing K, is equal to mn. The theorem can also be generalized to higher dimensions, where one consider a number of projective hypersurfaces in projective space. The Frenchman Étienne Bézout was the first to give a heuristic proof in 1779, after Isaac Newton had first stated the theorem in his *Principia* in 1687.

Mordell's theorem says that for elliptic curves over the field of rational numbers, the group of rational points is always finitely generated. The theorem was proved by the British mathematician Louis Mordell in 1922.

Definition 1.2. The *real projective plane* $\mathbb{RP}^2$ is the set of lines (one-dimensional subspaces) through the origin in $\mathbb{R}^3$. □

Definition 1.3. Each line through the origin in $\mathbb{R}^3$ is called a *projective point* in $\mathbb{RP}^2$. □

Definition 1.4. Each plane (two-dimensional subspace) through the origin in $\mathbb{R}^3$ is called a *projective line* in $\mathbb{RP}^2$. □

There are similar definitions for the *complex* projective plane, which we denote by $\mathbb{CP}^2$. When we work in projective space we somehow "go down" a dimension compared to the familiar Euclidean space. Planes in Euclidean space are lines in the projective space, and lines in Euclidean space are points in the projective space. As a point in $\mathbb{RP}^2$ is a line through the origin in $\mathbb{R}^3$, any nonzero point (x, y, z) on that line defines the line uniquely. The points (ax, ay, az) and (x, y, z), where a is nonzero, thus represents the same projective point. We can imagine a reference plane in $\mathbb{R}^3$ at $(x, y, 1)$, so that when z is nonzero, the projective point (x, y, z) is the same as $(x/z, y/z, 1)$. When $z = 0$, the projective point (x, y, z) lies in the xy-plane, and we say that we have a point at infinity. Such a system of coordinates on $\mathbb{RP}^2$ are called *homogeneous* and they play a crucial role in this topic, as in the aforementioned theorems by Bézout and Mordell.

A polynomial in (x, y, z) is homogeneous of degree n if it is the sum of terms $ax^r y^s z^t$, with $a \in K$ and $r + s + t = n$. We note that if F is a homogeneous polynomial of degree n, then $F(\lambda x, \lambda y, \lambda z) = F(\lambda(x, y, z)) = \lambda^n F(x, y, z)$, $\forall\, \lambda \in K$.

We want to formalize our discussion so far. Let K be a field. Then we say that two triples $(x_1, y_1, z_1) \neq 0$ and $(x_2, y_2, z_2) \neq 0$ are *equivalent* if there exists $\lambda \in K^*$ such that $(x_1, y_1, z_1) = (\lambda x_2, \lambda y_2, \lambda z_2)$. This is an equivalence relation of triples which only depends on the ratios x to y to z. We therefore denote the equivalence class of (x, y, z) by $(x : y : z)$.

We here give a small example of how to transform a polynomial equation in the ordinary *affine* plane into homogeneous coordinates. Let us say we have an equation given by $y^2 - x^3 + 3x = 0$. Replacing x by X/Z and y by Y/Z we get

$$(Y/Z)^2 - (X/Z)^3 + 3(X/Z) = 0, \tag{1.31}$$

$$Y^2 Z^{-2} - X^3 Z^{-3} + 3XZ^{-1} = 0, \tag{1.32}$$

$$Y^2 Z - X^3 + 3XZ^2 = 0. \tag{1.33}$$

The polynomial has the same degree in all nonzero terms and is thus homogeneous. The set (X, Y, Z) satisfying eq. (1.33) is a projective curve, which contains the point at infinity given by $Z = 0$, which then forces $X = 0$. By rescaling we see that $(0 : Y : 0) = (0 : 1 : 0)$ is the only point at infinity.

It is worth mentioning that any projective line in $\mathbb{RP}^2$ can be mapped to any other line by a projection. This is due to the fact that any two planes through the origin in $\mathbb{R}^3$ can be transformed to each other by an invertible linear map.

For an overview of the axioms used for affine and projective planes, see e.g. S. Balagopalan, *Elliptic Curves Over Finite Fields* [5], pp. $3 - 5$.

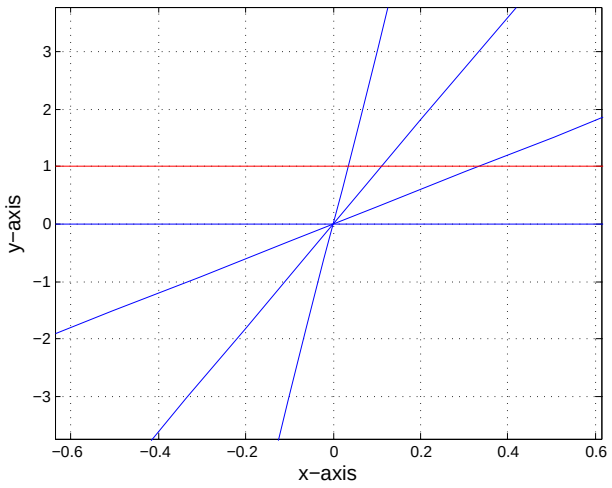

Figure 1.3: This figure illustrates the concept of a "point at infinity" on the projective line $\mathbb{RP}^1$. We here show some of the lines going through the origin. We see that each (except for one) line through the origin intersects the line at $y = 1$ in exactly one point, such that each line through the origin corresponds to a point on that line. However, there is one line which does not intersect the line at $y = 1$, and that is the line at $y = 0$. That line is then said to correspond to a point at infinity. Thus a point with coordinates $(x, 0)$ will be a point at infinity. We usually rescale such that $(x : 0) = (1 : 0)$. This notion can be generalized to any number of dimensions. In projective space, there is nothing "special" about a point at infinity, but it is treated in the same manner as all other points.

Chapter 2

Other equations and coordinate systems

There are also other types of equations for elliptic curves, which can have both advantages and disadvantages compared to the Weierstrass form. We will discuss some of these in this chapter.

2.1 Legendre equation

The Legendre equation is a variant of the Weierstrass equation which has as an advantage that it can express elliptic curves with only one parameter. It is necessary that the elliptic curve is over an algebraically closed field of characteristic not 2 (as is the case for the complex numbers). A Legendre equation can be transformed to a Weierstrass equation by an appropriate change of variables that uses rational functions.

Proposition 2.1. *Let K be a field, where $\mathrm{char}(K) \neq 2$ and let*

$$y^2 = x^3 + ax^2 + bx + c = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3) \tag{2.1}$$

be an elliptic curve over K with $\alpha_1, \alpha_2, \alpha_3 \in K$. Further, let
$x_1 = (\alpha_2 - \alpha_1)^{-1}(x - \alpha_1)$, $y_1 = y(\alpha_2 - \alpha_1)^{-3/2}$, $\lambda = (\alpha_2 - \alpha_1)^{-1}(\alpha_3 - \alpha_1)$.

Then $\lambda \neq 0, 1$ and

$$y_1^2 = x_1(x_1 - 1)(x_1 - \lambda). \tag{2.2}$$

Proof. Since the roots are distinct, λ is clearly different from 0 and 1. Furthermore, we have that

$$\begin{aligned} y_1^2 &= \frac{y^2}{(\alpha_2-\alpha_1)^3} \\ &= \frac{(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)}{(\alpha_2-\alpha_1)^3} \\ &= \frac{(x-\alpha_1)}{(\alpha_2-\alpha_1)}\frac{(x-\alpha_2)}{(\alpha_2-\alpha_1)}\frac{(x-\alpha_3)}{(\alpha_2-\alpha_1)} \\ &= \frac{(x-\alpha_1)}{(\alpha_2-\alpha_1)}\left(\frac{(x-\alpha_1)-(\alpha_2-\alpha_1)}{\alpha_2-\alpha_1}\right)\left(\frac{(x-\alpha_1)-(\alpha_3-\alpha_1)}{\alpha_2-\alpha_1}\right) \\ &= x_1(x_1-1)(x_1-\lambda). \end{aligned}$$

□

The six permutations of the roots $\alpha_1, \alpha_2, \alpha_3$ corresponds to the set $\left\{\lambda, \frac{1}{\lambda}, 1-\lambda, \frac{1}{1-\lambda}, \frac{\lambda}{\lambda-1}, \frac{\lambda-1}{\lambda}\right\}$, where each member yields a Legendre equation for E. Thus the parameter λ is not unique. It usually gives a 6 to 1 relation, but for some specific values of λ, this set has fewer than 6 elements. For instance, if $\lambda = 2$, we obtain the set $\{-1, 1/2, 2\}$.

2.2 QUARTIC EQUATIONS AND INTERSECTIONS

In this section we want to see how equations of degree four can be transformed into Weierstrass normal form, to give an equation for an elliptic curve.

Suppose we have a curve defined by the equation

$$v^2 = au^4 + bu^3 + cu^2 + du + e, \tag{2.3}$$

where $a, b, c, d, e \in K$. If we have a point (u_1, v_1) lying on the curve, the equation can be transformed into a Weierstrass equation by an invertible change of variables that uses rational functions with coefficients in the field K. By changing u to $u + u_1$, we may assume that $u_1 = 0$, so the point has the form $(0, v_1)$. We now have two cases:

Case 1. $v_1 = 0$.
If $d = 0$, then the curve has a singularity at $(u, v) = (0, 0)$. We therefore assume that $d \neq 0$. Then, dividing by u^4, we obtain

$$\left(\frac{v}{u^2}\right)^2 = d\left(\frac{1}{u}\right)^3 + c\left(\frac{1}{u}\right)^2 + b\left(\frac{1}{u}\right) + a.$$

This can now be easily transformed into Weierstrass equation (see section 1.1) in d/u and dv/u^2.

Case 2. $v_1 \neq 0$.

This case is more complicated. We will use the following result.

Theorem 2.1. *Let K be a field, where $char(K) \neq 2$. Consider the equation*

$$v^2 = au^4 + bu^3 + cu^2 + du + q^2, \tag{2.4}$$

where $a, b, c, d, q \in K$. Then we have the transformation

$$x = \frac{2q(v+q) + du}{u^2}, \qquad y = \frac{4q^2(v+q) + 2q(du + cu^2) - (d^2u^2/2q)}{u^3},$$

so that (x, y) satisfies

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{2.5}$$

Furthermore, we define

$$a_1 = d/q, \quad a_2 = c - (d^2/4q^2), \quad a_3 = 2qb, \quad a_4 = -4q^2a, \quad a_6 = a_2a_4.$$

Then we have the inverse transformation

$$u = \frac{2q(x+c) - (d^2/2q)}{y}, \qquad v = -q + \frac{u(ux - d)}{2q}, \tag{2.6}$$

where (u, v) satisfies eq. (2.5). The point $(u, v) = (0, q)$ corresponds to the point $(x, y) = \infty$ and $(u, v) = (0, -q)$ corresponds to $(x, y) = (-a_2, a_1a_2 - a_3)$.

Proof. The proof is a long and tedious, straightforward calculation which we omit here. □

Example 2.1. We consider the equation

$$v^2 = u^4 + 2u + 1. \tag{2.7}$$

Then $a = 1, b = c = 0, d = 2,$ and $q = 1$ by eq. (2.4). This gives that

$$x = \frac{2(v+1) + 2u}{u^2} \qquad y = \frac{4(v+1) + 4u - 2u^2}{u^3}.$$

We have that $a_1 = 2, a_2 = -1, a_3 = 0, a_4 = -4, a_6 = 4$. So the elliptic curve with eq. (2.5) is given by

$$y^2 + 2xy = x^3 - x^2 - 4x + 4.$$

This can now be easily transformed into Weierstrass equation as we did in section 1.1.

The inverse transformation is given by

$$u = \frac{2 \cdot 1(x+0) - (\frac{2^2}{2 \cdot 1})}{y} = \frac{2(x-1)}{y}$$

and

$$\begin{aligned} v &= -1 + \frac{\frac{2(x-1)}{y}\left(\frac{2(x-1)}{y}x - 2\right)}{2 \cdot 1} \\ &= -1 + \frac{\frac{4(x-1)^2 x}{y^2} - \frac{4(x-1)}{y}}{2} \\ &= -1 + \frac{2(x^2 - 2x + 1)x - 2y(x-1)}{y^2} \\ &= -1 + \frac{2(x^3 - 2x^2 + (1-y)x + y)}{y^2}. \end{aligned}$$

□

Given two quadric surfaces in projective three-dimensional space, the intersection of those surfaces, along with a rational point of intersection, is usually an elliptic curve. We consider two equations which each can be regarded as a surface in the uvw-space, given by

$$au^2 + bv^2 = e \quad \text{and} \quad cu^2 + dw^2 = f,$$

where a, b, c, d, e, f are nonzero elements of a field K of characteristic different from 2. We first have a look at the equation $au^2 + bv^2 = e$, which can be regarded as a curve C in the uv-plane. Further, let $P = (u_0, v_0)$ be a point on C. Now, let L be the line through P with slope m:

$$u = u_0 + t, \qquad v = v_0 + mt.$$

Now, we want to find the other point where the line L intersects the curve C. We get that

$$\begin{aligned} a(u_0 + t)^2 + b(v_0 + mt)^2 &= e, \\ a(u_0^2 + 2u_0 t + t^2) + b(v_0^2 + 2v_0 mt + m^2 t^2) &= e. \end{aligned}$$

Since $au_0^2 + bv_0^2 = e$, we get

$$a(2u_0 t + t^2) + b(2v_0 mt + m^2 t^2) = 0.$$

Now, $t = 0$ corresponds to (u_0, v_0), so we factor out t to obtain

$$\begin{aligned} t(2au_0 + at) + t(2bv_0m + bm^2t) &= 0, \\ 2au_0 + at + 2bv_0m + bm^2t &= 0, \\ \implies t &= -\frac{2au_0 + 2bv_0m}{a + bm^2}. \end{aligned}$$

Thus,

$$u = u_0 - \frac{2au_0 + 2bv_0m}{a + bm^2}, \quad v = v_0 - \frac{2amu_0 + 2bv_0m^2}{a + bm^2}.$$

We observe that if (u, v) is any point on the curve C with coordinates in the field K, then the slope m of the line through (u, v) and P is also in K (or is infinite). When $m = \infty$, it yields the point $(u_0, -v_0)$. We see that we have obtained a parametrization of the points on C, as we have a bijection between values of m (including ∞) and points on C (including points at infinity).

When m is the slope of the tangent line at (u_0, v_0), then the second point of intersection of the tangent line with the curve will obviously be the point (u_0, v_0) again. When $m = 0$, it yields the point $(-u_0, v_0)$, which can be seen from the formulas, or from the fact that the line through $(-u_0, v_0)$ and (u_0, v_0) clearly has slope 0.

Next, we want to find the intersection between C with the surface $cu^2 + dw^2 = f$ in uvw-space. We get that

$$\begin{aligned} dw^2 &= f - cu^2 \\ dw^2 &= f - c\Big(u_0 - \frac{2au_0 + 2bv_0m}{a + bm^2}\Big)^2 \\ \implies d(w(a + bm^2))^2 &= (a + bm^2)^2 f - c(bu_0m^2 - 2bv_0m - au_0)^2 \\ &= (b^2 f - cb^2u_0^2)m^4 + \dots. \end{aligned}$$

This can now be changed to Weierstrass normal form by the previously given procedure. Note that the leading coefficient $b^2 f - cb^2u_0^2$ is equal to $b^2dw_0^2$. We see that if $w_0 = 0$, the fourth degree polynomial becomes a cubic polynomial, so we can easily transform it into Weierstrass normal form as we did in Chapter 1.1.

Thus the intersection of two quadratic surfaces in three-dimensional space gives rise to elliptic curves.

2.3 PROJECTIVE AND JACOBIAN COORDINATES

Sometimes it is advantageous to avoid inversion in the formulas for point addition, as inversion takes the computer between 9 and 40 times as long to calculate than multiplication [1]. Obviously we want to calculate our points as quickly and efficiently as possible. This applies to most situations in cryptography. There does exist some alternative formulas to avoid inversion, which we will look at in this section.

We can represent all the points as points $(x : y : z)$ in projective space. We let $P_1 = (x_1 : y_1 : z_1)$ and $P_2 = (x_2 : y_2 : z_2)$ be points on $y^2z = x^3 + Axz^2 + Bz^3$, and want to find

$$(x_1 : y_1 : z_1) + (x_2 : y_2 : z_2) = (x_3 : y_3 : z_3).$$

How do we compute x_3, y_3 and z_3? When $P_1 \neq \pm P_2$ we have that

$$u = y_2z_1 - y_1z_2, \quad v = x_2z_1 - x_1z_2, \quad w = u^2z_1z_2 - v^3 - 2v^2x_1z_2 \tag{2.8}$$

and

$$x_3 = vw, \quad y_3 = u(v^2x_1z_2 - w) - v^3y_1z_2, \quad z_3 = v^3z_1z_2. \tag{2.9}$$

When $P_1 = P_2$,

$$t = Az_1^2 + 3x_1^2, \quad u = y_1z_1, \quad v = ux_1y_1, \quad w = t^2 - 8v, \tag{2.10}$$

where we have that

$$x_3 = 2uw, \quad y_3 = t(4v - w) - 8y_1^2u^2, \quad z_3 = 8u^3. \tag{2.11}$$

We could also have that $P_1 = -P_2$, in which case $P_1 + P_2 = \infty$.
In this way we will not need any inversions for point addition and point doubling, and as a consequence the computations go faster. Now the point addition takes 12 multiplications and 2 squarings, while the point doubling takes 7 multiplications and 5 squarings.

We can get a faster doubling procedure by using a modification of projective coordinates called *Jacobian* coordinates. Let $(x : y : z)$ represent the affine point $(\frac{x}{z^2}, \frac{y}{z^3})$. Then the elliptic curve $y^2 = x^3 + Ax + B$ becomes

$$\begin{aligned}\left(\frac{y}{z^3}\right)^2 &= \left(\frac{x}{z^2}\right)^3 + A\left(\frac{x}{z^2}\right) + B \\ \frac{y^2}{z^6} &= \frac{x^3}{z^6} + A\frac{x}{z^2} + B \\ y^2 &= x^3 + Axz^4 + Bz^6.\end{aligned}$$

Now, the point at infinity has coordinates $(1 : 1 : 0)$. We let $P_1 = (x_1 : y_1 : z_1)$ and

[1] See L. C. Washington, *Elliptic Curves - Number Theory and Cryptography* [1], p. 42.

$P_2 = (x_2 : y_2 : z_2)$ be points on the elliptic curve $y^2 = x^3 + Axz^4 + Bz^6$. Then

$$(x_1 : y_1 : z_1) + (x_2 : y_2 : z_2) = (x_3 : y_3 : z_3),$$

where x_3, y_3, z_3 are computed in the following way:

When $P_1 \neq P_2$, define

$$r = x_1 z_2^2, \quad s = x_2 z_1^2, \quad t = y_1 z_2^3, \quad u = y_2 z_1^3, \quad v = s - r, \quad w = u - t. \tag{2.12}$$

Then

$$x_3 = -v^3 - 2rv^2 + w^2, \quad y_3 = -tv^3 + (rv^2 - x_3)w, \quad z_3 = vz_1z_2. \tag{2.13}$$

When $P_1 = P_2$, define

$$v = 4x_1y_1^2, \quad w = 3x_1^2 + Az_1^4. \tag{2.14}$$

Then

$$x_3 = -2v + w^2, \quad y_3 = -8y_1^4 + (v - x_3)w, \quad z_3 = 2y_1z_1. \tag{2.15}$$

When $P_1 = -P_2$, we have that $P_1 + P_2 = \infty$. By using Jacobian coordinates, addition of points takes 12 multiplications and 4 squarings, while doubling takes 3 multiplications and 6 squarings (compared to 7 multiplications and 5 squarings for ordinary projective coordinates).

Example 2.2. Let E be the elliptic curve given by

$$y^2 = x^3 + 3xz^4 + 5z^6,$$

and let $P_1 = (x_1 : y_1 : z_1) = (1 : 3 : 1)$ be a point on E. We want to double the point to find $2P_1$. Then

$$\begin{aligned} v &= 4x_1y_1^2 = 4 \cdot 1 \cdot 3^2 = 36, \\ w &= 3x_1^2 + Az_1^4 = 3 \cdot 1^2 + 3 \cdot 1^4 = 6, \end{aligned}$$

which gives

$$\begin{aligned} x_3 &= -2v + w^2 = -2 \cdot 36 + 6^2 = -36, \\ y_3 &= -8y_1^4 + (v - x_3)w = -8 \cdot 3^4 + (36 + 36) \cdot 6 = -648 + 72 \cdot 6 = -216, \\ z_3 &= 2y_1z_1 = 2 \cdot 3 \cdot 1 = 6. \end{aligned}$$

Thus $(x_3, y_3, z_3) = (-36, -216, 6)$, so that $P_3 = (x_3 : y_3 : z_3) = (6, 36, 1)$. □

It is worth noting that when $A = -3$, we have that $w = 3(x_1^2 - z_1^4)$, which can be factored into $w = 3(x_1 + z_1^2)(x_1 - z_1^2)$. This can be computed in one squaring and one multiplication, so the doubling goes even faster (4 squarings and 4 multiplications in total). For this reason, elliptic curves with $A = -3$ is used a lot in cryptographic research and applications.

Chapter 3

OTHER BASIC THEORY

3.1 THE j-INVARIANT

We let E be the elliptic curve given by $y^2 = x^3 + Ax + B$, where $A, B \in K$ and $\text{char}(K) \neq 2, 3$.

Definition 3.1. The *j-invariant* of E is defined to be

$$j = j(E) = 1728\frac{4A^3}{4A^3 + 27B^2}. \tag{3.1}$$

□

Note that since the discriminant of E is different from 0 by assumption, the denominator of eq. (3.1) will also be nonzero. We see that two special values of j can occur:

1. $j = 0$: This means that $4A^3 = 0$ and so E has the form $y^2 = x^3 + B$.

2. $j = 1728$: Now $4A^3 = 4A^3 + 27B^2$ so $27B^2 = 0$, thus E has the form $y^2 = x^3 + Ax$.

For any elliptic curve in Weierstrass normal form, we have an automorphism given by $(x, y) \mapsto (x, -y)$. When $j = 0$ or $j = 1728$, there also exist other automorhpisms:

1. $y^2 = x^3 + B$ has the automorphism $(x, y) \mapsto (\zeta x, -y)$ of order 6, where ζ is a nontrivial cube root of 1.

2. $y^2 = x^3 + Ax$ has the automorphism $(x, y) \mapsto (-x, iy)$ of order 4, where $i^2 = -1$.

The j-invariant tells us when two curves are isomorphic over an algebraically closed field.

Definition 3.2. Let E_1 and E_2 be two elliptic curves over K with the same j-invariant. Then E_1 and E_2 are said to be *twists* of each other. □

Example 3.1. We want to show that the two elliptic curves $E_1 : y^2 = x^3 + 5x + 2$ and $E_2 : y^2 = x^3 + 80x + 128$ are twists of each other.

We calculate the j- invariants:

$$j(E_1) = 1728\,\frac{4\cdot 5^3}{4\cdot 5^3 + 27\cdot 2^2}$$

$$\begin{aligned} j(E_2) &= 1728\,\frac{4\cdot 80^3}{4\cdot 80^3 + 27\cdot 128^2} \\ &= 1728\,\frac{4\cdot (4^2\cdot 5)^3}{4\cdot (4^2\cdot 5)^3 + 27\cdot (4^3\cdot 2)^2} \\ &= 1728\,\frac{4^6\cdot 4\cdot 5^3}{4^6\cdot 5^3 + 4^6\cdot 27\cdot 2^2} \\ &= 1728\,\frac{4\cdot 5^3}{4\cdot 5^3 + 27\cdot 2^2}, \end{aligned}$$

so $j(E_1) = j(E_2)$ and thus E_1 and E_2 are twists of each other. □

We see that if $E_1 : y^2 = x^3 + Ax + B$ over a field K, then a curve $E_2 : y^2 = x^3 + Ad^2x + Bd^3$, with $d \in K^\star$, is a twist of E_1.

Example 3.2. The elliptic curve $E_2 : y^2 = x^3 + Ad^2x + Bd^3$ can be transformed into $E_1 : y^2 = x^3 + Ax + B$ over $K(\sqrt{d})$.

We can see this by letting the transformation be given by $(x, y) \mapsto (\mu^2 x, \mu^3 y)$, where $\mu = \sqrt{d}$. Then

$$\begin{aligned} (\mu^3 y)^2 &= (\mu^2 x)^3 + Ad^2(\mu^2 x) + Bd^3 \\ \mu^6 y^2 &= \mu^6 x^3 + Ad^2\mu^2 x + Bd^3 \\ d^3 y^2 &= d^3 x^3 + Ad^3 x + Bd^3 \\ y^2 &= x^3 + Ax + B \end{aligned}$$

and thus E_2 is transformed into E_1. □

Example 3.3. The elliptic curve $E_2 : y^2 = x^3 + Ad^2x + Bd^3$ can be transformed into $E_3 : dy_1^2 = x_1^3 + Ax_1 + B$ over K.

To see this, let the transformation be given by $(x, y) \mapsto (x_1 d, y_1 d^2)$. Then

$$\begin{aligned} (y_1 d)^2 &= (x_1 d)^3 + Ad^2(x_1 d) + Bd^3 \\ d^4 y_1^2 &= d^3 x_1^3 + Ad^3 x_1 + Bd^3 \\ dy^2 &= x_1^3 + Ax_1 + B \end{aligned}$$

□

Recall that the generalized Weierstrass equation is given by

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{3.2}$$

where a_1, a_2, a_3, a_4, a_6 are constants in a field K. We can define the coefficients

$$\begin{aligned} b_2 &= a_1^2 + 4a_2 \\ b_4 &= a_1a_3 + 2a_4 \\ b_6 &= a_3^2 + 4a_6 \\ b_8 &= a_1^2a_6 - a_1a_3a_4 + 4a_2a_6 + a_2a_3^2 - a_4^2. \end{aligned}$$

The discriminant of a curve in generalized Weierstrass form is then given by

$$\Delta' = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6. \tag{3.3}$$

Furthermore, we have the relations

$$\begin{aligned} c_4 &= b_2^2 - 24b_4 \\ c_6 &= -b_2^3 + 36b_2b_4 - 216b_6. \end{aligned}$$

The j-invariant can then be defined[1] for an elliptic curve in generalized Weierstrass form by

$$j = j(E) = \frac{c_4^3}{\Delta'}. \tag{3.4}$$

3.2 ELLIPTIC CURVES IN CHARACTERISTIC 2

We first begin with a definition:

Definition 3.3. A curve C in $K\mathbb{P}^2$ defined by $f(x, y, z) = 0$ is called *nonsingular* at a point P if at least one of the partial derivatives f_x, f_y, f_z is nonzero at P. □

We remark that $f(x, y, z)$ has to be homogeneous for this to make sense, and that $(0, 0, 0)$ is not a valid point.

By a *nonsingular curve* we mean a curve with no singular points in the algebraic closure of K.

[1] See Michael Pemberton, *Elliptic Curves and Their Applications in Cryptography* [4], pp. 10 – 11.

When we now will discuss elliptic curves in characteristic 2, we first observe that we cannot work with the normal Weierstrass equation as it now will be an equation of a singular curve:

To see this, we first let $f(x,y,z) = y^2z - x^3 - Az^2x - Bz^3$. Then we get that $f_y = 2zy = 0y = 0$. Further, we have that $f_x = -3x^2 - Az^2$. Now let x_0 be a root (which may exist in some extension of K) of $-3x^2 - Az^2 = 0$, and let y_0 be the square root of $x_0^3 + Az^2x_0 + Bz^3$. Then (x_0, y_0) will lie on the curve and $f_x(x_0, y_0) = f_y(x_0, y_0) = 0$. Since the partial derivatives are both zero, it means that the curve is singular, and thus we can not work with the Weierstrass equation on normal form as the curve will then not be an elliptic curve. Therefore we will now work with the generalized Weierstrass equation (as in eq. (1.2) and (3.2)) for an elliptic curve E, given by

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{3.5}$$

Proposition 3.1. *If $a_1 \neq 0$, the equation (3.5) is transformed to the form $y_1^2 + x_1y_1 = x_1^3 + a_2'x_1^2 + a_6'$ with the transformations $x = a_1^2x_1 + \frac{a_3}{a_1}$ and $y = a_1^3y_1 + \frac{a_1^2a_4 + a_3^2}{a_1^3}$.*

Proof.

$$\text{We have that } x^2 = \left(a_1^2x_1 + \frac{a_3}{a_1}\right)^2 = a_1^4x_1^2 + 2a_1a_3x_1 + \frac{a_3^2}{a_1^2} = a_1^4x_1^2 + \frac{a_3^2}{a_1^2}$$

$$\text{and } x^3 = \left(a_1^2x_1 + \frac{a_3}{a_1}\right)\left(a_1^4x_1^2 + \frac{a_3^2}{a_1^2}\right) = a_1^6x_1^3 + a_3^2x_1 + a_1^3a_3x_1^2 + \frac{a_3^3}{a_1^3}.$$

$$\text{Further, we have } y^2 = \left(a_1^3y_1 + \frac{a_1^2a_4 + a_3^2}{a_1^3}\right)^2 = a_1^6y_1^2 + \frac{(a_1^2a_4 + a_3^2)^2}{a_1^6} = a_1^6y_1^2 + \frac{a_1^4a_4^2 + a_3^4}{a_1^6}.$$

Note that the cross terms vanishes as $2 = 0$ in characteristic 2. Then we get that the left hand side of eq. (3.5) will be

$$\begin{aligned}
y^2 + a_1xy + a_3y &= a_1^6y_1^2 + \frac{a_1^4a_4^2 + a_3^4}{a_1^6} + a_1\left(a_1^2x_1 + \frac{a_3}{a_1}\right)\left(a_1^3y_1 + \frac{a_1^2a_4 + a_3^2}{a_1^3}\right) + a_3\left(a_1^3y_1 + \frac{a_1^2a_4 + a_3^2}{a_1^3}\right) \\
&= a_1^6y_1^2 + \frac{a_1^4a_4^2 + a_3^4}{a_1^6} + \left(a_1^3x_1 + a_3\right)\left(a_1^3y_1 + \frac{a_1^2a_4 + a_3^2}{a_1^3}\right) + a_1^3a_3y_1 + \frac{a_1^2a_3a_4 + a_3^3}{a_1^3} \\
&= a_1^6y_1^2 + \frac{a_1^4a_4^2 + a_3^4}{a_1^6} + a_1^6x_1y_1 + a_1^2a_4x_1 + a_3^2x_1 + 2a_1^3a_3y_1 + 2\frac{a_1^2a_3a_4 + a_3^3}{a_1^3} \\
&= a_1^6y_1^2 + \frac{a_1^4a_4^2 + a_3^4}{a_1^6} + a_1^6x_1y_1 + a_1^2a_4x_1 + a_3^2x_1 \\
&= a_1^6y_1^2 + a_1^6x_1y_1 + (a_1^2a_4 + a_3^2)x_1 + \frac{a_1^4a_4^2 + a_3^4}{a_1^6}.
\end{aligned}$$

The right hand side of eq. (3.5) becomes

$$\begin{aligned} x^3 + a_2x^2 + a_4x + a_6 &= a_1^6x_1^3 + a_1^3a_2x_1^2 + a_3^2x_1 + \frac{a_3^3}{a_1^3} + a_2\Big(a_1^4x_1^2 + \frac{a_3^2}{a_1^2}\Big) + a_4\Big(a_1^2x_1 + \frac{a_3}{a_1}\Big) + a_6 \\ &= a_1^6x_1^3 + a_1^3a_2x_1^2 + a_3^2x_1 + \frac{a_3^3}{a_1^3} + a_1^4a_2x_1^2 + \frac{a_2a_3^2}{a_1^2} + a_1^2a_4x_1 + \frac{a_3a_4}{a_1} + a_6 \\ &= a_1^6x_1^3 + (a_1^3a_2 + a_1^4a_2)x_1^2 + (a_1^2a_4 + a_3^2)x_1 + \frac{a_3^3}{a_1^3} + \frac{a_2a_3^2}{a_1^2} + \frac{a_3a_4}{a_1} + a_6 \end{aligned}$$

Taking left hand side and right hand side together, we get that

$$a_1^6y_1^2 + a_1^6x_1y_1 + \frac{a_1^4a_4^2 + a_3^4}{a_1^6} = a_1^6x_1^3 + (a_1^3a_2 + a_1^4a_2)x_1^2 + \frac{a_3^3}{a_1^3} + \frac{a_2a_3^2}{a_1^2} + \frac{a_3a_4}{a_1} + a_6$$

$$\Rightarrow y_1^2 + x_1y_1 = x_1^3 + \Big(\frac{a_1^3a_2 + a_1^4a_2}{a_1^6}\Big)x_1^2 + \frac{a_1^4a_4^2 + a_3^4}{a_1^{12}} + \frac{a_3^3}{a_1^9} + \frac{a_2a_3^2}{a_1^8} + \frac{a_3a_4}{a_1^7} + \frac{a_6}{a_1^6}.$$

We thus have transformed eq. (3.5) to the form

$$y_1^2 + x_1y_1 = x_1^3 + a_2'x_1^2 + a_6'. \tag{3.6}$$

□

This curve is nonsingular when $a_6' \neq 0$. In this case the j-invariant can be calculated to be equal to $1/a_6'$.

Proposition 3.2. *If $a_1 = 0$, we can change equation (3.5) to the form $y_1^2 + a_3'y_1 = x_1^3 + a_4'x_1 + a_6'$ with the transformations $x = x_1 + a_2$ and $y = y_1$.*

Proof.

$$\begin{aligned} \text{We have that } \; x^2 &= x_1^2 + 2a_2x_1 + a_2^2 = x_1^2 + a_2^2 \\ \text{and } \; x^3 &= (x_1^2 + a_2^2)(x_1 + a_2) = x_1^3 + a_2x_1^2 + a_2^2x_1 + a_2^3. \end{aligned}$$

The left hand side of eq. (3.5) then becomes

$$\begin{aligned} y^2 + a_1xy + a_3y &= y_1^2 + a_1(x_1 + a_2)y_1 + a_3y_1 = y_1^2 + a_1x_1y_1 + a_1a_2y_1 + a_3y_1, \\ &= y_1^2 + (a_1a_2 + a_1x_1 + a_3)y_1 \end{aligned}$$

while the right hand side of eq. (3.5) will be

$$\begin{aligned} x^3 + a_2x^2 + a_4x + a_6 &= x_1^3 + a_2x_1^2 + a_2^2x_1 + a_2^3 + a_2x_1^2 + a_2^3 + a_4x_1 + a_2a_4 + a_6 \\ &= x_1^3 + (a_2^2 + a_4)x_1 + a_2^3 + a_2a_4 + a_6, \end{aligned}$$

so that we have eq. (3.5) of the form

$$y_1^2 + a_3' y_1 = x_1^3 + a_4' x_1 + a_6'. \tag{3.7}$$

□

This curve is nonsigular when $a_3' \neq 0$, and the j-invariant can be calculated to be 0. The curves given by eq. (3.6) and eq. (3.7) can thus not be twists of each other.

When we make eq. (3.5) homogeneous, we obtain the curve E given by

$$y^2 z + a_1 xyz + a_3 yz^2 = x^3 + a_2 x^2 z + a_4 xz^2 + a_6 z^3. \tag{3.8}$$

We see that when $z = 0$, the equation becomes $0 = x^3$. Thus $\infty = (0 : 1 : 0)$ is the (only) point at infinity on E. Now, let (x_0, y_0) be a point on E. Then the other point of intersection of L and E is given by $(x_0, -a_1 x_0 - a_3 - y_0)$. If L is the line through (x_0, y_0) and ∞, then L is the vertical line $x = x_0$.

We now want to describe how addition of points works. By the definition of ∞, we have that $P + \infty = P$ for all points P on E. We know that three points P, Q and R are collinear if and only if they sum to ∞. Thus, we have that

$$-P = -(x, y) = (x, -a_1 x - a_3 - y).$$

To add two points P and Q, we draw the line L through P and Q (we take the tangent line if $P = Q$), which then will intersect E in a third point R. Then we compute $R = -P$ given by the above formula. Note that this is not the same as reflecting across the x-axis, as we did when the characteristic of the field was not 2. Then $P + Q = R$. The points on E then form an abelian group. The proof of associativity of this addition law is similar as for curves over fields of characteristic not 2, and will not be given here.

Chapter 4

Weil pairing

4.1 Endomorphisms

Let E be an elliptic curve. A group homomorphism $\alpha : E(\overline{K}) \to E(\overline{K})$ that is given by rational functions, where $\overline{K}$ is the algebraic closure of K, is called an *endomorphism* of E. This means that $\alpha(P+Q) = \alpha(P) + \alpha(Q)$ and that there exist rational functions $R_1(x,y)$ and $R_2(x,y)$ with coefficients in $\overline{K}$ such that $\alpha(x,y) = (R_1(x,y), R_2(x,y)), \forall (x,y) \in E(\overline{K})$. We will assume that α is nontrivial, so that there exists some (x,y) such that $\alpha(x,y) \neq \infty$.

Example 4.1. Let E be an elliptic curve on Weierstrass normal form, i.e. given by $y^2 = x^3 + Ax + B$. Let α be the homomorphism of E given by $\alpha(P) = 2P$. Then $\alpha(x,y) = (R_1(x,y), R_2(x,y))$, where

$$R_1(x,y) = \left(\frac{3x^2+A}{2y}\right)^2 - 2x$$
$$R_2(x,y) = \left(\frac{3x^2+A}{2y}\right)\left(3x - \left(\frac{3x^2+A}{2y}\right)^2\right) - y.$$

These are found by the formulas for doubling a point in Theorem 1.2. Now, since α is a homomorphism given by rational function, it is an endomorphism of E. □

We want to use a standard form for the rational forms that describe an endomorphism. This is done by the following theorem.

Theorem 4.1. *Let E be an elliptic curve defined over a field K and given by $y^2 = x^3 + Ax + B$. Then any endomorphism α can be defined by the following, where $p(x), q(x)$ are polynomials with no common factors, and likewise for the polynomials $s(x), t(x)$:*

$$\alpha(x,y) = (r_1(x,y), r_2(x,y)y) = \left(\frac{p(x)}{q(x)}, y\frac{s(x)}{t(x)}\right).$$

Proof. Since α is an endomorphism it can be expressed with rational functions, $\alpha(x,y) = (R_1(x,y), R_2(x,y))$. Now, since $y^2 = x^3 + Ax + B$, $\forall (x,y) \in E(\overline{K})$, we can replace every even power of y by a polynomial in x, and any odd power of y by y times a polynomial in x, so that

we get

$$R(x,y) = \frac{p_1(x) + p_2(x)y}{p_3(x) + p_4(x)y}.$$

Further, we can get rid of y in the denominator by multiplying both the numerator and the denominator by $p_3(x) - p_4(x)y$ and then replacing y^2 by $x^3 + Ax + B$. This gives

$$R(x,y) = \frac{q_1(x) + q_2(x)y}{q_3(x)}. \tag{4.1}$$

Since α is an endomorphism it will preserve the structure of the curve, so

$$\alpha(x,-y) = \alpha(-(x,y)) = -\alpha(x,y).$$

It follows that

$$R_1(x,-y) = R_1(x,y) \text{ and } R_2(x,-y) = -R_2(x,y).$$

By writing R_1 in the form of eq. (4.1) we see that $q_2(x) = 0$, and similarly for R_2, we have that $q_1 = 0$. Therefore we can assume that

$$\alpha(x,y) = (r_1(x), r_2(x)y),$$

where $r_1(x), r_2(x)$ are rational functions in x only.

It must also be considered what happens when one of the rational functions is not defined at a point. We write

$$r_1(x) = \frac{p(x)}{q(x)} \text{ and } r_2(x) = y\frac{s(x)}{t(x)},$$

where the polynomials $p(x)$ and $q(x)$ do not have a common factor, and likewise for the polynomials $s(x)$ and $t(x)$. If $q(x) = 0$ at some point (x,y), we define $\alpha(x,y) = \infty$. If $q(x) \neq 0$, then $r_2(x)$ will also be defined.[1] □

Definition 4.1. The *degree* of α, when α is nontrivial, is defined to be $\deg(\alpha) = \max\{\deg p(x), \deg q(x)\}$. If α is trivial, i.e. every point is mapped to ∞, we let $\deg(\alpha) = 0$. □

Definition 4.2. A nontrivial endomorphism α is called *separable* if the derivative $r_1'(x)$ is not identically zero, which is equivalent to saying that at least one of $p'(x)$ and $q'(x)$ is not identically zero. □

[1] See Matthew England, *Elliptic Curve Cryptography* [3], pp. 17 – 19.

Example 4.2. Continuing with our previous example, we had the endomorphism given by $\alpha(P) = 2P$. There we had that

$$R_1(x,y) = \left(\frac{3x^2+A}{2y}\right)^2 - 2x,$$

so we have

$$R_1(x,y) = \frac{9x^4+6Ax^2+A^2}{4y^2} - 2x.$$

Using the fact that $y^2 = x^3 + Ax + B$, we obtain

$$\begin{aligned} r_1(x) &= \frac{9x^4+6Ax^2+A^2}{4(x^3+Ax+B)} - 2x \\ r_1(x) &= \frac{9x^4+6Ax^2+A^2-8x(x^3+Ax+B)}{4(x^3+Ax+B)} \\ r_1(x) &= \frac{x^4-2Ax^2-8Bx+A^2}{4(x^3+Ax+B)}, \end{aligned}$$

□

and so $\deg(\alpha) = \max\{\deg\, p(x), \deg\, q(x)\} = \max\{4,3\} = 4$. Furthermore, we see that $q'(x) = 4(3x^2+A)$, which is not identically zero. Thus α is a separable endomorphism.

4.2 TORSION POINTS

The torsion points on an elliptic curve are the points of finite order. The points that are torsion points will depend on the choice of origin, but the *number* of such points are independent of the choice of origin. Let E be an elliptic curve defined over a field K, and let $n \in \mathbb{N}$. Then we define $E[n] = \{P \in E(\overline{K}) \mid nP = \infty\}$. Note that $E[n]$ contains points with coordinates in the algebraic closure of K, not just in K.

Let $\mathrm{char}(K) \neq 2$. Then E is of the form $y^2 =$ cubic in x. Moreover, let $y^2 = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$, where $\alpha_1, \alpha_2, \alpha_3 \in \overline{K}$. The points P that satisfies $2P = \infty$ are exactly those points who has a "vertical" tangent line at P, which means that for those points, the y-coordinate is 0. This gives that

$$E[2] = \{\infty, (\alpha_1, 0), (\alpha_2, 0), (\alpha_3, 0)\}.$$

As an abstract group this is isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_2$, as there are four elements of order 2. When $\mathrm{char}(K) = 2$, the elliptic curve E, as we saw in chapter 3.2, can have one of the two

following forms:

$$(I)\ \ y^2 + xy + x^3 + a_2x^2 + a_6 = 0 \quad \text{or} \quad (II)\ \ y^2 + a_3y + x^3 + a_4x + a_6 = 0.$$

In the first case we need that $a_6 \neq 0$, and in the second case we must have that $a_3 \neq 0$. Otherwise the curves would be singular. This can easily be seen by performing partial differentiation with respect to x and y and see which coefficients are forced to be nonzero for at least one of the partial derivatives to be nonzero. Now, if $P(x, y)$ is a point of order 2, it means that the tangent at P is vertical, and thus f_y vanishes.

For case (I) this gives $f_y = x = 0$. Substituting $x = 0$ into (I) we obtain that $0 = y^2 + a_6 = (y + \sqrt{a_6})^2$ and thus $(0, \sqrt{a_6})$ is the only nontrivial point of order 2. This gives that $E[2] = \{\infty, (0, \sqrt{a_6})\}$. As an abstract group this is isomorphic to $\mathbb{Z}_2$, as it is a group of order 2.

For case (II) we have that $f_y = a_3 \neq 0$ (since if $a_3 = 0$ the curve would be singular). This means that there is no nontrivial point of order 2 on the curve, so $E[2] = \{\infty\}$, which is obviously isomorphic to the trivial group. We summarize this in the following proposition.

Proposition 4.1. *Let E be an elliptic curve over a field K.*

If $char(K) \neq 2$, then

$$E[2] \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2.$$

If $char(K) = 2$, then

$$E[2] \simeq \mathbb{Z}_2 \ \text{ or } \ 0.$$

For $E[3]$ we can make a similar argument as for $E[2]$. By observing that a point P satisfies $3P = \infty$ if and only if $2P = -P$, the formulas can easily be derived.[2]

In general, the situation is given by the following theorem.

Theorem 4.2. *Let E be an elliptic curve over a field K and let $n \in \mathbb{N}$.*

If $char(K) \nmid n$ or $char(K) = 0$, then

$$E[n] \simeq \mathbb{Z}_n \oplus \mathbb{Z}_n.$$

If $char(K) = p > 0$ and $p \mid n$, we write $n = p^r n'$, where $p \nmid n'$. Then

$$E[n] \simeq \mathbb{Z}_{n'} \oplus \mathbb{Z}_{n'} \ \text{ or } \ \mathbb{Z}_n \oplus \mathbb{Z}_{n'}.$$

[2]See e.g. Matthew England, *Elliptic Curve Cryptography* [3], pp. 32 – 34.

Proof. For a full proof, see the discussion in section 3.2 in Lawrence C. Washington, *Elliptic Curves - Number Theory and Cryptography* [1], pp. $80 - 86$. □

Definition 4.3. An elliptic curve in characteristic p is called *ordinary* if $E[p] \simeq \mathbb{Z}_p$. □

Definition 4.4. An elliptic curve in characteristic p is called *supersingular* if $E[p] \simeq 0$. □

Example 4.3. The elliptic curve E_1 given by $y^2 = x^3 + 2x^2 + x + 2$ in characteristic 3 is ordinary, since $E[3] \simeq \mathbb{Z}_3$. This is an elliptic curve of the form $y^2 = x^3 + a_2x^2 + a_4x + a_6$, with $a_2 \neq 0$.

The elliptic curve E_2 given by $y^2 + y = x^3 + 1$ in characteristic 2 is supersingular, since $E[2] \simeq 0$. This is an elliptic curve of the form $y^2 + a_3y = x^3 + a_4x + a_6$, with $a_3 \neq 0$.

Proposition 4.2. *Let E be an elliptic curve over a field K and let $n \in \mathbb{N}$ such that $char(K) \nmid n$. Then each homomorphism $\alpha : E(\overline{K}) \to E(\overline{K})$, restricted to $E(n)$, can be represented by a 2×2 - matrix over $\mathbb{Z}_n$.*

Proof. Since $\text{char}(K) \nmid n$ we have that $E[n] \simeq \mathbb{Z}_n \oplus \mathbb{Z}_n$ by Theorem 4.2. Choose a basis $\{\varepsilon_1, \varepsilon_2\}$, such that each element of $E[n]$ can be expressed in the form $m_1\varepsilon_1 + m_2\varepsilon_2$, where $m_1, m_2 \in \mathbb{Z}$. We note that m_1, m_2 are uniquely determinded modulo n. We let $\alpha : E(\overline{K}) \to E(\overline{K})$ be a homomorphism, which thus maps $E[n]$ to $E[n]$. This means that there exists $a, b, c, d \in \mathbb{Z}_n$ such that

$$\alpha(\varepsilon_1) = a\varepsilon_1 + c\varepsilon_2 \quad \text{and} \quad \alpha(\varepsilon_2) = b\varepsilon_1 + d\varepsilon_2.$$

Thus each homomorphism $\alpha : E(\overline{K}) \to E(\overline{K})$ can be represented by a 2×2 -matrix

$$\alpha_n = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$ □

Composition of homomorphisms will correspond to multiplication of the corresponding matrices, a property which we will use in the next section. Often the homomorphism α will be an endomorphism, so that it is given by rational functions.

4.3 WEIL PAIRING

In this section we will discuss the *Weil pairing*, which is a useful tool in the study of elliptic curves.

Let E be an elliptic curve over a field K. Furthermore, let $n \in \mathbb{Z}$ such that $\text{char}(K) \nmid n$. Then $E[n] \simeq \mathbb{Z}_n \oplus \mathbb{Z}_n$ as discussed earlier. We let

$$\mu_n = \{x \in \overline{K} \mid x^n = 1\},$$

which is the nth roots of unity in $\overline{K}$. As the characteristic of K does not divide n, the equation $x^n = 1$ has no multiple roots. This means that it has n roots in the algebraic closure of K, which implies that μ_n is a cyclic group of order n. A generator ζ of μ_n is called a *primitive* n*th root of unity*, which is equivalent to saying that $\zeta^k = 1 \iff n \mid k$. We now state the theorem describing the Weil pairing.

Theorem 4.3. *Let E be an elliptic curve defined over a field K and let $n \in \mathbb{N}$. Furthermore, assume that $\text{char}(K) \nmid n$. Then there is a pairing*

$$e_n : E[n] \times E[n] \to \mu_n,$$

called the Weil pairing*, satisfying the following:*

1. *e_n is bilinear, i.e.*

$$e_n(S_1 + S_2, T) = e_n(S_1, T)e_n(S_2, T)$$

and

$$e_n(S, T_1 + T_2) = e_n(S, T_1)e_n(S, T_2)$$

for all $S, S_1, S_2, T, T_1, T_2 \in E[n]$.

2. *e_n is nondegenerate in each variable, i.e.*

$$\text{if } e_n(S, T) = 1, \ \forall\, T \in E[n], \text{ then } S = \infty$$

and

$$\text{if } e_n(S, T) = 1, \ \forall\, S \in E[n], \text{ then } T = \infty.$$

3. $e_n(T, T) = 1, \ \forall\, T \in E[n]$.

4. $e_n(T, S) = e_n(S, T)^{-1}, \ \forall\, S, T \in E[n]$.

5. *$e_n(\sigma S, \sigma T) = \sigma(e_n(S, T))$ for all automorphisms σ of $\overline{K}$ such that σ is the identity map on the coefficients of E.*

6. *$e_n(\alpha(S), \alpha(T)) = e_n(S, T)^{deg(\alpha)}$ for all endomorphisms α of E.*

Proof. See Lawrence C. Washington, *Elliptic Curves - Number Theory and Cryptography* [1], pp. 351 – 354. □

Corollary 4.1. *Let $\{T_1, T_2\}$ be a basis of $E[n]$ as a $\mathbb{Z}_n$ – module. Then $e_n(T_1, T_2)$ is a primitive* n*th root of unity.*

Proof. Suppose that $e_n(T_1.T_2) = \zeta$. Then we have

$$e_n(T_1, dT_2) = e_n(T_1, T_2 + \ldots + T_2) = e_n(T_1, T_2)^d = \zeta^d = 1.$$

In addition,

$$e_n(T_2, dT_2) = e_n(T_2, T_2 + \ldots + T_2) = e_n(T_2, T_2)^d = 1^d = 1$$

by part 1 and 3 of Theorem 4.3. Now, let $S \in E[n]$. Then $S = aT_1 + bT_2$ for some $a, b \in \mathbb{Z}$. Hence,

$$e_n(S, dT_2) = e_n(aT_1 + bT_2, dT_2) = e_n(T_1, dT_2)^a e_n(T_2, dT_2)^b = 1.$$

This holds for all $S \in E[n]$, so part 2 of Theorem 4.3 implies that $dT_2 = \infty$. We know that $dT_2 = \infty$ if and only if n divides d, so it follows that ζ is a primitive nth root of unity. □

This implies[3] that if $E[n] \subseteq E(K)$, then $\mu_n = K$.

We will now prove Proposition 4.3, but first we need a lemma:

Lemma 4.1. *Let M and N be 2×2 - matrices over a commutative ring, where $\tilde{N}$ is the adjugate matrix of N. Then $tr(M\tilde{N}) = det(M + N) - det(M) - det(N)$.*

Proof. Let $M = \begin{pmatrix} q & r \\ s & t \end{pmatrix}$ and $N = \begin{pmatrix} w & x \\ y & z \end{pmatrix}$ so $\tilde{N} = \begin{pmatrix} z & -x \\ -y & w \end{pmatrix}$. Then $M\tilde{N} = \begin{pmatrix} qz - ry & -qx + rw \\ sz - ty & -sx + tw \end{pmatrix}$ so that $\mathrm{tr}(M\tilde{N}) = qz - ry - sx + tw$. Further, we have that $M + N = \begin{pmatrix} q + w & r + x \\ s + y & t + z \end{pmatrix}$ and so $\det(M + N) = (q + w)(t + z) - (r + x)(s + y) = qt + qz + tw + wz - rs - ry - sx - xy$. Now since $\det(M) = qt - rs$ and $\det(N) = wz - xy$ we obtain $\det(M + N) - \det(M) - \det(N) = qt + qz + tw + wz - rs - ry - sx - xy - qt + rs - wz + xy = qz - ry - sx + tw$ and thus $\mathrm{tr}(M\tilde{N}) = \det(M + N) - \det(M) - \det(N)$. □

Proposition 4.3. *Let M and N be arbitrary 2×2 - matrices.*
Then $det(aM + bN) - a^2 det(M) - b^2 det(N) = ab(det(M + N) - det(M) - det(N))$ for all scalars a, b.

Proof. We observe that $\det(aM) = a^2\det(M)$ and $\det(bN) = b^2\det(N)$, so the proposition follows directly from Lemma 4.1.

[3] See L. C. Washington, *Elliptic Curves - Number Theory and Cryptography* [1], p. 88.

Let α and β be endomorphisms of E, and $a, b \in \mathbb{Z}$. Then the endomorphism $a\alpha + b\beta$ is defined in the natural way by

$$(a\alpha + b\beta)(P) = a\alpha(P) + b\beta(P).$$

Here $a\alpha(P)$ means multiplication on E of $\alpha(P)$ by the integer a, which is then added in E to $b\beta(P)$. This is a process which can be described by rational functions, as this is true for each individual step. Thus $a\alpha + b\beta$ is an endomorphism. The degree of this endomorphism is given by the following proposition.

Proposition 4.4. *Let α and β be endomorphisms of E and let $a, b \in \mathbb{Z}$.*
Then $deg(a\alpha + b\beta) = a^2 deg(\alpha) + b^2 deg(\beta) + ab(deg(\alpha + \beta) - deg(\alpha) - deg(\beta))$.

Proof. Let $n \in \mathbb{Z}$ where $\mathrm{char}(K) \nmid n$. As we saw in the previous section, we can represent the endomorphisms α and β by matrices α_n and β_n, so that $a\alpha_n + b\beta_n$ gives the action of $a\alpha + b\beta$ on $E[n]$. By Proposition 4.3 we have that

$$\det(a\alpha_n + b\beta_n) = a^2\det(\alpha_n) + b^2\det(\beta_n) + ab(\det(\alpha_n + \beta_n) - \det(\alpha_n) - \det(\beta_n))$$

for any matrices α_n and β_n. Thus

$$\deg(a\alpha + b\beta) \equiv a^2\deg(\alpha) + b^2\deg(\beta) + ab(\deg(\alpha + \beta) - \deg(\alpha) - \deg(\beta)) \pmod{n}.$$

As this holds for infinitely many n, it is an equality. □

This proposition will become useful when we in the next chapter will prove the celebrated *Hasse's theorem*.

Chapter 5

Elliptic curves over finite fields

5.1 Examples

In this section we will look at some examples of elliptic curves over finite fields. For elliptic curves over finite fields, all points are torsion points.

Example 5.1. Let C be the curve given by $y^2 = x^3 + 3x + 5$ over $\mathbb{F}_{29}$. Then C is not an elliptic curve, because

$$4A^3 + 27B^2 = 4 \cdot 3^3 + 27 \cdot 5^2 = 108 + 675 \equiv 0 \pmod{29}. \tag{5.1}$$

Thus the discriminant of C is zero and C is not an elliptic curve. □

Example 5.2. We consider the curve E given by $y^2 = x^3 + x + 7$ over $\mathbb{F}_{17}$. First we check that the discriminant is nonzero:

$$4A^3 + 27B^2 = 4 \cdot 1^3 + 27 \cdot 7^2 \equiv 4 + 10 \cdot (-2) \equiv 1 \pmod{17}, \tag{5.2}$$

so E is an elliptic curve. The point $Q = (2, 0)$ is on the curve, since $0^2 \equiv 2^3 + 2 + 7 \pmod{17}$, while the point $R = (6, 3)$ is not, since $3^2 = 9 \not\equiv 8 \equiv 6^3 + 6 + 7 \pmod{17}$. Further, we are given the point $P = (6, 5)$ and want to double, i.e. calculate $2P$. We apply the formulas from Case 3 in Theorem 1.2 and reduce modulo 17:

$$m = \frac{3x_1^2 + A}{2y_1} = \frac{3 \cdot 6^2 + 1}{10} = 109 \cdot 10^{-1} \equiv 7 \cdot 12 \equiv 16 \pmod{17}, \tag{5.3}$$

so we get that

$$x_3 = m^2 - 2x_1 = 16^2 - 2 \cdot 6 = 244 \equiv 6 \pmod{17} \tag{5.4}$$

and

$$y_3 = m(x_1 - x_3) - y_1 = 16 \cdot (6 - 6) - 5 \equiv 12 \pmod{17}. \tag{5.5}$$

Thus $2P = (6, 12)$, which is easily checked to satisfy $y^2 = x^3 + x + 7$ over $\mathbb{F}_{17}$. Figure 5.1 shows the points on the elliptic curve. □

Let $\mathbb{F}$ be a finite field, and let E be an elliptic curve defined over $\mathbb{F}$. As we can only have a finite number of pairs (x, y), where $x, y \in \mathbb{F}$, the group $E(\mathbb{F})$ will be finite.

Example 5.3. We consider the elliptic curve $y^2 = x^3 + 2x + 1$ over the finite field $\mathbb{F}_7$, and we are interested in finding the order of the group $E(\mathbb{F}_7)$. Table 5.1 shows the possible values of x, then of $x^3 + 2x + 1 \pmod{n}$, the square roots y and the points on E.

Table 5.1: Points on $E(\mathbb{F}_7)$

x	$x^3 + 2x + 1$	y	Points
0	1	± 1	$(0,1), (0,6)$
1	4	± 2	$(1,2), (1,5)$
2	6	-	-
3	6	-	-
4	3	-	-
5	3	-	-
6	5	-	-
∞		∞	∞

Thus the group has the elements $\{\infty, (0,1), (0,6), (1,2), (1,5)\}$, so the order of the group is 5. This means that $E(\mathbb{F}_7)$ is isomorphic to the group $\mathbb{Z}_5$. Then $E[5] \simeq \mathbb{Z}_5 \oplus \mathbb{Z}_5$ by Theorem 4.2.□

5.2 HASSE'S THEOREM

In this section we will prove the celebrated *Hasse's theorem*. This theorem gives a bound for the order of the group $E(\mathbb{F}_p)$. In doing so we will first need a few lemmas.

Let E be an elliptic curve defined over the finite field $\mathbb{F}_p$. Further, let Φ_p be the Frobenius map for $\mathbb{F}_p$, given by

$$\begin{aligned} \Phi_p \ : \ \overline{\mathbb{F}_p} &\to \overline{\mathbb{F}_p}, \\ x &\mapsto x^p. \end{aligned}$$

This means that

$$\Phi_p(x, y) = (x^p, y^p), \quad \Phi_p(\infty) = \infty,$$

for the coordinates of points in $E(\overline{\mathbb{F}_p})$.

Lemma 5.1. *Let E be defined over the finite field $\mathbb{F}_p$, and let $(x, y) \in E(\overline{\mathbb{F}_p})$. Then*
(I). $\Phi_p(x, y) \in E(\overline{\mathbb{F}_p})$ and
(II). $(x, y) \in (\mathbb{F}_p \times \mathbb{F}_p) \iff \Phi_p(x, y) = (x, y)$.

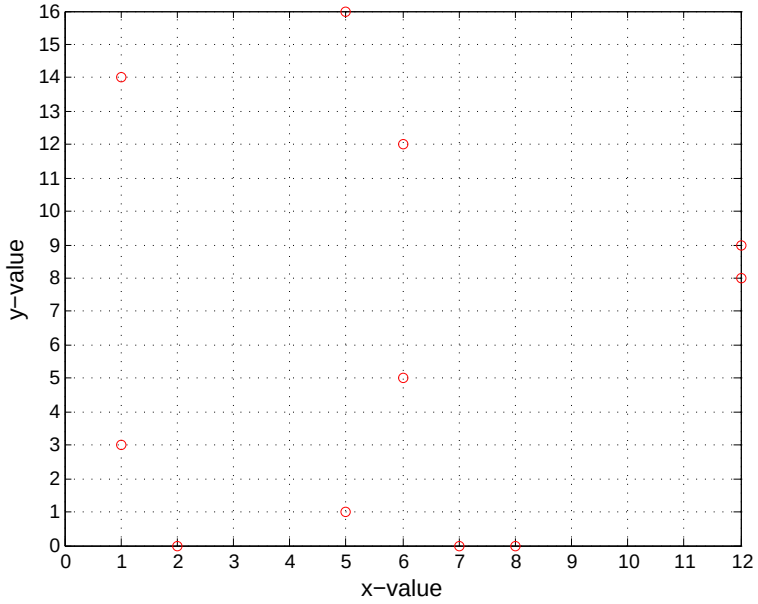

Figure 5.1: The figure shows the points on the elliptic curve $y^2 = x^3 + 3 + 7$ over $\mathbb{F}_{17}$. In addition to the points shown here we have the point at infinity, thus giving 12 points in total. Note that the points are symmetric about the line $y = 17/2 = 8.5$ in our representation in the plane.

Proof. Since $\mathbb{F}_p$ is a field with p elements, we have that $a^p = a,\ \forall a \in \mathbb{F}_p$. We also have that $(a+b)^p = a^p + b^p$ when p is a power of the characteristic of the field, which follows from the binomial theorem. Recall that the generalized Weierstrass form is given by

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{5.6}$$

with $a_i \in \mathbb{F}_p$. We could also have worked with the Weierstrass normal form, where the proof would be as easy. Now we raise eq. (5.6) to the pth power so that

$$\begin{aligned} &(y^2)^p + (a_1xy)^p + (a_3y)^p = (x^3)^p + (a_2x^2)^p + (a_4x)^p + (a_6)^p \\ \implies\ &(y^p)^2 + a_1(x^py^p) + a_3(y^p) = (x^p)^3 + a_2(x^p)^2 + a_4(x^p) + a_6. \end{aligned}$$

Thus (x^p, y^p) lies on the elliptic curve E, and so $\Phi_p(x,y) \in E(\overline{\mathbb{F}_p})$, proving (I).

Since $t \in \mathbb{F}_p \iff \Phi_p(t) = t$, we have that

$$(x,y) \in E(\overline{\mathbb{F}_p})_\Phi \iff x, y \in \mathbb{F}_p.$$

Here we have that (x,y) are the elements of $E(\overline{\mathbb{F}_p})$ fixed under Φ. Thus we obtain

$$(x,y) \in E(\overline{\mathbb{F}_p}) \cap (\mathbb{F}_p \times \mathbb{F}_p) \iff \Phi_p(x) = x \text{ and } \Phi_p(y) = y,$$

i.e.

$$(x,y) \in E(\overline{\mathbb{F}_p}) \cap (\mathbb{F}_p \times \mathbb{F}_p) \iff \Phi_p(x,y) = (x,y).$$

This completes the proof of (II). □

Lemma 5.2. *Let E be an elliptic curve defined over $\mathbb{F}_p$. Then Φ_p is a nonseparable endomorphism of E of degree p.*

Proof. We want to show that Φ_p is an endomorphism of degree p by showing that it is a homomorphism given by rational functions. Furthermore, we want to show that it satisfies the requirement for being nonseparable.

Since $\Phi_p(x,y) = (x^p, y^p)$, we see that the map is given by rational functions, where the degree is p. We now want to show that $\Phi_p : E(\overline{\mathbb{F}_p}) \to E(\overline{\mathbb{F}_p})$ is a homomorphism. We start by letting (x_1, y_1) and (x_2, y_2) be two points in $E(\overline{\mathbb{F}_p})$, with $x_1 \neq x_2$. The formulas for the sum (x_3, y_3), given in Theorem 1.2, then gives that

$$x_3 = m^2 - x_1 - x_2, \qquad y_3 = m(x_1 - x_3) - y_1, \quad \text{where } m = \frac{y_2 - y_1}{x_2 - x_1}.$$

Now we raise everything to the pth power:

$$(x_3)^p = (m^2 - x_1 - x_2)^p, \quad (y_3)^p = (m(x_1 - x_3) - y_1)^p, \quad \text{where } (m)^p = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^p.$$

Since we are in characteristic p, we obtain

$$x_3^p = m'^2 - x_1^p - x_2^p, \quad y_3^p = m'(x_1^p - x_3^p) - y_1^p, \quad \text{where } m' = \frac{y_2^p - y_1^p}{x_2^p - x_1^p}.$$

Similarly, we check the cases for when $x_1 = x_2$ or when one of the points is ∞.

This shows that $\Phi_p(x_3, y_3) = \Phi_p(x_1, y_1) + \Phi_p(x_2, y_2)$. Thus, Φ_p is a homomorphism, and since it is given by rational functions it is an endomorphism of E, which was seen to have degree p. Since we work in the finite field $\mathbb{F}_p$, we have that the derivative of x^p is identically zero, which is the requirement for Φ_p to be nonseparable. This completes the proof of the lemma. □

The following proposition will also be useful.

Proposition 5.1. *If α is a nontrivial separable endomorphism of an elliptic curve E, then*

$$deg(\alpha) = \#Ker(\alpha).$$

If α is a nontrivial nonseparable endomorphism of an elliptic curve E, then

$$deg(\alpha) > \#Ker(\alpha).$$

Proof. See Lawrence C. Washington, *Elliptic Curves - Number Theory and Cryptography* [1], p. 54. □

Proposition 5.2. *Let E be an elliptic curve defined over $\mathbb{F}_p$ and let $n \geq 1$. Then*
(I). $Ker(\Phi_p^n - I) = E(\mathbb{F}_{p^n})$ and
(II). $\Phi_p^n - I$ is a separable endomorphism, implying that $\#E(\mathbb{F}_{p^n}) = deg(\Phi_p^n - 1)$.

Here I is the identity.

Proof. The Frobenius map for $\mathbb{F}_{p^n}$ is Φ_p^n, so (I) is just a restatement of Lemma 5.1. As $(\Phi_p^n - 1)x = x^{p^n} - x$, we have that $\frac{\partial}{\partial x}(x^{p^n} - x) = -1 \neq 0$, so $\Phi_p^n - 1$ is separable. Thus (II) follows from Proposition 5.1. □

Theorem 5.1. *Let E be an elliptic curve defined over the finite field $\mathbb{F}_p$. Then*

$$E(\mathbb{F}_p) \simeq \mathbb{Z}_n \quad or \quad \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2},$$

for some integer $n \geq 1$, or for some integers $n_1, n_2 \geq 1$, where $n_1 \mid n_2$.

Proof. It is a well known fact of group theory that a finite abelian group is isomorphic to a direct sum of cyclic groups

$$\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_k},$$

with $n_i \mid n_{i+1}$ for $i \geq 1$.

For each i, the group $\mathbb{Z}_{n_i}$ has n_i elements of order dividing n_i. This means that $E(\mathbb{F}_p)$ has n_1^k elements of order dividing n_1. Theorem 4.2 implies that there are at most n_1^2 such points. This gives that $k \leq 2$, which proves the theorem. □

We are interested in finding the bound for the order of the group $E(\mathbb{F}_p)$. Let

$$a = p + 1 - \#E(\mathbb{F}_p) = p + 1 - \deg(\Phi_p - 1). \tag{5.7}$$

Hasse's theorem then says that $|a| \leq 2\sqrt{p}$. Before we prove the theorem, we will need one more lemma:

Lemma 5.3. *Let $r, s \in \mathbb{Z}$ such that $gcd(s, p) = 1$. Then $deg(r\Phi_p - s) = r^2p + s^2 - rsa$.*

Proof. Proposition 4.4 says that for endomorphisms α, β of E we have that $\deg(a\alpha + b\beta) = a^2\deg(\alpha) + b^2\deg(\beta) + ab(\deg(\alpha + \beta) - \deg(\alpha) - \deg(\beta))$. This gives that $\deg(r\Phi_p - s) = r^2\deg(\Phi_p) + s^2\deg(-1) + rs(\deg(\Phi_p - 1) - \deg(\Phi_p) - \deg(-1))$.

Obviously, $\deg(\Phi_p) = p$ and $\deg(-1) = 1$. This gives that $\deg(r\Phi_p - s) = r^2p + s^2 + rs(p + 1 - a - p - 1) = r^2p + s^2 - rsa$, where we used that $\deg(\Phi_p - 1) = p + 1 - a$ from eq. (5.7). □

We are now ready to state Hasse's theorem:

Theorem 5.2. *Let E be an elliptic curve over the finite field $\mathbb{F}_p$. Then the order of $E(\mathbb{F}_p)$ satisfies the relation*

$$|p + 1 - \#E(\mathbb{F}_p)| \leq 2\sqrt{p}. \tag{5.8}$$

Proof. We want to show that $|a| \leq 2\sqrt{p}$ in eq. (5.7). We have that $\deg(r\Phi_p - s) \geq 0$. Lemma 5.3 then implies that $r^2p + s^2 - rsa \geq 0$. Dividing by s^2, we get $p\left(\frac{r}{s}\right)^2 - a\left(\frac{r}{s}\right) + 1 \geq 0$, for all coprime integers r, s. Let $x = r/s$. Since the set of rational numbers r/s such that $\gcd(s, p)$ is dense in $\mathbb{R}$, we have that

$$px^2 - ax + 1 \geq 0, \ \forall\, x \in \mathbb{R}. \tag{5.9}$$

This gives that the discriminant of the polynomial is nonpositive, i.e. $a^2 - 4p \leq 0$. In other words, $|a| \leq 2\sqrt{p}$, which completes the proof. □

In Example 5.2, where $p = 17$ and $\#E(\mathbb{F}_p) = 12$, we have that $|17+1-12| = 6 \leq 2\sqrt{17} \approx 8.25$. In Example 5.3, where $p = 7$ and $\#E(\mathbb{F}_p) = 5$, we see that $|7 + 1 - 5| = 3 \leq 2\sqrt{7} \approx 5.29$.

Hasse's theorem can also be generalized to non-singular irreducible curves of arbitrary genus g over finite fields $\mathbb{F}_p$. Then the theorem, called Hasse-Weil, is given by

$$|p + 1 - \#E(\mathbb{F}_p)| \leq 2g\sqrt{p}. \tag{5.10}$$

Any non-singular curve given by a cubic equation is a curve of genus 1. The special case for $g = 1$ was first proven by the German mathematician Helmut Hasse $(1898 - 1979)$ in 1933, while the general case was proven by the Frenchman André Weil $(1906 - 1998)$. As a curiosity, Weil was also responsible for the introduction of the symbol for the empty set, $\varnothing$, which he took from the Norwegian alphabet.[1]

Given an elliptic curve E over a small field $\mathbb{F}_p$, the order of $E(\mathbb{F}_p)$ can be found by some elementary procedure (like listing the points). We are interested in finding the order of $E(\mathbb{F}_{p^n})$, when $n > 1$. The following theorem gives a nice way to determine the order for all n.

Theorem 5.3. *Let E be an elliptic curve over a finite field $\mathbb{F}_p$. Let $\#E(\mathbb{F}_p) = p + 1 - a$. Further, write $X^2 - aX + p = (X - \alpha)(X - \beta)$. Then*

$$\#E(\mathbb{F}_{p^n}) = p^n + 1 - (\alpha^n + \beta^n). \tag{5.11}$$

Proof. First we need to show that $\alpha^n + \beta^n$ is an integer. The following recurrence relation will become useful.

Lemma 5.4. *Let $\sigma_n = \alpha^n + \beta^n$. Then $\sigma_0 = 2$, $\sigma_1 = a$ and $\sigma_{n+1} = a\sigma_n - p\sigma_{n-1}, \quad \forall n \geq 1$.*

Proof. We multiply the relation $\alpha^2 - a\alpha + p = 0$ from Theorem 5.3 with α^{n-1} to obtain $\alpha^{n+1} = a\alpha^n - p\alpha^{n-1}$. Similarly, we multiply $\beta^2 - a\beta + p = 0$ with β^{n-1} to get $\beta^{n+1} = a\beta^n - p\beta^{n-1}$. Adding these together, we obtain $\alpha^{n+1} + \beta^{n+1} = a(\alpha^n + \beta^n) - p(\alpha^{n-1} + \beta^{n-1})$. This gives that $\sigma_{n+1} = a\sigma_n - p\sigma_{n-1}$. □

The lemma implies that $\alpha^n + \beta^n$ is an integer for all n.
Continuing our proof of Theorem 5.3, we let

$$f(X) = (X^n - \alpha^n)(X^n - \beta^n) = X^{2n} - (\alpha^n + \beta^n)X^n + p^n.$$

Then we have that $g(X) = X^2 - aX + p = (X - \alpha)(X - \beta)$ divides $f(X)$. The polynomial $g(X)$ is monic, and since $f(X)$ and $g(X)$ have integer coefficients, it follows that the quotient $Q(X) = f(X)/g(X)$ also has integer coefficients. This can easily be checked by standard polynomial division.

Furthermore, it can be shown[2] that a is the unique integer k such that $\Phi_p^2 - k\Phi_p + p = 0$,

[1] See his autobiography: André Weil - *The Apprenticeship of a Mathematician.*
[2] L. C. Washington, *Elliptic Curves - Number Theory and Cryptography* [1], pp 101 – 102.

where Φ_p is the Frobenius endomorphism. This gives that

$$(\Phi_p^n)^2 - (\alpha^n + \beta^n)\Phi_p^n + p^n = f(\Phi_p) = Q(\Phi_p)(\Phi_p^2 - a\Phi_p + p) = 0$$

as endomorphisms of E. We note that $\Phi_p^n = \Phi_{p^n}$. Since there is only one integer k such that $\Phi_{p^n}^2 - k\Phi_{p^n} + p^n = 0$, and such a k is determined by $k = p^n + 1 - \#E(\mathbb{F}_{p^n})$, we get that

$$\begin{aligned}
(\Phi_p^n)^2 - k\Phi_p^n + p^n &= (X - \alpha^n)(X - \beta^n) \\
\Rightarrow \Phi_p^{2n} - k\Phi_p^n + p^n &= X^{2n} - (\alpha^n + \beta^n)X^n + p^n \\
\Rightarrow k &= \alpha^n + \beta^n \\
\Rightarrow \#E(\mathbb{F}_{p^n}) &= p^n + 1 - (\alpha^n + \beta^n).
\end{aligned}$$

This completes our proof of Theorem 5.3. □

Example 5.4. Continuing from Example 5.3, we had the elliptic curve given by $y^2 = x^3 + 2x + 1$ over the finite field $\mathbb{F}_7$. The order of $E(\mathbb{F}_7)$ was found to be 5. Therefore, $a = p + 1 - E(\mathbb{F}_p) = 7 + 1 - 5 = 3$. Thus we obtain the polynomial

$$X^2 - 3X + 7 = \Big(X - \frac{3 + \sqrt{-19}}{2}\Big)\Big(X - \frac{3 - \sqrt{-19}}{2}\Big).$$

We are interested in finding the order of $E(\mathbb{F}_{7^2})$. By Theorem 5.3 we get

$$\begin{aligned}
\#E(\mathbb{F}_{7^2}) &= 49 + 1 - \Big(\frac{3 + \sqrt{-19}}{2}\Big)^2 - \Big(\frac{3 - \sqrt{-19}}{2}\Big)^2 \\
\#E(\mathbb{F}_{7^2}) &= 49 + 1 - \Big(\frac{6\sqrt{-19} - 10}{4}\Big) - \Big(\frac{-6\sqrt{-19} - 10}{4}\Big) \\
\#E(\mathbb{F}_{7^2}) &= 49 + 1 + \Big(\frac{10 - 6\sqrt{-19} + 10 + 6\sqrt{-19}}{4}\Big) \\
\#E(\mathbb{F}_{7^2}) &= 49 + 1 + 5 = 55.
\end{aligned}$$

We observe that this satisfies Hasse's theorem, as $|q + 1 - \#E(\mathbb{F}_q)| = |49 + 1 - 55| = 5 \leq 2\sqrt{q} = 2 \cdot 7 = 14$, where $q = p^2$. As $E(\mathbb{F}_7)$ for our elliptic curve $y^2 = x^3 + 2x + 1$ was isomorphic to $\mathbb{Z}_5$, we would already know that 5 must divide the order of the group $E(\mathbb{F}_{7^2})$. Together with the inequality given by Hasse's theorem, we could then deduce the feasible order for $E(\mathbb{F}_{7^2})$ as $40, 45, 50, 55$ or 60. Here we obtain that $E(\mathbb{F}_{7^2})$ is isomorphic to $\mathbb{Z}_5 \oplus \mathbb{Z}_{11}$.

Using the recurrence relation given by Lemma 5.4, we can easier calculate the order of $E(\mathbb{F}_{p^n})$ for larger n. Now we want to find the order of $E(\mathbb{F}_{7^{17}})$ for our elliptic curve $y^2 = x^3 + 2x + 1$. We obtain that

$$\#E(\mathbb{F}_{7^{17}}) = 7^{17} + 1 - \Big(\frac{3 + \sqrt{-19}}{2}\Big)^{17} - \Big(\frac{3 - \sqrt{-19}}{2}\Big)^{17}$$

Now we use that $p = 7$ and $a = 3$ which we found earlier in the example. The recurrence relation

was given by $\sigma_{n+1} = a\sigma_n - p\sigma_{n-1}$, where $\sigma_1 = a$ and $\sigma_0 = 2$. This gives that

$$\begin{aligned}
\sigma_2 &= 3\sigma_1 - 7\sigma_0 = 3 \cdot 3 - 7 \cdot 2 = -5 \\
\sigma_3 &= 3\sigma_2 - 7\sigma_1 = 3 \cdot (-5) - 7 \cdot 3 = -36 \\
\sigma_4 &= 3\sigma_3 - 7\sigma_2 = 3 \cdot (-36) - 7 \cdot (-5) = -73 \\
&\vdots \\
\sigma_{17} &= 3\sigma_{16} - 7\sigma_{15} = 3 \cdot (-11251873) - 7 \cdot (-1627956) = -22359927
\end{aligned}$$

Theorem 5.3 said that

$$\#E(\mathbb{F}_{p^n}) = p^n + 1 - (\alpha^n + \beta^n)$$

Together with $\sigma_n = \alpha^n + \beta^n$ we obtain

$$\begin{aligned}
\#E(\mathbb{F}_{7^{17}}) &= 7^{17} + 1 - \sigma_{17} \\
\#E(\mathbb{F}_{7^{17}}) &= 7^{17} + 1 + 22359927 \\
&= 232630536347135.
\end{aligned}$$

□

When n grows large, $\#E(\mathbb{F}_{p^n})$ grows asymptotically as p^n. This can be seen by taking the norms of the equation given in Theorem 5.3.

5.3 THE LEGENDRE SYMBOL

In Example 5.3 we made a list of all possible values of x and then found the square roots y of $x^3 + Ax + B$ in order to make a list of points on the curve. In that example, we worked over the field $\mathbb{F}_7$. Let's look at what happens when we run through all the elements in $\mathbb{F}_7$ and square

them:

$$\begin{aligned} 0^2 &\equiv 0 \pmod 7 \\ 1^2 &\equiv 1 \pmod 7 \\ 2^2 &\equiv 4 \pmod 7 \\ 3^2 &\equiv 2 \pmod 7 \\ 4^2 &\equiv 2 \pmod 7 \\ 5^2 &\equiv 4 \pmod 7 \\ 6^2 &\equiv 1 \pmod 7 \end{aligned}$$

We see that only $1, 2$ and 4 are possible nontrivial values, we call them *quadratic residues* of 7. Notice that if x_1 is a quadratic residue, then $p - x_1$ is also a quadratic residue. When p is an odd prime and $\gcd(x, p) = 1$ we say that x is a quadratic residue of p if the quadratic congruence $t^2 \equiv x \pmod p$ has a solution. This concept is very important in number theory, and we will see an example of its usefulness regarding elliptic curves.

Definition 5.1. Let p be an odd prime and let $\gcd(x, p) = 1$. The *Legendre symbol* (x/p) is defined by

$$(x/p) = \begin{cases} 1 & \text{if } t^2 \equiv x \pmod p \text{ has a solution } t \not\equiv 0 \pmod p \\ -1 & \text{if } t^2 \equiv x \pmod p \text{ has no solution } t \\ 0 & \text{if } x \equiv 0 \pmod p \end{cases}$$

□

For our field $\mathbb{F}_7$ we would thus obtain $(0/7) = 0, (1/7) = 1, (2/7) = 1, (3/7) = -1, (4/7) = 1, (5/7) = -1$ and $(6/7) = -1$. The symbol is named after the French mathematician Adrien Marie Legendre $(1752 - 1833)$ who made contributions to various fields of mathematics, including number theory.

We can generalize this definition to any finite field $\mathbb{F}_p$, where p is an odd prime and $x \in \mathbb{F}_p$, in the following way.

$$(x/\mathbb{F}_p) = \begin{cases} 1 & \text{if } t^2 = x \text{ has a solution } t \in \mathbb{F}_p^* \\ -1 & \text{if } t^2 = x \text{ has no solution } t \in \mathbb{F}_p \\ 0 & \text{if } x = 0 \end{cases}$$

Then we have a simple point counting algorithm, given by the following theorem.

Theorem 5.4. *Let E be an elliptic curve defined by $y^2 = x^3 + Ax + B$ over the finite field $\mathbb{F}_p$. Then*

$$\#E(\mathbb{F}_p) = p + 1 + \sum_{x \in \mathbb{F}_p} \left(x^3 + Ax + B \,/\, \mathbb{F}_p \right)$$

Proof. For a given (x_0), we see that there are two points (x, y) with $x-$ coordinate x_0 if $x_0^3 + Ax_0 + B$ is a nonzero square in $\mathbb{F}_p$. There is one such point if it is zero, and no points if it is not a square. This corresponds to the possible values of the Legendre symbol, and so the number of points with $x-$ coordinate x_0 is $1 + \left(x^3 + Ax + B \,/\, \mathbb{F}_p \right)$. We sum over all $x_0 \in \mathbb{F}_p$, and we include 1 for the point ∞, to obtain

$$\begin{aligned} \#E(\mathbb{F}_p) &= 1 + \sum_{x \in \mathbb{F}_p} \left(1 + \left(x^3 + Ax + B \,/\, \mathbb{F}_p \right) \right) \\ \#E(\mathbb{F}_p) &= p + 1 + \sum_{x \in \mathbb{F}_p} \left(x^3 + Ax + B \,/\, \mathbb{F}_p \right) \end{aligned}$$

which is what we wanted to prove. □

Example 5.5. Let E be an elliptic curve over $\mathbb{F}_7$ given by $y^2 = x^3 + 2x + 1$ as in Example 5.3. The nonzero squares modulo 7 are $1, 2$ and 4. This gives

$$\begin{aligned} \#E(\mathbb{F}_7) &= 7 + 1 + \sum_{x \in \mathbb{F}_7} \left(x^3 + 2x + 1 \,/\, 7 \right) \\ &= 8 + (1/7) + (4/7) + (6/7) + (6/7) + (3/7) + (3/7) + (5/7) \\ &= 8 + 1 + 1 - 1 - 1 - 1 - 1 - 1 = 5, \end{aligned}$$

as we found earlier. □

With computer programs, we can easily calculate the value of the Legendre symbol. This can come useful if we are working over a larger field and want to find the group order, as in the following example.

Example 5.6. Consider the elliptic curve given by $y^2 = x^3 + 59x + 173$ over $\mathbb{F}_{313}$. Using MATLAB® to calculate, we get that there are 151 nonquadratic residues of $x^3 + 59x + 173$, which thus have a Legendre value of -1, while $313 - 151 - 1 = 161$ have value 1 (the square 0^2 has value 0). This gives

$$\begin{aligned} \#E(\mathbb{F}_{313}) &= 313 + 1 + \sum_{x \in \mathbb{F}_{313}} \left(x^3 + 59x + 173 \,/\, 313 \right) \\ &= 314 + 161 - 151 = 324. \end{aligned}$$

□

Recall that the *order* of a point $P \in E(\mathbb{F}_p)$ is the smallest positive integer k such that $kP = \infty$. In group theory, *Lagrange's theorem* states that for any finite group G, the order of every subgroup H of G divides the order of G. An easy corollary is that the order of an element always divides the order of the group. We get that the order of a point on the elliptic curve always divides the order of the group $E(\mathbb{F}_p)$. Also, we have that $nP = \infty$ for an integer n if and only if the order of P divides n. Together with Hasse's theorem, this means that we can often easily find restrictions for the candidates for the order of the group, as we know that $\#E(\mathbb{F}_p)$ lies in an interval of length $4\sqrt{p}$.

Example 5.7. Continuing with the curve from the previous example, we want to find the order of the group based on the order of points. As we know from Lagrange's theorem, the order of the elements of the group has to divide the order of the group. We start by using the point $P = (3, 8)$. Calculating, we obtain that the point P has order 54 (see Table 5.2). As the order of $E(\mathbb{F}_{313})$ has to satisfy Hasse's theorem, we see that

$$313 + 1 - 2\sqrt{313} \leq \#E(\mathbb{F}_{313}) \leq 313 + 1 + 2\sqrt{313}$$
$$278 \leq \#E(\mathbb{F}_{313}) \leq 350$$

We see that $5 \cdot 54 = 270, 6 \cdot 54 = 324$ and $7 \cdot 54 = 378$. The only muliple of 54 which are within the interval $[278, 350]$ is thus 324, and we can conclude that $E(\mathbb{F}_{313})$ has order 324. □

Table 5.2: kP for $k = 1, 2, 3, \ldots, 56$.

P	(3, 8)	15P	(234, 91)	29P	(113, 58)	43P	(312, 48)
2P	(18, 107)	16P	(47, 6)	30P	(42, 145)	44P	(98, 3)
3P	(298, 236)	17P	(58, 151)	31P	(190, 242)	45P	(49, 258)
4P	(242, 98)	18P	(96, 251)	32P	(149, 129)	46P	(158, 75)
5P	(302, 178)	19P	(185, 304)	33P	(61, 94)	47P	(130, 135)
6P	(181, 186)	20P	(195, 120)	34P	(195, 193)	48P	(181, 127)
7P	(130, 178)	21P	(61, 219)	35P	(185, 9)	49P	(302, 135)
8P	(158, 238)	22P	(149, 184)	36P	(96, 62)	50P	(242, 215)
9P	(49, 55)	23P	(190, 71)	37P	(58, 162)	51P	(298, 77)
10P	(98, 310)	24P	(42, 168)	38P	(47, 307)	52P	(18, 206)
11P	(312, 265)	25P	(113, 255)	39P	(234, 222)	53P	(3, 305)
12P	(194, 135)	26P	(285, 36)	40P	(172, 288)	54P	(∞, ∞)
13P	(164, 234)	27P	(146, 0)	41P	(164, 79)	55P	(3, 8)
14P	(172, 25)	28P	(285, 277)	42P	(194, 178)	56P	(18, 107)

In the previous example, the interval spanned by $4\sqrt{313}$ was 72, while the order of the point $(3, 8)$ was 54. In general however, most p are such that all elliptic curves have points of order greater than $4\sqrt{p}$. When that is the case, we will be sure to find the order of the group as there can only be one possible point within the interval. In our example, we were lucky because a multiple of 54 was sufficiently in the middle of the interval to rule out other candidates.

Definition 5.2. Let E be an elliptic curve defined over $\mathbb{F}_p$, and let $d \in \mathbb{F}_p^*$ be a quadratic nonresidue modulo p. If E has the equation $y^2 = x^3 + Ax + B$, then the *quadratic twist* $\tilde{E}$ is given by the equation $y^2 = x^3 + Ad^2x + Bd^3$. □

We worked with the curve given by $y^2 = x^3 + Ad^2x + Bd^3$ in the examples of Chapter 3.1, where we saw that an elliptic curve and its quadratic twist has the same j-invariant and that they can be transformed into each other over $K(\sqrt{d})$.

Proposition 5.3. *If $\#E(\mathbb{F}_p) = p + 1 - a$, then $\#\tilde{E}(\mathbb{F}_p) = p + 1 + a$.*

Proof. As we run through all the elements in the set, it can be easily seen that $\#E(\mathbb{F}_p) + \#\tilde{E}(\mathbb{F}_p) = 2p + 2$. Thus $\#\tilde{E}(\mathbb{F}_p) = (2p + 2) - (p + 1 - a) = p + 1 + a$. □

Example 5.8. In Example 5.3 in the beginning of this chapter, we found that $\#E(\mathbb{F}_7)$ for the elliptic curve $y^2 = x^3 + 2x + 1$ was 5. This gave that $a = p + 1 - \#E(\mathbb{F}_p) = 7 + 1 - 5 = 3$. We also saw that the quadratic residues are $0, 1, 2$ and 4. Now choose $d = 3$. Then the quadratic twist of E is given by $y^2 = x^3 + 2 \cdot 3^2x + 1 \cdot 3^3$ which is congruent to $y^2 = x^3 + 4x + 6$ modulo 7. By Proposition 5.3, the number of points in $\tilde{E}(\mathbb{F}_p)$ is $p + 1 + a = 7 + 1 + 3 = 11$. As expected, this satisfies Hasse's theorem, as $|7 + 1 - 11| = 3 \leq 2\sqrt{7} \approx 5.29$.

For our elliptic curve $E : y^2 = x^3 + 59x + 173$ over $\mathbb{F}_{313}$ from Example 5.6, we have that 5 is a nonquadratic residue. This gives that the quadratic twist $\tilde{E}$ is given by $y^2 = x^3 + 59 \cdot 5^2x + 173 \cdot 5^3$ which is congruent to $y^2 = x^3 + 223x + 28$ modulo 313. In this case, $a = p + 1 - \#E(\mathbb{F}_p) = 313 + 1 - 324 = -10$, so that $\tilde{E}(\mathbb{F}_{313}) = p + 1 + a = 313 + 1 - 10 = 304$, which clearly satisfies the bound given by Hasse's theorem. □

In this chapter we have seen some examples of how we can determine the number of points on elliptic curves over finite fields. This continues to be an important topic in the study of elliptic curves, and subject to a lot of reasearch in cryptography today.

Chapter 6

PRIMALITY TESTING

Primality testing is a classical part of mathematics, which goes back at least to the days of Erastosthenes of Cyrene (around 200 BC), who developed his famous prime number sieve. In the last few decades a substantial effort has been made from mathematicians and computer scientists to develop relatively fast algorithms for deciding whether a given number is prime or not. In modern cryptography, the question of primality and factorization of numbers is essential. It is worth emphasizing that primality tests do not give *prime factors* in general, only a statement of whether the tested number is prime or not. Primality testing usually runs in polynomial time, but there does not exist an algorithm for integer factorization of (large) composite numbers which runs in polynomial time.

Since the days of Fermat, Euler, Legendre and Gauss, a large number of primality tests have been developed. Some of the most famous are the Miller-Rabin test, the Lucas-Lehmer test and the Fermat primality test. There are two types of primality tests: *deterministic* tests and *probabilistic* tests. The deterministic tests determine with absolute certainty whether a number is prime or not. Probabilistic tests tell with a very large probability whether a number is prime or not, but doesn't give the result with an absolute certainty. However, probabilistic tests usually are much faster than deterministic tests. A number who pass a probabilistic test as a prime without actually being a prime, is often called a *pseudoprime*.

In this text we will look at the *Pocklington-Lehmer* test and the *Goldwasser-Kilian* test, which is the elliptic curve analogue of Pocklington-Lehmer. Both of these tests are deterministic.

6.1 POCKLINGTON-LEHMER PRIMALITY TEST

The Pocklington-Lehmer primality test is a classical test of deciding whether a given natural number is prime or not.

Proposition 6.1. *Let $n \in \mathbb{N}$, and let $n - 1 = rs$ with $r \geq \sqrt{n}$. If, for each prime $l|r$, there exists*

an integer a_l with

$$a_l^{n-1} \equiv 1 \pmod{n}$$

and

$$\gcd\left(a_l^{(n-1)/l} - 1, n\right) = 1,$$

then n is prime.

Proof. Let p be a prime factor of n, and let l^e be the highest power of l dividing r. Further, let

$$b \equiv a_l^{(n-1)/l^e} \pmod{p}.$$

Then

$$b^{l^e} \equiv a_l^{(n-1)} \pmod{p}$$

and

$$b^{l^{e-1}} \equiv a_l^{(n-1)/l} \not\equiv 1 \pmod{p},$$

since $\gcd\left(a_l^{(n-1)/l} - 1, n\right) = 1$. We cannot have that $a_l^{(n-1)/l^e} - 1 \equiv 0 \pmod{p}$, because $p|n$ and $a_l^{(n-1)/l^e} - 1$ is relatively prime to n. It follows that the order of $b \pmod{p}$ is l^e. Therefore, $l^e|(p-1)$ by Fermat's little theorem. This is true for every prime power factor l^e of r, so $r|(p-1)$. In particular we have that $p > r \geq \sqrt{n}$. But if n is composite, it must have a prime factor at most $\sqrt{n}$, so we have a contradiction. Hence, n is prime. □

Example 6.1. Let $n = 3201529$. Then $n - 1 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 11 \cdot 67 \cdot 181$. We have $r = 11 \cdot 181 = 1991 \geq \sqrt{3201529} \approx 1789.28$. The primes dividing r are thus $l = 11$ and $l = 181$. Then

$$2^{n-1} \equiv 1 \pmod{n}$$

and

$$\gcd\left(2^{(n-1)/11} - 1, n\right) = 1,$$

so we can take $a_{11} = 2$. Further,

$$\gcd\left(2^{(n-1)/181} - 1, n\right) = 1,$$

so we can also take $a_{181} = 2$. Then, according to Proposition 6.1, the number 3201529 is prime. To make the proof complete, we should also show that 181 is prime (we regard the number 11 as a trivial case). To see that 181 is prime, we use the Pocklington-Lehmer test again. Here

$180 = 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5$. We let $r = 3 \cdot 5 = 15$, which is greater than $\sqrt{181} \approx 13.45$. Then

$$2^{180} \equiv 1 \pmod{181}$$

and

$$\gcd\left(2^{180/3} - 1, 181\right) = 1.$$

Also,

$$\gcd\left(2^{180/5} - 1, 181\right) = 1.$$

Hence, 181 is a prime. As a curiosity, by using a high precision calculator [1] we find that $2^{60} - 1 = 115292150406846975 = 3 \cdot 3 \cdot 5 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 31 \cdot 41 \cdot 61 \cdot 151 \cdot 331 \cdot 1321$. We also have the incredible factorization $2^{180} - 1 = 1532495540865888858358347027150309183618739122183602175 = 3 \cdot 3 \cdot 3 \cdot 5 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 19 \cdot 31 \cdot 37 \cdot 41 \cdot 61 \cdot 73 \cdot 109 \cdot 151 \cdot 181 \cdot 331 \cdot 631 \cdot 1321 \cdot 23311 \cdot 54001 \cdot 18837001 \cdot 29247661$. We see that the last two factors here are larger than the number $n = 3201529$ that we used in the example, and of course we could easily check if n is a prime by other means, but the point here was to illustrate the use of the Pocklington-Lehmer test. □

6.2 GOLDWASSER-KILIAN PRIMALITY TEST

The primality test named after Goldwasser and Kilian is an analogue for elliptic curves of the Pocklington-Lehmer primality test. For the Pocklington-Lehmer test, there might be the case that we cannot find enough factors of $n - 1$ to obtain $r \geq \sqrt{n}$, so that we would not know all the prime factors l of r. If we are working with really large numbers, such as numbers with a thousand digits, this can certainly be a possibility. Note that the number $n - 1$ is the order of the group $\mathbb{Z}_n^*$, so if we use elliptic curves, we can replace $n - 1$ with a group order near n. Then there will be enough choices for the elliptic curve, so we will probably find a number that can be partially factored. This is the idea of the Goldwasser-Kilian primality test.

Theorem 6.1. *Let $n > 1$ and let E be an elliptic curve modulo n. If there exists distinct prime numbers $l_1, \ldots, l_k$ and finite points $P_i \in E(\mathbb{Z}_n)$ such that*

1. $l_i P_i = \infty$ *for* $1 \leq i \leq k$
2. $\prod_{i=1}^{k} l_i > (n^{1/4} + 1)^2$,

[1] See e.g. http://www.mathsisfun.com/calculator-precision.html

then n is prime.

Proof. Let p be a prime factor of n, where $n = p^f n_1$ with $p \nmid n_1$. Then we have that

$$E(\mathbb{Z}_n) = E(\mathbb{Z}_{p^f}) \oplus E(\mathbb{Z}_{n_1}).$$

As P_i is a finite point in $E(\mathbb{Z}_n)$, it yields a point $P_i \pmod{p^f}$, which is a finite point in $E(\mathbb{Z}_{p^f})$. We can reduce further to obtain $P_{i,p} \equiv P_i \pmod{p}$, which is a finite point in $E(\mathbb{F}_p)$. Since $l_i P_i \equiv \infty \pmod{n}$, we have that $l_i P_i = \infty$ modulo every factor of n. Further, $P_{i,p}$ has order l_i, as $l_i P_{i,p} = \infty$ in $E(\mathbb{F}_p)$. This means that $P_{i,p}$ has order l_i, as l_i is prime. Then we have that $l_1 \mid \#E(\mathbb{F}_p)$ for all i, so that $E(\mathbb{F}_p)$ is divisible by $\prod_{i=1}^{k} l_i$. This gives that

$$(n^{1/4}+1)^2 < \prod_{i=1}^{k} l_i \leq \#E(\mathbb{F}_p) < p + 1 + 2\sqrt{p} = (p^{1/2}+1)^2.$$

Thus, $p > \sqrt{n}$. But the starting assumption was that p is a prime factor of n, so we arrive at a contradiction. Hence, n is prime. □

Example 6.2. We consider $n = 1231$ and want to use the Goldwasser-Kilian test to check whether n is prime or not.

Let E be the elliptic curve given by $E : y^2 = x^3 + 5x + 607 \pmod{1231}$. Furthermore, let $l = 173$. This number can be checked to be prime by the Pocklington-Lehmer test or by checking the possible factors up to $\sqrt{173}$. We see that

$$l = 173 > (1231^{0.25} + 1)^2 \approx 47.93.$$

We have the point $P = (2, 25)$ lying on E. Calculating using MATLAB®, we get that $173P = \infty$. See Table 6.1. Then, by Theorem 6.1, $n = 1231$ is prime. □

Table 6.1: kP for some selected values of k.

P	(2, 25)
2P	(36, 899)
3P	(380, 251)
4P	(702, 58)
5P	(485, 777)
⋮	⋮
171P	(36, 332)
172P	(2, 1206)
173P	(∞, ∞)
174P	(2, 25)
175P	(36, 899)

As we know that 1231 is prime, we can use that to find new primes. We see that $l = 1231 > (1349846^{0.25} + 1)^2 \approx 1230.999948$. Thus if we can find an elliptic curve modulo some $n \leq 1349846$, with a point P on the curve where $1231P = \infty$, then n will be prime.

Chapter 7

ZETA FUNCTIONS

In this chapter we will see a connection between elliptic curves and the famous Riemann hypothesis.

Let E be an elliptic curve over a finite field $\mathbb{F}_p$, and let $N_n = \#E(\mathbb{F}_{p^n})$ be the number of points on E over the field $\mathbb{F}_{p^n}$. We define the *Z-function* of E to be

$$Z_E(T) = \exp\Big(\sum_{n=1}^{\infty} \frac{N_n}{n} T^n\Big), \tag{7.1}$$

where $\exp(t) = \sum_{n=0}^{\infty} \frac{t^n}{n!}$ is the usual exponential function.

Proposition 7.1. *Let E be an elliptic curve defined over $\mathbb{F}_p$, and let $\#E(\mathbb{F}_p) = p + 1 - a$. Then*

$$Z_E(T) = \frac{pT^2 - aT + 1}{(1-T)(1-pT)}. \tag{7.2}$$

Proof. We factor $X^2 - aX + p = (X - \alpha)(X - \beta)$. Then Theorem 5.3 says that $N_n = \#E(\mathbb{F}_{p^n}) = p^n + 1 - (\alpha^n + \beta^n)$. We use the expansion $-\log(1-t) = \sum_n \frac{t^n}{n}$ to obtain

$$\begin{aligned}
Z_E(T) &= \exp\Big(\sum_{n=1}^{\infty} \frac{N_n}{n} T^n\Big) \\
&= \exp\Big(\sum_{n=1}^{\infty} (p^n + 1 - \alpha^n - \beta^n)\frac{T^n}{n}\Big) \\
&= \exp\Big(-\log(1-pT) - \log(1-T) + \log(1-\alpha T) + \log(1-\beta T)\Big) \\
&= \exp\left(\log\left(\frac{(1-\alpha T)(1-\beta T)}{(1-T)(1-pT)}\right)\right) \\
&= \frac{(1-\alpha T)(1-\beta T)}{(1-T)(1-pT)} \\
&= \frac{\alpha\beta T^2 - (\alpha+\beta)T + 1}{(1-T)(1-pT)} \\
&= \frac{pT^2 - aT + 1}{(1-T)(1-pT)},
\end{aligned}$$

which completes the proof. □

Example 7.1. Let E be the elliptic curve $y^2 = x^3 + 2x + 1$ over $\mathbb{F}_7$, as in Example 5.3 and 5.4. We found that $\#E(\mathbb{F}_7) = 5$ and $a = p + 1 - \#E(\mathbb{F}_p) = 7 + 1 - 5 = 3$. This gives that

$$\begin{aligned} Z_E(T) &= \frac{pT^2 - aT + 1}{(1-T)(1-pT)} \\ &= \frac{7T^2 - 3T + 1}{(1-T)(1-7T)} \end{aligned}$$

Taking $T = 5$ as an example, we obtain

$$\begin{aligned} Z_E(5) &= \exp\Big(\sum_{n=1}^{\infty} \frac{N_n}{n} 5^n\Big) \\ &= \frac{175 - 15 + 1}{(-4)(-34)} \\ &= \frac{161}{136}. \end{aligned}$$

□

We see that

$$\begin{aligned} Z_E(T) &= \frac{pT^2 - aT + 1}{(1-T)(1-pT)} \\ &= \frac{pT^2 - aT + 1}{pT^2 - (p+1)T + 1}. \end{aligned}$$

This means that $Z_E(T)$ is always larger than 1. For $Z_E(T)$ to be equal to 1, we would need that $a = p + 1$, but that would require that $\#E(\mathbb{F}_p) = 0$, which is impossible (the point ∞ is always in the set). We have that

$$\#E(\mathbb{F}_p) \geq 1 \implies (p+1) - a \geq 1,$$

so that the numerator is always bigger that the denominator, and hence $Z_E(T) > 1$.

We will now look at the analogue of the Riemann zeta function for elliptic curves, starting with the following definition.

Definition 7.1. Let E be an elliptic curve over a finite field. The *zeta function* of E is defined to be

$$\zeta_E(s) = Z_E(p^{-s}), \tag{7.3}$$

where $s \in \mathbb{C}$. □

This zeta function can be regarded as an analogue of the Riemann zeta function

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

Well-known values for $\zeta(s)$ is $\zeta(1) = \infty$, which is the divergent harmonic series, and $\zeta(2) = \frac{\pi^2}{6}$, which is the so-called Basel problem, solved by the prolific mathematician Leonhard Euler in 1735.

The Riemann zeta function satisfies a functional equation which relates the values at s and $1 - s$, given by

$$\pi^{-s/2}\Gamma(s/2)\zeta(s) = \pi^{-(1-s)/2}\Gamma((1-s)/2)\zeta(1-s).$$

Here $\Gamma(t)$ is the standard gamma function, defined by

$$\Gamma(t) = \int_0^{\infty} x^{t-1}e^{-x}\,\mathrm{d}x.$$

When $t \in \mathbb{N}$, we have that $\Gamma(t) = (t-1)!$. When the function argument is a positive half-integer, the function values are given by

$$\Gamma\left(\frac{t}{2}\right) = \sqrt{\pi}\,\frac{(t-2)!!}{2^{(t-1)/2}}.$$

The double factorial is defined as the product of all odd integers up to a given odd integer n. For instance, $7!! = 1 \cdot 3 \cdot 5 \cdot 7 = 105$. Also $0!! = 1$ by definition. We see that $\Gamma\left(\frac{1}{2}\right) = \sqrt{\pi}$, which is a commonly used value. There are no simple expressions known for the values at rational points in general.

There exists "trivial" zeros for the Riemann zeta function when $s = -2n$, where $n \in \mathbb{N}$, given in terms of the Bernoulli numbers. They are trivial in the sense that their existence is relatively easy to prove (with functional equations). It is a known fact that any non-trivial zero must lie in the so-called *critical strip* $\{s \in \mathbb{C} \mid 0 < \mathrm{Re}(s) < 1\}$. One of the greatest unsolved problems in mathematics, and one of the Millenium Prize Problems, is the *Riemann hypothesis*. The hypothesis says that any non-trivial zero has $\mathrm{Re}(s) = 1/2$. This is verified for the first 10^{13} zeros. The set $\{s \in \mathbb{C} \mid \mathrm{Re}(s) = 1/2\}$ is called the *critical line*.

If the Riemann hypothesis is true, it shows some remarkable properties regarding the distribution of primes. It is shown that it gives the best possible bound for the error term in the prime number theorem (which says that $\pi(x) \sim x/\ln x$), which is closely related to the position of the zeros. If the Riemann hypothesis is true, it shows that the primes are distributed as good and evenly as possible. The great significance that the Riemann hypothesis has for mathematics is illustrated by the following little anecdote: The great mathematician David Hilbert was once asked what his first question would be if he had awakened after having slept for a thousand years.

His reply was immediate: "*Has the Riemann hypothesis been proven?*"

The analogue statement of the Riemann hypothesis for elliptic curves is given by the following.

Theorem 7.1. *Let E be an elliptic curve defined over a finite field, where $s \in \mathbb{C}$. Then*
1. $\zeta_E(s) = \zeta_E(1-s)$.
2. *If $\zeta_E(s) = 0$, then $Re(s) = 1/2$.*

Proof. 1. We have, by Proposition 7.1, that

$$\begin{aligned}\zeta_E(s) = Z_E(p^{-s}) &= \frac{p^{1-2s} - ap^{-s} + 1}{(1-p^{-s})(1-p^{1-s})} \\ &= \frac{p^{2s-1} - ap^{s-1} + 1}{(1-p^{s-1})(1-p^s)} \\ &= Z_E(p^{-(1-s)}) = Z_E(p^{s-1}) = \zeta_E(1-s).\end{aligned}$$

2. The numerator of $Z_E(T)$ is $(1-\alpha T)(1-\beta T)$, so that $\zeta_E(s) = 0 \iff p^s = \alpha$ or β. We have that $(X-\alpha)(X-\beta) = X^2 - aX + p$. The quadratic formula then gives

$$\alpha, \beta = \frac{a \pm \sqrt{a^2 - 4p}}{2}.$$

By Hasse's theorem, $|a| \leq 2\sqrt{p}$. This gives that the discriminant is $a^2 - 4p \leq 0$. Hence, α and β are complex conjugates of each other, and so $|\alpha| = |\beta| = \sqrt{p}$. Now, if $p^s = \alpha \vee \beta$, then $p^{\mathrm{Re}(s)} = |p|^s = \sqrt{p}$. In other words, $\mathrm{Re}(s) = 1/2$. □

The truth of this analogue statement is regarded as the strongest argument for the validity of the Riemann hypothesis.

Example 7.2. Continuing from Example 7.1, we had that

$$Z_E(T) = \frac{pT^2 - aT + 1}{pT^2 - (p+1)T + 1},$$

where $p = 7$ and $a = 3$. Then we have that

$$\zeta(s) = Z_E(7^{-s}) = \frac{7 \cdot (7^{-s})^2 - 3 \cdot (7^{-s}) + 1}{7 \cdot (7^{-s})^2 - 8 \cdot (7^{-s}) + 1},$$

so $\zeta(s) = 0$ when $7 \cdot 7^{-2s} - 3 \cdot 7^{-s} + 1 = 0$.

This equation can be solved by elementary operations by considering angles in the complex plane and solve by well-known identities. Using WolframAlpha® to calculate[1], we find a zero for $\zeta(s)$ when $s = 0.5 + 3.72637i$. Other zeros can also be found, each having real part $1/2$. □

Only the future will tell whether the Riemann hypothesis will be proven to be true or not. We end this text by the following quote from the Norwegian number theorist Atle Selberg: "*If*

[1] See www.wolframalpha.com

anything at all in our universe is correct, it has to be the Riemann Hypothesis, if for no other reasons, so for purely esthetical reasons."

Bibliography

[1] Lawrence C. Washington, *Elliptic curves - Number Theory and Cryptography*. Taylor & Francis Group, Second Edition, 2008.

[2] Joseph H. Silverman and John Tate, *Rational Points on Elliptic Curves*. Springer Verlag New York Inc., First Edition, 1992.

[3] Matthew England, MSc dissertation *Elliptic Curve Cryptography*, 2006. [Online] Available: http://www.cs.bath.ac.uk/ me350/Publications/Matthew_England_MSc_Dissertation.pdf [Accessed 04 June 2014]

[4] Michael Pemberton, MSc dissertation *Elliptic Curves and Their Applications in Cryptography*, 2009. [Online] Available: https://mospace.umsystem.edu/xmlui/bitstream/handle/10355/5364/research.pdf?sequence=3 [Accessed 04 June 2014]

[5] Sonia Balagopalan, MSc dissertation *Elliptic Curves Over Finite Fields*, 2009. [Online] Available: http://eprints.nuim.ie/2250/1/SB_MSc.pdf [Accessed 04 June 2014]

[6] Ian Stewart and David Tall, *Algebraic Number Theory and Fermat's Last Theorem*. A K Peters, Ltd., Third Edition, 2002.