FACULTAD DE CIENCIAS

DEPARTAMENTO DE MATEMÁTICAS

MORDELL-WEIL GROUP OF AN ELLIPTIC CURVE: COMPUTATIONAL AND THEORETICAL ASPECTS OF THE TORSION SUBGROUP.

Master thesis, February 3, 2013

Fernando Sanz Ferrer

Supervised by:
Enrique González Jiménez

To everyone who know how important Mathematics are to me,
especially to my sister and my parents.

Contents

Introduction

> *"Knowing, my most esteemed friend Dionysius, that you are anxious to learn how to investigate problems in numbers, I have tried, beginning from the foundations on which the science is built up, to set forth to you the nature and power subsisting in numbers".*

A dedication from Diophantus to his friend Dionysius in the *Arithmetica* [17]. This is how *number theory* was born. Little is known about the life of Diophantus. He lived in Alexandria, Egypt, probably in the third century BC. The Arithmetica is the major work of Diophantus and the most prominent work on algebra in Greek mathematics. In this work, Diophantus showed how to solve linear equations and three different types of quadratic equations, but considered only rational solutions and he provided no general methods. The portion of the Arithmetica which is still conserved consists of the solution of 130 problems, involving both determinate and indeterminate equations, i.e., equations in one and multiple variables respectively. The method for solving the latter is now known as Diophantine analysis.

Diophantus developed his study from an algrebaic point of view, far away from the geometrical one used by other of his contemporary mathematicians. This algebraical approach led him to develop a brand new mathematical notation and symbolism: he introduced an abridged notation for frequently occurring operations and an abbreviation for the unknown and for the powers of the unknown.

We may focus on the indeterminate equations, which are the equations we are interested in, particularly in two variable equations. The simplest kind of such equations is the *linear* ones. If we have $a, b, c \in \mathbb{Q}$, then we look for rational solutions of

$$ax + by + c = 0.$$

Geometrically, this equation defines a line. We know that multiplying by the least common multiple of a, b and c, we can consider $a, b, c \in \mathbb{Z}$. Moreover, if we call $d = gcd(a, b)$ then the equation $ax + by + c = 0$ has (infinite) rational solutions if and only if $d|c$.

Diphantus did not, in his Arithmetica as we have it, treated of indeterminate equations of the first degree, but he already knew how to solve them: such equations were converted into determinate equations using change of variables.

The geometrical approach, rather than the algebraic one, to solve contruction problems prevailed for centuries. Even this geometrical approach was favored by most 16th and 17th century mathematicians, notably Pascal argued against the use of algebraic and analytical methods in geometry.

But there were the French mathematicians Viète, Descartes and Fermat whom revolutionized the conventional way of thinking about construction problems through the introduction of coordinate geometry, i.e., the study of geometry using a coordinate system and the principles of algebra and analysis. This perspective was the beginning of a new branch of mathematics known nowadays as *algebraic geometry*.

Particularly, Fermat was interested primarily in the properties of algebraic curves, those defined by Diophantine equations. In fact, by studying the Arithmetica of Diophantus, Fermat wrote his famous "Last Theorem" in the margins of his copy:

> *"If an integer n is greater than* 2*, then* $a^n + b^n = c^n$ *has no solutions in non-zero integers a, b and c. I have a truly marvelous proof of this proposition which this margin is too narrow to contain".*

It is known worldwide that this assertion was not as easy to prove as Fermat thought, and it took 300 years to get a proof by Wiles in the 1990s. We will return to this issue latter, but note that along these 300 years uncountable other discoveries have been made, and entire new fields of mathematics evolved.

We can consider now the problem of finding rational solutions of a *quadratic* polynomial in two variables with rational coefficients:

$$Ax^2 + Bxy + Cy^2 + Dx + Ey + F = 0.$$

This equation defines a conic, which geometrically is a curve that results from cutting a circle cone with a plane. So the problem becomes finding rational points on the conic.

What about the intersection of a rational line and a rational conic? Will it be true that the two points (counting multiplicities) of intersection are rational? If we consider the line and the conic given by

$$x^2 + y^2 = 1 \qquad \text{and} \qquad x - y = 0,$$

we have that the intersection points are $(1/\sqrt{2}, 1/\sqrt{2})$ and $(-1/\sqrt{2}, -1/\sqrt{2})$, which are not rational, so the answer is no.

We consider the general case, i.e., we look for the intersection of a rational conic and a rational line,

$$\begin{cases} Ax^2 + Bxy + Cy^2 + Dx + Ey + F = 0, \\ ax + by + c = 0. \end{cases}$$

By clearing x from the second equation and by replacing it in the first one, we obtain a quadratic equation with rational coefficients. So the two points of intersection will be

rational if and only if the roots of that quadratic equation are rational. However, if one of those points in the intersection is rational, then so is the other, since if a quadratic equation with rational coefficients has one rational root, then the other root is rational because the sum of the roots is the middle coefficient.

We have just seen that a conic have one rational point if and only if it has infinite rational points. In fact, if O is a point on a conic $\mathcal{C}$, there is a geometrical algorithm of getting all of the other rational points on $\mathcal{C}$. We just draw some rational line $\mathcal{L}$ and we project the conic $\mathcal{C}$ onto this line from the point O. (To project O itself onto the line, we use the tangent line to $\mathcal{C}$ at O). A line meets a conic in two points, so for every $P \in \mathcal{C}$ we get a point $Q \in \mathcal{L}$; and conversely, for every point $Q \in \mathcal{L}$ by joining it to the point O, we get a point $P \in \mathcal{C}$. (See figure 1). So we get a one-to-one correspondence between the points on the conic and the points on the line. But now we see by the remarks we have made that if the point $P \in \mathcal{C}$ has rational coordinates, then the point $Q \in \mathcal{L}$ will have rational coordinates too. And conversely, if $Q \in \mathcal{L}$ is rational, then because O is assumed to be rational, the line through P and Q meets the conic in two points, one of which is rational.

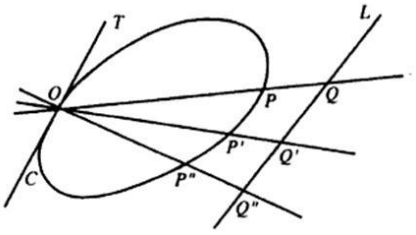


Figure 1: Rational points.

The study of some quadratic forms, in particular the question of whether a given integer can be the value of a quadratic form over the integers, dates back many centuries. One such case is Fermat's theorem on sums of two squares, which determines when an integer may be expressed in the form $x^2 + y^2$, where $x, y \in \mathbb{Z}$. This problem is related to the problem of finding Pythagorean triples, i.e., finding integer solutions for $x^2 + y^2 = z^2$, which appeared in the second millennium B.C.

In 628, the Indian mathematician Brahmagupta wrote *Brahmasphutasiddhanta* which includes, among many other things, a study of equations of the form $x^2 - ny^2 = c$. In particular, he considered what is now called Pell's equation, $x^2 - ny^2 = 1$, and found a method for its solution. In Europe this problem was studied by Brouncker, Euler and Lagrange along the 17th and 18th centuries.

In 1801, Gauss published *Disquisitiones Arithmeticae*, a major portion of which was devoted to a complete theory of binary quadratic forms over the integers. He considered questions of equivalence and reduction and introduced composition of binary quadratic forms. These investigations of Gauss strongly influenced both the arithmetical theory of quadratic forms in more than two variables and the subsequent development of algebraic number theory, where quadratic fields are replaced with more general number fields.

Remember our original problem involving quadratic equations: how could we know if a conic has one rational point? First, let us introduce one technic definition: let K be a field, let V be a K-vectorial space with dimension n and let $q : V \to K$ be a quadratic form. We can think in q as a homogeneous polynomial of degree 2 in n variables. We say that q represents $\alpha \in K$ if there exits $v \in V$ such that $q(v) = \alpha$.

If we consider a conic in the projective space $\mathbb{P}^2$, then its equation is given by a quadratic form

$$q(x, y, z) = Ax^2 + Bxy + Cy^2 + Dxz + Eyz + Fz^2$$

defined in $\mathbb{Q}$. We can restatement the latter question and the problem of finding a rational point on a conic so it becomes deciding whether the quadratic form $q(x, y, z)$ represents 0.

In 1921, the German mathematician Hasse wrote a dissertation, under Hensel's supervision, containing the Hasse-Minkowski theorem, which answered the question:

Theorem (Hasse-Minkowski) *Let K be a number field and let q be a quadratic form in n variables with coefficients in K. Then q represents 0 if and only if q represents 0 in every completion of K.*

Minkowski showed the result for $K = \mathbb{Q}$ and Hasse generalized it.

This theorem is an example of a *Local-Global principle*, discovered originally by Hasse in the 1920s, which let us deduce global properties (the existence of rational point of a conic) from local properties (the existence of points on $\mathbb{Q}_p$ and $\mathbb{R}$). There are more local-global principles in other branches of mathematics as the Gauss-Bonnet theorem in differential geometry.

If we go back to history of algebraic geometry we can stress that the second early 19th century development would lead Riemann to the development of Riemann surfaces and that in the same period began the algebraization of the algebraic geometry through commutative algebra. The prominent results in this direction are Hilbert's basis theorem and Nullstellensatz, which are the basis of the connexion between algebraic geometry and commutative algebra.

Later, in the 20th century, van der Waerden, Zariski and Weil developed a foundation for algebraic geometry based on contemporary commutative algebra, including valuation theory and the theory of ideals.

An important class of varieties, not easily understood directly from their defining equations, are the *abelian varieties*, which are the projective varieties whose points form an abelian group. The prototypical examples are *elliptic curves*, which have a rich theory and are the object of study of the present text.

Elliptic curves are particular cases of cubic equations. A cubic in two variables has the general form:

$$Ax^3 + Bx^2y + Cxy^2 + Dy^3 + Ex^2 + Fxy + Gy^2 + Hx + Iy + J = 0.$$

A cubic is said to be rational if the coefficients of its equation are rational numbers. A famous example is $x^3 + y^3 = 1$, or, in homogeneous form, $x^3 + y^3 = z^3$. To find rational solutions of $x^3 + y^3 = 1$ amounts to finding integer solutions of $x^3 + y^3 = z^3$, the first non-trivial case of Fermat's Last Theorem.

We cannot use the geometric principle that worked so well for conics because a line generally meets a cubic in three points. And if we have one rational point, we cannot project the cubic onto a line, because each point on the line would then correspond to two points on the curve.

But there is a geometric principle we can use. If we can find two rational points on the curve, then we can generally find a third one. Namely, draw the line connecting the two points we have found. This will be a rational line and it meets the cubic in one more point. If we look and see what happens when we try to find the three intersections of a rational line with a rational cubic, we find that we come out with a cubic equation with rational coefficients. If two of the roots are rational, so is the third one.

When dealing with elliptic curves, this geometric argument define a "composition law", which we can represent by $\oplus$. This leads us to discover that rational points on an elliptic curve E has an abelian group structure (section 2.2), i.e., $(E, \oplus)$ forms an abelian group. Particularly, an elliptic curve E has a special element, namely $\mathcal{O}$, such that for all $P \in E$ we have $P \oplus \mathcal{O} = P$. This is not only true for rational points of E but for points lying in an arbitrary field K.

Now that we know these facts, we could naturally wonder which porperties the group $(E, \oplus)$ has. As a first approach we could try to find torsion points on E. We say that $P \in E$ is a torsion point of order m if

$$mP = P \oplus \overset{m)}{\cdots} \oplus P = \mathcal{O},$$

and the set of all torsion points on E of order m is denoted by $E[m]$. It turns out that if E is defined over a field K with $\mathrm{char}(K) = 0$, then

$$E[m] \simeq \frac{\mathbb{Z}}{m\mathbb{Z}} \oplus \frac{\mathbb{Z}}{m\mathbb{Z}}.$$

This result is proven in chapter 2.

But we could go a little bit further and wonder which structure have rational points on a elliptic curve. Dealing with this issue, Poincaré conjectured in 1901 that there exists a finite set of points that would generate all of the (possibly infinite) rational points. This was later proven, not only for rational points but for points lying on a number field, by Mordell in 1922 [55]:

Theorem (Mordell-Weil) *Let K be a number field, and let E be an elliptic curve. Then the group of points in E whose coordinates are in K is finetely generated.*

Chapter 3 is devoted to its proof.

The Mordell-Weil theorem implies that the group of points in E whose coordinates are in K, wich we write as $E(K)$, must have the following structure:

$$E(K) \simeq E(K)_{tors} \oplus \mathbb{Z}^r,$$

where $E(K)_{tors}$ is the torsion subgroup and r is called the rank of $E(K)$. Little is known about the *rank* of an elliptic curve. One conjecture dealing with the rank is that there exists elliptic curves defined over $\mathbb{Q}$ of arbitrary large rank, but it remains unproven. In fact, the highest rank of an elliptic curve that is known so far is equal to 19 and it was recently found by Elkies in 2009 [19].

Antoher conjecture, the most important one that exists nowadays about the rank of an elliptic curve, is the Birch and Swinnerton-Dyer conjecture (BSD conjecture). It status as one of the most challenging mathematical questions that has become widely recognized; the conjecture was chosen as one of the seven Millennium Prize Problems listed by the Clay Mathematics Institute in 2000. It relates arithmetic data associated to an elliptic curve E over a number field K to the behaviour of an analytic function, called the Hasse-Weil L-function, $L(E, s)$. For further information see section 3.4 below.

More information is known about the *torsion subgroup* of an elliptic curve when K is a fixed number field of low degree. Chapter 4 presents a summary of the knowledge we have to date on this issue, including the most recent discoveries due to current mathematicians like Najman, Parent, Kamienny, Stein, Stoll or Derickx.

If $K = \mathbb{Q}$ or $[K : \mathbb{Q}] = 2$ all the posibilities for the torsion subgroup $E(K)_{tors}$ are known, are finite and are established by Mazur (theorem 4.1.1) and Kamienny-Kenku-Momose (theorem 4.2.13) respectively. Results like these for number fields of higher degree remain unknown, but some information is available, like a bound for the possible prime orders of points on a elliptic curve E defined over a number field K of degree d. In fact, for $d = 3, 4, 5$ all possible prime orders are known. In other cases the bound known depends only on d.

As Mazur's theorem establish all the finite possibilities for $E(\mathbb{Q})_{tors}$, the question now is the following: given an elliptic curve E defined on $\mathbb{Q}$, find $E(\mathbb{Q})_{tors}$. Four algorithms used nowadays to determine $E(\mathbb{Q})_{tors}$ are given in detail in chapter 5.

- **Lutz-Nagell algorithm** (section 5.2). A theorem due to Lutz [47] and Nagell [57], whom proved it independently in the 1930s, quite often allows a quick determination of the torsion points on an elliptic curve over $\mathbb{Q}$. A proof of this theorem is given in this text, see theorem 5.2.8.

- **Division polynomials algorithm** (section 5.3). Division polynomials are a poweful tool to determine wheter a point P is a m-torsion point of $E(\mathbb{Q})$.

- **Tate's algorithm** (section 5.4). This algorithm is based on the fact that an elliptic curve with a point of order $m \geq 4$ can be written in a parametrical form, known as Tate's Parametrization (theorem 5.4.6).

- **Dude's algorithm** (section 5.5). Dude's algorithm obtains torsion points of an elliptic curve using an isomorphism between the curve and a quotient of $\mathbb{C}$ by a lattice Λ.

Some of the most important problems in mathematics, both solved and unsolved nowadays (like Fermat's Last Theorem -proved by Wiles in 1995- or the BSD Conjecture -still unsolved-); and some practical applications in modern technologies like cryptography involves working with elliptic curves. An overview of how elliptic curves are implied in these areas is included in appendix A.

Chapter 1

Background

In this first chapter we present a compilation of basic concepts from commutative algebra, algebraic geometry and (algebraic) number theory. These concepts are supposed to be well-known by the reader, because of that we omit most of the proofs. The aim of this chapter is to make the present text as self-contained as possible. If the reader wants to deepen into some topic of this chapter you can consult some basic references in commutative algebra [2], algebraic geometry [27], algebraic curves [25] and algebraic number theory [54].

1.1 Affine Sets

Definition 1.1.1 (Algebraic Set and Hypersurface) Let K be a field. We define the set of K-rational points of $\mathbb{A}^n$ as

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

If we consider a set $S \subset K[x_1, \ldots, x_n]$, the **(affine) algebraic set** defined by S is

$$V(S) := \{P \in \mathbb{A}^n(K) : f(P) = 0 \; \forall f \in S\}$$

Particularly, if S is a principal ideal, $S = (f)$, we say that $V(S) = V(f)$ is a **hypersurface**.

Definition 1.1.2 (Ideal) Let $X \subset \mathbb{A}^n(K)$ be a set not necessarily algebraic. The **ideal associated to** X is the set

$$\mathcal{I}(X) := \{f \in K[x_1, \ldots, x_n] : f(P) = 0 \; \forall P \in X\}.$$

Remark 1.1.3. We have the next two properties:

- If V is an algebraic set, then $V(\mathcal{I}(V)) = V$.
- Generally, $\mathcal{I}(V(I)) \neq I$ although I is an ideal associated to an algebraic set.

Definition 1.1.4 (Radical of an ideal) Let R be a ring and let $I \subset R$ be an ideal. We define the **radical of** I as the set

$$rad(I) = \sqrt{I} := \{f \in R : \exists n \in \mathbb{Z}_{>0} \text{ with } f^n \in I\}.$$

Theorem 1.1.5 (Nullstellensatz) *Let $\overline{K}$ be an algebraically closed field and let $J \subset \overline{K}[x_1, \ldots, x_n]$ be an ideal. Then*

$$\mathcal{I}(V(J)) = \sqrt{J}.$$

This theorem let us set the following bijection

$$\{\text{Algebraic subsets in } \mathbb{A}^n(\overline{K})\} \longleftrightarrow \{\text{Radical ideals in } \overline{K}[x_1, \ldots, x_n]\}$$

Theorem 1.1.6 (Hilbert's Basis Theorem) *If R is a noetherian ring, then $R[x]$ is a noetherian ring as well.*

As ideals in a noetherian ring are finitely generated, the previous theorem tells us that we just need a finite number of equations to describe an (affine) algebraic set.

We can define a topology on $\mathbb{A}^n(K)$ defining the closed sets as the (affine) algebraic sets. This topology is known as **Zariski topology**.

Definition 1.1.7 (Irreducible affine set) Let $V \subseteq \mathbb{A}^n_K$ be a nonempty algebraic set. We say that V is **irreducible** if whenever we write V as $V = V_1 \cup V_2$ with V_1, V_2 closed sets, then either $V = V_1$ or $V = V_2$.

Theorem 1.1.8 (Decomposition Theorem) *Let $V \subset \mathbb{A}^n(K)$ be an algebraic set. Then:*

- *We can write $V = V_1 \cup \cdots \cup V_r$ with each V_i irreducible for $i = 1, \ldots, r$.*
- *Furthermore, if every V_i is different (particularly if $V_i \nsubseteq V_j$ for any i, j), then the sets $V_1, \ldots, V_r$ are unique and are called* **irreducible components** *of V.*

1.2 Projective Varieties

In this section, we recall the concept of projective space and define (projective) algebraic sets, which we will use to define a (projective) algebraic variety and (projective) algebraic curve. This sort of structure will be given by homogeneous polynomials. In the end of this section we define and characterize singular points of an algebraic variety.

Definition 1.2.1 (Projective Space, $\mathbb{P}^n(K)$) Let K be a field. We define the **projective n-space over** K as the set of $(n+1)$-tuples

$$\mathbb{P}^n(K) := \{[a_0 : \ldots : a_n] \neq 0 : a_i \in K\}/\sim,$$

where $\sim$ is an equivalence relation defined by:

$$[a_0 : \ldots : a_n] \sim [b_0 : \ldots : b_n] \overset{df}{\iff} \exists \lambda \in K, \lambda \neq 0, \text{ such that } a_i = \lambda b_i \ \ \forall i = 0, \ldots, n.$$

Definition 1.2.2 (Homogeneous Polynomial and Ideal) We say that a polynomial $F \in K[x_0, \ldots, x_n]$ is **homogeneous of degree** d if every monomial of its has degree d.

An ideal $I \subset K[x_0, \ldots, x_n]$ is **homogeneous** if it is generated by homogeneous polynomials.

Remark 1.2.3. Let I be a homogeneous ideal. It does not imply that every $F \in I$ is homogeneous. For example, if we consider $(x, y) \subset K[x, y]$ we have that (x, y) is a homogeneous ideal, but $F = x + y^2$ is not a homogeneous polynomial, even if $F \in (x, y)$.

Does homogeneous polynomials define functions? Let us cosider the next example.

Example 1.2.4 Let $F \in \overline{\mathbb{Q}}[x_0, x_1]$ given by $F(x_0, x_1) = x_0^2 + x_1^2$. We consider the point $P = [1 : 1] = [2 : 2] = Q \in \mathbb{P}^1(\overline{\mathbb{Q}})$. Then $F(P) = 2 \neq 8 = F(Q)$. So, F is not well-defined on $\mathbb{P}^1(\overline{\mathbb{Q}})$, i.e., the value of $F(P)$ depends on the choice of the homogeneous coordinates for P.

Despite this fact, it make sense to ask whether a homogeneous polynomial vanishes, $F(P) = 0$, since the answer is independent of the choice of P. Suppose that $F \in K[x_0, \ldots, x_n]$ is homogeneous of degree d and let $[a_0 : \ldots : a_n] \sim [b_0 : \ldots : b_n]$ be a point on $\mathbb{P}^n(K)$ with $F(a_0, \ldots, a_n) = 0$. Then

$$F(b_0, \ldots, b_n) = F(\lambda a_0, \ldots, \lambda a_n) = \lambda^d F(a_0, \ldots, a_n) = 0 \text{ for all } \lambda \in K.$$

We can now define a projective algebraic set:

Definition 1.2.5 (Algebraic Projective Set) Let $\mathcal{P} \subset K[x_0, \ldots, x_n]$ be a set of homogeneous polynomials. We define the **algebraic (projective) set** associated with $\mathcal{P}$ as the set:

$$V(\mathcal{P}) := \{P \in \mathbb{P}^n(K) : F(P) = 0 \ \forall F \in \mathcal{P}\}.$$

Particularly, if $I \subset K[x_0, \ldots, x_n]$ is a homogeneous ideal,

$$V(I) := \{P \in \mathbb{P}^n(K) : F(P) = 0 \ \forall F \in I, \ F \text{ is homogeneous}\}.$$

Notation. If the algebraic projective set V is defined over the field K we write V/K.

Theorem 1.2.6 (Projective Nullstellensatz) *There exists a bijection*

$$\{\textit{Algebraic subsets of } \mathbb{P}^n(K)\}$$
$$\updownarrow$$
$$\{\textit{Radical homogeneous ideals } I \in \overline{K}[x_0, \ldots, x_n] \textit{ such that } I \not\supseteq (x_0, \ldots, x_n)\}$$

As we have defined affine and projective algebraic sets, a natural question it is whether there is a relation between them. Note that there exists a relation between the affine space and the projective space, given recursively by

$$\mathbb{P}^n = \mathbb{A}^n \cup \mathbb{P}^{n-1},$$

where the points at "infinty" ($\mathbb{P}^{n-1}$) depends on the affine chart we are working with.

The relation between affine and projective sets is given by a homogenization process for the polynomials.

Definition 1.2.7 (Homogenized/dehomogenized polynomial) Let us define:

i) Let $F \in K[x_0, \ldots, x_n]$ be a homogeneous polynomial. The **dehomogenized polynomial associated with F with respect to x_i** is

$$F_* := F(x_0, \ldots, x_{i-1}, 1, x_{i+1}, \ldots, x_n) \in K[x_0, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n].$$

ii) Let $f \in K[x_1, \ldots, x_n]$, $f \neq 0$ be a polynomial of degree d. The **homogenized polynomial associated with f** is

$$f^* := x_0^d \cdot f\left(\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0}\right).$$

The homogenization/dehomogenization process behaves as follows:

$$\begin{array}{ccc} \text{Projective Part} & & \text{Affine Part} \\ V \overset{alg.}{\subset} \mathbb{P}^n & \overset{dehomog.}{\longrightarrow} & V \cap \mathbb{A}^n \\ \mathbb{P}^n \supset \overline{V} & \overset{homog.}{\longleftarrow} & V \subset \mathbb{A}^n \subset \mathbb{P}^n \end{array}$$

where $\overline{V}$ is the projective closure of V on Zariski topology of $\mathbb{P}^n$, i.e., $\overline{V}$ is the projective algebraic set whose homogeneous ideal $I(\overline{V})$ is generated by

$$\{f^* : f \in I(V)\}.$$

It is natural to wonder whether the previous process is bijective, i.e.,

- If $V \overset{alg.}{\subset} \mathbb{P}^n$ then $V = \overline{V \cap \mathbb{A}^n}$?
- If $V \overset{alg.}{\subset} \mathbb{A}^n$ then $V = \overline{V} \cap \mathbb{A}^n$?

The following proposition answers this question.

Proposition 1.2.8 *We have the following results:*

i) (Affine part of a projective set)
Let $V \subset \mathbb{P}^n$ be an algebraic set. We define

$$I_* := \langle F_* : F \in I(V) \text{ is homogeneous } \rangle; \qquad V_* := V(I_*) \subset \mathbb{A}^n.$$

Then, $V_* = V \cap \mathbb{A}^n$.

ii) (Projective closure of an affine algebraic set)
Let $V \in \mathbb{A}^n$ an algebraic set. We define

$$I^* := \langle f^* : f \in I(V) \rangle; \qquad V^* := V(I^*) \subset \mathbb{P}^n.$$

Then, $V^* = \overline{V}$.

iii) (The homogenization-dehomogenization process is bijective)
Let $V \subset \mathbb{A}^n$ be an affine algebraic set. Then $\overline{V} \cap \mathbb{A}^n = V$. Furthermore, if V is irreducible, then $\overline{V}$ is irreducible as well.

iv) (The dehomogenization-homogenization process is bijective for irreducible sets)
Let $V \subset \mathbb{P}^n$ be a projective irreducible set, then either $V \cap \mathbb{A}^n = \emptyset$, or $V \cap \mathbb{A}^n$ is irreducible. In the last case, we have $\overline{V \cap \mathbb{A}^n} = V$.

There are some projective algebraic sets which are of particular importance:

Definition 1.2.9 (Projective Variety) Let K be a field. We call **(algebraic) projective variety defined over** K to every algebraic irreducible projective set, $V \subseteq \mathbb{P}^n(K)$.

We define now the concept of singular point of a projective variety. The definition given here is actually a characterization of the set of singular points on projective hypersurfaces, i.e., it is not a formal definition, but is all we need to develop the theory further.

Definition 1.2.10 (Singular Point) Let F be a homogeneous polynomial in $K[x_0, \ldots, x_n]$, and let $V := V(F) \subset \mathbb{P}^n(K)$ be an algebraic projective variety. We say that a point $P \in V$ is **singular** if

$$\frac{\partial F}{\partial x_0}(P) = \frac{\partial F}{\partial x_1}(P) = \cdots = \frac{\partial F}{\partial x_n}(P) = 0.$$

Otherwise, we say that P is **nonsingular** or **smooth**.

Further, we say that V is **smooth** if every $P \in V$ is a smooth point.

1.3 Maps Between Projective Varieties

In this section we will see some different sort of maps between projective varieties and some important results.

Definition 1.3.1 (Rings and fields of functions) We have the following definitions:

i) Let $V \subseteq \mathbb{A}^n(K)$ be an algebraic set. We define the **affine coordinate ring of** V as

$$K[V] := K[x_1, \ldots, x_n]/\mathcal{I}(V).$$

ii) Moreover, if $V \subseteq \mathbb{A}^n(K)$ is irreducible, the **function field associated to affine coordinate ring of** V is

$$K(V) := Frac(K[V]).$$

iii) Let $V \subseteq \mathbb{P}^n(K)$ be a projective variety. We define the **projective coordinate ring of** V as

$$K[V] := K[x_0, \ldots, x_n]/\mathcal{I}(V).$$

iv) The **function field of** V is defined by

$$K(V) := \left\{ \frac{F}{G} : F, G \in K[x_0, \ldots, x_n] \text{ homogeneous, } \deg F = \deg G, G \notin \mathcal{I}(V) \right\}.$$

v) Let $V \subseteq \mathbb{P}^n(K)$ and let $P \in V \cap \mathbb{A}^n$ for some affine chart. We define the **local ring of** V **in** P as:

$$\begin{aligned} \mathcal{O}_P &:= K[V]_P \\ &= K[V \cap \mathbb{A}^n]_P \\ &= \{F/G \in K(V) : G(P) \neq 0\} \\ &= \{f/g \in K(V \cap \mathbb{A}^n) : g(P) \neq 0\}. \end{aligned}$$

Remark 1.3.2. We have $G \notin \mathcal{I}(V)$ in statement (iv) of the latter definition, but it may exists $P \in V$ such that $G(P) = 0$. This sort of points are called **poles** and they are said to be "at infinity".
Moreover, $\mathcal{O}_P$ is a local ring if P is smooth.

These definitions let us define the dimension of a projective variety as follows:

Definition 1.3.3 (Dimension of a projective variety) Let $V \subseteq \mathbb{P}^n(K)$ be a projective variety. We choose a chart such that $\mathbb{A}^n \cap V \neq \emptyset$ and define the **dimension** of V as

$$dim(V) := deg.tr.(\overline{K}(V))$$

where "*deg.tr.*" is the transcendence degree of the field extention $\overline{K}(V)/\overline{K}$.

If $P \in V$, we define

$$M_P := \{f \in \overline{K}[V] : f(P) = 0\}, \tag{1.1}$$

that is the maximal ideal of $\overline{K}[V]$, since the map

$$\overline{K}[V]/M_P \longrightarrow \overline{K}; \qquad f \mapsto f(P)$$

is an isomorphism.

And, finally, we can define an algebraic curve:

Definition 1.3.4 ((Projective) Algebraic curve) A **(projective) algebraic curve** is a projective variety of dimension 1.

The following theorem assures that we have always poles in functions defined over an algebraic curve.

Theorem 1.3.5 *Let $C \subset \mathbb{P}^n$ be an algebraic curve and let $f : C \longrightarrow \mathbb{P}^1$. Then, either $f(C)$ is constant or $f(C) = \mathbb{P}^1$.*

Definition 1.3.6 (Rational map) Let $V_1 \subseteq \mathbb{P}^m$ and $V_2 \subseteq \mathbb{P}^n$ two projective varieties. A **rational map** between them, $\varphi : V_1 \longrightarrow V_2$, is $\varphi = [f_1, \ldots, f_n]$ where $f_i \in \overline{K}(V_1)$ such that $\exists i_0$ with $f_{i_0} \neq 0$ and such that if $P \in V_1$, then every $f_i \in \mathcal{O}_P$ and at least $f_i(P) \neq 0$ for some i.

Definition 1.3.7 (Regular map) Let $V_1 \subseteq \mathbb{P}^m$ and $V_2 \subseteq \mathbb{P}^n$ two projective varieties. A **map** between them, $\varphi : V_1 \longrightarrow V_2$, is said to be **regular at** P or to be **defined in** P if $\exists g \in \overline{K}(V_1)$ such that:

- $gf_i \in \mathcal{O}_P \ \ \forall i = 1, \ldots, n.$
- $\exists i$ such that $gf_i(P) \neq 0$.

In other words, $\varphi = [f_1, \ldots, f_n] = [gf_1, \ldots, gf_n]$.

The most interesting maps are those which are defined in all points of a variety:

Definition 1.3.8 (Morphism between projective varieties) A rational map between projective varieties, $\varphi : V_1 \longrightarrow V_2$, is called a **morphism** if it is regular at P for all $P \in V_1$.

The following result tells us that morphisms between projective varieties are essentially unique.

Proposition 1.3.9 *Let $\varphi, \psi : X \longrightarrow Y$ be two morphisms between projective varieties. If there exists a non-empty open set $U \subseteq X$ such that $\varphi|_U = \psi|_U$, then $\varphi = \psi$.*

Definition 1.3.10 (Birational equivalence) Two projective varieties X and Y are **biracionally equivalents** if there exist rational maps $\varphi : X \to Y$ and $\psi : Y \to X$ such that $\varphi \circ \psi = id_Y$ and $\psi \circ \varphi = id_X$ as rational maps.

The following result charaterize birational equivalent varieties.

Theorem 1.3.11 *Let X and Y be two projective varieties. The following statements are equivalent*

i) X and Y are birationally equivalents.

ii) There exist nontrivial open sets $U \subset X$ and $U' \subset Y$ such that $U \simeq U'$.

iii) The function fields are isomorphic, $K(X) \simeq K(Y)$.

We may have rational maps between projective varieties whose composition is the identity but this does not mean that these two varieties are isomorphic, as we will see in the following example.

Example 1.3.12 Let $S = V(y^2z = x^3 + x^2z)$ and the following two maps:

$$S \dashrightarrow \mathbb{P}^1$$

$$(x, y, z) \longmapsto (y, x)$$

$$(t(t^2 - s^2), s(t^2 - s^2), t^3) \longmapsto (s, t)$$

It is easy to see that if we compose each map in both directions we obtain the identity map, so S is birationally equivalent to $\mathbb{P}^1$. Nevertheless, they are not isomorphic because S has a singular point, $P = [0 : 0 : 1]$, and $\mathbb{P}^1$ is smooth. Alcutally, there exist open sets of S and $\mathbb{P}^1$ which are isomorphic.

Proposition 1.3.13 *Let C be a curve, let $P \in C$ be a smooth point and let $\varphi : C \to Y$ be a rational map onto a projective variety Y. Then φ is defined on P.*

Corollary 1.3.14 *If C is a smooth curve and $\varphi : C \to Y$ is a rational map, then φ is a morphism.*

Example 1.3.15 Let C/K be a smooth curve and let $f \in K(C)$ be a function. Then f defines a rational map, which also be denote by f,

$$f : C \to \mathbb{P}^1; \qquad P \mapsto [f(P) : 1].$$

From Corollary 1.3.14, this map is actually a morphism. It is given explicity by

$$f(P) = \begin{cases} [1 : 0], & \text{if } f \text{ has a pole at } P, \\ [f(P) : 1], & \text{if } f \text{ is regular at } P. \end{cases}$$

Proposition 1.3.16 *Let X, Y be two projective varieties and let $\varphi : X \to Y$ be a morphism between them. Then φ is closed, i.e., it takes closed sets into closed sets.*

Proposition 1.3.17 *Let $\phi : C_1 \to C_2$ be a map of degree one (see definition 1.5.4) between two smooth curves. Then ϕ is an isomorphism.*

1.4 Discrete valuation rings

Definition 1.4.1 (Discrete valuation) Let K be a field. A **discrete valuation** on K is a map $v : K \to \mathbb{Z}$ such that:

- $v(xy) = v(x) + v(y)$,
- $v(x + y) \geq \min\{v(x), v(y)\}$,

- $v(0) =$ " $+\infty$" (by definition).

The pair (K, v) is called a **discrete valuation field**.

If we have a map $v : K \to \mathbb{R}$ with the same properties as above, we say that v is a **nondiscrete valuation** or just a **valuation** on K.

Definition 1.4.2 (Equivalent valuations) Two valuations v_1 and v_2 are **equivalent** on K if there exists $s \in \mathbb{R}^+$ such that $v_1 = sv_2$.

Definition 1.4.3 (Discrete Valuation Ring, DVR) Let (K, v) be a discrete valuation field. We define its associated **discrete valuation ring** as

$$A_v := \{k \in K : v(k) \geq 0\}.$$

So defined, A_v is a local ring with maximal ideal $\mathcal{M}_v := \{k \in K : v(k) > 0\}$. As, in particular, every DVR is a principal ideal domain (PID) the maximal ideal is generated by one element. This element is so important that we are going to give it a name.

Definition 1.4.4 (Uniformizer) Suppose that $\mathcal{M}_v = (t)$. Then the element t is called **uniformizer**. Another way of defining it is as an element $t \in A_v$ such that $v(t)$ is minimum in $v(K) \cap \mathbb{Z}_{\geq 0}$.

Moreover, if t is a uniformizer and $x \in A_v$ it holds that $v(t)|v(x)$, so we can suppose that the valuation of a uniformizer is always 1. If not, since the image of the valuation v is a subgroup of $\mathbb{Z}$, namely $v(t)\mathbb{Z}$, we can 'normalize' the valuation v defining $\tilde{v}$ as

$$\tilde{v}(x) = \frac{v(x)}{v(t)}.$$

Proposition 1.4.5 *If A is a PID then the following statements are equivalent:*

i) A has exactly a nonzero prime ideal.

ii) Except for multiplication by units, A has exactly one prime element.

iii) A is a local ring which is not a field.

Particularly, if A is a DVR the statements above hold. It is very important to emphasize that if A is a DVR with uniformizer t, then every element $a \in A$ can be written uniquely as

$$a = ut^m,$$

where u is a unit in A, i.e., $u \in \mathcal{U}(A)$; and $m \in \mathbb{Z}_{\geq 0}$.

Theorem 1.4.6 *Let C be a projective curve.*

$$P \in C \text{ is smooth} \iff \mathcal{O}_P \text{ is a DVR.}$$

Example 1.4.7 (Local ring of rational functions) Let C be a projective algebraic curve and let $P \in C$ be a smooth point. We know that if $t_P \in \mathcal{O}_P$ is a uniformizer, then any element on the local ring of rational functions in P, $f \in \mathcal{O}_P$, can be written uniquely as

$$f = ut_P^m,$$

where u is an invertible element and m is a nonnegative integer.

In fact, if t_P is a uniformizer and we restrict the valuation (originally defined on the field of functions) to the local ring (see the following example 1.4.8) , we have that $ord_P(t) = 1$. This means that every uniformizer on $\mathcal{O}_P$ has a simple zero and no poles at P.

Example 1.4.8 (The ord_P valuation) Let C be a curve and let $P \in C$ a smooth point on C. We define the ord_P valuation on $\mathcal{O}_P$ as follows:

$$ord_P : \mathcal{O}_P \longrightarrow \{0, 1, 2, \ldots\} \cup \{\infty\}; \qquad f \mapsto ord_P(f) := \sup\{d \in \mathbb{Z} : f \in M_P^d\},$$

where M_P is the maximal ideal defined in expression 1.1.

This valuation can be extended to a valuation on the rational function field $\overline{K}(C)$ as follows: let $F \in \overline{K}(V)$, then $F = f/g$ with $f, g \in \mathcal{O}_P$. Then

$$ord_P(F) = ord_P(f) - ord_P(g) = \#\{\text{Zeros of } F \text{ at } P\} - \#\{\text{Poles of } F \text{ at } P\}$$

Given one point P and a pair of functions $f, g \in K(V)$ it is clear that the latter expression defines a valuation.

Example 1.4.9 (The p-adic valuation) Let $K = \mathbb{Q}$ and let p a prime number. We define the **p-adic valuation** on $\mathbb{Q}$ as follows:

If $x \in \mathbb{Q}$, we write $x = p^n \dfrac{a}{b}$, where $\gcd(p, a) = 1 = \gcd(p, b)$ and the $n \in \mathbb{Z}$ is unique. Then

$$v_p(x) := n,$$

is a valuation defined on $\mathbb{Q}$.

1.5 Some properties of maps between curves

In this section we present some useful results about maps between curves.

Proposition 1.5.1 *Let C_1 and C_2 be two projective curves defined over a field K and let $f : C_1 \to C_2$ be a nonconstant rational map. Then f is surjective.*

PROOF. By theorem 1.3.11, we have that f is actually a morphism; and by proposition 1.3.16, f is closed, thus $f(C_1)$ is a closed set in C_2 and therefore f is surjective.

□

Moreover, the composition with f induces an injection of function fields fixing K:

$$\begin{aligned} f^* : K(C_2) &\to K(C_1) \\ \phi &\mapsto f^*(\phi) = \phi \circ f. \end{aligned}$$

Theorem 1.5.2 *i) Let C_1 and C_2 be curves over a field K and let $f : C_1 \to C_2$ a nonconstant map defined over K. Then $K(C_1)$ is a finite extension of $f^*K(C_2)$.*

ii) Let $\iota : K(C_2) \to K(C_1)$ be an injection of function fields fixing K. Then there exists a unique nonconstant map $f : C_1 \to C_2$ defined over K such that $f^* = \iota$.

PROOF.

i) See [28, II.6.8]

ii) Let $C_2 \subset \mathbb{P}^n(K)$ and for each i, let $g_i \in K(C_2)$ be the function on C_2 corresponding to X_i/X_0. We assume that C_2 is not contained on the hyperplane $X_0 = 0$, relabeling if necessary. Then,

$$f = [1, \iota(g_1), \ldots, \iota(g_n)]$$

gives a map $f : C_1 \to C_2$ with $f^* = \iota$:

Let $h \in K(C_2)$ and $P \in C_1$,

$$\begin{aligned} f^*h(P) &= (h \circ f)(P) \\ &= h([1, \iota(g_1)(P), \ldots, \iota(g_n)(P)]) \\ &= h([\iota(1), \iota(g_1)(P), \ldots, \iota(g_n)(P)]) \\ &= h(\iota([1, g_1(P), \ldots, g_n(P)])) \\ &= (h \circ \iota)([1, g_1(P), \ldots, g_n(P)]) \\ &= \iota(h(P)) \end{aligned}$$

Note that f is not constant, since g_i's cannot be all constant and ι is injective. Finally, if $\hat{f} = [f_0, \ldots, f_n]$ is another map with $\hat{f}^* = \iota$, then for each i, we take

$$f_i/f_0 = \hat{f}^* g_i = f^* g_i = \iota(g_i),$$

which shows that $\hat{f} = f$.

□

Definition 1.5.3 (Ramification Index) Let C_1 and C_2 be two smooth curves defined over a field K, let $f : C_1 \to C_2$ be a nonconstant map and let $P \in C_1$. The **ramification index of f at P** is given by

$$e_f(P) = ord_P(t_{f(P)} \circ f)$$

where $t_{f(P)}$ is a uniformizer at $f(P)$. Note that $e_f(P) \geq 1$. We say that f is **unramified at P** if $e_f(P) = 1$; and f is **unramified** if it is unramified at every point $P \in C_1$.

Definition 1.5.4 (Degree of a map) Let $f : C_1 \to C_2$ be a map between two curves defined over K. If f is constant, we define $\deg f = 0$; otherwise we say that f is finite and define its **degree** by

$$\deg f := [K(C_1) : f^*K(C_2)].$$

The context in which we are working, the extension $K(C_1)/f^*K(C_2)$ will be always separable, so f will be always a separable map as well.

Proposition 1.5.5 *For all $P \in C_2$ we have that $\deg f = \#f^{-1}(P)$, counting multiplicities.*

Note that this proposition tells us that if C is a smooth curve and $\varphi : C \to \mathbb{P}^1$ is a morphism, then $\#\{\text{Zeros of } \varphi\} = \#\{\text{Poles of } \varphi\}$, since $\deg(\varphi) = \#\varphi^{-1}(0) = \#\varphi^{-1}(\mathcal{O})$.

Proposition 1.5.6 *Let $f : C_1 \to C_2$ be a nonconstant map between smooth curves.*

i) For every $Q \in C_2$,

$$\sum_{P \in f^{-1}(Q)} e_f(P) = \deg f.$$

ii) For all but finitely many $Q \in C_2$,

$$\#f^{-1}(Q) = \deg f.$$

iii) Let $g : C_2 \to C_3$ be a nonconstant map. Then for all $P \in C_1$,

$$e_{g\circ f}(P) = e_f(P)e_g(f(P)).$$

PROOF.

i) See [28, II.6.9]

ii) See [28, II.6.8]

iii) Let $t_{f(P)}$ and $t_{gf(P)}$ be uniformizers at $f(P)$ and $(g\circ f)(P)$ respectively. By definition of ramification index,

$$\operatorname{ord}_{f(P)}(t_{f(P)}^{e_g(f(P))}) = e_g(f(P)) \stackrel{\text{def}}{=} \operatorname{ord}_{f(P)}(t_{g(f(P))} \circ g).$$

Aplying f^* and taking orders at P yields

$$\operatorname{ord}_P(t_{f(P)}^{e_g(f(P))} \circ f) = \operatorname{ord}_P(t_{g(f(P))} \circ (g \circ f)) \;\Rightarrow\; e_f(P)e_g(f(P)) = e_{g\circ f}(P).$$

□

Remark 1.5.7. This last proposition tell us that if we have two nonconstant maps between smooth curves $C_1 \xrightarrow{f} C_2 \xrightarrow{g} C_3$ then

$$\deg(g \circ f) = (\deg g)(\deg f).$$

PROOF. On one hand we have that for every $Q \in C_3$ and for every $R \in C_2$, respectively

$$\deg g = \sum_{R \in g^{-1}(Q)} e_g(R); \qquad \deg f = \sum_{P \in f^{-1}(R)} e_f(P).$$

So if we fix $Q \in C_3$ and consider, for every $R \in g^{-1}(Q)$, the set $\mathcal{P}_R = f^{-1}(R)$, then $R = f(P)$ for every $P \in \mathcal{P}_R$, and thus

$$R \in g^{-1}(Q) \iff f(P) \in g^{-1}(Q) \iff P \in (f \circ g)^{-1}(Q)$$

Then we have

$$\begin{aligned}
(\deg f)(\deg g) &= \left(\sum_{P \in f^{-1}(R)} e_f(P) \right) \left(\sum_{R \in g^{-1}(Q)} e_g(R) \right) \\
&= \left(\sum_{P \in f^{-1}(R)} e_f(P) \right) \left(\sum_{P \in (f \circ g)^{-1}(Q)} e_g(R) \right) \\
&= \sum_{P \in (f \circ g)^{-1}(Q)} e_f(P) \cdot e_g(f(P)) \\
&= \sum_{P \in (f \circ g)^{-1}(Q)} e_{g \circ f}(P) \\
&= \deg(g \circ f).
\end{aligned}$$

□

Corollary 1.5.8 *A map $f : C_1 \to C_2$ is unramified if and only if $\#f^{-1}(Q) = \deg f$ for all $Q \in C_2$.*

PROOF. From proposition 1.5.6.i, $\#f^{-1}(Q) = \deg f$ for all $Q \in C_2$ is equivalent to

$$\sum_{P \in f^{-1}(Q)} e_f(P) = \#f^{-1}(Q).$$

But since $e_f(P) \geq 1$, this occurs if and only if $e_f(P) = 1$, it is to say, f is unramified.

□

1.6 Divisors and differentials

We now recall the divisors and differentials of a curve and their main properties. From now on, C will be a smooth projective curve.

Definition 1.6.1 (Divisor) A **divisor** of C is the following formal sum

$$D := \sum_{P \in C} n_P \cdot P,$$

where $n_P \in \mathbb{Z}$ with $n_P = 0$ for all but finitely many $P \in C$.

Moreover, given a divisor D of a curve C, we define its **support** and its **degree** as

$$\sup D := \{P \in C : n_P \neq 0\}, \qquad \deg D := \sum_{P \in C} n_P.$$

The set of divisors of a curve, denoted by $Div(C)$, is a free abelian group over the points of C. We also define

$$Div^d(C) := \{D \in Div(C) : \deg D = d\}.$$

Definition 1.6.2 (Divisor of a rational map) Let $f \in K(C)$ be a nontrivial rational map. We define its **divisor** as

$$(f) := \sum_{P \in C} ord_P(f) \cdot P.$$

Note that the degree of (f) will be always zero since the number of zeros and poles of f has to be equal by proposition 1.5.5.

Definition 1.6.3 (Principal divisors subgroup and Picard group) The set

$$Prin(C) := \{(f) : f \in K(C)\}$$

is known as **principal divisors subgroup** of C and

$$Pic(C) := Div(C)/Prin(C)$$

is called **Picard group** of C.

As $Pic(C)$ is a quotient, there exists an equivalence relation between divisors:

$$D \equiv D' \iff \exists f \in K(C) : D - D' = (f).$$

Note that $D \equiv D' \Rightarrow \deg D = \deg D'$, but it does not hold the other implication.

Furthermore, an order relation can be defined between divisors of a curve:
If $D = \sum n_P P$ and $D = \sum n'_P P$ are two divisors of C,

$$D \geq D' \overset{def}{\iff} n_P \geq n'_P \ \ \forall P \in C.$$

Example 1.6.4 *Let $char(\overline{K}) \neq 2$ and let $e_1, e_2, e_3 \in \overline{K}$ be three different elements. Let*

$$C : y^2 = (x - e_1)(x - e_2)(x - e_3).$$

It is easy to prove that C is a smooth plane cubic curve with an unique point at infinity, namely

$$P_\infty = [0 : 1 : 0].$$

Let $P_i = [e_i : 0 : 1]$ and let $F_i, G \in \overline{K}(C)$ for $i = 1, 2, 3$ defined as

$$F_i = x - e_i \overset{Hom.}{=} \frac{x - ze_i}{z}, \qquad G = y \overset{Hom.}{=} \frac{y}{z},$$

We want to find (F_i) and (G).

Let $P_0 = (x_0, y_0) \in C$ with $P_0 \neq P_1, P_2, P_3$. In $\mathcal{O}_{P_0}$ we have

$$M_{P_0} = (x - x_0, y - y_0).$$

And clearly $ord_{P_0}(F_i) = 0$ because F_i has neither zeros nor poles at P_0.

In $\mathcal{O}_{P_i}$ we have

$$M_{P_i} = (x - e_i, y), \qquad M_{P_i}^2 = ((x - e_i)^2, (x - e_i)y, y^2).$$

As we have

$$F_i = x - e_i = \frac{y^2}{(x - e_j)(x - e_k)},$$

then

$$ord_{P_i}(F_i) = ord_{P_i}(y^2) - ord_{P_i}((x - e_j)(x - e_k)) = 2 \cdot ord_{P_i}(y) - 0 = 2 \cdot 1 = 2,$$

because y is a uniformizer at P_i since it has a simple zero at it; and clearly

$$ord_{P_j}(F_i) = 0.$$

Now, by proposition 1.5.5, F_i has the same number of zeros and poles, and we have just seen that $ord_P(F_i) = 0$ for all $P \neq P_1, P_\infty$ and P_i is a double zero, thus P_∞ must be a double pole. We can write then

$$(F_i) = (x - e_i) = 2P_i - 2P_\infty.$$

On the other hand, if we let $P_0 = (x_0, y_0) \in C$ with $P \neq P_1, P_2, P_3$, then

$$ord_{P_0}(G) = ord_{P_0}\left(\frac{y}{z}\right) = 0,$$

because clearly G has no poles at P_0 and the only zeros it has are at P_1, P_2 and P_3 since

$$C \cap \{y = 0\} = \{[x : 0 : z] : \frac{(x - ze_1)(x - ze_2)(x - ze_3)}{z} = 0\} = \{P_1, P_2, P_3\}.$$

If we take a look at M_{P_i} and $M_{P_i}^2$, we can write

$$ord_{P_i}(G) = 1, \quad \text{for } i = 1, 2, 3;$$

and using again proposition 1.5.5 we can conclude

$$(G) = (y) = P_1 + P_2 + P_3 - 3P_\infty.$$

We introduce now the vector space of differential forms on a curve which will be useful for proving that an elliptic curve can always be written in a Weierstrass form -theorem 2.1.2-.

Definition 1.6.5 (Differential) Let C be a curve. The **space of (meromorphic) differential forms** on C, denoted by Ω_C, is the $\overline{K}$-vector space generated by symbols of the form dx for $x \in \overline{K}(C)$, subjet to the usual relations:

i) $d(x + y) = dx + dy$ for all $x, y \in \overline{K}(C)$.

ii) $d(xy) = xdy + ydx$ for all $x, y \in \overline{K}(C)$.

iii) $d\lambda = 0$ for all $\lambda \in \overline{K}$.

The following proposition collects some properties of differential forms:

Proposition 1.6.6 *Let C be a curve and let $t \in \overline{K}(C)$ be a uniformizer at $P \in C$.*

i) For every $\omega \in \Omega_C$ there exists a unique function $g \in \overline{K}(C)$ depending on ω and t satisfying

$$\omega = g\ dt.$$

We denote $g = \omega/dt$.

ii) Let $f \in \overline{K}(C)$ be a regular map at P. Then df/dt is also regular at P.

iii) Let $\omega \in \Omega_C$ with $\omega \neq 0$. The quantity

$$ord_P(\omega/dt)$$

depends only on ω and P, and it is independent of the choice of uniformizer t. We call this value **order of ω at P** *and denote it by $ord_P(\omega)$.*

iv) Let $x, f \in \overline{K}(C)$ with $x(P) = 0$ and let $char(\overline{K}) = 0$. Then

$$ord_P(fdx) = ord_P(f) + ord_P(x) - 1.$$

v) Let $\omega \in \Omega_C$ with $\omega \neq 0$. Then

$$ord_P(\omega) = 0$$

for all but finitely many $P \in C$.

Definition 1.6.7 (Divisor of a differential form) Let $\omega \in \Omega_C$. The **divisor associated to** ω is

$$(\omega) = \sum_{P \in C} ord_P(\omega) \cdot P.$$

Note that $(\omega) \in Div(C)$.

The differential $\omega \in \Omega_C$ is called **regular** (or **holomorphic**) if

$$ord_P(w) \geq 0 \qquad \text{for all } P \in C;$$

and it is **nonvanishing** if

$$ord_P(w) \leq 0 \qquad \text{for all } P \in C;$$

Remark 1.6.8. If $\omega_1, \omega_2 \in \Omega_C$ are two nonzero differentials, then proposition 1.6.6.i implies that there exists a function $f \in \overline{K}(C)^*$ such that $\omega_1 = f\omega_2$. Thus

$$(\omega_1) = (f) + (\omega_2),$$

which shows that the following definition makes sense.

Definition 1.6.9 (Canonical divisor class) The **canonical divisor class** on C is the image in $Pic(C)$ of (ω) for any nonzero differential $\omega \in \Omega_C$. Any element on this divisor class is called **canonical divisor**.

We can associate one divisor to every differential form of a curve C as in the following example:

Example 1.6.10 *Let C be the curve*

$$C : y^2 = (x - e_1)(x - e_2)(x - e_3),$$

where we continue with the notation from example 1.6.4. We want to calculate (dx) and (dx/y).

Let $P_0 = (x_0, y_0) \in C$ with $P_0 \neq P_1, P_2, P_3$. Note that $t = x - x_0$ is a uniformizer on $\mathcal{O}_P$ and that $dx = d(x - x_0)$. Thus we have, by proposition 1.6.6.iv,

$$ord_{P_0}(dx) = ord_{P_0}(d(x - x_0)) = ord_{P_i}(1) + ord_{P_0}(x - x_0) - 1 = 0 + 1 - 1 = 0.$$

Now, we study the points P_i for $i = 1, 2, 3$. We also have that $t = x - e_i$ is a uniformizer for P_i and $dx = d(x - e_i)$ for $i = 1, 2, 3$. Using proposition 1.6.6.iv again we have that

$$ord_{P_i}(dx) = ord_{P_i}(d(x - e_i)) = ord_{P_i}(1) + ord_{P_i}(x - e_i) - 1 = 0 + 2 - 1 = 1.$$

The last point that remains unstudied is $P_\infty = [0:1:0]$. Note that

$$dx = d\left(\frac{x}{z}\right) = d\left(\frac{x/y}{z/y}\right) = \frac{d(x/y)\cdot z/y - x/y \cdot d(z/y)}{(z/y)^2}. \tag{1.2}$$

A uniformizer for P_∞ is $t = x/y$ and as we saw in Example 1.6.4, $ord_{P_\infty}(y/z) = -3$, so we can write

$$\frac{z}{y} = t^3 f,$$

for come $f \in \overline{K}(C)$ and $f(P_\infty) \neq 0$. Using now $t = x/y$, $z/y = t^3 f$ and equation 1.2,

$$dx = d\left(\frac{x}{z}\right) = \frac{t^3 f - t(3t^2 f + t^3 f')}{t^6 f^2} dt = \frac{t^3(-2f + tf')}{t^6 f^2} dt = t^{-3} g dt,$$

where $g \in \overline{K}(C)$ with $g(P_\infty) \neq 0$. We can conclude that

$$ord_{P_\infty}(dx) = -3.$$

Summing up all the work above, we get

$$(dx) = P_1 + P_2 + P_3 - 3P_\infty.$$

We thus see that

$$\left(\frac{dx}{y}\right) \overset{Rem.1.6.8}{=} \left(\frac{1}{y}\right) + (dx) = -(y) + (dx) = -P_1 - P_2 - P_3 + 3P_\infty + P_1 + P_2 + P_3 - 3P_\infty = 0.$$

Hence the differential dx/y is both holomorphic and nonvanishing.

1.7 The Riemann-Roch theorem

Definition 1.7.1 (Positive divisor) A divisor $D = \sum n_P P$ is **positive**, denoted by $D \geq 0$, if $n_P \geq 0$ for every $P \in C$.

Definition 1.7.2 (The $L(D)$ space) Let D be a divisor of C. We define

$$L(D) := \{f \in \overline{K}(C) : D + (f) \geq 0\} \cup \{0\}.$$

If we write $D = D_+ - D_- = \sum n_i P_i - \sum m_j Q_j$ with $n_i, m_j > 0$, we can see the space $L(D)$ as maps which have zeros of order at least m_j at Q_j and which can have poles only at P_i with order at most n_i.

Proposition 1.7.3 *Some properties of the $L(D)$ space are:*

i) $L(D)$ is a finite-dimensional $\overline{K}$-vector space which dimension is denoted by

$$\ell(D) = dim_{\overline{K}}(L(D))$$

ii) $D \leq D' \Rightarrow L(D) \subseteq L(D')$.

iii) $D \equiv D' \Rightarrow L(D) \cong L(D')$ *as vectorial spaces over* $\overline{K}$.

iv) $\deg D = 0 \Rightarrow L(D) = \{0\}$.

v) $L(D)$ *has a basis consisting of functions in* $\overline{K}(C)$.

Theorem 1.7.4 (Riemann-Roch theorem) *Let* C *be a smooth projective curve.*

(Riemann) *There exists an integer* $g = g(C)$*, called* **genus of** C*, such that for all* $D \in Div(C)$ *the following inequality holds:*

$$\ell(D) \geq \deg D + 1 - g.$$

(Roch) *There exist an integer* g *and a canonical divisor* K_C*, such that for all* $D \in Div(C)$ *the following equality holds:*

$$\ell(D) = \deg D + 1 - g + l(K_C - D).$$

Corollary 1.7.5 *Some important results which can be deduced from the Riemann-Roch theorem are the following:*

i) $D = 0 \Rightarrow \ell(K_C) = g$.

ii) $D = K_C \Rightarrow \deg K_C = 2g - 2$.

iii) $\deg D > 2g - 2 \Rightarrow \ell(D) = \deg D + 1 - g$.

iv) If C *is a smooth plane curve with degree* d*, then* $g(C) = \dfrac{(d-1)(d-2)}{2}$.

v) The dimension of $L(D)$ *is finite.*

Proposition 1.7.6 *Let* C *be a smooth curve and let* $D \in Div_K(C)$*. Then* $L(D)$ *has a basis consisting of functions in* $K(C)$.

1.8 The Hurwitz formula and Bezout's theorem

In this section we recall two fundamental results: the Hurwitz formula, which provides a relation between the genus of projective varieties and ramification index of separable morphisms of curves; and Bezout's theorem, which concerns the number of intersection points of two plane algebraic curves.

The Hurwitz formula

Let C_1 and C_2 be two smooth projective curves defined over a field K and let $f : C_1 \to C_2$ be a separable nonconstant morphism. We fix a point $P \in C_1$ and call $Q = f(P)$. Let t_Q be a uniformizer in $\mathcal{O}_Q$. If we consider the composition $f^*t := t \circ f : C_2 \to \mathbb{P}^1$, we have $f^*t \in \mathcal{O}_P$.

Theorem 1.8.1 (Hurwitz formula) *Let C_1 and C_1 be two (smooth) curves defined over a field K of genus g_1 and g_2 respectively. Then,*

$$2g_1 - 2 \geq (\deg f)(2g_2 - 2) - \sum_{P \in C_1} (e_P - 1).$$

Moreover, the equality holds if $char(K) \nmid e_P$ for any $P \in C_1$.

Bezout's theorem

Let $\overline{K}$ be an algebraically closed field and let $F, G \in K[x, y, z]$ two homogeneous polynomials of degree d and e respectively and with no common factors.

Note that it is not required that the two polynomials above are irreducible or have all their factors different. For example, we admit two different lines $F = xy$ or a double line $G = z^2$.

Definition 1.8.2 (Multiplicity of intersection) Given two plane projective curves $F = 0$ y $G = 0$ and $P \in \mathbb{P}^2$, we want to define the **multiplicity of intersection** of F and G at P. As this definition is local, we can consider an affine chart, $f := F_*, g := G_*$, and define the intersection for affine curves. Bearing in mind this consideration, we define the multiplicity of intersection as the nonnegative integer

$$I(P, F \cap G) := I(P, f \cap g) = \dim_K \frac{\mathcal{O}_P(\mathbb{A}^2)}{(f, g)},$$

where $\mathcal{O}_P(\mathbb{A}^2) = \mathcal{O}_P(\mathbb{P}^2)$ is the local ring on the plane (not on the curves) at P.

Theorem 1.8.3 (Bezout's theorem) *Let $F = 0, G = 0$ be two plane projective curves with no common components. Then,*

$$\sum_{P \in \mathbb{P}^2} I(P, F \cap G) = \deg F \cdot \deg G.$$

1.9 Absolute values, valuations and completions

Recall the definition of an absolute value defined on a field K:

Definition 1.9.1 (Absolute Value) Let K be a field. An **absolute value** on K is a map $|\cdot|: K \to \mathbb{R}_{\geq 0}$ such that for all $x, y \in K$,

i) $|x| = 0 \iff x = 0$,

ii) $|xy| = |x| \cdot |y|$,

iii) $|x + y| \leq |x| + |y|$.

Lemma 1.9.2 *Let $|\cdot|$ be an absolute value on a field K. Then*

a) $|1| = 1$.

b) $|\zeta| = 1$ *for all* $\zeta \in K$, *with* $\zeta^d = 1$ *for some* $d \in \mathbb{N}$, $d \neq 0$.

c) $|x^{-1}| = |x|^{-1}$ *for all* $x \in K$.

d) $||x| - |y|| \leq |x - y|$ *for all* $x, y \in K$.

PROOF.

a) $|1|^2 = |1^2| = |1| \Rightarrow |1| = 1$.

b) $|\zeta|^d = |\zeta^d| = |1| = 1 \Rightarrow |\zeta| = 1$.

c) $1 = |xx^{-1}| = |x||x^{-1}| \Rightarrow |x|^{-1} = |x^{-1}|$.

d) $||x| - |y|| = ||x - y + y| - |y|| \leq ||x - y| + |y| - |y|| = |x - y|$.

□

We say that an absolute value is **non-archimedian** if for all $x, y \in K$ the following inequality holds:

$$|x + y| \leq \max\{|x|, |y|\}.$$

Example 1.9.3 The usual absolute value over $\mathbb{Q}$ is archimedian.

If we define

$$d : K \times K \longrightarrow \mathbb{R}; \qquad d(x, y) = |x - y|,$$

d is clearly a metric on K and we have a topological structure on K.

Definition 1.9.4 (Equivalent absolute values) We say that two absolute values are **equivalent** if they define the same topology on K.

It is easy to prove these two following results:

Theorem 1.9.5 *Let $|\cdot|_1$ and $|\cdot|_2$ be two absolute values on K.*

$$|\cdot|_1, |\cdot|_2 \text{ are equivalents} \iff \exists s \in \mathbb{R} \text{ such that } |x|_1 = |x|_2^s, \ \forall x \in K.$$

Corollary 1.9.6 *Let $|\cdot|_1$ and $|\cdot|_2$ be two absolute values on K. They are equivalent if, and only if,*

$$|x|_1 < 1 \iff |x|_2 < 1 \ \forall x \in K.$$

If we call Abs_K to the set of all absolute values defined over K, we can define a equivalence relation on Abs_K as follows:

$$|\cdot|_1 \mathcal{R} |\cdot|_2 \overset{\text{def.}}{\iff} |\cdot|_1 \text{ and } |\cdot|_2 \text{ are equivalent.}$$

Definition 1.9.7 (Place) Let K be a field, let Abs_K be the set of absolute values defined on K and let $\mathcal{R}$ be the previous relation. Then we call the quotient set

$$M_K := Abs_K/\mathcal{R}$$

a **place** of K.

We also define the following sets::

$$M_K^\infty := \{|\cdot|_v \in M_K : v \text{ archimedian on } K\};$$

$$M_K^0 := \{|\cdot|_v \in M_K : v \text{ nonarchimedian on } K\}.$$

We show now the relation between nonarchimedian absolute values and valuations.

Theorem 1.9.8 *Let $|\cdot| \in M_K^0$ and $s \in \mathbb{R}$, $s > 0$ then the map*

$$v_s : K \to \mathbb{R} \cup \{\infty\}; \qquad v_s(x) = \begin{cases} -s \log |x|, & \text{if } x \neq 0 \\ \infty, & \text{if } x = 0 \end{cases}$$

is a valuation on K. Furthermore, if $s, s' \in \mathbb{R}$, with $s, s' > 0$ and $s \neq s'$, v_s is equivalent to $v_{s'}$.

Conversely, if v is a valuation on K and $q \in \mathbb{R}$, $q > 1$, the function

$$|\cdot|_q : K \to \mathbb{R}; \qquad |x|_q = \begin{cases} q^{-v(x)}, & \text{if } x \neq 0. \\ 0, & \text{if } x = 0, \end{cases}$$

defines an absolute value on K.

PROOF. We just have to prove that v_s and $|\cdot|_q$ are respectively a valuation and an absolute value on K checking the definitions. We start with v_s. Let $x, y \in K$.

i) Obviously, $v_s(x) = \infty \iff x = 0$, by definition.

ii) If $x = 0$ or $y = 0$, $v_s(xy) = \infty = v_s(x) + v_s(y)$; but if $x, y \neq 0$,

$$v_s(xy) = -s \log |xy| = -s(\log |x| + \log |y|) = -s \log |x| - s \log |x| = v_s(x) + v_s(y).$$

iii) It remains to check that $v_s(x + y) \geq \min\{v_s(x), v_s(y)\}$.
It is obvious for $x = 0$ or $y = 0$. Suppose that $x, y \neq 0$, then we have

$$\begin{aligned} v_s(x + y) &= -s \log |x + y| \\ &\overset{|\cdot| \in M_K^0}{\leq} -s \log(\max\{|x|, |y|\}) \\ &= \min\{-s \log |x|, -s \log |y|\} \\ &= \min\{v_s(x), v_s(y)\}. \end{aligned}$$

Furthermore, let $s, s' \in \mathbb{R}^+$ with $s \neq s'$, then

$$v_s(x) = -s \log |x| = \frac{s}{s'} \cdot (-s' \log |x|) = \frac{s}{s'} \cdot v_{s'}(x).$$

We check now that $| \cdot |_q$ is an absolute value on K.

i) Obviously, $|x|_q = 0 \iff x = 0$, by definition.

ii) If $x = 0$ or $y = 0$, then $|xy|_q = 0 = |x|_q |y|_q$; but if $x, y \neq 0$,

$$|xy|_q = q^{-v(xy)} = q^{-v(x)-v(y)} = q^{-v(x)} q^{-v(y)} = |x|_q |y|_q.$$

iii) It remains to check that $|x + y|_q \leq |x|_q + |y|_q$.
It is obvious if $x = 0$ or $y = 0$. Suppose that $x, y \neq 0$, then we have

$$\begin{aligned} |x + y|_q &= q^{-v(x+y)} \\ &\leq q^{-\min\{v(x), v(y)\}} \\ &= \max\{q^{-v(x)}, q^{-v(y)}\} \\ &= \min\{|x|_q, |y|_q\} \\ &\leq |x|_q + |y|_q. \end{aligned}$$

Therefore, we have just checked that $|\cdot|_q$ is a nonarchimedean absolute value on K. Assume now that $q, q' \in \mathbb{R}$ with $q, q' > 1$ and $q \neq q'$. If we set $r := \dfrac{\log q}{\log q'}$, then for all nontrivial $x \in K$, we have

$$|x|_q = q^{-v(x)} = (q')^{-rv(x)} = |x|_{q'}^r$$

□

So, if $|\cdot|_v \in M_K^0$, we can set

$$v(x) := -\log |x|_v$$

and consider the normalized valuation for v, ord_v, satisfying $\mathrm{ord}_v(K^*) = \mathbb{Z}$.

Moreover, we denote the ring of integers of $(K, |\cdot|_v)$

$$R = \{x \in K : |x|_v \leq 1\} = \{x \in K : v(x) \geq 0\};$$

and unit group of R

$$R^* = \{x \in K : |x|_v = 1\} = \{x \in K : v(x) = 0\}.$$

We recall now the definition of a complete field and define the concept of completion.

Definition 1.9.9 (Cauchy sequence) Let K be a field and $|\cdot| \in M_K$. A sequence (x_n) in K is called a **Cauchy sequence** if for all $\varepsilon > 0$ there exists $N \in \mathbb{N}$ such that

$$|x_n - x_m| < \varepsilon \quad \forall n, m \geq N.$$

Definition 1.9.10 (Complete field) A field K with an absolute value $|\cdot| \in M_K$ is **complete** if any Cauchy sequence converges to an element in K.

Theorem 1.9.11 *Let K be a field and $|\cdot|_v \in M_K$. Then, there exists a unique, up to K-isomorphism, complete field K_v with an absolute value $|\cdot|_{K_v}$ such that K is embedded in K_v as a dense subfield and $|\cdot|_v$ is a restriction of $|\cdot|_{K_v}$, i.e., $|x|_{K_v} = |x|_v$ if $x \in K$.*

PROOF. Let $\mathcal{C}$ be the set of all the Cauchy sequences in K with respect to $|\cdot|_v$. Define the addition and multiplication as follows

$$(x_n) + (y_n) := (x_n + y_n); \qquad (x_n)(y_n) := (x_n y_n) \quad \forall n \in \mathbb{N}.$$

Indeed $(\mathcal{C}, +, \cdot)$ is a ring. Let $\mathcal{M} \subset \mathcal{C}$ be the set of all the Cauchy sequences which converges to zero. It is easy to see that $\mathcal{M}$ is a maximal ideal of $\mathcal{C}$. Set now

$$K_v := \mathcal{C}/\mathcal{M}.$$

Clearly, K_v is a field. Moreover, we have the an injection $K \hookrightarrow K_v$ by sending $a \in K$ to the equivalence class of the sequence $(a, a, a \ldots)$. We can write then $K \subset K_v$.

Now we have to define an absolute value in K_v. Take $a \in K_v$ and let $(a_n) \in \mathcal{C}$ be a representative of the equivalence class of a. As (a_n) is a Cauchy sequence, we have that $(|a_n|_v)$ converges in $\mathbb{R}$ because we have $||a_n|_v - |a_m|_v|_v \leq |a_n - a_m|_v$ by lemma 1.9.2. Set

$$|a|_{K_v} := \lim_{n\to\infty} |a_n|_v.$$

Then $|\cdot|_{K_v}$ is an absolute value on K_v and if $a \in K$ we have $|a|_{K_v} = |a|_v$. Furthermore,

$$\lim_{n\to\infty} a_n = a$$

is in K_v, so K is dense in K_v and K_v is complete with respect to $|\cdot|_{K_v}$.

It remains to see that K_v is unique up to K-isomorphism. Let K'_v be another field complete with respect to an absolute value $|\cdot|_{K'_v}$ such that K is dense in K'_v and for all $x \in K$, $|x|_{K'_v} = |x|_v$. Take $a \in K_v$ and let (a_n) be a representative of a. Then in K'_v this Cauchy sequence converges to an element $a' \in K'_v$ because K is dense in K'_v. Define now the function

$$\sigma : K_v \to K'_v; \qquad \sigma(a) = a'.$$

Defined like this, σ is a K-isomorphism and we have that $|a|_{K_v} = |\sigma(a)|_{K'_v}$ because

$$|a|_{K_v} = \lim_{n\to\infty} |a_n|_v = \lim_{n\to\infty} |a'|_{K'_v} = |\sigma(a)|_{K'_v}.$$

□

Definition 1.9.12 (Completion) The field K_v is called the **completion** of $(K, |\cdot|_v)$.

Chapter 2

Group structure of an elliptic curve

An **elliptic curve** E defined over a (perfect) field K, denoted by E/K, is a pair $(E, \mathcal{O})$ such that E is a projective smooth curve of genus 1 defined over K with a rational basepoint $\mathcal{O} \in E(K)$.

In this text we want to focus on the study of the set of K-rational points on an elliptic curve E:

$$E(K) = \{(x, y) \in E : \ x, y \in K\} \cup \{\mathcal{O}\}.$$

Integer points on elliptic curves are well understood. Siegel [72] proved that on any curve of positive genus there are only finitely many integer points. If we consider elliptic curves (genus 1), Baker and Coates [3] established an effective version of this result. In fact, they found an explicit upper bound on the size of the possible integer points.

For rational points on elliptic curves, Poincaré [66] conjectured in 1901 that there exists a finite set of points that would generate all of the (possibly infinite) rational points. This was later proven by Mordell in 1922 [55]. So far, Mordell's method often allows one to find such a finite generating set, but it has not been proven to always work.

In this chapter, we focus on the study of the structure of rational points on an elliptic curve E defined over a number field K. We show that the set $E(K)$ forms an abelian group and analyze its structure and the m-torsion subgroup structure. The m-torsion subgroup of an elliptic curve E/K, denoted by $E(K)[m]$, is the group of points on $E(K)$ whose order is exactly m.

We first show, using the Riemann-Roch theorem, that elliptic curves can always be written in a special way: the Weierstrass form (section 2.1). We will see then that points on elliptic curves form an abelian group with an explicit group law given by rational functions (section 2.2). Then we introduce the natural morphisms between elliptic curves, known as isogenies (section 2.3) wich are important to deduce the m-torsion subgroup structure of an elliptic curve (section 2.4).

2.1 Elliptic curves and Weierstrass form

First we show that, using the Rieman-Roch theorem 1.7.4, every elliptic curve can be written as a plane cubic, an conversely, that every smooth plane cubic written in a **Weierstrass form**:

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

with $a_i \in K$, is an elliptic curve.

Before, we prove an auxiliary result:

Lemma 2.1.1 *Let C be a singular algebraic curve defined over K given in a Weierstrass form,*

$$C : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

with $a_i \in K$. Then C is birationally equivalent to $\mathbb{P}^1$.

PROOF. If C is a singular algebraic curve given by a Weierstrass equation, then it has only one singular point (see proposition 2.1.6 below). Making a linear change of variables, we may assume that the singular point is $(x, y) = (0, 0)$. Checking partial derivatives, we see that the Weierstrass equation has the form

$$C : y^2 + a_1xy = x^3 + a_2x^2.$$

Then the rational map

$$\psi : C \to \mathbb{P}^1; \qquad (x, y) \mapsto [x : y],$$

shows that C and $\mathbb{P}^1$ are birationally equivalent, since it has an inverse given by

$$\varphi : \mathbb{P}^1 \to C; \qquad [1 : t] \mapsto (t^2 + a_1t - a_2, t^3 + a_1t^2 - a_2t).$$

This inverse is reached by calling $t = y/x$ and dividing the Weierstrass equation by x^2, obtaining

$$t^2 + a_1t = x + a_2,$$

which shows that both x and $y = tx$ are in $\overline{K}(t)$.

□

Theorem 2.1.2 *Let E be an elliptic curve defined over K.*

(i) There exist functions $x, y \in K(E)$ such that the map

$$\phi : E \to \mathbb{P}^2; \qquad \phi = [x : y : 1],$$

gives an isomorphism of E onto a curve given by a Weierstrass equation,

$$C : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

with $a_i \in K$ and satisfying $\phi(\mathcal{O}) = [0 : 1 : 0]$. Functions x and y are called Weierstrass coordinates for the elliptic curve E.

(ii) Any two Weierstrass equations for E as in (i) are related by a linear change of variables of the form

$$x = u^2x' + r, \qquad y = u^3y' + su^2x' + t,$$

with $u \in K^*$ and $r, s, t \in K$.

(iii) Conversely, every smooth cubic curve C given by a Weierstrass equation as in (i) is an elliptic curve defined over K with a base point $\mathcal{O} = [0 : 1 : 0]$.

PROOF.

(i) Let E be an elliptic curve. We want to find a plane cubic curve C isomorphic to E. We know that, by definition, E has genus one, i.e.,

$$g_E = 1.$$

The Riemann-Roch theorem 1.7.4 tells us that

$$\ell(D) = \deg D \ \text{ provided } \ \deg D \geq 1.$$

Particularly,

$$\ell(n\mathcal{O}) = n, \qquad \text{for all } n \in \mathbb{N}.$$

By proposition 1.7.6, we can choose functions in $K(E)$ which form a basis of $L(n\mathcal{O})$. Let $x, y \in K(E)$ be two functions with poles of order 2 and 3 at $\mathcal{O}$ respectively. Let us consider some cases:

(a) Let $P \in E$. Then $\ell(P) = 1$ and then $L(P) = K$. But $L(P)$ certainly contains the constant functions, which have no poles. In particular, if we set $P = \mathcal{O}$, this shows there are no functions on E having a single simple pole.

(b) $\ell(2\mathcal{O}) = 2$, and $\{1, x\}$ provides a basis for $L(2\mathcal{O})$ since

$$ord_{\mathcal{O}}(x) = -2 \qquad and \qquad x \notin L(\mathcal{O}).$$

(c) $\ell(3\mathcal{O}) = 3$, and $\{1, x, y\}$ provides a basis for $L(3\mathcal{O})$ since

$$ord_{\mathcal{O}}(y) = -3 \qquad and \qquad y \notin L(2\mathcal{O}).$$

(d) $\ell(4\mathcal{O}) = 4$, and $\{1, x, y, x^2\}$ provides a basis for $L(4\mathcal{O})$ since

$$ord_{\mathcal{O}}(x^2) = -4 \qquad and \qquad x^2 \notin L(3\mathcal{O}).$$

(d) $\ell(5\mathcal{O}) = 5$, and $\{1, x, y, x^2, xy\}$ provides a basis for $L(5\mathcal{O})$ since

$$ord_{\mathcal{O}}(xy) = -5 \qquad and \qquad xy \notin L(4\mathcal{O}).$$

(e) Finally, we have that $\ell(6\mathcal{O}) = 6$ and $\{1, x, y, x^2, xy, x^3, y^2\} \subseteq L(6\mathcal{O})$ since

$$ord_{\mathcal{O}}(x^3) = ord_{\mathcal{O}}(y^2) = -6 \qquad and \qquad x^3, y^2 \notin L(5\mathcal{O}).$$

But the set $\{1, x, y, x^2, xy, x^3, y^2\}$ consist on 7 functions, so they must be linearly dependent, i.e., there exist coefficients $A_i \in K$ for $i = 1, \ldots, 7$, not all zero, such that

$$A_1 + A_2x + A_3y + A_4x^2 + A_5xy + A_6x^3 + A_7y^2 = 0.$$

Note that $A_6 \cdot A_7 \neq 0$ because otherwise we would have that the set $\{1, x, y, x^2, xy\}$ would be linearly dependent and it is not. We make now the following change of variables

$$x = -A_6A_7x, \qquad y = A_6A_7^2y$$

and divide by $A_6^3A_7^4$ and we obtain the following Weierstrass equation:

$$C : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

with $a_i \in K$ for $i = 1, \ldots, 6$. This gives a map

$$\phi : E \to \mathbb{P}^2; \qquad \phi(P) = [x(P) : y(P) : 1],$$

whose image lies in the locus decribed by a Weierstrass equation. Moreover, as $\phi : E \to C$ is a rational map and E is a smooth curve then, by corollary 1.3.14, ϕ is a morphism. We have also that

$$\phi(\mathcal{O}) = [x(\mathcal{O}) : y(\mathcal{O}) : 1] = \left[\frac{x(\mathcal{O})}{y(\mathcal{O})} : 1 : \frac{1}{y(\mathcal{O})}\right] = [0 : 1 : 0],$$

since y has a higher-order pole than x at the point $\mathcal{O}$.

We can assure that ϕ is nonconstant because, as $y \in K(E)$, there are a finite number of points $P \in E(K)$ such that $ord_P(y) \neq 0$. If P is such a point, then we have that

$$\phi(P) = [x(P) : y(P) : 1] = \left[\frac{x(P)}{y(P)} : 1 : \frac{1}{y(\mathcal{O})}\right] \neq [0 : 1 : 0].$$

This proves that $\phi : E \to C$ is a nonconstant morphism between curves and then by proposition 1.5.1, ϕ is surjective.

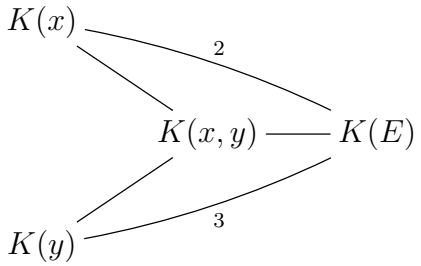
Provided $\phi : E \to C \subseteq \mathbb{P}^2$, the next step is to prove that $\deg \phi = 1$ or, equivallently, using theorem 1.5.2, that $K(E) = K(x, y) = K(C)$. Consider the map

$$\pi_1 : E \to \mathbb{P}^1; \qquad P \mapsto [x(P) : 1].$$

Since x has a double pole at $\mathcal{O}$, and no other poles, proposition 1.5.6.a says that π_1 has degree 2, so $[K(E) : K(x)] = 2$. Similarly, if we consider the map

$$\pi_2 : E \to \mathbb{P}^1; \qquad P \mapsto [y(P) : 1],$$

it has degree 3, so $[K(E) : K(y)] = 3$. We have then the following tower of fields:



Therefore $[K(E) : K(x, y)]$ divides both 2 and 3, so it must equal 1.

Now we show that C is smooth. Suppose that C is singular. Then, by lemma 2.1.1, there exists a rational map $\psi : C \to \mathbb{P}^1$ with $\deg \psi = 1$. It follows that the composition $\phi \circ \psi : E \to \mathbb{P}^1$ is a map of degree 1 between two smooth curves, so by proposition 1.3.17, it is an isomorphism. But this contradicts the fact that E has genus one and $\mathbb{P}^1$ has genus zero. Therefore C is smooth.

Applying again proposition 1.3.17, as $\phi : E \to C$ is a map of degree one between smooth curves, it is an isomorphism.

(ii) Let $\{x, y\}$ and $\{x', y'\}$ be two sets of Weierstrass coordinate functions on E. Then x and x' have poles of order 2 at $\mathcal{O}$ and y and y' have poles of order 3 at $\mathcal{O}$. Hence $\{1, x\}$ and $\{1, x'\}$ are both basis for $L(2\mathcal{O})$ and similary $\{1, x, y\}$ and $\{1, x', y'\}$ are both basis of for $L(3\mathcal{O})$. Thus there are constants $u_1, u_2 \in K^*$ and $r, s_2, t \in K$ such that

$$x = u_1 x' + r, \qquad \textit{and} \qquad y = u_2 y' + s_2 x' + t.$$

Since both (x, y) and (x', y') satisfy Weierstrass equations in which Y^2 and X^3 have coefficient 1, we have $u_1^3 = u_2^3$. Letting $u = u_2/u_1$ and $s = s_2/u^2$ puts the change of variables formula into the desired form.

c) Let C be an elliptic curve given by a nonsingular Weierstrass equation. As C is a smooth plane curve of degree $d = 3$, by a corollary of the Riemann-Roch theorem (corollary 1.7.5.v), we have that

$$g(C) = \frac{(d-1)(d-2)}{2} = 1.$$

so C has genus one, and taking $\mathcal{O} = [0 : 1 : 0]$ as the base point makes C into an elliptic curve.

□

Moreover, if $char(\overline{K}) \neq 2$, we can simplify the Weierstrass equation by completing squares and replacing $y \mapsto \frac{1}{2}(y - a_1x - a_3)$, which gives an equation of the form

$$E : y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6,$$

where

$$\begin{aligned} b_2 &= a_1^2 + 4a_2, \\ b_4 &= 2a_4 + a_1a_3, \\ b_6 &= a_3^2 + 4a_6. \end{aligned} \tag{2.1}$$

We also define the following quantities:

$$\begin{aligned} b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2, \\ c_4 &= b_2^2 - 24b_4, \\ c_6 &= b_2^3 + 36b_2b_4 - 216b_6, \\ \Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6, \\ j &= c_4^3/\Delta. \end{aligned}$$

Δ is called the **discriminant** and j, the j**-invariant** of the elliptic curve.

If also $char(\overline{K}) \neq 3$, a simpler equation yields by replacing $x \mapsto (x - 3b_2)/36$ and $y \mapsto y/216$:

$$E : y^2 = x^3 - 27c_4x - 54c_6 \xrightarrow{A=-27c_4,\ B=-54c_6} E : y^2 = x^3 + Ax + B. \tag{2.2}$$

And in this new equation, known as **Weierstrass short normal form**, we have

$$\Delta = -16(4A^2 + 27B^2), \qquad j = 1728(4A)^3/\Delta.$$

Remark 2.1.3. We could wonder which change of variables fixes $\mathcal{O} = [0 : 1 : 0]$ and preserves the Weierstrass form of the equation. This change of variables is called the **standard change** and is given by

$$\begin{aligned} x &= u^2x' + r, \\ y &= u^3y' + u^2sx' + t, \end{aligned}$$

where $u, r, s, t \in \overline{K}, u \neq 0$. It is now easy to make this substitution and compute the a_i's

coefficients and associated quantities:

Associated quantities
$ua_1' = a_1 + 2s$
$u^2a_2' = a_2 - sa_1 + 3r - s^2$
$u^3a_3' = a_3 + ra_1 + 2t$
$u^4a_4' = a_4 - sa_3 + 2ra_2 - (t + rs)a_1 + 3r^2 - 2st$
$u^6a_6' = a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1$
$u^2b_2' = b_2 + 12r$
$u^4b_4' = b_4 + rb_2 + 6r^2$
$u^6b_6' = b_6 + 2rb_4 + r^2b_2 + 4r^3$
$u^8b_8' = b_8 + 3rb_6 + 3r^2b_4 + r^3b_2 + 3r^4$
$u^4c_4' = c_4$
$u^6c_6' = c_6$
$\Delta' = u^{12}\Delta$
$j' = j$

Remark 2.1.4 (Preserving the Weierstrass Short Normal Form in $\mathbb{Q}$). Assume that we have an elliptic curve E defined over $\mathbb{Q}$ whose Weierstrass short normal form is given by

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

Then, the only linear changes of variables preserving this Weierstrass short normal form are given by

$$x \mapsto u^2x', \qquad y \mapsto u^3y',$$

for some $u \in \mathbb{Q}$. Such a change behaves as follows:

$$y^2 = x^3 + Ax + B \;\Rightarrow\; u^6(y')^2 = u^6(x')^3 + Au^2x' + B \;\Rightarrow\; (y')^2 = (x')^3 + \frac{A}{u^4}x' + \frac{B}{u^6}.$$

In fact, this argument shows that one can always assume A and B to be in $\mathbb{Z}$. If they were not in $\mathbb{Z}$, we could write

$$A = \frac{p_1}{q_1}, \qquad B = \frac{p_2}{q_2},$$

with $p_1, p_2, q_1, q_2 \in \mathbb{Z}$ and $q_1, q_2 \neq 0$. If we consider the change of variables

$$x \mapsto \left(\frac{1}{q_1q_2}\right)^2 x', \qquad y \mapsto \left(\frac{1}{q_1q_2}\right)^3 y',$$

we obtain the equation

$$(y')^2 = (x')^3 + A'x' + B'$$

where $A' = p_1q_1^3q_2^4 \in \mathbb{Z}$ and $B' = p_2q_1^6q_2^5 \in \mathbb{Z}$.

Moreover, it also implies that the number A^3/B^2 is an invariant of the equivalence class of elliptic curves in Weierstrass short normal form up to linear changes of variables, because

$$\frac{(A')^3}{(B')^2} = \frac{\left(\frac{A}{u^4}\right)^3}{\left(\frac{B}{u^6}\right)^2} = \frac{A^3u^{12}}{B^2u^{12}} = \frac{A^3}{B^2}.$$

Of course, even if two curves

$$E : y^2 = x^3 + Ax + B \qquad and \qquad E' : y^2 = x^3 + Cx + D$$

verify $A^3/B^2 = C^3/D^2$ this does not mean that they are equal up to some linear change of variables in the previous form. In fact, it is fairly elementary that this happens if and only if the following condition holds: there exists a rational solution u for the system

$$\begin{cases} u^4 = \dfrac{A}{C}, \\ \\ u^6 = \dfrac{B}{D}. \end{cases}$$

This fact is easy to prove:

($\Rightarrow$) Suppose that $E \simeq E'$. It means that there exists $u \in \mathbb{Q}$ such that the linear change of variables $x \mapsto u^2x'$, $y \mapsto u^3y'$ gives us

$$\begin{cases} \dfrac{A}{u^4} = C, \\ \\ \dfrac{B}{u^6} = D. \end{cases} \iff \begin{cases} u^4 = \dfrac{A}{C}, \\ \\ u^6 = \dfrac{B}{D}. \end{cases}$$

In other words, that there exists a rational solution of this system.

($\Leftarrow$) Starting from E and using the change of variables $x \mapsto u^2x'$, $y \mapsto u^3y'$, where $u \in \mathbb{Q}$ is a solution of the system, we get

$$y^2 = x^3 + \frac{A}{u^4}x + \frac{B}{u^6} \;\Rightarrow\; y^2 = x^3 + \frac{A}{A/C}x + \frac{B}{B/D} \;\Rightarrow\; y^2 = x^3 + Cx + D.$$

This proves that $E \simeq E'$.

□

We can rewrite this last result as follows

Theorem 2.1.5 *Let E and E' be two elliptic curves defined over $\mathbb{Q}$ given in Weierstrass short normal form*

$$E : y^2 = x^3 + Ax + B \qquad \text{and} \qquad E' : y^2 = x^3 + Cx + D$$

and such that $A^3/B^2 = C^3/D^2$. Then

$$E \simeq E' \iff \text{there exists a rational solution } u \text{ for the system } \begin{cases} u^4 = \dfrac{A}{C}, \\ u^6 = \dfrac{B}{D}. \end{cases}$$

Proposition 2.1.6 *A curve given in a Weierstrass equation is nonsingular if and only if $\Delta \neq 0$. Otherwise it has only one singular point.*

PROOF. Let E be an elliptic curve given in a Weierstrass form

$$E : f(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0.$$

We prove first that $\mathcal{O} = [0 : 1 : 0]$ is not a singular point. Considering E in $\mathbb{P}^2$, the associated homogeneous equation is

$$F(x, y, z) = y^2z + a_1xyz + a_3yz^2 - x^3 - a_2x^2z - a_4xz^2 - a_6z^3 = 0.$$

We have $\dfrac{\partial F}{\partial z}(\mathcal{O}) = 1 \neq 0$, hence $\mathcal{O}$ is a nonsigular point of E.

Now suppose that $P = (x_0, y_0) \in E$ is a singular point. The change of variables

$$x = x' + x_0, \qquad y = y' + y_0$$

leaves Δ invariant, so without loss of generality we can assume that $P = (0, 0)$. Then

$$a_6 = f(0, 0) = 0, \qquad a_4 = \frac{\partial f}{\partial x}(0, 0) = 0, \qquad a_3 = \frac{\partial f}{\partial y}(0, 0) = 0,$$

So the equation for E takes the form

$$E : f(x, y) = y^2 + a_1xy - x^3 - a_2x^2 = 0.$$

This equation has $\Delta = 0$.

Conversely, let us prove that if E is nonsingular then $\Delta \neq 0$. To simplify the computation, assume $\text{char}(K) \neq 2$ and consider a Weierstrass equation of the form

$$E : y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6.$$

E is singular if and only if there exists a point $P = (x_0, y_0)$ satisfying

$$2y_0 = 12x_0^2 + 2b_2x_0 + 2b_4 = 0$$

In other words, the singular points are exactly of the form $(x_0, 0)$ such that x_0 is a double root of the cubic polynomial $4x^3 + b_2x^2 + 2b_4x + b_6$. But this polynomial has a double root if and only if its discriminant, which is 16Δ, vanishes.

Further, since a cubic polynomial cannot have two double roots, E has at most one singular point.

□

Remark 2.1.7. We have defined an elliptic curve E over a (perfect) field K as a smooth curve. The latter proposition says that if E is an elliptic curve given by a Weierstrass equation then $\Delta \neq 0$, i.e., whenever we talk about elliptic curves we will suppose that $\Delta \neq 0$.

Proposition 2.1.8 *Two elliptic curves are isomorphic over $\overline{K}$ if and only if they both have the same j-invariant.*

PROOF. ($\Rightarrow$) If two elliptic curves are isomorphic, the standard change of variables (remark 2.1.3) shows that both curves have the same j-invariant.

($\Leftarrow$) For simplicity, assume that $char(\overline{K}) \neq 2, 3$, hence we can write the equations in the Weierstrass short normal form. Let E and E' be two elliptic curves with the same j-invariant, say with equations

$$E : y^2 = x^3 + Ax + B, \qquad E' : y^2 = x^3 + A'x + B'.$$

The assumption $j(E) = j(E')$ means that

$$\begin{aligned} \frac{(4A)^3}{4A^3 + 27B^2} &= \frac{(4A')^3}{4A'^3 + 27B'^2} \\ &\Rightarrow \ (4A)^3 \cdot 4(A')^3 + (4A)^3 \cdot 27(B')^2 = (4A')^3 \cdot 4A^3 + (4A')^3 \cdot 27B^2 \\ &\Rightarrow A^3(B')^2 = (A')^3B^2. \end{aligned}$$

We look for an isomorphism of the form $(x, y) = (u^2x', u^3y')$, as we saw in remark 2.1.4. Consider three cases:

Case 1. $A = 0$ ($j = 0$). Then $B \neq 0$ since $\Delta \neq 0$, so $A' = 0$, and we obtain an isomorphism using $u = (B/B')^{1/6}$.

Case 2. $B = 0$ ($j = 1728$). Then $A \neq 0$, so $B' = 0$ and we take $u = (A/A')^{1/4}$.

Case 3. $AB \neq 0$ ($j \neq 0, 1728$). Then $A'B' \neq 0$ because if any of them were zero, then both of them would be 0, contradicting $\Delta' \neq 0$. Taking $u = (A/A')^{1/4} = (B/B')^{1/6}$ gives the desired isomorphism.

□

2.2 The group law

Let E be an elliptic curve given by a Weierstrass equation. By Bezout's theorem 1.8.3 we have that, if L is a line in $\mathbb{P}^2$, L intersects E at exactly three points, say P, Q, R, which could be the same if L is tangent to E, for example. We define an operation, $\oplus$ (that we will denote by $+$ for simplicity), which gives E an abelian group estructure:

Definition 2.2.1 (Composition Law for Elliptic Curves) Let E be an elliptic curve defined over an algebraically closed field $\overline{K}$. Let $P, Q \in E$ and let L be the line connecting P and Q. We call R to the third point of intersection of L with E. Let L' be the line connecting R and $\mathcal{O}$. Then $P + Q$ is the third point of intersection of L' with E.

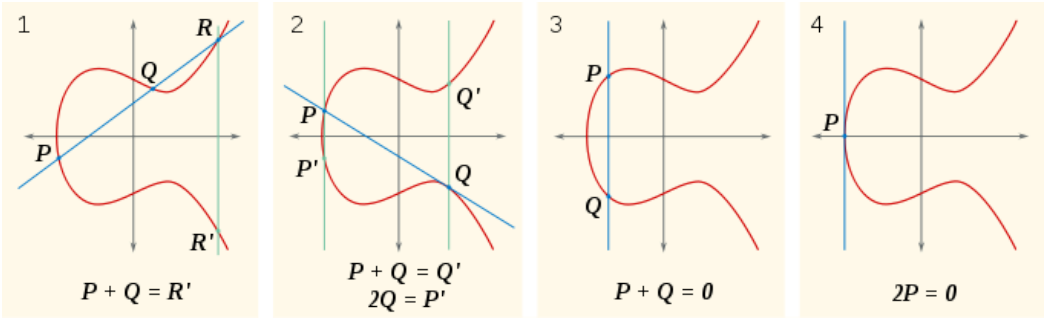


Figure 2.1: Group law for $E(\overline{K})$: four different cases.

Proposition 2.2.2 *The composition law has the following properties:*

i) If a line L intersects E at the (not necesarily dinstinct) points P, Q and R, then

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

ii) $P + \mathcal{O} = P$ for all $P \in E$.

iii) $P + Q = Q + P$ for all $P, Q \in E$.

iv) Let $P \in E$. There exists another point on E, denoted by $-P$, satisfying

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

v) Let $P, Q, R \in E$. Then

$$(P + Q) + R = P + (Q + R).$$

In other words, the composition law makes E into an abelian group with identity element $\mathcal{O}$. Further,

vi) Suppose that E is defined over a field K. Then the set of K-rational points on E,

$$E(K) = \{(x, y) \in K^2 : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{\mathcal{O}\},$$

is a subgroup of E.

PROOF. See [73, III.2.2].

□

Notation. If E is an elliptic curve, $P \in E$ and $m \in \mathbb{Z}$, we define

$$\begin{cases} mP &= P + \overset{m)}{\cdots} + P, \quad (m > 0), \\ 0P &= \mathcal{O}, \\ mP &= (-m)(-P), \quad (m < 0). \end{cases}$$

We now derive explicit formulas for the group operations on E. Let E be an elliptic curve given by a Weierstrass equation

$$F(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0,$$

and let $P_0 = (x_0, y_0) \in E$.

Calculus of the opposite element

In order to calculate $-P_0$, we take a line L through P_0 and $\mathcal{O}$ and find its third point of intersection with E. The line L is given by

$$L : x - x_0 = 0.$$

Substituting this into the equation for E,

$$\begin{aligned} F(x_0, y) &= y^2 + \underbrace{(a_1x_0 + a_3)}_{c_1} y + \underbrace{(-x_0^3 - a_2x_0^2 - a_4x_0 - a_6)}_{c_2} \\ &= y^2 + c_1y + c_2 \\ &= 0, \end{aligned}$$

yields a quadratic polynomial which roots are y_0 and y_0', where $-P_0 = (x_0, y_0')$. In order to find an expression of y_0' in terms of x_0 and y_0, we write out

$$F(x_0, y) = (y - y_0)(y - y_0') = y^2 + (-y_0 - y_0')y + y_0y_0'.$$

And equating the coefficients of y gives $y_0' = -y_0 - a_1x_0 - a_3$. This yields

$$-P_0 = -(x_0, y_0) = (x_0, -y_0 - a_1x_0 - a_3).$$

Calculus of the addition of two elements

Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be two points on E. If $x_1 = x_2$ and $y_1+y_2+a_1x_2+a_3 = 0$, we have already shown that $P_1 + P_2 = \mathcal{O}$. Otherwise, the line through P_1 and P_2 (or the tangent line if $P_1 = P_2$) has an equation of the form

$$L : y = \mu x + \nu;$$

where formulas for μ and ν are given below (table 2.1). Substituting the equation of L into the equation of E, we have

$$\begin{aligned} F(x, \mu x + \nu) &= (\mu x + \nu)^2 + a_1(\mu x + \nu)x + a_3(\mu x + \nu) - x^3 - a_2x^2 - a_4x - a_6 \\ &= -x^3 + \underbrace{(\mu^2 + a_1\mu - a_2)}_{c_2} x^2 + \underbrace{(2\mu\nu + a_1\nu + a_3\mu - a_4)}_{c_1} x + \underbrace{(\nu^2 + a_3\nu - a_6)}_{c_0} \\ &= -x^3 + c_2x^2 + c_1x + c_0 \\ &= 0, \end{aligned}$$

which has roots x_1, x_2 and x_3, where $P_3 = (x_3, y_3)$ is the third point of $L \cap E$. From proposition 2.2.2.i we have

$$P_1 + P_2 + P_3 = \mathcal{O}.$$

We write out

$$F(x, \mu x + \nu) = -(x - x_1)(x - x_2)(x - x_3)$$

and equating the coefficient of x^2 yields

$$x_1 + x_2 + x_3 = \mu^2 + a_1\mu - a_2.$$

This gives a formula for x_3, and substituting in the equation of L gives the value of $y = \mu x_3 + \nu$. Finally, to find $P_1 + P_2 = -P_3$, we apply the negation formula to P_3.

All this information is summarized in the following proposition.

Proposition 2.2.3 (Group Law Algorithm) *Let E be an elliptic curve given by a Weierstrass equation*

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

i) Let $P_0 = (x_0, y_0)$. Then

$$-P_0 = (x_0, -y_0 - a_1x_0 - a_3).$$

Now, let

$$P_1 + P_2 = P_3 \quad \textit{with} \quad P_i = (x_i, y_i) \quad \textit{for } i = 1, 2, 3.$$

ii) If $x_1 = x_2$ and $y_1 + y_2 + a_1x_1 + a_3 = 0$, then

$$P_1 + P_2 = \mathcal{O}.$$

Otherwise, define μ and ν by the following formulas:

	μ	ν
$x_1 \neq x_2$	$\dfrac{y_2 - y_1}{x_2 - x_1}$	$\dfrac{y_1x_2 - y_2x_1}{x_2 - x_1}$
$x_1 = x_2$	$\dfrac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}$	$\dfrac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3}$

Table 2.1: Formulas for the slope and the intercept of the line through P_1 and P_2.

Then $y = \mu x + \nu$ is the line through P_1 and P_2, or tangent to E if $P_1 = P_2$.

iii) With notation as in (ii), $P_3 = P_1 + P_2$ has coordinates

$$x_3 = \mu^2 + a_1\mu - a_2 - x_1 - x_2,$$
$$y_3 = -(\mu + a_1)x_3 - \nu - a_3.$$

iv) As special cases of (iii), we have for $P_1 \neq \pm P_2$,

$$x(P_1 + P_2) = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 + a_1\left(\frac{y_2 - y_1}{x_2 - x_1}\right) - a_2 - x_1 - x_2,$$

and the **duplication formula** *for $P = (x, y) \in E$,*

$$x(2P) = \frac{x^4 - b_4x^2 - 2b_6x - b_8}{4x^3 + b_2x^2 + 2b_4x + b_6},$$

where b_2, b_4, b_6, b_8 are the polynomials in a_i's given in equation (2.1).

Corollary 2.2.4 *With notation as in proposition 2.2.3, a function $f \in \overline{K}(E) = \overline{K}(x, y)$ is said to be* **even** *if $f(P) = f(-P)$ for all $P \in E$. We have*

$$f \text{ is even} \qquad \Longleftrightarrow \qquad f \in \overline{K}(x).$$

PROOF. ($\Leftarrow$) From proposition 2.2.3, if $P = (x_0, y_0)$, then $-P = (x_0, -y_0 - a_1x_0 - a_3)$. It follows immediately that every element of $\overline{K}(x)$ is even.
($\Rightarrow$) Suppose that $f \in \overline{K}(x, y)$ is even. Using the Weierstrass equation for E, we have

$$y^2 = x^3 + a_2x^2 + a_4x + a_6 + (-a_1x - a_3)y = f_1(x) + f_2(x)y,$$

so whenever we found y^2 we can exchange if for $f_1(x) + f_2(x)y$. Thus, we can write f in the form

$$f(x, y) = g(x) + h(x)y \quad \text{for some } g, h \in \overline{K}(x).$$

Then the eveness provided for f implies that

$$\begin{aligned} f(x,y) &= f(x,-y-a_1x-a_3), \\ g(x)+h(x)y &= g(x)+h(x)(-y-a_1x-a_3) \\ (2y+a_1x+a_3)h(x) &= 0. \end{aligned}$$

This holds for all $(x,y) \in E$, so either h is identically 0, or else $a_1 = 2$ and $a_3 = 0$. The latter implies that the discriminant satisfies $\Delta = 0$, which contradicts our assumption that the Weierstrass equation is nonsingular. Hence $h = 0$ and $f(x,y) = g(x) \in \overline{K}(x)$.

□

The following definition will be important in order to study below the structure of the group $E(K)$.

Definition 2.2.5 (Torsion subgroup) Let E be an elliptic curve and $m \in \mathbb{Z}, m \neq 0$ defined over a field K. The **m-torsion subgroup of** $E(K)$ is defined by

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

The **torsion subgroup of** $E(K)$ is

$$E(K)_{tors} = \bigcup_{m=1}^{\infty} E(K)[m].$$

Singular Weierstrass Equations

Suppose that a given Weierstrass equation has discriminant $\Delta = 0$, so it has only one singular point by proposition 2.1.6. What extent does our analysis of the composition law fail in this case? As we will see, everything is fine provided that we discard the singular point; and in fact, the resulting group has a particularly simple structure.

Definition 2.2.6 (Non-singular part of a elliptic curve) Let E be a (possibly singular) curve given by a Weierstrass equation. The **non-singular part of E,** E_{ns} is the set of non-singular points of E. If E is defined over a field K, then $E(K)_{ns}$ is the set of non-singular points of $E(K)$.

Proposition 2.2.7 *Let E be a singular curve given by a Weierstrass equation, i.e., $\Delta = 0$, so E has only one singular point, namely S. Then the composition law makes E_{ns} into an abelian group.*

PROOF. See [73, Prop.III.2.5].

□

Further, $E_{ns}(K)$ is an abelian group even when K is not algebraically closed. For a group-theoretic description of $E_{ns}(K)$, see [73, Ex.3.5].

2.3 Isogenies and the dual isogeny

We study in this section a special sort of morphisms between elliptic curves: isogenies. Since an elliptic curve has a distinguised zero point, it is natural to study those maps which respect this property. The theory of isogenies is going to let us find the group structure of $E(K)$.

Definition 2.3.1 (Isogeny) Let E_1 and E_2 be two elliptic curves. An **isogeny** between them is a morphism $f : E_1 \to E_2$ satisfying $f(\mathcal{O}) = \mathcal{O}$. We say that two elliptic curves are **isogenous** if there is an isogeny between them.

Remark 2.3.2. Since elliptic curves have group structure, the maps between them form groups too. Thus let

$$\mathrm{Hom}(E_1, E_2) = \{\text{isogenies } f : E_1 \to E_2\}.$$

Then the group law implies that $\mathrm{Hom}(E_1, E_2)$ is a group under addition

$$(f + g)(P) = f(P) + g(P).$$

PROOF.

- $(f + g)(\mathcal{O}) = \mathcal{O} = \mathcal{O} + \mathcal{O} = f(\mathcal{O}) + g(\mathcal{O})$.
- The associative law is inherited from the associative group law of $(E_2, +)$.
- The neutral element is the isogeny $[0](P) := \mathcal{O}$, for all $P \in E_1$. (By convention, we set $deg[0] = 0$).
- If f is an isogeny such that $f(P) = Q$, then its inverse is $g(P) = -Q$.

□

Example 2.3.3 (Multiplication by m isogeny) Let $m \in \mathbb{Z}$ and E be an elliptic curve. We can define an isogeny, called *multiplication by m isogeny*, in a natural way as follows:

$$[m] : E \to E, \qquad [m](P) = \begin{cases} \underbrace{P + \cdots + P}_{m)}, & \text{if } m > 0, \\ \mathcal{O}, & \text{if } m = 0, \\ [-m](-P), & \text{if } m < 0, \end{cases}$$

for every $P \in E$.

Moreover, $[m]$ is an isogeny by the group law. Note that if E is defined over a field K, then $[m]$ is also defined over K.

Example 2.3.4 (Traslation-by-Q map) Let E/K be an elliptic curve and let $Q \in E$. Then we can define a *traslation by Q map*

$$\tau_Q : E \to E; \qquad P \mapsto P + Q.$$

This is cleary not an isogeny, unless $Q = \mathcal{O}$; and it is an isomorphism, since τ_{-Q} provides an inverse. Nevertheless this map has a very useful property. Let $f : E_1 \to E_2$ be a morphism of elliptic curves as alegrbraic curves. Then the map

$$\phi = \tau_{-f(\mathcal{O})} \circ f$$

is an isogeny (since $\phi(\mathcal{O}) = \mathcal{O}$). We have thus shown that any morphism f is the composition of an isogeny ϕ and a traslation $\tau_{f(\mathcal{O})}$,

$$f = \tau_{f(\mathcal{O})} \circ \phi.$$

Proposition 2.3.5 *The following statements hold:*

i) Let E/K be an elliptic curve and let $m \in \mathbb{Z}$, $m \neq 0$. Then the multiplication by m map, $[m] : E \to E$ is non-constant.

ii) Let E_1 and E_2 be two elliptic curves. Then the group of isogenies $Hom(E_1, E_2)$ is a torsion-free $\mathbb{Z}$-module.

PROOF.

i) We start showing that $[2] \neq [0]$. The duplication formula from proposition 2.2.3.iv says that if a point $P = (x, y) \in E$ has order 2, then it must satisfy

$$4x^3 + b_2x^2 + 2b_4x + b_6 = 0.$$

If $char(K) \neq 2$, this shows immediatly that there are only finitely many such points. Further, even for $char(K) = 2$, the only way to have $[2] = [0]$ is for the cubic polynomial to be identically 0, which means that $b_2 = b_6 = 0$, which in turn implies $\Delta = 0$. Hence in all cases we have $[2] \neq [0]$. Now, using the fact that $[mn] = [m] \circ [n]$, we are reduced to considering the case that m is odd.

Assume now that $char(K) \neq 2$. Then, using long division, it is easy to verify that the polynomial

$$4x^3 + b_2x^2 + 2b_4x + b_6$$

does not divide the polynomial

$$x^4 - b_4x^2 - 2b_6x - b_8.$$

More precisely, if the first polynomial divides the second, then $\Delta = 0$. Hence we can find an $x_0 \in \overline{K}$ such that the first polynomial vanishes to higher order at x_0 than does the second. Choosing $y_0 \in \overline{K}$ so that $P_0 = (x_0, y_0) \in E$, the doubling formula

implies that $[2]P_0 = \mathcal{O}$. In other words, we have shown that E has a nontrivial point P_0 of order 2. Then for odd integers m we have

$$[m]P_0 = P_0 \neq \mathcal{O},$$

so clearly $[m] \neq [0]$.

Finally, if $char(K) = 2$, then one can proceed as above using the "triplication formula" to produce a point of order 3.

ii) That $\mathrm{Hom}(E_1, E_2)$ is a $\mathbb{Z}$-module is clear, because it is an abelian group.
Suposse $f \in \mathrm{Hom}(E_1, E_2)$ and $m \in \mathbb{Z}$ such that

$$[m] \circ f = [0].$$

Taking degrees, we have, by remark 1.5.7,

$$(\deg[m])(\deg f) = 0;$$

so either $m = 0$; or else, (i) implies that $(\deg[m]) \geq 1$, in which case we have $f = [0]$. So, the only one torsion element in $\mathrm{Hom}(E_1, E_2)$ is $[0]$.

□

Now we are going to show some important and useful properties of isogenies.

Theorem 2.3.6 *Every isogeny is a group homomorphism. It is to say, if $f : E_1 \to E_2$ is an isogeny, then $f(P + Q) = f(P) + f(Q)$, for all $P, Q \in E_1$.*

PROOF. See [73, III.4.8].

□

Corollary 2.3.7 *If $f : E_1 \to E_2$ is a nonzero isogeny, then $\ker f = f^{-1}(\mathcal{O})$ is a finite subgroup.*

PROOF. $f^{-1}(\mathcal{O})$ is a subgroup because f is a group homomorphism and it is finite from proposition 1.5.6.

□

Theorem 2.3.8 *Let $f : E_1 \to E_2$ be a nonconstant isogeny.*

i) For every $Q \in E_2$,

$$\#f^{-1}(Q) = \deg f.$$

ii) The map

$$\begin{aligned} \ker f &\to Aut[\overline{K}(E_1)/f^*\overline{K}(E_2)] \\ T &\mapsto \tau_T^* \end{aligned}$$

is an isomorphism, where τ_T is the traslation-by-T map and τ_T^* is the automorphism that τ_T induces in $\overline{K}(E_1)$.

iii) Assume that f is separable. Then f is unramified,

$$\#\ker f = \deg f,$$

and $\overline{K}(E_1)/f^*\overline{K}(E_2)$ is Galois.

PROOF.

i) From proposition 1.5.6.ii we know that $\#f^{-1}(Q) = \deg f$ for all but finitely many $Q \in E_2$. We want to see that this happens for all $Q \in E_2$. Let $Q, Q' \in E_2$. We can choose some $R \in E_1$ such that $f(R) = Q' - Q$. Since f is a homomorphism, there is a ono-to-one correspondence

$$f^{-1}(Q) \to f^{-1}(Q'); \qquad P \mapsto P + R.$$

Let us prove it:

- *Well-defined.* Let $P \in f^{-1}(Q)$, then $f(P) = Q$. Using $f(R) = Q' - Q$,

$$\begin{aligned} f(R) = Q' - f(P) &\iff f(R) + f(P) = Q' \\ &\iff f(R+P) = Q' \\ &\iff R + P \in f^{-1}(Q'). \end{aligned}$$

- *Injective.* It is clear.
- *Surjective.* If $T \in f^{-1}(Q')$ we have $f(T - R) = T$.

Hence, for all $Q \in E_2$ we have $\#f^{-1}(Q) = \deg f$.

ii)
- *Well-defined.* Let $T \in \ker f$ and $\alpha \in \overline{K}(E_2)$. Remember that

$$\begin{array}{rccc} \tau_T^* : & \overline{K}(E_1) & \to & \overline{K}(E_1) \\ & g & \mapsto & \tau_T^* g = g \circ \tau_T; \end{array} \qquad \begin{array}{rccc} f^* : \overline{K}(E_2) & \to & \overline{K}(E_1) \\ h & \mapsto & f^*h = h \circ f. \end{array}$$

Since $f \circ \tau_T = f$ (because τ_T is an automorphism of E_1), we have

$$\tau_T^*(f^*\alpha) = (f \circ \tau_T)^*\alpha = f^*\alpha.$$

So, τ_T^* fixes $f^*\overline{K}(E_2)$, hence is a $f^*\overline{K}(E_2)$-automorphism of $\overline{K}(E_1)$.

- *Homomorphism.* It is clear from the fact $\tau_T \circ \tau_S = \tau_{T+S} = \tau_S \circ \tau_T$.

- *Bijective.* We have
$$\#\ker f = \#f^{-1}(\mathcal{O}) \overset{\text{(i)}}{=} \deg f;$$
while from basic Galois theory,
$$\#\mathrm{Aut}([\overline{K}(E_1)/f^*\overline{K}(E_2)]) \leq \deg f.$$
Hence, it suffices to show that the map is injective. Let $T \mapsto \tau_T^* = \mathrm{id}_{\overline{K}(E_1)}$. Then, if $g \in \overline{K}(E_1)$, we have $\tau_T^* g(P) = (g \circ \tau_T)(P) = g(P)$ for all $P \in E_1$ and this is possible only if $T = \mathcal{O}$.

iii) If f is separable, from (i) we have
$$f^{-1}(Q) = \deg f \qquad \text{for all } Q \in E_2,$$
then f is unramified from corollary 1.5.8. Choosing $Q = \mathcal{O}$, we have
$$\#\ker f = \#f^{-1}(\mathcal{O}) = \deg f.$$
Then from (ii) we find that
$$\#\mathrm{Aut}([\overline{K}(E_1)/f^*\overline{K}(E_2)]) = [\overline{K}(E_1) : f^*\overline{K}(E_2)]$$
so $\overline{K}(E_1)/f^*\overline{K}(E_2)$ is Galois.

□

Corollary 2.3.9 *Let $f : E_1 \to E_2$ and $g : E_1 \to E_3$ be two nonconstant isogenies with f separable. If*
$$\ker f \subset \ker g$$
then there exists a unique isogeny
$$h : E_2 \to E_3$$
such that $h \circ f = g$.

PROOF. Since f is separable theroem 2.3.8.iii states that $\overline{K}(E_1)/f^*\overline{K}(E_2)$ is Galois. The inclusion $\ker f \subset \ker g$ and the identification in theorem 2.3.8.ii implies that every element of $\mathrm{Gal}(\overline{K}(E_1)/f^*\overline{K}(E_2))$ fixes $g^*\overline{K}(E_3)$. Hence by Galois theory, there are the inclusions
$$g^*\overline{K}(E_3) \subset f^*\overline{K}(E_2) \subset \overline{K}(E_1).$$
Now, theorem 1.5.2.ii gives a map $h : E_2 \to E_3$ satisfying $f^*(h^*\overline{K}(E_3)) = g^*\overline{K}(E_3)$. And this implies that $h \circ f = g$. Finally, h is an isogeny, since
$$h(\mathcal{O}) = h(f(\mathcal{O})) = g(\mathcal{O}) = \mathcal{O}.$$

□

We introduce now the concept of dual isogeny.

Theorem 2.3.10 *Let $f : E_1 \to E_2$ be a nonconstant isogeny of degree m between two elliptic curves. There exists a unique isogeny*

$$\hat{f} : E_2 \to E_1$$

such that $\hat{f} \circ f = [m]$.

PROOF. (Uniqueness). Suppose $\hat{f}$ and $\hat{f}'$ are such two isogenies. Then,

$$(\hat{f} - \hat{f}') \circ f = (\hat{f} \circ f) - (\hat{f}' \circ f) = [m] - [m] = [0].$$

Since f is nonconstant, it follows from theorem 1.3.5 that $\hat{f} - \hat{f}'$ is constant, so $\hat{f} = \hat{f}'$.

(Existence). Suppose now that $g : E_2 \to E_1$ is another nonconstant isogeny of degree n and suppose that we know that $\hat{f}$ and $\hat{g}$ exist. Then,

$$(\hat{f} \circ \hat{g}) \circ (g \circ f) = \hat{f} \circ (\hat{g} \circ g) \circ f \ = \hat{f} \circ [n] \circ f \overset{(*)}{=} [n] \circ \hat{f} \circ f \ = [n] \circ [m] = [nm].$$

Where in $(*)$ we are using that every isogeny is a homomorphism. Let $P \in E_2$,

$$(\hat{f} \circ [n])(P) = \hat{f}([n]P) = \hat{f}(P \overset{n)}{+ \ldots +} P) \overset{\text{hom.}}{=} \hat{f}(P) \overset{n)}{+ \ldots +} \hat{f}(P) = [n](\hat{f}(P)) = ([n] \circ \hat{f})(P).$$

Thus $\hat{f} \circ \hat{g}$ has the requisite property to be $\widehat{f \circ g}$. Hence, as we are working in characteristic zero, it suffices to prove the existence of $\hat{f}$ when f is separable. Thus suppose f to be separable. Since f has degree m, we have from theorem 2.3.8,

$$\# \ker f = m;$$

so clearly,

$$\ker f \subset \ker[m].$$

It now follows from corollary 2.3.9 that there exists an isogeny

$$\hat{f} : E_2 \to E_1$$

such that $\hat{f} \circ f = [m]$.

□

An isogeny related to another one given as in latter theorem deserves a special name.

Definition 2.3.11 (Dual Isogeny) Let $f : E_1 \to E_2$ be an isogeny of degree m. The **dual isogeny** to f is the isogeny

$$\hat{f} : E_2 \to E_1$$

given in the previous theorem. (This assumes $f \neq [0]$. If so, we set $\hat{f} = [0]$).

Here we introduce some important properties of dual isogeny needed to find out the structure of the m-torsion subgroup $E(K)[m]$.

Proposition 2.3.12 *Let $f : E_1 \to E_2$ be an isogeny.*

i) Let $m = \deg f$. Then

$$\hat{f} \circ f = [m] \quad \text{on } E_1 \qquad \text{and} \qquad f \circ \hat{f} = [m] \quad \text{on } E_2.$$

ii) Let $h : E_2 \to E_3$ be another isogeny. Then,

$$\widehat{h \circ f} = \hat{f} \circ \hat{h}.$$

iii) Let $g : E_1 \to E_2$ be another isogeny. Then,

$$\widehat{g + f} = \hat{f} + \hat{g}.$$

iv) For all $m \in \mathbb{Z}$,

$$\widehat{[m]} = [m] \quad \text{and } \deg[m] = m^2.$$

PROOF. If any of the isogenies in (i), (ii) or (iii) is constant, the theorem is trivial. We will assume that all isogenies are nonconstant.

i) The first statement is the defining property of $\hat{f}$. For the second,

$$(f \circ \hat{f}) \circ f = f \circ (\hat{f} \circ f) = f \circ [m] = [m] \circ f.$$

Then, since f is nonconstant, $f \circ \hat{f} = [m]$.

ii) Let $n = \deg h$. Then $\deg(h \circ f) = (\deg h)(\deg f) = nm$. We have

$$(\hat{f} \circ \hat{h}) \circ (h \circ f) = \hat{f} \circ [n] \circ f = [n] \circ \hat{f} \circ f = [nm].$$

And using the uniqueness from theorem 2.3.10, we can deduce that $\hat{f} \circ \hat{h} = \widehat{h \circ f}$.

iii) [73, Th.III.6.2,c]

iv) To prove the first assertion we apply induction in m.

- *Base case.*
  If $m = 0$, $\widehat{[m]} = [0]$ by definition.
  If $m = 1$, $\widehat{[m]} = [1]$ clearly.
- *General case.* Suppose that $\widehat{[m]} = [m]$ for $m \leq N$.

$$\widehat{[N+1]} \overset{(iii)}{=} \widehat{[N]} + \widehat{[1]} \overset{\text{hip.}}{=} [N] + [1] \overset{\text{gr. law}}{=} [N+1].$$

For the second assertion let $d = \deg[m]$. We have

$$[d] = \widehat{[m]} \circ [m] = [m] \circ [m] = [m^2].$$

Since the endomorphism ring of an elliptic curve is a torsion-free $\mathbb{Z}$-module by proposition 2.3.5, $d = m^2$.

□

2.4 Structure of $E[m]$

Before writing the structure of $E[m]$, we recall a result from group theory:

Lemma 2.4.1 *Let A be a finite abelian group of order n^r. Assume that for every $d|n$ we have $\#A[d] = d^r$, where*

$$A[d] = \{a \in A : ord(a) = d\}.$$

Then

$$A \simeq \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^r.$$

PROOF. First, let A be a finite abelian group of order p^r, with p prime, and such that $\#A[p] = p^r$. This means that every element in A has order p. By Classification Theorem of Finite Abelian Groups, the only possibility is

$$A \simeq \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^r.$$

Suppose now that $n = p^\alpha$, hence A is a finite abelian group of order $n^r = p^{\alpha r}$. By assumption, we know that $\#A[p^\alpha] = p^{\alpha r}$, so A is isomorphic to its Sylow p-subgroup and every element of its has order p^α. Again, by Classification Theorem of Finite Abelian Groups, the only possibility is

$$A \simeq \left(\frac{\mathbb{Z}}{p^\alpha\mathbb{Z}}\right)^r.$$

Finally, let A be a finite abelian group of order n^r, with $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$. We know that, since A is a finite abelian group, it is isomorphic to the direct sum of its distinct Sylow p-subgroups. Thus,

$$A \simeq \left(\frac{\mathbb{Z}}{p_1^{\alpha_1}\mathbb{Z}}\right)^r \oplus \cdots \oplus \left(\frac{\mathbb{Z}}{p_k^{\alpha_k}\mathbb{Z}}\right)^r \simeq \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^r.$$

□

Now we can establish the structure of the m-torsion subgroup of an elliptic curve E, $E[m]$, in the following theorem. Note that $E[m]$ is another notation for $\ker[m]$.

Theorem 2.4.2 (Structure of the m-torsion subgroup) *Let E be an elliptic curve over a field K with $char(K) = 0$ and let m to be a positive integer. Then*

$$E[m] \cong \frac{\mathbb{Z}}{m\mathbb{Z}} \oplus \frac{\mathbb{Z}}{m\mathbb{Z}}.$$

PROOF. As $\deg[m] = m^2$, then $[m]$ is separable, since it is finite over a perfect field, thus algebraic and then separable. Using theorem 2.3.8.iii we have

$$m^2 = \deg[m] = \#\ker[m] = \#E[m].$$

Further, for every integer d dividing m we have $\#E[d] = d^2$. Now, as $E[m]$ is a finite abelian group, by lemma 2.4.1 we have

$$E[m] \cong \frac{\mathbb{Z}}{m\mathbb{Z}} \oplus \frac{\mathbb{Z}}{m\mathbb{Z}}.$$

□

Chapter 3

The Mordell-Weil Theorem

The main aim of this chapter is proving the Mordell-Weil theorem:

Theorem 3.0.3 *Let K be a number field, and let E/K be an elliptic curve. Then the group $E(K)$ is finetely generated.*

To achieve this purpose, we are going to follow two quite distinct steps:

I) **To prove the Weak Mordell-Weil Theorem.** (Section 3.1.5).

Theorem 3.0.4 (Weak Mordell-Weil Theorem) *Let K be a number field, let E/K be an elliptic curve and let $m \in \mathbb{Z}$ with $m \geq 2$. Then*

$$E(K)/mE(K)$$

is a finite group.

This assertion is neccesary for the proof of the Mordell-Weil theorem but it is not enough because it does not implies that $E(K)$ is a finitely generated group. For example, we have that $\mathbb{R}/m\mathbb{R} = \{0\}$ for every integer $m \geq 1$, yet $(\mathbb{R},+)$ is not a finitely generated group.

To prove the Weak Mordell-Weil theorem, we need to develope some theory about formal groups (subsection 3.1.2), minimal Weierstrass equations (subsection 3.1.3) and reduction modulo π of a curve (subsection 3.1.4).

II) **To use the Descent Procedure** (Section 3.2).

Theorem 3.0.5 (Descent Theorem) *Let A be an abelian group. Suppose that there exists a (height) function*

$$h : A \to \mathbb{R},$$

with the following properties:

(a) Let $Q \in A$. There is a constant C_1, depending on A and Q, such that

$$h(P+Q) \leq 2h(P) + C_1 \qquad \text{for all } P \in A.$$

(b) There are an integer $m \geq 2$ and a constant C_2, depending on A, such that

$$h(mP) \geq m^2 h(P) - C_2 \qquad \text{for all } P \in A.$$

(c) For every constant C_3, the set

$$\{P \in A : h(P) \leq C_3\}$$

is finite.

Suppose further that for the integer m in (ii), the quotient group A/mA is finite. Then A is finitely generated.

To use this theorem to prove the Mordell-Weil theorem, we have to develope some theory about heighs on projective spaces (subsection 3.2.1), and find a heigh function on elliptic curves (subsection 3.2.2).

It is clear that Mordell-Weil theorem follows from these two steps.

3.1 The Weak Mordell-Weil Theorem

In this section we are going to prove the Weak Mordell-Weil Theorem, for which we need some previous results. In this section we will use the following notation:

- K is a field complete with respect to a discrete valuation v.
- R is the ring of integers of K, $R = \{x \in K : v(x) \geq 0\}$.
- R^* is the unit group of R, $R^* = \{x \in K : v(x) = 0\}$.
- $\mathcal{M}$ is maximal ideal of R, $\mathcal{M} = \{x \in K : v(x) > 0\}$.
- π, a uniformizer of R, $\mathcal{M} = \pi R$.
- k the residue field of R, $k = R/\mathcal{M}$.

3.1.1 Hensel's Lemma

We present now the Hensel's Lemma (also called Hensel's Lifting), which is going to be needed in this chapter. Then we adapt its content to the situation we are interested in. To prove this lemma we have used [39, th. C.1] and [82, section 5].

Lemma 3.1.1 (Hensel's Lemma) *Let K be a local field, complete with respect to a valuation v, R the ring of integers in K and $\mathcal{M} = \pi R$ its maximal ideal. Let $f(x) \in R[x]$ and suppose that there exist $\alpha \in R$ such that*

$$f(\alpha) = 0 \ (mod\ \pi), \qquad f'(\alpha) \neq 0 \ (mod\ \pi)$$

where f' is the formal derivative of f. Then, there exists an element $\beta \in R$ satisfying

$$f(\beta) = 0, \qquad \beta = \alpha \ (mod\ \pi).$$

PROOF. We build a sequence $(x_n) \subset R$ with $x_1 = \alpha$ and such that for all n,

i) $f(x_n) = 0 \pmod{\pi^n}$,

ii) $x_{n+1} = x_n \pmod{\pi^n}$.

It is clear from the hypothesis that $\alpha = x_1$ satisfies the first condition. Suppose that x_n satisfies it too. Then, $f(x_n) = c\pi^n$ for any $c \in R$. Let $x_{n+1} = x_n + b\pi^n$ for a $b \in R$, to be chosen later.

Note that if $f(X+Y) = f_0(X) + f_1(X)Y + f_2(X)Y^2 + \dots$ for $f_i \in R[X]$ we have $f_0(X) = f(X), f_1(X) = f'(X), \dots$ Then,

$$f(x_{n+1}) = f(x_n + b\pi^n) = f(x_n) + f'(x_n)b\pi^n = c\pi^n + f'(x_n)b\pi^n = \pi^n[c + bf'(x_n)] \pmod{\pi^{n+1}}.$$

Note also that since $x_n = x_1 = \alpha \pmod{\pi}$, we have $f'(x_n) = f'(\alpha) \pmod{\pi}$. Namely, $f'(x_n)$ is a unit in $R/\pi R$, so we can write $f'(x_n) = u\pi$ for any $u \in R^*$.

Now, set $b = -u^{-1}c \in R \implies bf'(x_n) = -u^{-1}cu\pi = -c\pi$. We have then

$$\begin{aligned} f(x_{n+1}) &= \pi^n[c + bf'(x_n)] && (\text{mod } \pi^{n+1}) \\ &= (\pi^n c - \pi^{n+1}c) && (\text{mod } \pi^{n+1}) \\ &= f(x_n) && (\text{mod } \pi^{n+1}) \\ &= 0 && (\text{mod } \pi^{n+1}). \end{aligned}$$

(ii) $\implies$ (x_n) is Cauchy.
(i) $\implies$ $\beta = \lim x_n$ is a root of f and $\beta \in R$ because K is complete.
Moreover, as $x_n = \alpha \pmod{\pi}$ $\forall n$, then $\beta = \alpha \pmod{\pi}$.

□

Remark 3.1.2. We can generalize Hensel's Lemma as follows:

Let R be commutative a ring complete with respect to an ideal $I \subset R$, i.e., R is complete with respect to the topology in which $\{I^n\}_{n\geq 1}$ forms a basis of open neighborhoods of 0; and let $F(w) \in R[w]$ be a polynomial. Suppose that there exists $\alpha \in R$ such that (for some integer $n \geq 1$)

$$F(\alpha) \in \mathcal{M}^n \quad \text{and} \quad F'(\alpha) \in R^*.$$

Then for any $\gamma \in R$ satisfying $\gamma = F'(\alpha) \pmod{I}$, the sequence

$$w_0 = \alpha \quad w_{m+1} = w_m + F(w_m)/\gamma$$

converges to an element $\beta \in R$ satisfying

$$F(\beta) = 0 \quad \text{and} \quad \beta = \alpha \pmod{I}$$

Further, if R is an integral domain, then these conditions determine β uniquely.

3.1.2 The Formal Group of an Elliptic Curve

Let E be an elliptic curve. In this subsection we study an 'infinitesimal' neighborhood of E centered at its origin, $\mathcal{O}$. As we will see, this leads to a power series ring in one variable, say $K[[z]]$, for some uniformizer z at $\mathcal{O}$. We can express the Weierstrass coordinates x and y as a formal Laurent series in z. Further, we can write down a power series $F(z_1, z_2) \in K[[z_1, z_2]]$ which formally gives the group law on E.

Expansion around $\mathcal{O}$

We are about to study the structure of an elliptic curve and its addition law "close to the origin". To do this it is convenient to make a change of variables, so let

$$z = -\frac{x}{y} \text{ and } w = -\frac{1}{y} \quad \left(\text{so } x = \frac{z}{w} \text{ and } y = -\frac{1}{w}\right).$$

The origin $\mathcal{O}$ on E is now the point $(z, w) = (0, 0)$, and z has a zero of order 1 at $\mathcal{O}$, namely z is a local uniformizer at $\mathcal{O}$. The Weierstrass equation for E in variables x and y,

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

becomes

$$E : w = z^3 + (a_1z + a_2z^2)w + (a_3 + a_4z)w^2 + a_6w^3 \qquad (= f(z, w)).$$

The idea is to substitute this equation into itself recursevely so as to express w as a power series in z:

$$\begin{aligned} w &= z^3 + (a_1 z + a_2 z^2)w + (a_3 + a_4 z)w^2 + a_6 w^3 \\ &= z^3 + (a_1 z + a_2 z^2)[z^3 + (a_1 z + a_2 z^2)w + (a_3 + a_4 z)w^2 + a_6 w^3] \\ &+ (a_3 + a_4 z)[z^3 + (a_1 z + a_2 z^2)w + (a_3 + a_4 z)w^2 + a_6 w^3]^2 \\ &+ a_6[z^3 + (a_1 z + a_2 z^2)w + (a_3 + a_4 z)w^2 + a_6 w^3]^3 \\ &\vdots \\ &= z^3 + a_1 z^4 + (a_1^2 + a_2)z^5 + (a_1^3 + 2a_1 a_2 + a_3)z^6 + \dots \\ &= z^3(1 + A_1 z + A_2 z^2 + \dots), \end{aligned}$$

where $A_i \in \mathbb{Z}[a_1, \dots, a_6]$ is a polynomial in the coefficients of E. We must show that this procedure convergs to a power series $w(z) \in \mathbb{Z}[a_1, \dots, a_6][[z]]$ and that the equality

$$w(z) = f(z, w(z))$$

holds in the power series ring.

To more precisely decribe the algorithm for producing $w(z)$, define a sequence

$$f_1(z, w) = f(z, w) \qquad \text{and} \qquad f_{m+1} = f(z, f_m(z, w)). \tag{3.1}$$

Then we take

$$w(z) = \lim_{m \to \infty} f_m(z, 0)$$

provided this limit makes sense in $\mathbb{Z}[a_1, \dots, a_6][[z]]$.

The two following assertions are special cases of the generalization of Hensel's Lemma, remark 3.1.2:

Proposition 3.1.3 *We have the following two facts:*

i) The procedure described above gives a power series

$$w(z) = z^3(1 + A_1 z + A_2 z^2 + \dots) \in \mathbb{Z}[a_1, \dots, a_6][[z]].$$

ii) $w(z)$ is the unique power series satisfying

$$w(z) = f(z, w(z)).$$

PROOF. It suffices to use the generalization of Hensel's Lemma 3.1.2 with

$$R = \mathbb{Z}[a_1, \dots, a_6][[z]], \qquad I = (z),$$

$F(w) = f(z, w) - w = z^3 + (a_1 z + a_2 z^2)w + (a_3 + a_4 z)w^2 + a_6 w^3 - w, \qquad \alpha = 0, \qquad \gamma = -1.$
With this assumptions, we have

$$F(0) = f(z, 0) \in (z),$$

$$\begin{aligned} F'(w) &= \frac{\partial}{\partial w} f(z,w) - 1 \\ &= a_1 z + a_2 z^2 + 2(a_3 + a_4 z)w + 3a_6 w^2 - 1, \\ F'(0) &= a_1 z + a_2 z^2 - 1. \end{aligned}$$

As the independent term of $F'(0) \neq 0$, $F'(0) \in R^*$. If we take $\gamma = -1$ we have $-1 = a_1 z + a_2 z^2 - 1 \pmod{(z)}$, so the sequence

$$w_0 = 0 \qquad w_{m+1} = w_m + F(w_m) = w_m + f(z, w_m) - w_m = f(z, w_m)$$

converges to a unique element $\beta \in \mathbb{Z}[a_1, \ldots, a_6][[z]]$:

$$\beta = \lim_{m\to\infty} w_m = \lim_{m\to\infty} f(z, w_{m-1}) = f(z, \beta).$$

But $w_m = f_m(z, 0)$ (where f_m is defined in equation (3.1) above) as we can prove by induction in m:

- For $m = 1$ we have

$$w_1 = w_0 + F(w_0) = w_0 + f(z, w_0) - w_0 = f(z, w_0) \overset{w_0=0}{=} f(z, 0) = f_1(z, 0).$$

- Suppose that $w_m = f_m(z, 0)$. Thus,

$$w_{m+1} = w_m + F(w_m) \;\; = f(z, w_m) \overset{\text{Hip.}}{=} f(z, f_m(z, 0)) \;\; = f_{m+1}(z, 0).$$

So,

$$\beta = \lim_{m\to\infty} w_m = \lim_{m\to\infty} f_m(z, 0) = w(z)$$

And thus, $w(z) \in \mathbb{Z}[a_1, \ldots, a_6][[z]]$ and is the unique element with $w(z) = f(z, w(z))$.

□

Using the power series $w(z)$ we can find the **Laurent series** for x and y,

$$x = \frac{z}{w(z)} = \frac{1}{z^2} - \frac{a_1}{z} - a_2 - a_3 z - (a_4 + a_1 a_3) z^2 + \cdots$$

$$y = -\frac{1}{w(z)} = -\frac{1}{z^3} + \frac{a_1}{z^2} + \frac{a_2}{z} + a_3 + (a_4 + a_1 a_3) z + \cdots .$$

We note that $x(z), y(z) \in \mathbb{Z}[a_1, \ldots, a_6][[z]]$ and the pair $(x(z), y(z))$ provides a 'formal solution' to the Weierstrass equation

$$E : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6,$$

that is, a solution in the field of formal power series. If E is defined over a field K, we might try to produce points of E by taking $z \in K$ and looking at $(x(z), y(z))$. In general, there

is no way to attach a meaning to an infinite series as $x(z)$. But if K is a complete local field with ring of integers R and maximal ideal $\mathcal{M}$, and if the coefficients satisfy $a_i \in R$ and $z \in \mathcal{M}$, then the power series $x(z)$ and $y(z)$ converge to give a point of $E(K)$. This gives an injection (with inverse $z = -x(z)/y(z)$)

$$\mathcal{M} \to E(K),$$

and it is easy to characterize the image as those (x, y) with $x^{-1} \in \mathcal{M}$. But we will focus on this question later in this chapter.

Returning to formal series, we now look for the power series formally giving the addition law on E. Let z_1, z_2 be independent inderterminates and let $w_i = w(z_i)$ for $i = 1, 2$. In the (z, w)-plane, the line connecting (z_1, w_1) to (z_2, w_2) has slope

$$\lambda = \lambda(z_1, z_2) = \frac{w_2 - w_1}{z_2 - z_1} = \sum_{n=3}^{\infty} A_n \frac{z_2^n - z_1^n}{z_2 - z_1} \in \mathbb{Z}[a_1, \ldots, a_6][[z_1, z_2]]$$

Note that λ has no constant or linear term. Letting

$$\nu = \nu(z_1, z_2) = w_1 - \lambda z_1 \in \mathbb{Z}[a_1, \ldots, a_6][[z_1, z_2]]$$

the connecting line has the equation $w = \lambda z + \nu$. Substituting this into the Weierstrass equation gives a cubic in z

$$C_3 z^3 + C_2 z^2 + C_1 z + C_0 = 0$$

with

$$\begin{aligned} C_3 &= a_6\lambda^3 + a_4\lambda^2 + a_2\lambda + 1, \\ C_2 &= 3a_6\lambda^3\nu + 2a_4\lambda\nu + a_3\lambda^2 + a_2\nu + a_1\lambda, \\ C_1 &= 3a_6\lambda\nu^2 + a_4\nu^2 + 2a_3\lambda\nu + a_1\nu - \lambda, \\ C_0 &= a_6\nu^3 + a_3\nu^3 - \nu. \end{aligned}$$

If we want the main coefficient to be 1 we define the new coefficients $C_i' = C_i/C_1$ for $i = 1, 2, 3, 4$. Two of the roots of this equation are z_1 and z_2. Looking at the quadratic term, the third root, say z_3, can be expressed as a power series in z_1 and z_2. To see this, we write

$$(z - z_1)(z - z_2)(z - z_3) = z^3 - (z_1 + z_2 + z_3)z^2 + (z_1z_2 + z_1z_3 + z_2z_3)z + z_1z_2z_3,$$

and equate the coefficients with the C_i' from above, getting

$$z_3 = z_3(z_1, z_2) = -z_1 - z_2 - \frac{3a_6\lambda^3\nu + 2a_4\lambda\nu + a_3\lambda^2 + a_2\nu + a_1\lambda}{a_6\lambda^3 + a_4\lambda^2 + a_2\lambda + 1} \in \mathbb{Z}[a_1, \ldots, a_6][[z_1, z_2]]$$

For the group law in E, $(z_1, w_1) + (z_2, w_2) + (z_3, w_3) = \mathcal{O}$, so to add the first two, we need the formula for the inverse. In the (x, y)-plane, the opposite element of (x, y) is

$(x, -y - a_1x - a_3)$ as we saw in the previous chapter, section 2.2. Hence, recalling that $z = -x/y$, the inverse of (z, w) in the (z, w)-plane will have z-coordinate:

$$i(z) = \frac{x(z)}{y(z) + a_1x(z) + a_3} = \frac{z^{-2} - a_1z^{-1} - \cdots}{-z^{-3} + 2a_1z^{-2} + \cdots} \in \mathbb{Z}[a_1, \ldots, a_6][[z_1, z_2]].$$

Definition 3.1.4 (Formal Addition Law) The work above leads us to define the **formal addition law**:

$$\begin{aligned} F(z_1, z_2) &= i(z_3(z_1, z_2)) \\ &= z_1 + z_2 - a_1z_1z_2 - a_2(z_1^2z_2 + z_1z_2^2) - (2a_3z_1^3 - (a_1a_2 - 3a_3)z_1^2z_2^2 + 2a_3z_1z_2^2) + \cdots \\ &\in \mathbb{Z}[a_1, \ldots, a_6][[z_1, z_2]]. \end{aligned}$$

From the corresponding properties for E we deduce that $F(z_1, z_2)$ satifies

$$\begin{array}{rcll} F(z_1, z_2) & = & F(z_2, z_1) & \text{(commutativity)} \\ F(z_1, F(z_2, z)) & = & F(F(z_1, z_2), z) & \text{(associativity)} \\ F(z, i(z)) & = & 0 & \text{(inverse).} \end{array}$$

The power series $F(z_1, z_2)$ might be described as *a group law without any group elements*. Such objects are called formal groups and we will see some of their properties in the following section.

Formal groups

Let R be a ring. We are about to define a new structure over R: a formal group.

Definition 3.1.5 (Formal Group) A **(one-parameter commutative) formal group $\mathscr{F}$ defined over** R is a power series $F(X, Y) \in R[[X, Y]]$ satisfying:

i) $F(X, Y) = X + Y +$ (terms of degree ≥ 2).

ii) $F(X, F(Y, Z)) = F(F(X, Y), Z)$ (associativity).

iii) $F(X, Y) = F(Y, X)$ (commutativity).

iv) There is a unique power series $i(T) \in R[[T]]$ such that $F(T, i(T)) = 0$ (inverse).

v) $F(X, 0) = X$ and $F(0, Y) = Y$.

We call $F(X, Y)$ the **formal group law of $\mathscr{F}$**.

Example 3.1.6 (Formal group of an elliptic curve) Let E be an elliptic curve given by a Weierstrass equation with coefficients in R. The **formal group associated to** E, denoted by $\hat{E}$, is given by the power series $F(z_1, z_2)$ decribed in definition 3.1.4.

Definition 3.1.7 (Homomorphisms between formal groups) Let $(\mathscr{F}, F)$ and $(\mathscr{G}, G)$ be two formal groups over R. A **homomorphism from $\mathscr{F}$ to $\mathscr{G}$ over** R is a power series (with no constant term) $f(T) \in R[[T]]$ satisfying

$$f(F(X,Y)) = G(f(X), f(Y)).$$

$\mathscr{F}$ and $\mathscr{G}$ are **isomorphic over** R if there are homorphisms $f : \mathscr{F} \to \mathscr{G}$ and $g : \mathscr{G} \to \mathscr{F}$ defined over R with

$$g(f(T)) = T = f(g(T)).$$

Example 3.1.8 (Multiplication-by-m map) Let $(\mathscr{F}, F)$ be a formal group. We can define homomorphisms

$$[m] : \mathscr{F} \to \mathscr{F}$$

inductively for $m \in \mathbb{Z}$ by

$$[0](T) = 0, \quad [m+1](T) = F([m](T), T), \quad [m-1](T) = F([m](T), i(T)).$$

We can see, by indution in m, that for every $m \in \mathbb{Z}$,

$$[m]F(X,Y) = F([m]X, [m]Y).$$

- If $m = 0$.
  It is trivial since $[0]F(X,Y) = 0$ and $F([m]0, [m]0) = F(0,0) = 0$.

- Suppose that $[m]F(X,Y) = F([m]X, [m]Y)$ holds for $m > 0$.

$$\begin{aligned} F(X,Y) &= F([m]F(X,Y), F(X,Y)) \\ &\overset{\text{Hip.}}{=} F(F([m]X, [m]Y), F(X,Y)) \\ &\overset{\text{as.}}{=} F([m]X, F([m]Y, F(X,Y))) \\ &\overset{\text{co.}}{=} F([m]X, F(F(X,Y), [m]Y)) \\ &\overset{\text{as.}}{=} F([m]X, F(X, F(Y, [m]Y))) \\ &\overset{\text{as.}}{=} F(F([m]X, X), F([m]Y, Y)) \\ &= F([m+1]X, [m+1]Y). \end{aligned}$$

- Suppose that $[m]F(X,Y) = F([m]X, [m]Y)$ holds for $m < 0$.

$$\begin{aligned}
F(X,Y) &= F([m-1]F(X,Y), i(Y)) \\
&= F([m-1]F(X,0), i(Y)) \\
&= F(F([m]X,0)i(Y)) \\
&= F([m]X, F(0, i(Y))) \\
&= F([m]X, F(F(0,0), i(Y))) \\
&= F([m]X, F(0, F(0, i(Y)))) \\
&= F([m]X, F(0, [m-1]F(0,Y))) \\
&= F([m]X, F(0, [m-1]Y)) \\
&= F(F([m]X,0), [m-1]Y) \\
&= F([m-1]F(X,0), [m-1]Y) \\
&= F([m-1]X, [m-1]Y).
\end{aligned}$$

Proposition 3.1.9 *Let $\mathscr{F}$ be a formal group over R, and let $m \in \mathbb{Z}$.*

i) $[m](T) = mT +$ *(higher order terms).*

ii) If $m \in R^*$, then $[m] : \mathscr{F} \to \mathscr{F}$ is a homomorphism.

PROOF.

i) For $m \geq 0$ this is a trivial induction using the recursive definition of $[m]$ and the fact that $f(X,Y) = X + Y + \cdots$. Then, from

$$0 = F(T, i(T)) = T + i(T) + \cdots .$$

we have $i(T) = -T + \cdots$; and now the downward induction for $m < 0$ is also clear.

ii) This follows from (i) and the following lemma.

□

Lemma 3.1.10 *Let $a \in R^*$ and $f(T) \in R[[T]]$ a power series starting*

$$f(T) = aT + \cdots .$$

Then there is a unique power series $g(T) \in R[[T]]$ such that $f(g(T)) = T$ and $g(f(T)) = T$.

PROOF. We contruct a sequence of polynomials $g_n(T) \in R[T]$ such that

$$f(g_n(T)) \equiv T \pmod{T^{n+1}} \qquad \text{and} \qquad g_{n+1}(T) \equiv g_n(T) \pmod{T^{n+1}}.$$

As R is complete, there exists the limit $g(T) = \lim g_n(T) \in R[T]$. And from the fact

$$f(g_{n+1})(T) \equiv f(g_n(T)) \pmod{T^{n+1}} \equiv T \pmod{T^{n+1}} \ \forall n,$$

we have that $f(g(T)) = T$.

To start the induction, let $g_1(T) = a^{-1}T$, which clearly satisfies the condition

$$f(g_1(T)) \equiv T \pmod{T^2}.$$

Suppose now $g_{n-1}(T)$ satisfies them too. We look for $\lambda \in R$ such that

$$g_n(T) = g_{n-1}(T) + \lambda T^n$$

has the desired property. We compute

$$\begin{aligned} f((g_n)(T)) &= f(g_{n-1}(T) + \lambda T^n) \\ &\equiv f(g_{n-1}(T)) + a\lambda T^n \pmod{T^{n+1}} \\ &\equiv T + bT^n + a\lambda T^n \pmod{T^{n+1}} \end{aligned}$$

for some $b \in R$ by the induction hypothesis. It thus suffices to take $\lambda = -ba^{-1} \in R$. This shows that $g(T)$ exists.
Now, applying g to $f(g(T)) = T$ gives $g(f(g(T))) = g(T)$, which is the identity in the power-series ring $R[[g(T)]]$, so $g(f(T)) = T$. Finally, if $f(h(T)) = T$,

$$g(T) = g(f(h(T))) = (g \circ f)(h(T)) = h(T),$$

which shows the uniqueness of $g(T)$.

□

Groups Associated to Formal Groups

In general a formal group is nothing but a group operation, without "real" elements of group. But if the ring R is local and complete and if the variables are assigned to values in the maximal ideal $\mathcal{M} \subset R$, the power series giving the formal group will converge.

Definition 3.1.11 (Group associated to a formal group) The **group associated to the formal group $\mathscr{F}$ over** R, denoted $\mathscr{F}(\mathcal{M})$ is the set $\mathcal{M}$ with the group operations

$$x \oplus_{\mathscr{F}} y = F(x, y),$$

$$\ominus_{\mathscr{F}} x = i(x).$$

Where $x, y \in \mathcal{M}$.

Similary, for $n \geq 1$, $\mathscr{F}(\mathcal{M}^n)$ is the subgroup of $\mathscr{F}(\mathcal{M})$ consisting of the set of $\mathcal{M}^n$.

Since R is complete, the power series $F(x, y)$ and $i(x)$ converge in R for $x, y \in \mathcal{M}$; and then the axioms for a formal group inmediately imply that $\mathscr{F}(\mathcal{M})$ is a group and $\mathscr{F}(\mathcal{M}^n)$ is a subgroup.

The following example contains the main idea of the use of formal groups and the reduction procedure (which we will see in next section) to study $E(K)$ in a simpler way.

Example 3.1.12 Let $\hat{E}$ be the formal group associated to the elliptic curve E/K (example 3.1.6), where K is the quotient field of R. As we noted above, the power series $x(z)$ and $y(z)$ give a map

$$\mathcal{M} \to E(K); \qquad z \mapsto (x(z), y(z)).$$

In the way the power series for $\hat{E}$ was defined, this map gives a homomorphism

$$\hat{E}(\mathcal{M}) \to E(K).$$

As we will see in the next section, there is often an exact sequence

$$0 \to \hat{E}(\mathcal{M}) \to E(K) \to \tilde{E}(k) \to 0,$$

where $\tilde{E}$ is a certain elliptic curve defined over the residue field k. This way, to study $E(K)$ we can study the formal group $\hat{E}$ and an elliptic curve over a smaller (and hopefully simpler) field k.

Proposition 3.1.13 *The following statements hold:*

i) For each $n \geq 1$, the map

$$\mathscr{F}(\mathcal{M}^n)/\mathscr{F}(\mathcal{M}^{n+1}) \to \mathcal{M}^n/\mathcal{M}^{n+1}$$

induced by the identity map on sets is an isomorphism of groups.

ii) Let $p = $ char k ($p = 0$ is allowed), where k is the residue field $k = K/R$. Then every torsion element of $\mathscr{F}(\mathcal{M})$ has order a power of p.

PROOF.

i) Since essentially the underlying sets are the same, it suffices to show that the map is a homomorphism. But for $x, y \in \mathcal{M}^n$,

$$x \oplus_{\mathscr{F}} y = F(x, y) \equiv x + y \pmod{\mathcal{M}^{2n}}.$$

Hence $x + y \in M^{2n} \subset M^n$.

ii) Let $x \in \mathscr{F}(\mathcal{M})$ be a m-torsion element. To show that there exists $n \in \mathbb{N}$ such that $[p^n]x = 0$ we can consider the element $[p^{n-1}]x$ and show that its order is p. In other words, it suffices to prove that there are no non-zero torsion elements of order prime to p.

Thus let $m \geq 1$ be prime to p (arbitrary if $p = 0$) and $x \in \mathscr{F}(\mathcal{M})$ an element with $[m]x = 0$. We must see that $x = 0$.

Since m is prime to p, $m \notin \mathcal{M}$, namely, $m \in R^*$. From proposition 3.1.9.ii, $[m]$ is an isomorphism of the formal group $\mathscr{F}$ over R to itself, so induces an isomorphism

$$[m] : \mathscr{F}(\mathcal{M}) \xrightarrow{\sim} \mathscr{F}(\mathcal{M}).$$

In particular, it has trivial kernel, so $x = 0$.

□

3.1.3 Minimal Weierstrass Equations

Let E/K be an elliptic curve. Recall that if we have the curve in a Weierstrass form, we can change coordinates doing

$$(x, y) \mapsto (u^{-2}x, u^{-3}y),$$

with $u \in \mathcal{M}$. Hence, we have

$$\begin{aligned} y^2 + a_1xy + a_3y &= x^3 + a_2x^2 + a_4x + a_6, \\ u^{-6}y^2 + a_1u^{-5}xy + a_3u^{-3}y &= u^{-6}x^3 + a_2u^{-4}x^2 + a_4u^{-2}x + a_6, \\ y^2 + a_1uxy + a_3u^3y &= x^3 + a_2u^2x^2 + a_4u^4x + a_6u^6. \end{aligned}$$

Namely, each a_i becomes $a_i \cdot u^i$. If we choose u divisible by a large power of π, we can have the coefficients of the Weiestrass form in R, because $v(a_i \cdot u^i) \geq 0$ for every i. Then $\Delta \in R$ too, (recall the associated quantities table 2.1); and since v is discrete, we can look for an equation with $v(\Delta)$ as small as possible.

Definition 3.1.14 (Minimal equation of an elliptic curve) Let E/K be an elliptic curve. A Weierstrass equation is called a **minimal (Weiestrass) equation for** E **at** v if $v(\Delta)$ is minimized, subjet to the condition $a_1, a_2, a_3, a_4, a_6 \in R$. This value of $v(\Delta)$ is the valuation of the minimal discriminant of E at v.

Remark 3.1.15. How can one tell that a given Weierstrass equation is minimal? Let $\Delta \in R$ be the discriminant of the equation. If the equation is not minimal, there is a change of variables (remark 2.1.3) giving a new equation with discriminant $\Delta' = u^{12}\Delta \in R$. Then,

$$v(\Delta') = v(u^{12}\Delta) = v(u^{12}) + v(\Delta) = 12k + v(\Delta)$$

for any $k \in \mathbb{Z}$. Thus $v(\Delta)$ can only be changed by multiples of 12, so we can conclude that

$$\text{if } a_i \in R \text{ and } v(\Delta) < 12, \text{ then the equation is minimal.}$$

In fact, if $\text{char}(K) \neq 2, 3$ the converse holds. Moreover, for an arbitrary field K there is an algorithm, known as Tate's algorithm [74, pg. 36], which determines whether a given equation is minimal.

Proposition 3.1.16 *We have the following statements:*

i) Every elliptic curve E/K has a minimal Weierstrass equation.

ii) A minimal Weierstrass equation is unique up to a change of variables

$$\begin{aligned} x &= u^2x' + r, \\ y &= u^3y' + u^2sx' + t, \end{aligned}$$

with $u \in R^*$ and $r, s, t \in R$.

iii) Conversely, if one starts with any Weierstrass equation with coefficients $a_i \in R$, then any change of coordinates

$$x = u^2x' + r,$$
$$y = u^3y' + u^2sx' + t,$$

used to produce a minimal equation satisfies $u, r, s, t \in R$.

PROOF.

i) It is followed by the fact that one can find some Weierstrass equation with $a_i \in R$ and v is discrete.

ii) We know that any Weierstrass equation for E/K is unique up to the standard change of variables by remark 2.1.3, with $u \in K^*$ and $r, s, t \in K$. Now suppose the given equation and the new equation are both minimal and that the coefficients are in R. From the definition of minimality, $v(\Delta) = v(\Delta')$, but $\Delta' = u^{12}\Delta$. Thus, $u \in R^*$. Now, from the associated quantities table 2.1.3, we have that from the transformation of b_6 it follows $4r^3 \in R$, so $r \in R$. Finally, the transformation for a_2 gives $s \in R$ and that for a_6 gives $t \in R$.

iii) Since $\Delta' = u^{12}\Delta$ and $v(\Delta) \geq v(\Delta')$, because the new equation is to be minimal, we see that $v(u) \geq 0$, hence $u \in R$. To show that $r, s, t \in R$ we can repeat the argument in the statement above.

□

3.1.4 Reduction Modulo π

Let us consider the natural reduction map

$$R \longrightarrow k = R/\pi R; \qquad t \mapsto \tilde{t},$$

and suppose that we have a minimal Weierstrass equation for E/K. We reduce its coefficients modulo π to obtain a (possibly singular) curve:

$$\tilde{E} : y^2 + \tilde{a}_1xy + \tilde{a}_3y = x^3 + \tilde{a}_2x^2 + \tilde{a}_4x + \tilde{a}_6.$$

The curve $\tilde{E}/K$ is called the **reduction of E modulo π**. From proposition 3.1.16.ii, since we started with a minimal equation for E, the equation for $\tilde{E}$ is unique up to the standard change of coordinates (remark 2.1.3) for Weierstrass equations over k.

Let $P \in E(K)$. We can find homogeneous coordinates $P = [x_0 : y_0 : z_0]$ with $x_0, y_0, z_0 \in R$ and at least one in R^*. Then the reduced point $\tilde{P} = [\tilde{x}_0 : \tilde{y}_0 : \tilde{z}_0]$ is in $E(k)$. This gives a **reduction map**

$$E(K) \to E(k); \qquad P \mapsto \tilde{P}.$$

Remark 3.1.17. More generally, one can define a reduction map

$$\mathbb{P}^n(K) \to \mathbb{P}^n(k)$$

and the above map is just the restriction to $E(K) \subset \mathbb{P}^2(K)$.

Now the curve $\tilde{E}/K$ may or may not be singular, but in any case, $\tilde{E}_{ns}(k)$ forms a group from proposition 2.2.7. We define two subsets of $E(K)$, the **non-singular reduction** and the **kernel of reduction** respectively, as follows:

$$E_0(K) = \{P \in E(K) : \tilde{P} \in \tilde{E}_{ns}(k)\},$$
$$E_1(K) = \{P \in E(K) : \tilde{P} = \tilde{\mathcal{O}}\}.$$

Proposition 3.1.18 *There is a short exact sequence of abelian groups*

$$0 \to E_1(K) \xrightarrow{\alpha} E_0(K) \xrightarrow{\beta} \tilde{E}_{ns}(k) \to 0,$$

where β is the restriction to $E_0(K)$ of the reduction map modulo π.

PROOF.

- $E_0(K)$ is a subgroup of $E(K)$.
  We just have to see that

  $$P, Q \in E_0(K) \implies P + Q \in E_0(K).$$

  But from the definition of $E_0(K)$, this is equivalent to

  $$\tilde{P}, \tilde{Q} \in \tilde{E}_{ns}(k) \implies \widetilde{P + Q} \in \tilde{E}_{ns}(k).$$

  As the group law on $E(K)$ and $\tilde{E}(k)$ are defined by taking intersection of E with lines in $\mathbb{P}^2$, it is suffice to check that the reduction map $\mathbb{P}^2(K) \xrightarrow{\gamma} \mathbb{P}^2(k)$ takes lines to lines. But this is easy to prove. Let $P = [x_0 : y_0 : z_0] \in \mathbb{P}^2(K)$ with $x_0, y_0, z_0 \in R$ and let $L : Y = mX + bZ$ be a line in $\mathbb{P}^2(K)$. We have to see that $\gamma(P) = \tilde{P}$ satisfies the equation of the reduction of L, namely $\tilde{L} : Y = \tilde{m}X + \tilde{b}Z$. As $P \in L$ we have $y_0 = mx_0 + bz_0$, then $P = [x_0 : mx_0 + bz_0 : z_0]$ and

  $$\tilde{P} = [\tilde{x}_0 : \widetilde{mx_0 + bz_0} : \tilde{z}_0] = [\tilde{x}_0 : \tilde{m}\tilde{x}_0 + \tilde{b}\tilde{z}_0 : \tilde{z}_0]$$

  Thus, $\tilde{y}_0 = \tilde{m}\tilde{x}_0 + \tilde{b}\tilde{z}_0$ and $\tilde{P} \in \tilde{L}$.

- The map β is a homomorphism.
  It is also followed from the fact that γ takes lines to lines.

- The map α is an injective homomorphism.
  It is clear from the fact that $E_1(K) \subset E_0(K)$: let $P \in E_1(K)$, thus $\tilde{P} = \tilde{\mathcal{O}}$. But $\tilde{\mathcal{O}} \in \tilde{E}_{ns}(k)$, hence $P \in E_0(K)$. So we can take $\alpha : E_1(K) \hookrightarrow E_0(K)$ as the inclusion map and then Im $\alpha = E_1(K)$.

- $\ker \beta = \text{Im } \alpha$.
  It is clear from the definition of $E_1(K)$:

$$P \in \ker \beta \iff \tilde{P} = \tilde{\mathcal{O}} \iff P \in E_1(K) = \text{Im } \alpha.$$

- The map β is sujerctive.
  Let

$$f(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0$$

  be a minimal Weierstrass equation, let $\tilde{f}(x, y)$ be the corresponding polynomial with coefficients reduced modulo π, and let $\tilde{P} = (\lambda, \mu) \in \tilde{E}_{ns}(k)$ be any point. Since $\tilde{P}$ is a non-singular point of $\tilde{E}$ we know that either

$$\frac{\partial \tilde{f}}{\partial x}(\tilde{P}) \neq 0 \quad \text{or} \quad \frac{\partial \tilde{f}}{\partial y}(\tilde{P}) \neq 0.$$

  Suppose that it holds the former (the other case is enterily similar). Choose any $y_0 \in R$ such that $\tilde{y}_0 = \mu$, and look at the equation

$$f(x, y_0) = 0.$$

  When reduced modulo π this equation has λ as a single root, since $\partial \tilde{f}/\partial x \neq 0$. Hence, by Hensel's Lemma (lemma 3.1.1) the root λ can be lifted to an $x_0 \in R$ such that $\tilde{x}_0 = \lambda$ and $f(x_0, y_0) = 0$. Then the point $P = (x_0, y_0) \in E_0(K)$ reduces to $\tilde{P}$.

□

Note that if $\tilde{E}$ is non-singular, $\tilde{E}_{ns} = \tilde{E}$, and so $E_0(K) = E(K)$. In this case, the proposition above says that

$$\tilde{E}(k) \simeq E(K)/E_1(K).$$

Or, equivalently, that $E(K)$ is built up from two pieces, $E_1(K)$ and $\tilde{E}(k)$, where k is a smaller field.

The next result says that $E_1(K)$ is essentially $\hat{E}(\mathcal{M})$.

Proposition 3.1.19 *Let E/K be an elliptic curve given by a minimal Weierstrass equation, let $\hat{E}/R$ be the formal group associated to E (example 3.1.6), and let $w(z) \in R[[z]]$ be the power series from proposition 3.1.3. Then the map*

$$\hat{E}(\mathcal{M}) \to E_1(K); \qquad z \mapsto \left(\frac{z}{w(z)}, -\frac{1}{w(z)} \right)$$

is an isomorphism. (We understand that $z = 0$ goes to $\mathcal{O}$).

PROOF. From proposition 3.1.3.ii, the point $\left(\frac{z}{w(z)}, -\frac{1}{w(z)}\right)$, when considered as a pair of power series, satisfies the Weierstrass equation for E. Since

$$w(z) = z^3(1 + \cdots) \in R[[z]],$$

we see that $w(z)$ converges for every $z \in \mathcal{M}$. It follows that $\left(\frac{z}{w(z)}, -\frac{1}{w(z)}\right)$ is in $E(K)$ for $z \in \mathcal{M}$, and since $v(-1/w(z)) = -3v(z) < 0$, it is even in $E_1(K)$. Thus we have a well-defined map of sets

$$\hat{E}(\mathcal{M}) \to E_1(K), \qquad z \mapsto \left(\frac{z}{w(z)}, -\frac{1}{w(z)}\right).$$

Further, in deriving the power series giving the group law on $\tilde{E}$, we simply used the group law on E in the (z, w)-plane and replaced w with $w(z)$. Therefore the map is a homomorphism. Further, since $w(x) = 0$ only for $z = 0$, the map is injective, so it remains to show that the image is all of $E_1(K)$.

Let $(x, y) \in E_1(K)$. Since (x, y) reduces modulo π to the point at infinity on $\tilde{E}(k)$, we see that $v(x) < 0$ and $v(y) < 0$. But then from the Weierstrass equation $y^2 + \cdots = x^3 + \cdots$, we must have

$$3v(x) = 2v(y) = -6r,$$

for some integer $r \geq 0$. Hence $x/y \in \mathcal{M}$, so the map

$$E_1(K) \to \hat{E}(\mathcal{M}), \qquad (x, y) \mapsto -\frac{x}{y},$$

is well-defined. Again, since the group law on $\hat{E}(\mathcal{M})$ is defined using the group law on E, this map is a homomorphism, and it is clearly injective. Hence we have two injections

$$\hat{E}(\mathcal{M}) \hookrightarrow E_1(K) \hookrightarrow \hat{E}(\mathcal{M})$$

whose composition is the identity map, so they are isomorphisms.

□

The following proposition gives a fundamental tool to prove the weak Mordell-Weil theorem.

Proposition 3.1.20 *Let E/K be an elliptic and $m \geq 1$ an integer relatively prime to char(k).*

i) The subgroup $E_1(K)$ has no non-trivial points of order m.

ii) If the reduced curve $\tilde{E}/k$ is non-singular, then the reduction map

$$E(K)[m] \to \tilde{E}(k)$$

is injective.

PROOF. From proposition (3.1.18) we have an exact sequence

$$0 \to E_1(K) \to E_0(K) \to \tilde{E}_{ns}(k) \to 0.$$

i) From proposition 3.1.19, $E_1(K) \simeq \hat{E}(\mathcal{M})$, where $\hat{E}$ is the formal group associated to E, and from our general result on formal groups, proposition (3.1.13), $\hat{E}(\mathcal{M})$ has no non-trivial elements of order m.

ii) Now, if $\tilde{E}$ is non-singular, than $E_0(K) = E(K)$ and $\tilde{E}_{ns}(k) = \tilde{E}(k)$, so the m-torsion in $E(K)$ injects into $\tilde{E}(k)$.

□

3.1.5 Proof of Weak Mordell-Weil Therorem

Our goal in this section is to prove the Weak Mordell-Weil Theorem. For the rest of the chapter, E/K and m will be as the statement above. Moreover, we use the following notation:

$$\begin{aligned} K_v &: \text{ completion of } K \text{ in } v \text{ for } v \in M_K. \\ R_v &: \text{ ring of integers of } K_v \text{ for } v \in M_K^0. \\ \mathcal{M}_v &: \text{ maximal ideal of } R_v \text{ for } v \in M_K^0. \\ k &: \text{the residue field of } R_v \text{ for } v \in M_K^0. \end{aligned}$$

Lemma 3.1.21 *Let L/K be a finite Galois extension.*

$$E(L)/mE(L) \text{ is finite } \Rightarrow E(K)/mE(K) \text{ is finite.}$$

PROOF. The inclusion $E(K) \subset E(L)$ induces a natural map

$$E(K)/mE(K) \xrightarrow{\phi} E(L)/mE(L)$$

which kernel is

$$\ker \phi = \frac{E(K) \cap mE(L)}{mE(K)}.$$

Then for each $P \bmod(mE(K)) \in \ker \phi$, there exists $Q_P \in E(L)$ such that $[m]Q_P = P$. We define now a map of sets (which is not, in general, a group homomorphism)

$$\lambda_P : Gal(L/K) \to E[m]; \qquad \lambda_P(\sigma) = Q_P^\sigma - Q_P.$$

This map is well defined since $\lambda_P(\sigma) \in E[m]$ because

$$[m](Q_P^\sigma - Q_P) = [m]Q_P^\sigma - [m]Q_P = ([m]Q_P)^\sigma - P = P^\sigma - P = \mathcal{O}.$$

Suppose that $P, P' \in E(K) \cap mE(L)$ satisfy $\lambda_P = \lambda_{P'}$. Then for all $\sigma \in Gal(L/K)$,

$$\begin{aligned}\lambda_P(\sigma) = \lambda_{P'}(\sigma) &\Rightarrow Q_P^\sigma - Q_P = Q_{P'}^\sigma - Q_{P'} \\ &\Rightarrow Q_P^\sigma - Q_{P'}^\sigma = Q_P - Q_{P'} \\ &\Rightarrow (Q_P - Q_{P'})^\sigma = Q_P - Q_{P'} \\ &\Rightarrow Q_P - Q_{P'} \in E(K).\end{aligned}$$

It follows that

$$P - P' = [m]Q_P - [m]Q_{P'} = [m](Q_P - Q_{P'}) \in mE(K),$$

and hence, $P \equiv P' \bmod(mE(K))$. This proves that the association

$$\ker\phi \to Map(Gal(L/K), E[m]); \qquad P \mapsto \lambda_P;$$

is one-to-one. But $Gal(L/K)$ is finite because L/K is finite; and $E[m]$ is also finite by theorem 2.4.2, hence there is only a finite number of maps between them. Therefore, $\ker\phi$ is finite.

Finally, the exact sequence

$$0 \to \ker\phi \to E(K)/mE(K) \to E(L)/mE(L) \to 0$$

nests $E(K)/mE(K)$ between two finite groups, so it is finite too.

□

So, if we want to prove the weak Mordell-Weil theorem (theorem 3.1.35) for an arbitrary K it suffices to prove it under the assuption that

$$E[m] \subset E(K).$$

because the previous lemma tells us that if $E(K)/mE(K)$ is finite, $E(K')/mE(K')$ is finite too for any subfield K' of K. For the reminder of this chapter we will assume that this inclusion is true.

We recall now the definition of pairing and perfect pairing.

Definition 3.1.22 (Pairing) Let R be a commutative ring with unit and let M, N, L be R-modules. A **pairing** is any R-bilinear homomorphism

$$\rho : M \times N \to L,$$

i.e., ρ satisfies:

- $\rho(rm, n) = \rho(m, rn) = r\rho(m, n)$ for all $r \in R$, $m \in M$ and $n \in N$.
- $\rho(m_1 + m_2, n) = \rho(m_1, n) + \rho(m_2, n)$ for all $m_1, m_2 \in M$ and $n \in N$.
- $\rho(m, n_1 + n_2) = \rho(m, n_1) + \rho(m, n_2)$ for all $m \in M$ and $n_1, n_2 \in N$.

Definition 3.1.23 (Perfect pairing) Let R be a commutative ring with unit and let M, N, L be R-modules. We say that a pairing $\rho : M \times N \to L$ is **perfect** if

$$\rho(m, \cdot) : N \to L \text{ is the trivial homomorphism, i.e., } \rho(m, \cdot) = 1_L \iff m = 1_M,$$

and

$$\rho(\cdot, n) : M \to L \text{ is the trivial homomorphism, i.e., } \rho(\cdot, n) = 1_L \iff n = 1_N.$$

Remark 3.1.24. Let R be a commutative ring with unit and let M, N, L be R-modules. The pairing $\rho : M \times N \to L$ can also be considered as a homomorphism of R-modules:

$$\Phi_1 : M \to Hom_R(N, L); \qquad \Phi_1(m)(n) := \rho(m, n),$$

or

$$\Phi_2 : N \to Hom_R(M, L); \qquad \Phi_2(n)(m) := \rho(m, n).$$

Particulary, if ρ is perfect, then $\ker \Phi_1$ and $\ker \Phi_2$ are both trivial, i.e., Φ_1 and Φ_2 are both injective.

In fact, it can be shown that ρ is perfect if, and only if, Φ_1 and Φ_2 are both isomorphisms, but we do not need this in our context.

Lemma 3.1.25 *Let M, N and L be $\mathbb{Z}$-modules, i.e. abelian groups, and let $\rho : M \times N \to L$ be a perfect pairing. If L is finite then either M and N are both infinite, or M and N are both finite.*

PROOF. Without loss of generality, suppose M finite and N infinite. As M is finite, $Hom(M, L) \subset Maps(M, L)$ is finite and we have the map

$$\Phi : N \to Hom_R(M, L); \qquad \Phi(n)(m) := \rho(m, n).$$

to the infinite group N into the finite group $Hom(M, L)$. But as ρ is a perfect pairing, Φ is injective, which is impossible.

□

Now we are going to translate the putative finiteness of $E(K)/mE(K)$ into a statement about certain field extension of K. In order to do this, we use the following tool.

Definition 3.1.26 (Kummer pairing) The **Kummer pairing**

$$\kappa : E(K) \times Gal(\overline{K}/K) \to E[m]$$

is defined as follows. Let $P \in E(K)$ and choose any point $Q \in E(\overline{K})$ satisfying $[m]Q = P$. Then

$$\kappa(P, \sigma) = Q^\sigma - Q.$$

The basic properties of the Kummer pairing are exposed in the following proposition.

Proposition 3.1.27 *The following statements hold:*

i) The Kummer pairing is well-defined.

ii) The Kummer pairing is bilinear.

iii) The kernel of the Kummer pairing on the left is $mE(K)$.

iv) The kernel of the Kummer pairing on the right is $Gal(\overline{K}/L)$, where

$$L = K([m]^{-1}E(K))$$

is the compositum of all fields $K(Q)$ as Q ranges over the points in $E(\overline{K})$ satisfying $[m]Q \in E(K)$.

Hence the Kummer pairing induces a perfect bilinear pairing

$$E(K)/mE(K) \times Gal(L/K) \to E[m],$$

where L is the field given in (iv).

PROOF.

i) We must show that $\kappa(P, \sigma) \in E[m]$ and it does not depend on the choice of Q. For the first statement, we have

$$[m](Q^\sigma - Q) = [m]Q^\sigma - [m]Q = ([m]Q)^\sigma - P = P^\sigma - P = \mathcal{O}.$$

since $P \in E(K)$ and σ fixes K. For the second statement, we note that any other choice has the form $Q + T$ for some $T \in E[m]$. Then

$$\kappa(P, \sigma) = (Q + T)^\sigma - (Q - T) = Q^\sigma + T^\sigma - Q - T = Q^\sigma - Q,$$

since we have assumed $T \in E[m] \subset E(K)$.

ii) To check linearity in the first coordinate, let $P, P' \in E(K)$ and $Q, Q' \in E(\overline{K})$ such that $[m]Q = P$ and $[m]Q' = P'$.

$$\kappa(P, \sigma) + \kappa(P', \sigma) = Q^\sigma - Q + (Q')^\sigma - Q' = (Q + Q')^\sigma - (Q + Q') = \kappa(P + P', \sigma).$$

To check linearity in the second coordinate, let $\sigma, \tau \in Gal(\overline{K}/K)$ and compute

$$\kappa(P, \sigma\tau) = Q^{\sigma\tau} - Q = Q^{\sigma\tau} - Q^\tau + Q^\tau - Q = (Q^\sigma - Q)^\tau + Q^\tau - Q = \kappa(P, \sigma)^\tau + \kappa(P, \tau)$$

but as $\kappa(P, \sigma) \in E[m] \subset K$, then $\kappa(P, \sigma)^\tau = \kappa(P, \sigma)$.

iii) $(mE(K) \subset \ker \kappa(\cdot, \sigma))$ Suppose that $P \in mE(K)$, say $P = [m]Q$ for some $Q \in E(K)$. Then Q is fixed by every $\sigma \in Gal(\overline{K}/K)$ so

$$\kappa(P, \sigma) = Q^\sigma - Q = \mathcal{O}.$$

$(\ker \kappa(\cdot, \sigma) \subset mE(K))$ Suppose that $\kappa(P, \sigma) = \mathcal{O}$ for all $\sigma \in Gal(\overline{K}/K)$. Then choosing some $Q \in E(\overline{K})$ with $[m]Q = P$ we have

$$Q^\sigma = Q \text{ for all } \sigma \in Gal(\overline{K}/K).$$

Therefore $Q \in E(K)$, so $P = [m]Q \in mE(K)$.

iv) $(Gal(\overline{K}/L) \subset \ker \kappa(P, \cdot))$ If $\sigma \in Gal(\overline{K}/L)$ then

$$\kappa(P, \sigma) = Q^\sigma - Q = \mathcal{O}$$

because $Q \in E(L)$ by definition of L.

$(\ker \kappa(P, \cdot) \subset Gal(\overline{K}/L))$ Suppose that $\sigma \in Gal(\overline{K}/K)$ satifies $\kappa(P, \sigma) = \mathcal{O}$. Then, for every point $Q \in E(\overline{K})$ satisfying $[m]Q = P$ we have

$$\mathcal{O} = \kappa(P, \sigma) = Q^\sigma - Q$$

But, by definition, L is compositum of $K(Q)$ over all such Q, so σ fixes L. Hence, $\sigma \in Gal(\overline{K}/L)$.

Moreover, as we have the pairing $\kappa : E(K) \times Gal(\overline{K}/K) \to E[m]$, then there exists a homomorphism

$$\Phi : Gal(\overline{K}/K) \to Hom(E(K), E[m]); \qquad \sigma \mapsto \kappa(\cdot, \sigma).$$

The kernel of this homomorphism is $\ker \Phi = Gal(\overline{K}/L)$ by (iv), so $Gal(\overline{K}/L)$ is a normal subgroup of $Gal(\overline{K}/K)$, thus L/K is Galois. The last statement is clear from this fact, definition 3.1.23 and statements (iii) and (iv) of this proposition.

□

It follows from the previous proposition and lemma 3.1.25 that the finiteness of $E(K)/mE(K)$ is equivalent to the finiteness of the extension L/K. Let us analyze this extension.

Definition 3.1.28 (Good and bad reduction) Let K be a local field complete with respect to a discrete valuation v, let R be the ring of integers of K and $\mathcal{M}$ its maximal ideal. Let E/K be an elliptic curve and let $\tilde{E}$ be the reduction modulo $\mathcal{M}$ of a minimal Weierstrass equation for E. We say that E has **good reduction** if $\tilde{E}$ is nonsingular; and that E has **bad reduction** in other case.

Definition 3.1.29 Let K be a number field and let E/K be an alliptic curve. Let $v \in M_K^0$ be a discrete valuation. Then E is said to have **good (bad) reduction at** v if E has good reduction when cosidered over the completion K_v. Taking a minimal Weierstrass equation for E over K_v we denote the reduced curve over the residue field by $\tilde{E}_v/k_v$.

If we take any Weierstrass equation for E/K, for example,

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

say with discriminant Δ. Then for all but finitely many $v \in M_K^0$ we have

$$v(a_i) \geq 0 \text{ for } i = 1, \ldots, 6 \text{ and } v(\Delta) = 0.$$

For any v satisfying these conditions, the given equation is already a minimal Weierstrass equation, because $v(\Delta) = 0$ and it cannot be lower; and the reduced curve $\tilde{E}_v/k_v$ is nonsingular.

Proposition 3.1.30 (Restatement of 3.1.20.ii) *Let $v \in M_K^0$ be a discrete valuation such that $v(m) = 0$ and such that E has good reduction at v. Then the reduction map*

$$E(K)[m] \to \tilde{E}_v(k_v)$$

is injective.

Definition 3.1.31 (Unramified extensions of fields) If L/K is a field extension with residue fields l and k respectively, we say that L/K is **unrimified** if

$$[L : K] = [l : k].$$

Unrimified extensions of K correspond to extensions of the residue field k, so $Gal(\overline{K}/K)$ descomposes as

$$\begin{array}{ccccccc} 1 & \longrightarrow & Gal(\overline{K}/K^{nr}) & \longrightarrow & Gal(\overline{K}/K) & \longrightarrow & Gal(K^{nr}/K) \longrightarrow 1 \\ & & \| & & & & \| \\ & & I_v & & & & Gal(\overline{k}/k) \end{array}$$

where K^{nr} is the maximal unramified extension of K and I_v is the inertia subgroup of $Gal(\overline{K}/K)$. In other words, the **inertia group** I_v is the set of elements of $Gal(\overline{K}/K)$ that act trivially on the residue field $\overline{k}$.

Definition 3.1.32 (Set unrimified at v) Let Σ be a set on which $Gal(\overline{K}/K)$ acts. We say that Σ is **unrimified at** v if the action of I_v on Σ is trivial.

Proposition 3.1.33 *Let*

$$L = K([m]^{-1}E(K))$$

be the field defined in proposition 3.1.27.

i) The extension L/K is abelian and has exponent m, i.e, $Gal(L/K)$ is abelian every element of $Gal(L/K)$ has order dividing m.

ii) Let

$$S = \{v \in M_K^0 : E \text{ has bad reduction at } v\} \cup \{v \in M_K^0 : v(m) \neq 0\} \cup M_K^\infty.$$

The L/K is unrimified outside S, i.e., if $v \in M_K \setminus S$ then L/K is unrimified at v.

PROOF.

i) As we have the pairing $\kappa : E(K) \times Gal(\overline{K}/K) \to E[m]$, then there exists a homomorphism

$$\Phi : Gal(\overline{K}/K) \to Hom(E(K), E[m]); \qquad \sigma \mapsto \kappa(\cdot, \sigma)$$

with $\ker \Phi = Gal(\overline{K}/L)$, by the first isomorphism theorem,

$$Gal(\overline{K}/K)/Gal(\overline{K}/L) \simeq Im(\Phi) \subset Hom(E(K), E[m])$$

But by the first isomorphism theorem for groups,

$$Gal(L/K) \simeq Gal(\overline{K}/K)/Gal(\overline{K}/L),$$

so there is an injection

$$Gal(L/K) \to Hom(E(K), E[m]), \qquad \sigma \mapsto \kappa(\cdot, \sigma).$$

But $E(K)$ and $E[m]$ are both abelian, so L/K is abelian; and

$$(f + \overset{m)}{\cdots} + f)(P) = f(P) + \overset{m)}{\cdots} + f(P) = [m]f(P) = \mathcal{O} \text{ for all } f \in Hom(E(K), E[m])$$

so $o(f)|m$.

ii) Let $v \in M_K \setminus S$, let $Q \in E(\overline{K})$ such that $[m]Q \in E(K)$ and let $K' = K(Q)$. It suffices to show that K'/K is unrimified at v, since L is defined as the compositum of all such K'. Let $v' \in M_{K'}$ be a place of K' which extends v and let k'_v/k_v be the corresponding extension of residue fields. The assumption that $v \notin S$ ensures that E has good reduction at v, so it also has good reduction at v', since we can take the same Weierstrass equation and $|\Delta|_{v'} = |\Delta|_v = 0$. Thus, we have the reduction map

$$E(K') \to \tilde{E}(k'_{v'}).$$

Let $I_{v'/v} \subset Gal(\overline{K}/K)$ be the inertia group for v'/v, and take any element $\sigma \in I_{v'/v}$. We have to show that σ acts trivially on $k'_{v'}$. By definition, an element of inertia such as σ acts trivially on $\tilde{E}(k'_{v'})$, so

$$\widetilde{Q^\sigma - Q} = \tilde{Q}^\sigma - \tilde{Q} = \tilde{\mathcal{O}}.$$

On the other had, as $[m]Q \in E(K)$,

$$[m](Q^\sigma - Q) = ([m]Q)^\sigma - [m]Q = \mathcal{O}.$$

Hence $Q^\sigma - Q$ is a point of order m that is in the kernel of the reduction-modulo-v' map. But as the reduction map

$$E(K)[m] \to \tilde{E}_v(k_v)$$

is injective by proposition 3.1.30, we have

$$Q^\sigma - Q = \mathcal{O},$$

so Q is fixed by every element of $I_{v'/v}$ and hence that $K' = K(Q)$ is unrimified over K at v'. As this is for all v' lying over v for every $v \notin S$, K'/K is unrimified outside of S.

□

The only thing it remains to show is that L/K is finite. We use Hermite's theorem, which is a corollary of Minkowski's theorem.

Theorem 3.1.34 (Hermite's theorem) *Let K be a number field and let S be a finite set of places on K. Then there exists a finite number of unrimified extensions K'/K outside of S such that*

$$[K' : K] < N_0,$$

for any $N_0 \in \mathbb{Z}^+$.

We are finally in position to prove the Weak Mordell-Weil theorem. Recall that the statement of the theorem was the following:

Theorem 3.1.35 (Weak Mordell-Weil Theorem) *Let K be a number field, let E/K be an elliptic curve and let $m \in \mathbb{Z}$ with $m \geq 2$. Then*

$$E(K)/mE(K)$$

is a finite group.

PROOF. Let

$$L = K([m]^{-1}E(K)),$$

and

$$S = \{v \in M_K^0 : E \text{ has bad reduction at } v\} \cup \{v \in M_K^0 : v(m) \neq 0\} \cup M_K^\infty.$$

Proposition 3.1.33 tells us that if $Q \in E(\overline{K})$ such that $[m]Q \in E(K)$ then the extension K'/K, with $K' = K(Q)$ is finite and unramified outside of S. Moreover, if $Q' \in E(\overline{K})$

is another point such that $[m]Q' = [m]Q$, then Q' must have the form $Q' = Q + T$, with $T \in E[m] \subset E(K)$. In other words, the Galois conjugations of Q must have the form $Q + T$, with $T \in E[m]$, hence

$$[K(Q) : K] \leq m^2.$$

So, if Q is going over $[m]^{-1}E(K)$ it only appears in a finite number of extensions $K' = K(Q)/K$, each of them with finite index by Hermite's theorem 3.1.34. Now as L is defined as the compositum of all such K', L/K is finite. But by proposition 3.1.27, the pairing

$$E(K)/mE(K) \times Gal(L/K) \to E[m]$$

is a prefect pairing, hence the finiteness of $E(K)/mE(K)$ is equivalent to the finiteness of L/K, the result has been shown.

□

3.2 The Descent Procedure

In this section we prove the Descent Theorem, setting the sort of function (known as height function) needed to show that an abelian group is finitely generated. Recall from theorem 3.0.5 the statement of the Descent Theorem:

Theorem 3.2.1 (Descent Theorem) *Let A be an abelian group. Suppose that there exists a (height) function*

$$h : A \to \mathbb{R},$$

with the following properties:

i) Let $Q \in A$. There is a constant $C_1 \in \mathbb{R}$, depending on A and Q, such that

$$h(P + Q) \leq 2h(P) + C_1 \quad \text{for all } P \in A.$$

ii) There are an integer $m \geq 2$ and a constant $C_2 \in \mathbb{R}$, depending on A, such that

$$h(mP) \geq m^2 h(P) - C_2 \quad \text{for all } P \in A.$$

iii) For every constant $C_3 \in \mathbb{R}$, the set

$$\{P \in A : h(P) \leq C_3\}$$

is finite.

Suppose further that for the integer m in (ii), the quotient group A/mA is finite. Then A is finitely generated.

PROOF. Choose $Q_1, \ldots, Q_r \in A$ to represent the finitely many cosets in A/mA, and let $P \in A$ be an arbitrary element.

The idea is to show that the difference between P and an appropiate linear combination of $Q_1, \ldots, Q_r$ is a multiple of a point whose height is smaller that a constant independent of P. Then $Q_1, \ldots, Q_r$ and the finitely many points with height less than this constant are genetators for A.

We begin writing

$$P = mP_1 + Q_{i_1} \qquad \text{for some } 1 \leq i_1 \leq r.$$

Next we do the same thing with P_1, then with P_2, etc., which gives us a list of points

$$\begin{aligned} P &= mP_1 + Q_{i_1}, \\ P_1 &= mP_2 + Q_{i_2}, \\ &\vdots \\ P_{n-1} &= mP_n + Q_{i_n}, \end{aligned}$$

For any index j we have

$$\begin{aligned} h(P_j) &\overset{(ii)}{\leq} \frac{1}{m^2}(h(mP_j) + C_2) \\ &= \frac{1}{m^2}(h(P_{j-1} + Q_{i_j}) + C_2) \\ &\overset{(i)}{\leq} \frac{1}{m^2}(2h(P_{j-1}) + C_1' + C_2) \end{aligned}$$

where C_1' is the maximum of the constants in (i) for $Q \in \{-Q_1, \ldots - Q_r\}$. Note that C_1' depends on A and $Q \in \{-Q_1, \ldots - Q_r\}$; and C_2 depends on A, so netiher C_1' nor C_2 depend on P.

We use this inequality repeatedly, starting from P_n and working back to P. This yields

$$\begin{aligned}
h(P_n) &\leq \frac{1}{m^2}(2h(P_{n-1}) + C_1' + C_2) = \frac{2}{m^2}h(P_{n-1}) + \frac{1}{m^2}(C_1' + C_2) \\
&\leq \frac{2}{m^2}(\frac{1}{m^2}(2h(P_{n-2}) + C_1' + C_2)) + \frac{1}{m^2}(C_1' + C_2) \\
&= \left(\frac{2}{m^2}\right)^2 h(P_{n-1}) + \left(\frac{1}{m^2} + \frac{2}{m^2}\right)(C_1' + C_2) \\
&\leq \left(\frac{2}{m^2}\right)^2 (\frac{1}{m^2}(2h(P_{n-3}) + C_1' + C_2)) + \left(\frac{1}{m^2} + \frac{2}{m^2}\right)(C_1' + C_2) \\
&= \left(\frac{2}{m^2}\right)^3 h(P_{n-3}) + \left(\frac{1}{m^2} + \frac{2}{m^2} + \frac{4}{m^2}\right)(C_1' + C_2) \\
&\vdots \\
&\leq \left(\frac{2}{m^2}\right)^n h(P) + \left(\frac{1}{m^2} + \frac{2}{m^2} + \frac{4}{m^2} + \cdots + \frac{2^{n-1}}{m^2}\right)(C_1' + C_2) \\
&= \left(\frac{2}{m^2}\right)^n h(P) + \frac{2^n}{m^2}(C_1' + C_2) \\
&\overset{m\geq 2}{\leq} \frac{1}{2^n}h(P) + \frac{1}{2}(C_1' + C_2).
\end{aligned}$$

It follows that if n is large enough, then

$$h(P_n) \leq 1 + \frac{1}{2}(C_1' + C_2).$$

Since P is a linear combination of P_n and $Q_1, \ldots, Q_r$,

$$P = m^n P_n + \sum_{j=1}^{n} m^{j-1} Q_{i_j},$$

it follows that every $P \in A$ is a linear combination of points in the set

$$\{Q_1, \ldots, Q_r\} \cup \{Q \in A : h(Q) \leq 1 + \frac{1}{2}(C_1' + C_2)\}.$$

Property (iii) from theorem 3.0.5 tells us that this is a finite set, which completes the proof that A is finitely generated.

□

Remark 3.2.2. What is needed to allow us to find generators for the group A? First, we must be able to calculate the constants $C_1 = C_1(Q_i)$ for each of the elements $Q_1, \ldots, Q_r \in A$, representants of the cosets of A/mA. Second, we must be able to calculate the constant C_2. Third, for any constant C_3, we must be able to determine the elements

in the finite set $\{P \in A : h(P) \leq C_3\}$. It can be shown that for the height fuctions used on elliptic curves, all of these constants are effectively computable, provided that we can find elements of $E(K)$ that generate the finite group $E(K)/mE(K)$. The problem is that nowadays there is no known procedure that is guaranteed to give generators for $E(K)/mE(K)$.

3.2.1 Heights on Projective Space

In order to use the descent theorem 3.0.5 to prove the Mordell-Weil theorem, we need to define a height function on the K-rational points of an elliptic curve. As elliptic curves are given as subsets of projective space, in this section we study height functions defined on projective space.

Example 3.2.3 Let $P \in \mathbb{P}^n(\mathbb{Q})$ be a point with rational coordinates. As $\mathbb{Z}$ is a principal ideal domain, we can find homogeneus coordinates $P = [x_0 : \ldots : x_n]$ satisfying $x_0, \ldots, x_n \in \mathbb{Z}$ and $\gcd(x_0, \ldots, x_n) = 1$. Then a natural measure of *height of* P is

$$H(P) = \max\{|x_0|, \ldots, |x_n|\}.$$

With this definition, it is clear that for any constant $C \in \mathbb{R}$, the set

$$\{P \in \mathbb{P}^n(\mathbb{Q}) : H(P) \leq C\}$$

is finite. Indeed, it has at most $(2C + 1)^n$ elements.

H will be used to define a height in $\mathbb{P}^n(\mathbb{Q})$.

If we try to generalize this example to arbitrary number fields, we run into the difficulty that the ring of integers need not to be a principal ideal domain. We thus take a somewhat different approach.

Definition 3.2.4 (Set of standard absolute values) The **set of standard absolute values** on $\mathbb{Q}$, $M_{\mathbb{Q}}$, consists of the following:

i) $M_{\mathbb{Q}}$ contains one archimedian absolute value defined by

$$|x|_\infty = \max\{x, -x\},$$

i.e., the usual absolute value.

ii) For each prime $p \in \mathbb{Z}$, the set $M_{\mathbb{Q}}$ contains one nonarchimedian **(p-adic)** absolute value defined by

$$\left|p^n \frac{a}{b}\right| = p^{-n}, \qquad \text{for } a, b \in \mathbb{Z} \text{ satisfying } p \nmid ab.$$

The **set of standard absolute values** on a number field K, M_K, is the set of absolute values of K whose restriction to $\mathbb{Q}$ is one of the absolute values in $M_{\mathbb{Q}}$

From now on, and until the end of this chapter, M_K is the set of standard absolutes values on a number field K.

Definition 3.2.5 (Local degree) Let $v \in M_K$. The **local degree at** v, denoted by n_v, is

$$n_v = [K_v : \mathbb{Q}_v],$$

where K_v and $\mathbb{Q}_v$ denote the completions of K and $\mathbb{Q}$ with respect to the absolute value v.

Theorem 3.2.6 (Extension Formula) *Let $L/K/\mathbb{Q}$ be a tower of number fields, and let $v \in M_K$. Then*

$$\sum_{\substack{w \in M_L \\ w|v}} n_w = [L : K] \cdot n_v,$$

where $w|v$ means that w restricted to K is equal to v.

Theorem 3.2.7 (Product Formula) *Let $x \in K^*$. Then*

$$\prod_{v \in M_K} |x|_v^{n_v} = 1.$$

As this is not a text on number field theory, we are not proving these two formulae. To see the proof we can consult any text on algebraic number theory such as [45, chap. II, §1] (for extention formula) and [54, chap. 8] (for product formula).

We now define the height of a point in projective space.

Definition 3.2.8 (Height in $\mathbb{P}^n(K)$) Let $P \in \mathbb{P}^n(K)$ be a point with homogeneous coordinates $P = [x_0 : \ldots : x_n]$, $x_0, \ldots, x_n \in K$. The **height of P (relative to K)** is defined by

$$H_K(P) = \prod_{v \in M_K} \max\{|x_0|_v, \ldots, |x_n|_v\}^{n_v}.$$

As in example 3.2.3, we will use this H_K function to define a height on $\mathbb{P}^n(K)$ in the next section.

Proposition 3.2.9 *Let $P \in \mathbb{P}^n(K)$.*

i) The definition of $H_K(P)$ does not depend on the choice of homogeneous coordinates for P.

ii) $H_K(P) \geq 1$.

iii) Let L/K be a finite extension. Then $H_L(P) = H_K(P)^{[L:K]}$.

PROOF.

i) Any other choice of homogeneous coordinates for P has the form $P' = \lambda P = [\lambda x_0, \ldots, \lambda x_n]$ for some $\lambda \in K^*$. Using the product formula 3.2.7, we have

$$\begin{aligned} H_K(P') &= \prod_{v \in M_K} \max\{|\lambda x_0|_v, \ldots, |\lambda x_n|_v\}^{n_v} \\ &= \prod_{v \in M_K} |\lambda|_v^{n_v} \max\{|x_0|_v, \ldots, |x_n|_v\}^{n_v} \\ &= \prod_{v \in M_K} \max\{|x_0|_v, \ldots, |x_n|_v\}^{n_v} \\ &= H_K(P). \end{aligned}$$

ii) Given any point $P \in \mathbb{P}^n(K)$, we can find an homogeneous coordinates for P such that at least one of the coordinates is 1. Then every factor in the product defining H_K is at least 1.

iii) It suffices to compute

$$\begin{aligned} H_L(P) &= \prod_{w \in M_L} \max\{|x_0|_w, \ldots, |x_n|_w\}^{n_w} \\ &\overset{x_i \in K}{=} \prod_{v \in M_K} \prod_{\substack{w \in M_L \\ w|v}} \max\{|x_0|_v, \ldots, |x_n|_v\}^{n_w} \\ &= \prod_{v \in M_K} \max\{|x_0|_v, \ldots, |x_n|_v\}^{\sum n_w} \\ &\overset{3.2.6}{=} \prod_{v \in M_K} \max\{|x_0|_v, \ldots, |x_n|_v\}^{[L:K] n_v} \\ &= H_K(P)^{[L:K]} \end{aligned}$$

□

Remark 3.2.10. If $K = \mathbb{Q}$, then $H_{\mathbb{Q}}$ agrees with the more intuitive height function given in example 3.2.3. To see this, let $P = [x_0 : \ldots : x_n] \in \mathbb{P}^n(\mathbb{Q})$ with homogeneous coordinates such that $x_1 \in \mathbb{Z}$ and $\gcd(x_0, \ldots, x_n) = 1$. Then for any nonarchimedian absolute value $v \in M_{\mathbb{Q}}$, we have $|x_i|_v \leq 1$ for all i and $|x_i|_v = 1$ for al least one x_i. Hence in the product defining $H_{\mathbb{Q}}(P)$, only the factor of archimedian absolute values contributes, so

$$H_{\mathbb{Q}}(P) = \max\{|x_0|_\infty, \ldots, |x_n|_\infty\}.$$

In particular, it follows that for any constant C, the set

$$\{P \in \mathbb{P}^n(\mathbb{Q}) : H_{\mathbb{Q}} \leq C\}$$

is finite.

Our goal is to extend this statement to H_K somehow.

Definition 3.2.11 (Absolute height) Let $P \in \mathbb{P}^n(\overline{\mathbb{Q}})$. The **(absolute) height of** P, denoted by $H(P)$, is defined as follows. Choose a number field such that $P \in \mathbb{P}^n(K)$. Then

$$H(P) = H_K(P)^{1/[K:\mathbb{Q}]},$$

where we take the positive root.

We see from proposition 3.2.9.iii that $H(P)$ is well-defined and independent of the choice of K and proposition 3.2.9.ii implies $H(P) \geq 1$.

We now investigate how the height changes under mapping between projective spaces. Let us recall what a morphism of degree d is defined:

Definition 3.2.12 (Morphism of degree d) A **morphism of degree** d between projective spaces is a map

$$F : \mathbb{P}^n \to \mathbb{P}^m; \qquad F(P) = [f_0(P) : \ldots : f_m(P)],$$

where $f_0, \ldots, f_m \in \overline{\mathbb{Q}}[X_0, \ldots, X_n]$ are homogeneus polynomials of degree d which not vanishes together in $\overline{\mathbb{Q}}^{n+1}$ except for $(X_0, \ldots, X_n) = (0, \ldots, 0)$.

If F can be written having coefficients in K, F is said to be defined over K.

Theorem 3.2.13 *Let*

$$F : \mathbb{P}^n \to \mathbb{P}^m$$

be a morphism of degree d. Then there are positive contants C_1 and C_2, depending on F, such that

$$C_1 H(P)^d \leq H(F(P)) \leq C_2 H(P)^d, \quad \text{for all } P \in \mathbb{P}^n(\overline{\mathbb{Q}}).$$

PROOF. Let $F = [f_0, \ldots, f_m]$, where $f_i \in \overline{\mathbb{Q}}[X_0, \ldots, X_n]$ are homogeneus polynomials of degree d having no common zeros; let $P = [x_0 : \ldots : x_n] \in \mathbb{P}^n(\overline{\mathbb{Q}})$ be a point with algebraic coordinates. Choose a number field K that contains $x_0, \ldots, x_n$ and all of the coefficients of the f_i, for all $i = 0, \ldots, n$.

For each absolute value $v \in M_K$ we define

$$|P|_v := \max_{0 \leq i \leq n} |x_i|_v \qquad \text{and} \qquad |F(P)|_v := \max_{0 \leq j \leq m} |f_j(P)|_v$$

and we also define

$$|F|_v := \max\{|a|_v : a \text{ is a coefficient of some } f_i\}.$$

Then from the definition of height, there are some natural definitions

$$H_K(P) := \prod_{v \in M_K} |P|_v^{n_v} \qquad \text{and} \qquad H_K(F(P)) := \prod_{v \in M_K} |F(P)|_v^{n_v},$$

and it also makes sense to define

$$H_K(F) := \prod_{v \in M_K} |F|_v^{n_v} = H([a_0 : a_1 : \ldots]),$$

where a_j are the coefficients of the f_i.

Finally, we let C_1 and C_2 be two constants that depend on n, m and d, and we set

$$\rho(v) := \begin{cases} 1, & \text{if } v \in M_K^\infty, \\ 0, & \text{if } v \in M_K^0. \end{cases}$$

In other words, the function ρ discriminates whether $v \in M_K$ is archimedian or not. With this definition, we can write the triangle inequality as

$$|t_1 + \cdots + t_n|_v \leq n^{\rho(v)} \max\{|t_1|_v, \ldots, |t_n|_v\} \tag{3.2}$$

for all $v \in M_K$, both archimedian and nonarchimedian.

With all this notation, we prove first the upper inequality of theorem 3.2.13. Suppose that for each $i = 1, \ldots, m$ we have

$$f_i(P) = a_{i_0} x_0^{\alpha_0^{i_0}} \cdots x_n^{\alpha_n^{i_0}} + a_{i_1} x_0^{\alpha_0^{i_1}} \cdots x_n^{\alpha_n^{i_1}} + \cdots + a_{i_{r_i}} x_0^{\alpha_0^{i_{r_i}}} \cdots x_n^{\alpha_n^{1_{r_i}}},$$

with

$$\sum_{j=0}^{n} \alpha_j^{i_k} = d, \qquad \text{for } i = 1, \ldots, m; \text{ and } k = 1, \ldots, r_i.$$

where $\alpha_j^{i_k}$ denotes the exponent of the coordinate x_j, whose coefficient is a_{i_k} and r_i is the number of terms of the polynomial f_i.

The triangle inequality yields

$$\begin{aligned} |f_i(P)|_v &= |a_{i_0} x_0^{\alpha_0^{i_0}} \cdots x_n^{\alpha_n^{i_0}} + a_{i_1} x_0^{\alpha_0^{i_1}} \cdots x_n^{\alpha_n^{i_1}} + \cdots + a_{i_{r_i}} x_0^{\alpha_0^{i_{r_i}}} \cdots x_n^{\alpha_n^{1_{r_i}}}|_v \\ &\overset{Eq.(3.2)}{\leq} r_i^{\rho(v)} \cdot \max\{|a_{i_0}|_v |x_0^{\alpha_0^{i_0}} \cdots x_n^{\alpha_n^{i_0}}|_v, \ldots, |a_{i_{r_i}}|_v |x_0^{\alpha_0^{i_{r_i}}} \cdots x_n^{\alpha_n^{i_{r_i}}}|_v\} \\ &\leq r_i^{\rho(v)} \cdot \max\{|a_{i_0}|_v, \ldots, |a_{i_{r_i}}|_v\} \cdot \max\{|x_0^{\alpha_0^{i_0}} \cdots x_n^{\alpha_n^{i_0}}|_v, \ldots, |x_0^{\alpha_0^{i_{r_i}}} \cdots x_n^{\alpha_n^{i_{r_i}}}|_v\} \\ &\leq C_1^{\rho(v)} \cdot |F|_v \cdot |P|_v^d \end{aligned}$$

where $C_1 := \max_{0 \leq i \leq m} r_i$, which is at most $\binom{n+d}{n}$, i.e., the number of monomials of degree d in $n+1$ variables. Since this estimate holds for every $i = 0, \ldots, m$, we have

$$|F(P)|_v \leq C_1^{\rho(v)} \cdot |F|_v \cdot |P|_v^d.$$

But then, if we raise to the n_v power, multiply over all $v \in M_K$, and take the $[K:\mathbb{Q}]^{th}$ root, it yields the desired upper bound:

$$\begin{aligned}
|F(P)|_v \leq C_1^{\rho(v)} \cdot |F|_v \cdot |P|_v^d & \\
\Rightarrow\ & |F(P)|_v^{n_v} \leq C_1^{\rho(v)n_v} \cdot |F|_v^{n_v} \cdot |P|_v^{n_v d} \\
\Rightarrow\ & \prod_{v\in M_K} |F(P)|_v^{n_v} \leq \prod_{v\in M_K} C_1^{\rho(v)n_v} \cdot \prod_{v\in M_K} |F|_v^{n_v} \cdot \prod_{v\in M_K} |P|_v^{n_v d} \\
\Rightarrow\ & H_K(F(P)) \leq C_1^{\sum_{v\in M_K}\rho(v)n_v} \cdot H_K(F) \cdot H_K(P)^d \\
\Rightarrow\ & H_K(F(P))^{1/[K:\mathbb{Q}]} \leq (C_1^{\sum_{v\in M_K}\rho(v)n_v})^{1/[K:\mathbb{Q}]} \cdot H_K(F)^{1/[K:\mathbb{Q}]} \cdot H_K(P)^{d\cdot 1/[K:\mathbb{Q}]} \\
\Rightarrow\ & H(F(P)) \leq C_1 H(F) H(P)^d,
\end{aligned}$$

where in the last inequality, we have used the extension formula 3.2.6,

$$\sum_{v\in M_K} \rho(v) n_v = \sum_{v\in M_K^\infty} n_v = [K_v : \mathbb{Q}_v] = [K:\mathbb{Q}].$$

And this equality holds because $v = |\cdot|_\infty$, and then $K_v/\mathbb{Q}_v = K/\mathbb{Q}$.

Thus, setting $C_2' = C_1 H(F)$, we have the upper bound

$$H(F(P)) \leq C_2' H(P)^d.$$

It is worth mentioning that along the proof for the upper bound, we have not used the fact that the f_i have no common nontrivial zeros. However, we will certainly need to use this property to prove the lower bound, since without it there are counterexamples.

We now assume that the set

$$\{Q \in \mathbb{A}^{n+1}(\overline{\mathbb{Q}}) : f_0(Q) = \cdots = f_m(Q) = 0\}$$

consists of the single point $(0,\ldots,0)$. It follows from the Nullstellensatz (theorem 1.1.5), that the ideal

$$I = (f_0,\ldots,f_m) \in \overline{\mathbb{Q}}[X_0,\ldots,X_n]$$

contains some power $X_i^{d_i}$ for each $i = 0,\ldots,n$, since

$$X_i \in \sqrt{I} = \mathcal{I}(V(f_0,\ldots,f_m)),$$

because X_i vanishes on $V(f_0,\ldots,f_m) = \{(0,\ldots,0)\}$. Thus, there exist some polynomials $g_{ij} \in \overline{\mathbb{Q}}[X_0,\ldots,X_n]$ and $e \in \mathbb{Z}$, $e \geq 1$ such that

$$X_i^e = \sum_{j=0}^m g_{ij} f_i, \quad \text{for each } i = 0,\ldots,n. \tag{3.3}$$

Replacing K by a finite extension if necessary, we may assume that each $g_{ij} \in K[X_0, \ldots, X_n]$, and discarding all terms of the right-hand side except those that are homogeneous with degree e, we may assume that each g_{ij} is homogeneous of degree $e - d$. We further set the following natural notation

$$|G|_v := \max\{|b|_v : b \text{ is a coefficient of some } g_{ij}\},$$

$$H_K(G) := \prod_{v \in M_K} |G|_v^{n_v}.$$

We observe that e and $H_K(G)$ may be bounded in terms of m, n, d and $H_K(F)$, although finding a good bound is not easy. For our aim it is enough to know that e and $H_K(G)$ do not depend on the point P.

Recalling that $P = [x_0 : \ldots : x_n]$, we see that the identity for X_i^e, equation (3.3), implies that

$$\begin{aligned} |x_i|_v^e &= \left| \sum_{j=0}^{m} g_{ij}(P) f_i(P) \right|_v \\ &\overset{Eq.(3.2)}{\leq} C_2^{\rho(v)} \max_{0 \leq j \leq m} \{|g_{ij}(P) \cdot f_i(P)|_v\} \\ &\leq C_2^{\rho(v)} \cdot \max_{0 \leq j \leq m} \{|g_{ij}(P)|_v\} \cdot \max_{0 \leq j \leq m} \{|f_i(P)|_v\} \\ &\leq C_2^{\rho(v)} \cdot \max_{0 \leq j \leq m} \{|g_{ij}(P)|_v\} \cdot |F(P)|_v. \end{aligned}$$

Taking now the maximum over i, we obtain

$$|P|_v^e = \max_{0 \leq i \leq n} |x_i|_v^e \leq C_2^{\rho(v)} \cdot \max_{\substack{0 \leq j \leq m \\ 0 \leq i \leq n}} \{|g_{ij}(P)|_v\} \cdot |F(P)|_v. \tag{3.4}$$

Each g_{ij} is homogeneous of degree $e - d$, so the usual application of the triangle inequality, as we have done before with F, yields

$$|g_{ij}(P)|_v \leq C_3^{\rho(v)} |G|_v |P|_v^{e-d},$$

where C_3 may depend on e, but as noted earlier, we can bound e in terms of m, n and d. Substituting this estimate into the inquality (3.4) and multiplying by $|P|_v^{d-e}$ gives

$$|P|_v^d \leq C_4^{\rho(v)} |G|_v |F(P)|_v.$$

And now, as we did before, we raise this inequality to the n_v power, multiply over $v \in M_K$ and take the $[K : Q]^{th}$ root, yields the lower bound,

$$C_1' H(P)^d \leq H(F(P))$$

for some positive constant C_1'.

□

The next corollary records the special cases of the theorem 3.2.13 for an automorphism of $\mathbb{P}^n$.

Corollary 3.2.14 *Let $A \in GL_{n+1}(\overline{\mathbb{Q}})$, so multiplication by A induces an automorphism $A : \mathbb{P}^n \to \mathbb{P}^n$. There are positive constants C_1 and C_2, depending on the entries of the matrix A, such that*

$$C_1 H(P) \le H(AP) \le C_2 H(P), \quad \text{for all } P \in \mathbb{P}^n(\mathbb{Q}).$$

PROOF. This is theorem 3.2.13 for morphisms of degree one.

□

We now wonder if there is any relation between the coefficients of a polynomial and the height of its roots. We will set the following notation to simplify our work.
Notation. For $x \in \overline{\mathbb{Q}}$, let

$$H(x) = H([x : 1]),$$

and similarly for $x \in K$, let

$$H_K(x) = H_K([x : 1]).$$

Theorem 3.2.15 *Let $f(T) \in \overline{\mathbb{Q}}[T]$ be a polynomial of degree d defined by*

$$f(T) = a_0 T^d + a_1 T^{d-1} + \cdots + a_d = a_0 (T - \alpha_1) \cdots (T - \alpha_d),$$

with $a_0 \neq 0$. Then

$$2^{-d} \prod_{j=1}^{d} H(\alpha_j) \le H([a_0 : a_1 : \ldots : a_n]) \le 2^{d-1} \prod_{j=1}^{d} H(\alpha_j).$$

PROOF. Without loss of generality, we can assume that $a_0 = 1$ because the inequality to be proven remains unchanged if $f(T)$ is multiplied by a nonzero constant.

Let $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_d)$, and for $v \in M_K$,

$$\epsilon(v) := \begin{cases} 2, & \text{if } v \in M_K^\infty, \\ 1, & \text{if } v \in M_K^0. \end{cases}$$

Note that this notation differs from the notation used for $\rho(v)$ in the proof of theorem 3.2.13. In the present instance, the triangle inequality reads

$$|x + y|_v \le \epsilon(v) \max\{|x|_v, |y|_v\} \quad \text{for } v \in M_K \text{ and } x, y \in K. \tag{3.5}$$

with equality if $v \in M_K^0$ and $|x|_v = |y|_v$.

To get the desired result, it suffices to prove that

$$\epsilon(v)^{-d}\prod_{j=1}^{d}\max\{|\alpha_j|_v,1\}\leq\max_{0\leq i\leq d}\{|a_i|_v\}\leq\epsilon(v)^{d-1}\prod_{j=1}^{d}\max\{|\alpha_j|_v,1\}$$

beause once we have showed this, we just have to raise to the n_v power, multiply over all $v\in M_K$ and take the $[K:\mathbb{Q}]^{th}$ root.

The proof is by induction on $d=\deg f$.

- Base case.

  For $d=1$, we have $f(T)=T-\alpha_1$, we have $a_1=\alpha_1$, so

  $$\epsilon(v)^{-1}\max\{|\alpha_1|_v,1\}\leq\max\{|\alpha_1|_v,1\}\leq\epsilon(v)^{0}\max\{|\alpha_1|_v,1\},$$

  and the inequality clearly holds.

- Induction step.

  Assume now that we know the result for all polynomials with roots in K of degree $d-1$, i.e.,

  $$\epsilon(v)^{-d+1}\prod_{j=1}^{d-1}\max\{|\alpha_j|_v,1\}\leq\max_{0\leq i\leq d-1}\{|a_i|_v\}\leq\epsilon(v)^{d-2}\prod_{j=1}^{d-1}\max\{|\alpha_j|_v,1\}$$

  Let $f(T)\in\overline{\mathbb{Q}}[T]$ be a polynomial of degree d with all its roots on K and choose an index $i=k$ such that

  $$|\alpha_k|_v\geq|\alpha_j|_v\quad\text{ for all }0\leq j\leq d,$$

  and define a polynomial

  $$\begin{aligned}g(T)&=(T-\alpha_1)\cdots(T-\alpha_{k-1})(T-\alpha_{k+1})\cdots(T-\alpha_d)\\&=b_0T^{d-1}+b_1T^{d-2}+\cdots+b_{d-1}.\end{aligned}$$

  Thus $f(T)=(T-\alpha_k)g(T)$, so comparing coefficients yields

  $$a_i=b_i-\alpha_k b_{i-1}.$$

  for all $0\leq i\leq d$, setting $b_{-1}=b_d=0$.

  The upper bound is obtained this way:

  $$\begin{aligned}\max_{0\leq i\leq d}\{|a_i|_v\}&=\max_{0\leq i\leq d}\{|b_i-\alpha_k b_{i-1}|_v\}\\&\overset{(3.5)}{\leq}\epsilon(v)\max_{0\leq i\leq d}\{|b_i|_v,|\alpha_k b_{i-1}|_v\}\\&\leq\epsilon(v)\max_{0\leq i\leq d-1}\{|b_i|_v\}\max\{|\alpha_k|_v,1\}\\&\overset{\text{Hyp.}}{\leq}\epsilon(v)^{d-1}\prod_{j=1}^{d}\max\{|\alpha_j|_v,1\}\end{aligned}$$

  Next, to prove the lower bound, we consider two cases.

– If $|\alpha_k|_v \leq \epsilon(v)$, then by the choice of the index k, we have

$$\prod_{j=1}^{d} \max\{|\alpha_j|_v, 1\} \leq (\max\{|\alpha_k|_v, 1\})^d \leq \epsilon(v)^d,$$

thus

$$\epsilon(v)^{-d} \prod_{j=1}^{d} \max\{|\alpha_j|_v, 1\} = \epsilon(v)^{-d}\epsilon(v)^d = 1 \leq \max_{0\leq i\leq d}\{|a_i|_v\},$$

since $a_0 = 1$ by assumption.

– If $|\alpha_k|_v > \epsilon(v)$. Then

$$\begin{aligned} \max_{0\leq i\leq d}\{|a_i|_v\} &= \max_{0\leq i\leq d}\{|b_i - \alpha_k b_{i-1}|_v\} \\ \overset{3.5}{\geq} \epsilon(v)^{-1} \max_{0\leq i\leq d}\{|b_i|_v, |\alpha_k b_{i-1}|_v\} & \\ &\geq \epsilon(v)^{-1}|\alpha_k|_v \max_{0\leq i\leq d-1}\{|b_i|_v\} \end{aligned}$$

The last inequality turns into an equality when $v \in M_K^0$, while for $v \in M_K^\infty$ we are using the calculation

$$\begin{aligned} \max_{0\leq i\leq d}\{|b_i - \alpha_k b_{i-1}|_v\} &\geq (|\alpha_k|_v - 1) \max_{0\leq i\leq d-1}\{|b_i|_v\} \\ &> \epsilon(v)^{-1}|\alpha_k|_v \max_{0\leq i\leq d-1}\{|b_i|_v\} \end{aligned}$$

since $|\alpha_k|_v > \epsilon(v) = 2$.

Now, applying the hypothesis, we have

$$\begin{aligned} \max_{0\leq i\leq d}\{|a_i|_v\} &\geq \epsilon(v)^{-1}|\alpha_k|_v \max_{0\leq i\leq d-1}\{|b_i|_v\} \\ &\geq \epsilon(v)^{-d} \prod_{j=1}^{d} \max\{|\alpha_j|_v, 1\}. \end{aligned}$$

□

The previous theorem will let us show that there are only finitely many points of bounded height in projective space. To do this, we first need to show that the action of the Galois group does not affect the height of a point.

Theorem 3.2.16 *Let $P \in \mathbb{P}^n(\overline{\mathbb{Q}})$ and let $\sigma \in Gal(\overline{\mathbb{Q}}/\mathbb{Q})$. Then*

$$H(P^\sigma) = H(P).$$

PROOF. Let $K/\mathbb{Q}$ be a field such that $P \in \mathbb{P}^n(K)$. The field K may not be Galois over $\mathbb{Q}$, but in any case σ induces an isomorphism

$$\sigma : K \xrightarrow{\sim} K^\sigma = \{\alpha^\sigma : \alpha \in K\}.$$

This isomorphism induces another isomorphism in the absolute value set

$$\sigma : M_K \longrightarrow M_{K^\sigma}; \qquad v \mapsto v^\sigma,$$

where, if $x \in K$ and $v \in M_K$, the associated absolute value v^σ is such that satisfies

$$|x^\sigma|_{v^\sigma} = |x|_v.$$

It is clear that σ also induces an isomorphism

$$\sigma : K_v \xrightarrow{\sim} K_v^\sigma,$$

so the local degrees satisfy $n_v = n_{v^\sigma}$.

We now compute

$$\begin{aligned} H_{K^\sigma}(P^\sigma) &= \prod_{w \in M_{K^\sigma}} \max\{|x_i^\sigma|_w\}^{n_w} \\ &= \prod_{v \in M_K} \max\{|x_i^\sigma|_{v^\sigma}\}^{n_{v^\sigma}} \\ &= \prod_{v \in M_K} \max\{|x_i|_v\}^{n_v} \\ &= H_K(P). \end{aligned}$$

Since $[K : \mathbb{Q}] = [K^\sigma : \mathbb{Q}]$, we have $H(P) = H(P^\sigma)$.

□

Theorem 3.2.17 *Let C and d be constants. Then the set*

$$\{P \in \mathbb{P}^n(\overline{\mathbb{Q}}) : H(P) \le C \text{ and } [\mathbb{Q}(P) : \mathbb{Q}] \le d\}$$

is a finite set of points, where, if $P = [x_0 : \ldots : x_n]$, then $\mathbb{Q}(P) = \mathbb{Q}(x_0/x_i, \ldots, x_n/x_i)$ for some $x_i \neq 0$, known as the minimal field of definition for P. In particular, for any number field K,

$$\{P \in \mathbb{P}^n(K) : H(P) \le C\}$$

is a finite set.

PROOF. Let $P \in \mathbb{P}^n(\overline{\mathbb{Q}})$ with homogeneous coordinates, say, $P = [x_0 : \ldots : x_n]$, with some $x_j = 1$. Then $\mathbb{Q}(P) = \mathbb{Q}(x_0, \ldots, x_n)$, and we have the estimate

$$H_{\mathbb{Q}(P)}(P) = \prod_{v \in M_{\mathbb{Q}(P)}} \max_{0 \le i \le n} \{|x_i|_v\}^{n_v} \ \ge \max_{0 \le i \le n} \left(\prod_{v \in M_{\mathbb{Q}(P)}} \max\{|x_i|_v, 1\}^{n_v} \right) = \max_{0 \le i \le n} H_{\mathbb{Q}(P)}(x_i).$$

Thus, as by hypothesis $H(P) \leq C$ and $[\mathbb{Q}(P) : \mathbb{Q}] \leq d$, then

$$\begin{aligned} C \geq H(P) &= H_{\mathbb{Q}(P)}(P)^{1/[\mathbb{Q}(P):\mathbb{Q}]} \\ &\geq (\max_{0\leq i\leq n} H_{\mathbb{Q}(P)}(x_i))^{1/[\mathbb{Q}(P):\mathbb{Q}]} \\ &= \max_{0\leq i\leq n} H_{\mathbb{Q}(P)}(x_i)^{1/[\mathbb{Q}(P):\mathbb{Q}]} \\ &= \max_{0\leq i\leq n} H(x_i), \end{aligned}$$

and $\max_{0\leq i\leq n}[\mathbb{Q}(x_i) : \mathbb{Q}] \leq d$.

It thus suffices to prove that the set

$$\{x \in \overline{\mathbb{Q}} : H(x) \leq C \text{ and } [\mathbb{Q}(x) : \mathbb{Q}] \leq d\}$$

is finite, i.e., we have reduced to the case $n = 1$.

Suppose that $x \in \overline{\mathbb{Q}}$ is in this set and let $e = [\mathbb{Q}(x) : \mathbb{Q}]$, so $e \leq d$. Further, let $x_1, \ldots, x_e \in \overline{\mathbb{Q}}$ be the conjugates of x by $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$, where we take $x_1 = x$.

The minimal polynomial of x over $\mathbb{Q}$ is

$$f_x(T) = (T - x_1) \cdots (T - x_e) = T^e + a_1 T^{e-1} + \cdots + a_e \in \mathbb{Q}[T].$$

We estimate

$$\begin{aligned} H([1, x_1, \ldots, x_e]) &\overset{th.3.2.13}{\leq} 2^{e-1} \prod_{j=1}^{n} H(x_i) \\ &\overset{th.3.2.16}{=} 2^{e-1} H(x)^e \\ &\leq (2C)^d, \end{aligned}$$

since $H(x) \leq C$ and $e \leq d$.

Since the $a_i \in \mathbb{Q}$ for $i = 1, \ldots, e$, as we saw in example 3.2.3, there are only finitely many points $P \in \mathbb{P}^e(\mathbb{Q})$ such that $H(P) \leq (2C)^d$, hence there are finitely many posibilities for the polynomial $f_x(T)$, i.e., for the conjugates of x. Since each polynomial $f_x(T)$ has at most d roots in K, and thus it contributes at most d elements to our set, the set

$$\{P \in \mathbb{P}^n(\overline{\mathbb{Q}}) : H(P) \leq C \text{ and } [\mathbb{Q}(P) : \mathbb{Q}] \leq d\}$$

is finite for any constants C and d. Furthermore, if K is a number field with $[K : \mathbb{Q}] = e$, we have $H_K(P) = H(P)^e$ and thus

$$\{P \in \mathbb{P}^n(K) : H_K(P) \leq C\} \subset \{P \in \mathbb{P}^n(\overline{\mathbb{Q}}) : H(P) \leq C^{1/e} \text{ and } [\mathbb{Q}(P) : \mathbb{Q}] \leq e\}$$

is finite because is a subset of a finite set.

□

3.2.2 Heights on Elliptic Curves

In this subsection we use the theory of heights developed in the previously to define height functions on elliptic curves. We will deduce from this work, the fact that $E(K)/mE(K)$ is finite, the Descent Theorem and thus the Mordell-Weil Theorem for arbitrary number fields.

We begin recalling the *"big-O" notation*. If $f, g : S \to \mathbb{R}$, we write

$$f = g + O(1)$$

if there are constants C_1 and C_2 such that

$$C_1 \leq f(P) - g(P) \leq C_2, \quad \text{for all } P \in S.$$

Let E be an elliptic curve defined over a number field K. We know from example 1.3.15 that any nonconstant function $f \in \overline{K}(E)$ determines a surjective morphism,

$$f : E \to \mathbb{P}^1, \qquad P \mapsto \begin{cases} [1:0], & \text{if } P \text{ is a pole of } f, \\ [f(P):1], & \text{otherwise.} \end{cases}$$

We use f to define a height function on $E(\overline{K})$ by setting

$$H_f(P) = H(f(P)).$$

The height function H tends to behave multiplicatively, but for our purpose is more convenient to have a height function which behaves additively. This prompt the following definitions.

Definition 3.2.18 (Logaritmic height) The **(absolute) logarithmic height** on projective space is the function

$$h : \mathbb{P}^n(\overline{\mathbb{Q}}) \to \mathbb{R}; \qquad h(P) = \log H(P).$$

Note that proposition 3.2.9.ii tells us that $h(P) \geq 0$ for all P.

Definition 3.2.19 (Height on a elliptic curve) Let E/K be an elliptic curve, and let $f \in \overline{K}(E)$ be a function. The **height on E (relative to f)** is the function

$$h_f : E(\overline{K}) \to \mathbb{R}; \qquad h_f(P) = h(f(P)).$$

We start by translating the finiteness result from the previous section (theorem 3.2.17) into the current setting.

Proposition 3.2.20 *Let E/K be an elliptic curve and let $f \in K(E)$ be a nonconstant function. Then for any constant C, the set*

$$\{P \in E(K) : h_f(P) \leq C\}$$

is finite.

PROOF. The function $f \in K(E)$ is defined over K, so it maps points $P \in E(K)$ to points $f(P) \in \mathbb{P}^1(K)$. But we can write

$$\begin{aligned}\{P \in E(K) : h_f(P) \leq C\} &= \{P \in E(K) : h(f(P)) \leq C\} \\ &= \{P \in E(K) : \log H(f(P)) \leq C\} \\ &= \{P \in E(K) : H(f(P)) \leq e^C\}\end{aligned}$$

We have then the following correspondence:

$$\{P \in E(K) : h_f(P) \leq C\} \longleftrightarrow \{Q \in \mathbb{P}^1(K) : H(Q) \leq e^C\}.$$

The relation between the cardinals of these two sets depends on the degree of f, but by proposition (1.5.6.i), the preimage by f of any $Q \in \mathbb{P}^1(K)$ must be finite. But theorem 3.2.17 tells us that the last set is finite, so the first one is finite too.

□

The following theorem gives a relation between height functions and the addition law on an elliptic curve.

Theorem 3.2.21 *Let E/K be an elliptic curve and let $f \in K(E)$ be an even function, i.e., a function satisfying $f \circ [-1] = f$. Then for all $P, Q \in E(\overline{K})$, we have*

$$h_f(P+Q) + h_f(P-Q) = 2h_f(P) + 2h_f(Q) + O(1).$$

The constants inherent in the $O(1)$ depend on the elliptic curve E and the function f, but are independent of the points P and Q.

PROOF. Let E be given in a Weierstrass short normal form

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

We start by proving the theorem for $f = x$. The general case is then a collorary.

Since $h_x(\mathcal{O}) = 0$ and $h_x(-P) = h_x(P)$,the desired result is clear if $P = \mathcal{O}$ or $Q = \mathcal{O}$. We now assume that $P \neq \mathcal{O}$ and $Q \neq \mathcal{O}$ and we write

$$x(P) = [x_1 : 1], \qquad x(Q) = [x_2 : 1], \qquad x(P+Q) = [x_3 : 1], \qquad x(P-Q) = [x_4 : 1].$$

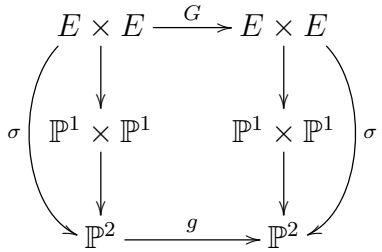
Here x_3 or x_4 may equal $\mathcal{O}$ if $P = \pm Q$. The addition formula form propositoin 2.2.3 and some algebra yield the relations

$$x_3 + x_4 = \frac{2(x_1+x_2)(A+x_1x_2)+4B}{(x_1+x_2)^2 - 4x_1x_2}, \qquad x_3x_4 = \frac{(x_1x_2 - A)^2 - 4B(x_1+x_2)}{(x_1+x_2)^2 - 4x_1x_2}.$$

Define a map $g : \mathbb{P}^2 \to \mathbb{P}^2$ by

$$g([u,v,w]) = [v^2 - 4uv, 2(Au+w) + 4Bu^2, (w - Au)^2 - 4Buv].$$

Then the formulas for x_3 and x_4 show that there is a commutative diagram



Where $G(P,Q) = (P+Q, P-Q)$ and the vertical map σ is the composition of two maps:

$$E \times E \longrightarrow \mathbb{P}^1 \times \mathbb{P}^1, \qquad (P,Q) \mapsto (x(P), x(Q)),$$

and

$$\mathbb{P}^1 \times \mathbb{P}^1 \longrightarrow \mathbb{P}^2, \qquad ([\alpha_1 : \beta_1], [\alpha_2 : \beta_2]) \mapsto [\beta_1\beta_2, \alpha_1\beta_2 + \alpha_2\beta_1, \alpha_1\alpha_2].$$

The idea here is that we are viewing u, v and w as representating 1, $x_1 + x_2$ and x_1x_2, so $g([u,v,w])$ becomes $[1, x_3 + x_4, x_3x_4]$.

The next step is to show that g is a morphism, which will allow us to apply theorem 3.2.13. We must show that the three homogeneous polynomials defining g have no common zeros other than $u = v = w = 0$. Suppose that $g([u,v,w]) = 0$. If $u = 0$, then from

$$v^2 - 4uw = 0 \qquad \text{and} \qquad (w - Au)^2 - 4Buv = 0,$$

we see that $v = w = 0$. Thus we may assume that $u \neq 0$, so we may define a new quantity $x = v/2u$. [*Intuition:* if we identify

$$u = 1, \qquad v = x_1 + x_2, \qquad w = x_1x_2,$$

then the equation $v^2 - 4uw = 0$ becomes $(x_1 - x_2)^2 = 0$, so $x_1 = x_2 = v/2u$. In other words, we are now dealing with the case $P = \pm Q$].

Using the new quantity x, the equation $v^2 - 4uw = 0$ can be written as $x^2 = w/u$. Now dividing the equalities

$$2v(Au + w) + 4Bu^2 = 0 \qquad \text{and} \qquad (w - Au)^2 - 4Buv = 0,$$

by t^2 and rewriting them in terms of x yields the two equations

$$\begin{aligned} \psi(x) &= 4x(A + x^2) + 4B = 4x^3 + 4Ax + 4B = 0, \\ \phi(x) &= (x^2 - A)^2 - 8Bx = x^4 - 2Ax^2 - 8Bx + A^2 = 0. \end{aligned}$$

These polynomials should be familiar, since their ratio is the rational function that appears in the duplication formula (proposition 2.2.3). In order to show that $\psi(x)$ and $\phi(x)$ have no common root, it suffices to verify the following identity:

$$(12x^2 + 16A)\phi(x) - (3x^3 - 5Ax - 27B)\psi(x) = 4(4A^3 + 27B^2) \neq 0,$$

because $4A^3 + 27B^2 = \Delta \neq 0$ since E is a nonsingular elliptic curve. This completes the proof that g is a morphism.

We return to our commutative diagram and compute

$$\begin{aligned} h(\sigma(P+Q, P-Q)) &= h(\sigma \circ G(P,Q)) \\ &= h(g \circ \sigma(P,Q)) \\ &\overset{th.3.2.13}{=} 2h(\sigma(P,Q)) + O(1), \end{aligned}$$

since g is a morphism of degree 2. To complete the proof of theorem 3.2.21 for $f = x$, we will show that

$$h(\sigma(R_1, R_2)) = h_x(R_1) + h_x(R_2) + O(1), \quad \text{for all } R_1, R_2 \in E(\overline{K}).$$

Then, applying this relation to each side of the equation

$$h(\sigma(P+Q, P-Q)) = 2h(\sigma(P,Q)) + O(1)$$

gives the result.

It is clear that if either $R_1 = \mathcal{O}$ or $R_2 = \mathcal{O}$, then $h(\sigma(R_1, R_2))$ is equal to $h_x(R_1) + h_x(R_2)$. Otherwise, we write

$$x(R_1) = [\alpha_1 : 1] \qquad \text{and} \qquad x(R_2) = [\alpha_2 : 1],$$

and then

$$h(\sigma(R_1, R_2)) = h([1 : \alpha_1 + \alpha_2, \alpha_1\alpha 2]) \qquad \text{and} \qquad h_x(R_1) + h_x(R_2) = h(\alpha_1) + h(\alpha_2).$$

We apply theorem 3.2.15 to the polynomial $(T+\alpha_1)(T+\alpha_2)$ to obtain the desired estimate

$$h(\alpha_1) + h(\alpha_2) - \log 4 \leq h([1 : \alpha_1 + \alpha_2, \alpha_1\alpha 2]) \leq h(\alpha_1) + h(\alpha_2) - \log 2.$$

Finally, in order to deal with an arbitrary even function $f \in K(E)$, we prove in the next lemma that

$$h_f = \frac{1}{2}(\deg f)h_x + O(1).$$

Then theorem 3.2.21 follows immediately on multiplying the proven relation for h_x by $\frac{1}{2}\deg f$.

□

Lemma 3.2.22 *Let $f, g \in K(E)$ be two even functions. Then*

$$(\deg g)h_f = (\deg f)h_g + O(1).$$

PROOF. Let $x, y \in K(E)$ be Weierstrass coordinates for E/K. We know from corollary 2.2.4 that the subfield of $K(E)$ consisting of even functions is exactly $K(x)$, so we can find a rational function $f(X) \in K(X)$ such that there is a commutative diagram

$$\begin{array}{ccc} E & & \\ {\scriptstyle x}\downarrow & \searrow^{f} & \\ \mathbb{P}^1 & \xrightarrow{r} & \mathbb{P}^1 \end{array}$$

Hence, using theorem 3.2.13, and the fact that r is a morphism (from corollary 1.3.14), we deduce that

$$h_f = h_x \circ r = (\deg r) h_x + O(1).$$

The diagram tells us that

$$\deg f = (\deg x)(\deg r) = 2 \deg r,$$

so we find that

$$2h_f = (\deg f) h_x + O(1).$$

The same reasoning applied to g yields

$$2h_g = (\deg g) h_x + O(1),$$

and combining these last two equalities gives the desires result.

□

Corollary 3.2.23 *Let E/K be an elliptic curve, and let $f \in K(E)$ be an even function.*

i) Let $Q \in E(\overline{K})$. Then

$$h_f(P+Q) \le 2h_f(P) + O(1), \qquad \text{for all } P \in E(\overline{K}),$$

where $O(1)$ depends on E, f and Q.

ii) Let $m \in \mathbb{Z}$. Then

$$h_f([m]P) = m^2 h_f(P) + O(1), \qquad \text{for all } P \in E(\overline{K}),$$

where $O(1)$ depends on E, f and m.

PROOF.

i) It is clear from theorem 3.2.21, since $h(P-Q) \ge 0$.

$$h_f(P+Q) \le 2h_f(P) + \underbrace{2h_f(Q) + O(1)}_{O(1)},$$

where the new $O(1)$ depends on E, f and Q.

ii) Since f is even, it suffices to consider $m \geq 0$. We use induction to complete the proof.

- Base case.
  If $m = 0$ and $m = 1$ is clear.
- General case.
  Suppose that the result is known for $m-1$ and for m. We take $P = [m]P$ and $Q = P$ in Theorem 3.2.21, so we find that

$$\begin{aligned} h_f([m+1]P) &= -h_f([m-1]P) + 2h_f([m]P) + 2h_f(P) + O(1) \\ &\overset{\text{Hyp.}}{=} -(m-1)^2 h_f(P) + 2(m^2 h_f(P)) + 2h_f(P) + O(1) \\ &= (2m^2 - (m-1)^2 + 2)h_f(P) + O(1) \\ &= (m^2 + 2m + 1)h_f(P) + O(1) \\ &= (m+1)^2 h_f(P) + O(1). \end{aligned}$$

□

Remark 3.2.24. We can restatement lemma 3.2.23.i as follows:

Let $Q \in E(K)$. Then there is a constant C_1, depending on E, f and Q, such that

$$h_f(P+Q) \leq 2h_f(P) + C_1 \quad \text{for all } P \in E(K).$$

3.3 Proof of the Mordell-Weil Theorem

We now prove the theorem which we began this chapter:

Theorem 3.3.1 (Mordell-Weil Theorem) *Let K be a number field, and let E/K be an elliptic curve. Then the group $E(K)$ is finetely generated.*

PROOF. Choose any even nonconstant function $f \in K(E)$, for example, the x-coordinate on a Weierstrass equation

$$x : E(K) \to \mathbb{P}^1(K);$$

with

$$x([x_0 : y_0 : 1]) = [x_0 : 1] \qquad \text{and} \qquad x(\mathcal{O}) = [1 : 0].$$

The Mordell-Weil Theorem follows immediatly from the Weak Mordell-Weil Theorem (theorem 3.0.4) with $m = 2$, which assures that $E(K)/2E(K)$ is finite; and the Descent Theorem (theorem 3.0.5) as soon as we show that the height function

$$h_f : E(K) \to \mathbb{R}$$

has the following three properties:

a) Let $Q \in E(K)$. Then there is a constant C_1, depending on E, f and Q, such that

$$h_f(P+Q) \leq 2h_f(P) + C_1 \quad \text{for all } P \in E(K).$$

b) There is a constant C_2, depending on E and f, such that

$$h_f([2]P) \geq 4h_f(P) - C_2 \quad \text{for all } P \in E(K).$$

c) For every constant C_3, the set

$$\{P \in E(K) : h_f(P) \leq C_3\}$$

is finite.

Here (a) is remark 3.2.24, while (b) is immediate from the $m = 2$ case of lemma 3.2.23.ii. Finally, (c) is theorem 3.2.20.

□

3.4 Remarks on the Mordell-Weil group

The Mordell-Weil theorem says that the **Mordell-Weil group** $E(K)$ of an elliptic curve can be written in the form

$$E(K) \simeq E(K)_{tors} \times \mathbb{Z}^r,$$

where, as we will see in the following chapters, the torsion subgroup $E(K)_{tors}$ is relatively easy to compute, both in theory and in practice; nevertheless the **rank** r (also known as **geometric rank,** r_g) is more unknown and an effective procedure for determining it in all cases is still been sought. There are a very few general facts known concerning the rank of elliptic curves, but there are a large number of incredible conjectures.

The rank of a "randomly chosen" elliptic curve over $\mathbb{Q}$ tends to be quite small, and it is difficult to produce curves $E/\mathbb{Q}$ having even moderately high rank.

Nontheless, there exists the following conjecture:

Conjecture 3.4.1 There exist elliptic curves $E/\mathbb{Q}$ of arbitrary large rank.

A key piece of evidence for this conjecture comes from work of Shafarevich and Tate [69] who showed that the analogous result is true for function fields, i.e., with $\mathbb{Q}$ replaced by the field of rational functions $\mathbb{F}_p(T)$. The Shafarevich-Tate construction leads to curves with constant j-invariant, $e_E \in \mathbb{F}_p$, but subsequent contructions by Shioda [70] for $\overline{\mathbb{F}}_p(T)$ and Ulmer [78] for $\mathbb{F}_p(T)$ give examples with nonconstant j-invariants.

Néron [60] constructed an infinite family of elliptic curves over $\mathbb{Q}$ having rank at least 10 and later authors have constructed families of rank up to 19. Within these families,

clever search techniques due to Mestre [51] and others have yielded individual curves of higher rank. For example, if we set Elkies [20] has produced the elliptic curve.

$$\begin{aligned} y^2 + xy + y = x^3 - x^2 \\ - 2006776241557552658503320820933854275093023031217895650 2x \\ + 3448161179503055646703298569039 07/ \\ 4203748559443593191803612660082962919394487322434 29. \end{aligned}$$

with rank $E(\mathbb{Q}) \geq 28$.

In fact, the highest rank of an elliptic curve that is known so far (not only a lower bound of rank) is equal 19 and it was found by Elkies in 2009 [19]. It improves previous recoreds due to Kretschmer ($r = 10$), Schneiders-Zimmer ($r = 11$), Fermigier ($r = 14$), Dujella ($r = 15$) and Elkies ($r = 17$, $r = 18$).

The following table contains some historical data on elliptic curve rank records.

Rank $\geq$	Year	Author(s)
3	1938	Billing
4	1945	Wiman
6	1974	Penney - Pomerance
7	1975	Penney - Pomerance
8	1977	Grunewald - Zimmert
9	1977	Brumer - Kramer
12	1982	Mestre
14	1986	Mestre
15	1992	Mestre
17	1992	Nagao
19	1992	Fermigier
20	1993	Nagao
21	1994	Nagao - Kouya
22	1997	Fermigier
23	1998	Martin - McMillen
24	2000	Martin - McMillen
28	2006	Elkies

Table 3.1: Historical data on elliptic curve rank records [31].

From another point of view, we could wonder what is the rank of an elliptic curve E on average. In order to ask this question more precisely, we need a natural way to measure the size of elliptic curves, so that we can order them by size. If E is an elliptic curve given by $y^3 = x^2 + Ax + B$, we can define the (naive) heigh of E as

$$h(E) := \max 4|A|^3, 27B^2.$$

There are other mesures we can use to order elliptic curves by size, as the discriminant of the curve. Then, if all elliptic curves defined over $\mathbb{Q}$ are ordered by their discriminants, what is the average size of the rank?

Conjecture 3.4.2 (Goldfeld, Katz-Sarnak) If we use the (naive) heigh, the average size of the rank of all elliptic curves defined over $\mathbb{Q}$ is equal to $1/2$.

However, previously this average has not even been known to be finite.

The first theoretical result towards the boundedness of average rank is due to Brumer [7]. In 1992, he showed that the Generalized Riemann Hypothesis (GRH) and the Birch and Swinnerton-Dyer Conjecture (BSD) -conjecture 3.4.4- together imply that the average rank is bounded. In fact, bounded by 2,3. In 2004, Heath-Brown (still assuming GRH + BSD) improved this to average rank ≤ 2, [30]. And in 2006, Young further improved this (again assuming GRH + BSD) to $\leq 25/14$, [81]. But in 2010 Bhargava and Shankar [4] proved the main theorem:

Theorem 3.4.3 (Bhargava, Shankar) *The average rank of the Mordell-Weil group of an elliptic curve over $E/\mathbb{Q}$ is bounded above by* $7/6$.

There exists also a function called **L-function** associated to an elliptic curve E and related to the Riemann zeta function $\zeta(s)$, defined by

$$L(E,s) = \prod_{p \ prime} (1 - a_p p^{-s} + p^{1-2p})^{-1}.$$

This function is known as the Hasse-Weil L-function and defines a complex analytic function on some right half plane $\Re(z) > 3/2$.

Wiles' theorem [80] implies that $L(E,s)$ can be analytically continued to an analytic function on $\mathbb{C}$. This implies that $L(E,s)$ has a Taylor series expansion at $s = 1$:

$$L(E,s) = c_0 + c_1(s-1) + c_2(s-1)^2 + \cdots .$$

Define the *analytic rank* r_a of E to be the order of vanishing of $L(E,s)$ as $s = 1$, so

$$L(E,s) = c_{r_a}(s-1)^{r_a} + \cdots .$$

Note that the definitions of the analytic and geometric ranks could not be more different - one is completely analytic and the other is purely algebraic. Nevertheless, the Birch and Swinnerton-Dyer Conjecture states the following:

Conjecture 3.4.4 (Birch and Swinnerton-Dyer, BSD) For any elliptic curve E defined over $\mathbb{Q}$ the analytic and geometric rank are equal, i.e.,

$$r_g = r_a.$$

This problem is extremely difficult. The conjecture was made in the 1960s and hundredsod people have thought about it for over 5 decades. The work of Wiles on modularity in late 1999, combined with earlier work of Gross, Zagier and Kolyvagin and many others proved the following partial result toward the conjecture:

Theorem 3.4.5 *Let E be an elliptic curve over $\mathbb{Q}$. Suppose $r_a \leq 1$. Then $r_a = r_g$.*

Nowadays, the class of curves for which we know the conjecture is still the set of curves over $\mathbb{Q}$ with $r_a \leq 1$, along with a finite set of individual curves on which further computer calculations have been performed (by Cremona, Watkins, Stein and others). For furhter reading about the BSD Conjecture , see [75].

In addition to wanting an effective method for computing the rank of an elliptic curve, it would be good to have a theoretical bound for the size of a generating set. Based on an analogy with the problem of computing generators for the unit group in a number field and partly on a number of deep conjectures in analytic number theory, Serge Lang [44] suggested the following estimate:

Conjecture 3.4.6 (Lang) Let $\varepsilon > 0$ and let $E/\mathbb{Q}$ be an elliptic curve of rank r. Then there exits a basis $P_1, \ldots, P_r$ for the free part of $E(\mathbb{Q})$ satisfying

$$\max_{1 \leq i \leq r} \hat{h}(P_i) \leq C_\varepsilon^{r^2} |\mathcal{D}_{E/\mathbb{Q}}|^{\frac{1}{12}+\varepsilon}.$$

Here $\hat{h}$ is the canonical heigh on E, $\mathcal{D}_{E/\mathbb{Q}}$ is the minimal discriminant of $E/\mathbb{Q}$ and C_ε is a constant depending only on ε.

Since $\hat{h}$ is a logaritmic height, the conjecture says that the x-coordinates of the generators may grow exponentially with the discriminant of the curve. The following example, due to Bremmer and Cassels [6], illustrates this exponential behaviour. They showed that

$$y^2 = x^3 + 877x$$

has rank 1 and that the x-coordinate of the smallest generator P is

$$x(P) = \left(\frac{612776083187947368101}{78841535860683900210} \right)^2.$$

We compute

$$\frac{\log \hat{h}(P)}{\log |\mathcal{D}_{E/\mathbb{Q}}|} \approx 0.158,$$

so this example is roughly in the range suggested by Lang's Conjecture.

Chapter 4

The torsion subgroup over number fields

Let K be a number field and let E/K be an elliptic curve. In this chapter we want to study the torsion subgroup $E(K)_{tors}$, specifically when has low degree. Recall that this subgroup is defined as

$$E(K)_{tors} = \bigcup_{m=1}^{\infty} E(K)[m],$$

where

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

4.1 Torsion subgroup over $\mathbb{Q}$

The torsion subgroup of $E/\mathbb{Q}$ is relatively easy to calculate. We will see some methods for doing it in the next chapter, but now we focus on giving some current interesting results about its structure.

The following result classifies all the possible torsion subgroups of an elliptic curve E defined over $\mathbb{Q}$. The first conjecture of the theorem, due to Levi [46] around 1908, was restated by Ogg [62] and finally Mazur [48, 49] proved it in 1978.

Theorem 4.1.1 (Mazur) *Let $E/\mathbb{Q}$ be an elliptic curve. Then the torsion subgroup $E(\mathbb{Q})_{tors}$ of $E(\mathbb{Q})$ is isomorphic to one of the following fifteen groups*

$$E(\mathbb{Q})_{tors} \simeq \begin{cases} \mathbb{Z}/n\mathbb{Z}, & \text{with } 1 \leq n \leq 10 \text{ or } n = 12, \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & \text{with } 1 \leq n \leq 4 \end{cases}$$

Mazur's proof is far beyond this text.

It must be said that all the groups in the list above occurs for infinitely many dinstinct j-invariants.

Table 4.1 contains fifteen elliptic curves defined over $\mathbb{Q}$ with different torsion subgroups. To find methods of computing these curves see [41, chap. V, sc. 5]

$E(\mathbb{Q})_{tors}$	E
$\{\mathcal{O}\}$	$y^2 = x^3 + 2$
$\mathbb{Z}/2\mathbb{Z}$	$y^2 = x^3 + x$
$\mathbb{Z}/3\mathbb{Z}$	$y^2 = x^3 + 4$
$\mathbb{Z}/4\mathbb{Z}$	$y^2 = x^3 + 4x$
$\mathbb{Z}/5\mathbb{Z}$	$y^2 + y = x^3 - x^2$
$\mathbb{Z}/6\mathbb{Z}$	$y^2 = x^3 + 1$
$\mathbb{Z}/7\mathbb{Z}$	$y^2 - xy + 2y = x^3 + 2x^2$
$\mathbb{Z}/8\mathbb{Z}$	$y^2 + 7xy + 6y = x^3 - 6x^2$
$\mathbb{Z}/9\mathbb{Z}$	$y^2 + 3xy + 6y = x^3 + 6x^2$
$\mathbb{Z}/10\mathbb{Z}$	$y^2 - 7xy - 36y = x^3 - 18x^2$
$\mathbb{Z}/12\mathbb{Z}$	$y^2 + 43xy - 210y = x^3 - 210x^2$
$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$	$y^2 = x^3 - x$
$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$	$y^2 = x^3 + 5x^2 + 4x$
$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$	$y^2 + 5xy - 6y = x^3 - 3x^2$
$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$	$y^2 = x^3 + 337x^2 + 20736x$

Table 4.1: Elliptic curves and torsion subgroups.

4.2 Torsion subgroup over number fields

Let E be an elliptic curve defined over a number field K with degree d, i.e., $[K : \mathbb{Q}] = d$. A natural question is whether a classification as in Mazur's theorem 4.1.1 can be found for $E(K)_{tors}$. In this section we make a first approach.

One important issue is to know how the structure of $E(K)_{tors}$ looks like. If we consider the elliptic curve E defined over $\mathbb{C}$, then E is isomorphic to a torus (see [73], chap. VI, sc. 1) obtained as a quotient of $\mathbb{C}$ by a lattice. Then, $\mathbb{C}$-rational points of E are

$$E(\mathbb{C}) \simeq \mathbb{T} \simeq S^1 \times S^1.$$

Using the group homomorphism

$$(\mathbb{R}, +) \longrightarrow (S^1, \cdot); \qquad x \mapsto e^{2\pi i x},$$

we obtain

$$(\mathbb{R}/\mathbb{Z}, +) \simeq (S^1, \cdot).$$

From this result, we can deduce

$$E(\mathbb{C})_{tors} \simeq \mathbb{Q}/\mathbb{Z} \times \mathbb{Q}/\mathbb{Z}.$$

As Mordell-Weil theorem 3.0.3 establishes that $E(K)$ is a finitely generated abelian group and $E(K) \subseteq E(\mathbb{C})$, we have

$$E(K) \simeq \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \mathbb{Z}^r,$$

where $n_1, n_2 \in \mathbb{Z}$ such that $n_1, n_2 > 0$ with $n_1 | n_2$ and $r \geq 0$. As we already know, r is called the rank of $E(K)$ and we will call the pair (n_1, n_2) **the type of torsion** of $E(K)$.

Definition 4.2.1 ($\phi(d)$) We denote by $\phi(d)$ the isomorphism class of finite groups G such that there exits a number field K of degree d and an elliptic curve E/K with

$$E(K)_{tors} \simeq G.$$

It is to say,

$$\phi(d) = \{(n_1, n_2) : \exists K \text{ with } |K : \mathbb{Q}| = d \text{ and } \exists E/K \text{ s.t. } E(K)_{tors} \simeq \mathbb{Z}/n_1\mathbb{Z} \oplus \mathbb{Z}/n_2\mathbb{Z}\}.$$

For example, Mazur's therorem 4.1.1 says that

$$\phi(1) = \{(1), (2), (3), (4), (5), (6), (7), (8), (9), (10), (12), (2, 2), (2, 4), (2, 6), (2, 8)\}.$$

Another important question is whether the list of possible torsion subgroups we look for is finite. The following theorem, which was conjectured by Mazur, provides the answer. In the rest of this section we are showing some results obtained by other mathematicians until the proof of this theorem, due to Merel [50] in February 1996.

Theorem 4.2.2 (Uniform Boundedness Conjecture) *For all $d \in \mathbb{Z}, d \geq 1$ there exists a constant $B(d) \geq 0$ such that for all elliptic curves E defined over a number field K with degree d, then*

$$|E(K)_{tors}| \leq B(d).$$

Another form of reading the latter theorem is "for all $d \in \mathbb{Z}, d \geq 1$, $\phi(d)$ is finite."

Definition 4.2.3 (Torsion primes and $S(d)$) A prime p is called a **torsion prime for degree** d if there exists a number field K of degree d and an elliptic curve E/K such that $p | \#E(K)_{tors}$. Let

$$S(d) = \{\text{Torsion primes for degree } d\}.$$

For example, Mazur's theorem 4.1.1 tells us that

$$S(1) = \{2, 3, 5, 7\}.$$

Thanks to some results due to Frey [24] and Faltings [22] it was proved that, assuming the finiteness of $S(d)$, the list of posibilities for the group $E(K)_{tors}$ for infinitely many elliptic curves E/K defined over infinitely many number fields K of degree $\leq d$ is finite.

Theorem 4.2.4 *If $S(d)$ is finite, then the set of groups $E(K)_{tors}$ as E runs through all elliptic curves over all number fields K of degree $\leq d$ is finite.*

But this result leaves still doubts about the existence of other possible torsion subgroups which could appear a finite number of times.

Years after, in 1988, Kamienny and Mazur [40] reached the following result, getting the list of torsion primes for $d = 2$.

Theorem 4.2.5 (Kamienny, Mazur) $S(2) = \{2, 3, 5, 7, 11, 13\}$.

And some years later, in 1995, also Kamienny and Mazur [37] proved the finiteness of $S(d)$ and $\phi(d)$ for small d:

Theorem 4.2.6 (Kamienny, Mazur) *We have the following results:*

i) $S(d)$ *is finite* $\iff$ $\phi(d)$ *is finite.*

ii) $S(d)$ *is finite for* $d \leq 8$.

Paragraph (ii) of the latter theorem is a consequence of a result due to Frey in 1992, which is, in turn, a consequence of a theorem due to Faltings. It was proven by Kamienny and Mazur using the Kamieny criteria.

Abromovich proved in [1] soon later, also in 1995, the following statement:

Theorem 4.2.7 (Abromovich) $S(d)$ *is finite for* $d \leq 14$.

Corollary 4.2.8 *There is a fixed constant B such that if E/K is an elliptic curve defined over a number field of degree $d \leq 14$, then*

$$\#E(K)_{tors} \leq B.$$

Finally, Merel [50] proved that $S(d)$ is bounded for all d.

Theorem 4.2.9 (Merel's bound) $\max S(d) \leq d^{3d^2}$ *for* $d \geq 2$.

This bound assures that $S(d)$ is finite for all $d \geq 2$ but it is "useless" in practice for $d \geq 4$ because the bound is too large. Fortunately, shorly thereafter Oesterlé [61] modified Merel's argument to get a much better upper bound:

Theorem 4.2.10 (Oesterlé's bound) $\max S(d) \leq (3^{d/2} + 1)^2$ *for* $d \geq 1$.

To see how Oesterlé's bound is better than Merel's one, we can compute them both for $d = 1, \ldots, 10$:

d	Oesterle's bound	Merel's bound
1	7	$---$
2	16	4096
3	38	7625597484987
4	100	792281625142643375935439503 36
5	275	26469779601696885595885078146238811314105987548828125
6	784	$\geq 10^{84}$
7	2281	$\geq 10^{124}$
8	6724	$\geq 10^{173}$
9	19964	$\geq 10^{231}$
10	59536	10^{300}

Table 4.2: Oesterlé and Merel's bounds on $S(d)$.

Unfortunately, as we can see, Oesterlé's bound is not effective. However, in 1999, Parent [63] gave a bound for the p^k-torsion ($k \geq 1$, p prime) and thus obtained a global effective bound for the torsion (later improved again by Oesterlé).

Theorem 4.2.11 (Parent) *Let E be an elliptic curve defined over a number field K of degree d. If $E(K)$ has a point of order p^k, with $k \geq 1$ and p prime, then*

$$p^k \leq \begin{cases} 65(3^d-1)(2d)^6 & \text{if } p \neq 2,3, \\ 65(5^d-1)(2d)^6 & \text{if } p = 3, \\ 129(3^d-1)(3d)^6 & \text{if } p = 2. \end{cases}$$

Merel remarked in a personal communication to Stain on May, 10th 2010, talks about two important facts about bounds for $\#E(K)_{tors}$:

i) The bounds for $S(d)$ known to date are exponential in d. However a *polynomial bound on $S(d)$ is expected*. Therefore, one cannot expect to computationally determine the exact list of torsion primes in degree d for many more d's.

ii) If you want a bound depending on the field K, you can obtain a bound like

$$O(\text{size of the residue field of } K \text{ of smallest order}).$$

If we wonder what do we know nowadays about $S(d)$, we can sum it up as in the following table:

d	S(d)	Authors
1	$\{2,3,5,7\}$	Mazur, 1978 ([48], [49])
2	$\{2,3,5,7,11,13\}$	Kamienny, Kenku and Momose, 1988 ([36], [40])
3	$\{2,3,5,7,11,13\}$	Parent, 2000-2003 ([64], [65])
4	$\{2,3,5,7,11,13,17\}$	Derickx, Kamienny, Stein and Stoll ([16])
5	$\{2,3,5,7,11,13,17,19\}$	Derickx, Kamienny, Stein and Stoll ([16])

Table 4.3: Some known bounds on $S(d)$.

Note that the article [16] is still in preparation. A large part for calculating $S(4)$ consist of using a computer to check for a lot of primes p whether the hypotheses of [64, th. 1.10] are satisfied, showing that for these primes we have $p \notin S(d)$. Simply running the same computer calculations for $S(5)$ would take too long, this is why Kamienny, Stein and Stoll did not do it for other d. Nevertheless, Derickx [15] have made the algorithm computationally more efficient to check the hypotheses of [64, th. 1.10] so that these techniques can also be used for $S(5)$, $S(6)$ and $S(7)$. Moreover, these techniques can also be used to improve the results for $S(5)$. In fact, it is now known that $S(5) = \{2,3,5,7,9,11,13,17,19\}$ since Stoll managed to show $29, 31, 41 \notin S(5)$. A proof of this will be also given in [16].

4.2.1 Torsion subgroup over a quadratic field

Let E be an elliptic curve defined over a number field K of degree 2. The complete list for all possible torsion subgroups $E(K)_{tors}$ is knowm too.

By theorem 4.2.5 we know that

$$S(2) = \{2,3,5,7,11,13\}.$$

Some years before, in 1992 , Kamienny [36] proved the following result:

Theorem 4.2.12 (Kamienny) *If a torsion point of an elliptic curve E defined over a quadratic field K has prime order p, then $p \leq 13$.*

This theorem, when combined with some previous work of Kenku and Momose [40] (1988), gave a complete list of possible torsion structures over quadratic fields:

Theorem 4.2.13 (Kamienny, Kenku, Momose) *Let K be a quadratic field and let E/K be an elliptic curve. Then*

$$E(K)_{tors} \simeq \begin{cases} \mathbb{Z}/n\mathbb{Z}, & \text{with } 1 \leq n \leq 16 \text{ or } n = 18, \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & \text{with } 1 \leq n \leq 6, \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3n\mathbb{Z}, & \text{with } n = 1,2 \text{ and } K = \mathbb{Q}(\sqrt{-3}), \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}, & \text{if } K = \mathbb{Q}(i). \end{cases}$$

As occurs in Mazur's theorem, all the groups in the list occurs for infinitely many dinstinct j-invariants but note that not all of these groups occurs for a given quadratic number field.

Najman [58] gave in 2010 a classification of the torsion subgroups of elliptic curves defined over quadratic cyclotomic fields (as $\mathbb{Q}(i)$ or $\mathbb{Q}(\sqrt{-3})$) and Najman and Kamienny [38] have given recently, in 2012, a procedure how to make such classification. Also in [58], Najman classify the possible torsion structures over quadratic fields for elliptic curves defined over $\mathbb{Q}$:

Theorem 4.2.14 (Najman) *Let $E/\mathbb{Q}$ be an elliptic curve and let $K/\mathbb{Q}$ be a quadratic extension.*

i) Then

$$E(K)_{tors} \simeq \begin{cases} \mathbb{Z}/n\mathbb{Z}, & \text{with } 1 \leq n \leq 10 \text{ or } n = 12, 15, 16, \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & \text{with } 1 \leq n \leq 6, \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3n\mathbb{Z}, & \text{with } n = 1, 2, \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}. \end{cases}$$

ii) Each of these groups, except for $\mathbb{Z}/15\mathbb{Z}$, appears as the torsion structure over a quadratic field for infinitely many elliptic curves E defined over $\mathbb{Q}$.

iii) The elliptic curves 50b1 and 50a3 (Cremona labels [12, 13]) have 15-torsion over $\mathbb{Q}(\sqrt{5})$, 50b2 and 450b4 have 15-torsion over $\mathbb{Q}(\sqrt{-15})$. These are the only elliptic curves defined over $\mathbb{Q}$ having nontrivial 15-torsion over any quadratic field.

4.2.2 Torsion subgroup over a cubic field

Let E be an elliptic curve defined over a number field K of degree 3. Classification for $E(K)_{tors}$ is still unknown. Nevertheless we already have some information about it.

First of all, Oesterlé's theorem (theorem 4.2.10) tells us that $\max S(3) \leq 38$. But the work of Parent [64, 65] between 2000 and 2003 let him show that

$$S(3) = \{2, 3, 5, 7, 11, 13\}.$$

Later in 2004, Jeon, Kim and Schweizer [35] proved the following result:

Theorem 4.2.15 *All the torsion structures that appear infinitely many times as one runs through all elliptic curves over all cubic fiels are*

$$E(K)_{tors} \simeq \begin{cases} \mathbb{Z}/n\mathbb{Z}, & \text{with } 1 \leq n \leq 16 \text{ or } n = 18 \text{ or } n = 20 \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & \text{with } 1 \leq n \leq 7 \end{cases}$$

But if one runs through all elliptic curves over all cubic number fields, does there exist torsion structures that appear only finitely many times? It can be shown that there exists a curve defined over a cubic field with torsion $\mathbb{Z}/21\mathbb{Z}$, so the answer is 'yes' and then the list of theorem 4.2.15 is not complete.

Nowadays we are near the complete classification of torsion structures for elliptic curves $E/\mathbb{Q}$ defined over cubic fields. In [59], a nonpublished paper to date, Najman classify the possible torsion structures over cubic fields for elliptic curves defined over $\mathbb{Q}$:

Theorem 4.2.16 (Najman) *Let $E/\mathbb{Q}$ be an elliptic curve and let $K/\mathbb{Q}$ be a cubic extension. Then*

$$E(K)_{tors} \simeq \begin{cases} \mathbb{Z}/n\mathbb{Z}, & \text{with } 1 \leq n \leq 10 \text{ or } n = 12, 13, 14, 18, 21, \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & \text{with } n = 1, 2, 3, 4, 7. \end{cases}$$

Each of these groups, except for $\mathbb{Z}/21\mathbb{Z}$, appears as the torsion structure over a cubic field for infinitely many elliptic curves E defined over $\mathbb{Q}$.

Moreover, in [59] it is proven that the elliptic curve $162b1$ (Cremona label, [12, 13]) defined over $\mathbb{Q}(\zeta_9)^+$ is the unique elliptic curve $E/\mathbb{Q}$ with torsion isomorphic to $\mathbb{Z}/21\mathbb{Z}$ over a cubic field.

4.2.3 Torsion subgroup over a quartic field

Let E be an elliptic curve defined over a number field K of degree 4. Once again, Oesterlé's theorem (theorem 4.2.10) tells us that $\max S(4) \leq 97$.

Recently, in 2011, Kamienny, Stein and Stoll [16] have shown that

$$S(4) = \{2, 3, 5, 7, 11, 13, 17\}.$$

Jeon, Kim and Park [34] showed in 2006 that groups that happen for infinitely many j-invariants for an elliptic curve E defined over a quartic field K are

$$E(K)_{tors} \simeq \begin{cases} \mathbb{Z}/n\mathbb{Z}, & \text{with } 1 \leq n \leq 18 \text{ or } n = 20, 21, 22, 24, \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & \text{with } 1 \leq n \leq 9, \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3n\mathbb{Z}, & \text{with } 1 \leq n \leq 3, \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4n\mathbb{Z}, & \text{with } 1 \leq n \leq 2, \\ \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}, & \\ \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}. & \end{cases}$$

Chapter 5

Computing the torsion subgroup over $\mathbb{Q}$

In this last chapter we will see four methods to calculate the torsion subgroup of an elliptic curve E defined over $\mathbb{Q}$, i.e., the group $E(\mathbb{Q})_{tors}$. As we know by Mazur's theorem 4.1.1 there is a finite number of posibilities for this group:

$$E(\mathbb{Q})_{tors} \simeq \begin{cases} \mathbb{Z}/n\mathbb{Z}, & \text{with } 1 \leq n \leq 10 \text{ or } n = 12, \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & \text{with } 1 \leq n \leq 4. \end{cases}$$

First of all, in section 5.1 we establish a first approach in order to find the structure of the torsion subgroup: a bound for the size of $E(\mathbb{Q})_{tors}$.

In section 5.2, based on [73, sc. VIII.7], we use the Lutz-Nagell theorem 5.2.8 which establishes some important properties that torsion points have. Lutz-Nagell algorithm 5.2.10 provides the torsion subgroup $E(\mathbb{Q})_{tors}$ but it is computationally expensive. A similar algorithm to Lutz-Nagell's one is the division polynomial algorithm 5.3.4 shown in section 5.3. It consists on the use of a tool called *division polynomials* (see [8] and [77]) which let us find points with prescribed torsion if exist.

In section 5.4 we show a way of writing elliptic curves defined over $\mathbb{Q}$ using the so-called Tate's normal form 5.4.2 and Tate's parametrizations 5.4.6, which depend on the order of the points that we are looking for. This way, we will be able to determine torsion points and the torsion subgroup. The study is based on a paper written by I. García, M. Olalla and J.M. Tornero [26].

Finally, in section 5.5, we introduce some theory about lattices and double periodic functions defined on $\mathbb{C}$ (particularly about the Weierstrass $\wp$-function) wich will let us study elliptic curves defined over $\mathbb{C}$. There is a very close relation between lattices and elliptic curves defined over $\mathbb{C}$; and this relation let us study torsion points on elliptic curves defined over $\mathbb{Q}$ from an analytic point of wiew. The method used to perform the determination of the torsion subgroup is called Dude's algorithm 5.5.27. The information about the algorithm exposed in this section is based on a paper plublished by Dude [18].

5.1 Bounding the torsion subgroup order

The first step in any algorithm we use should be choosing a reasonable bound for the size of $E(\mathbb{Q})_{tors}$. To manage this, we use a particular case of proposition 3.1.20. Let us recall this result:

Let E/K be an elliptic curve and $m \geq 1$ an integer relatively prime to char(k), where k is the residue field $k = R/\mathcal{M}$, where R is the ring of integers of K and $\mathcal{M}$ a maximal ideal of R.

i) The subgroup $E_1(K)$ has non-trivial points of order m.

ii) If the reduced curve $\tilde{E}/K$ is non-singular, then the reduction map

$$E(K)[m] \to \tilde{E}(k)$$

is injective.

Taking $K = \mathbb{Q}$, which implies $R = \mathbb{Z}$; and taking $p > 2$ a prime number, we consider $\mathcal{M} = (p)$, which implies $k = \mathbb{F}_p$. The latter result tells us that if m does not divide p, then if the reduced curve $\tilde{E}/\mathbb{Q}$ is non-singular, i.e., p does not divide Δ, the reduction map

$$\pi_p : E(\mathbb{Q})[m] \to \tilde{E}(\mathbb{F}_p)$$

is injective.

So, given an elliptic curve $E/\mathbb{Q}$ if we choose some prime p not dividing Δ and computing how many points lie in $\tilde{E}(\mathbb{F}_p)$, we must obtain a multiple of the order of $E(\mathbb{Q})_{tors}$, since π_p is an injective homomorphism of finite groups for every m. The practical choice in Tate's algorithm is taking five primes, as small as possible, which we call **good primes** from now on; computing the number of points in $\tilde{E}(\mathbb{F}_p)$ in each case; and finding the greatest common divisor of all those quantities. In most cases, this bound is find to be the actual order of $E(\mathbb{Q})_{tors}$.

Example 5.1.1 Let $E/\mathbb{Q}$ be the elliptic curve

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

The discriminant of E is $\Delta = -2^4 \cdot 3^5$, so $\tilde{E}$ is nonsingular modulo p for every prime $p \geq 5$. One can easily check that

$$E(\mathbb{F}_5) = \{\mathcal{O}, (3,0), (1,2), (1,3), (2,1), (2,4)\},$$
$$E(\mathbb{F}_7) = \{\mathcal{O}, (1,2), (1,5), (2,2), (2,5), (3,3), (3,4), (4,2), (4,5), (5,3), (5,4), (6,3), (6,4)\},$$

hence $\#E(\mathbb{F}_5) = 6$ and $\#E(\mathbb{F}_7) = 13$. If we call $d = gcd(6, 13) = 1$, then $\#E_{tors}(\mathbb{Q})|1$, i.e., $E(\mathbb{Q})$ has no nontrivial torsion, $E(\mathbb{Q})_{tors} = \{\mathcal{O}\}$.

Example 5.1.2 Let $E/\mathbb{Q}$ be the elliptic curve

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

The discriminant of E is $\Delta = -64 = -2^6$. First, we calculate the 2-torsion points of the curve E. Suppose that $P = (x_0, y_0)$ is a torsion point of order 2. Then $P = -P$. Using the group law algorithm, proposition 2.2.3, $-P = (x_0, -y_0 - a_1x_0 - a_3)$. In our particular case, we have $a_1 = a_3 = 0$, and then

$$P = -P \;\Rightarrow\; y_0 = -y_0 \;\Rightarrow\; y_0 = 0.$$

Using the equation of E we get $x_0 = 0$. So, $(0, 0) \in E(\mathbb{Q})$ is the only one point of order 2.

We compute now

$$\begin{aligned}
\tilde{E}(\mathbb{F}_3) &= \{\mathcal{O}, (0,0), (2,1), (2,2)\},\\
\tilde{E}(\mathbb{F}_5) &= \{\mathcal{O}, (0,0), (2,0), (3,0)\},\\
\tilde{E}(\mathbb{F}_7) &= \{\mathcal{O}, (0,0), (1,3), (1,4), (3,3), (3,4), (5,2), (5,5)\}.
\end{aligned}$$

We see that $\#E(\mathbb{F}_3) = 4$, $\#E(\mathbb{F}_5) = 4$ and $\#E(\mathbb{F}_7) = 8$, so $d = gdc(4, 4, 8) = 4$. We only can assure that $\#E(\mathbb{Q})_{tors}|4$, so we have three posibilities for the order of the group: 1, 2 or 4. However, we gain additional information by looking at the group structure modulo 3 and 5:

$$\tilde{E}(\mathbb{F}_3) \simeq \mathbb{Z}/4\mathbb{Z}, \qquad \tilde{E}(\mathbb{F}_5) \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}.$$

Since $E(\mathbb{Q})_{tors}$ injects into $\tilde{E}(\mathbb{F}_3)$, it must be a cyclic group, because a subgroup of a cyclic group is also cyclic. Moreover, $E(\mathbb{Q})_{tors}$ injects into $\tilde{E}(\mathbb{F}_5)$, so $E(\mathbb{Q})_{tors}$ can have at most order 2, since $\tilde{E}(\mathbb{F}_5)$ has no cyclic subgroups of order grater than 2. Then, we see that $(0, 0)$ is the only nonzero torsion point in $E(\mathbb{Q})$, so

$$E(\mathbb{Q})_{tors} = \{\mathcal{O}, (0,0)\} \simeq \mathbb{Z}/2\mathbb{Z}.$$

The latter example tells us that we should be a bit more accurate by choosing the bound. So we compute not only the order of $\tilde{E}(\mathbb{F}_p)$, but also how many elements of order 2 it has. This way, if $\tilde{E}(\mathbb{F}_p)$ presents more points of order 2 than $E(\mathbb{Q})$ itself, our choosing for the bound can be smaller than the order of $\tilde{E}(\mathbb{F}_p)$. In the latter example above, the bound would be 2, which actually is the order of $E(\mathbb{Q})_{tors}$.

So if $\#\tilde{E}(\mathbb{F}_p) = M$, the number of points of order 2 in $E(\mathbb{Q})$ is s and the number of points of order 2 in $\tilde{E}(\mathbb{F}_p)$ is t, the choosing of the bound goes like this:

i) If $s = t$, we choose M.

ii) If $(s, t) \in \{(0, 1), (1, 3)\}$, we choose $M/2$.

iii) If $(s, t) = (0, 3)$, we choose $M/4$.

5.2 Lutz-Nagell Algorithm

We start now a study about torsion points of $E(\mathbb{Q})$. The idea is trying to establish a criteria about some conditions which torsion points must have.

Recall from example 1.4.9 that if we have $x \in \mathbb{Q}$ and $p \in \mathbb{N}$ a prime number, we can write $x = p^n(a/b)$ with $(a, b) = 1$. Then we defined the p-adic valuation as

$$v_p(x) = n,$$

with $v_p(0) = +\infty$.

Let E be an elliptic curve over $\mathbb{Q}$. It is known from section 3.1.3 that if E is given in the Weierstrass form

$$y^3 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

we can choose the a_i in $\mathbb{Z}$. Further, we recall from equation (2.2) in section 2.1 that, as $\text{char}(\mathbb{Q}) = 0$, this equation can be reduced to a simpler equation of the form

$$y^2 = x^3 + Ax + B, \tag{5.1}$$

with $A, B \in \mathbb{Z}$ by definition of A and B.

Proposition 5.2.1 *Let $E/\mathbb{Q}$ be an elliptic curve given by $y^2 = x^3+Ax+B$ with $A, B \in \mathbb{Z}$, and let $(x, y) \in E(\mathbb{Q})$. Let $p \in \mathbb{N}$ be a prime number. Then*

$$v_p(x) < 0 \quad \Longleftrightarrow \quad v_p(y) < 0.$$

In this case there exists an integer $r \geq 1$ such that

$$v_p(x) = -2r \quad \textit{and} \quad v_p(y) = -3r.$$

PROOF. It is easy to see that p divides the denominator of x if, and only if, p divides the denominator of y.

($\Rightarrow$) Assume $x = \dfrac{a}{pb}$, with $p \nmid a$, and $y = \dfrac{c}{d}$. As $(x, y) \in E(\mathbb{Q})$,

$$\begin{aligned} y^2 = x^3 + Ax + B \;&\Rightarrow\; \frac{c^2}{d^2} = \frac{a^3}{p^3b^3} + A \cdot \frac{a}{pb} + B \\ &\Rightarrow\; p^3b^3c^2 = d^2(a^3 + Ap^2ab^2 + Bp^3b^3). \end{aligned}$$

Suppose that $p \nmid d$. Then $p|(a^3 + Ap^2ab^2 + Bp^3b^3)$ but this happens if $p|a^3$ and this is not possible since $p \nmid a$ by assumption. So, $p|d$.

($\Leftarrow$) Assume now that $x = \dfrac{a}{b}$ and $y = \dfrac{c}{pd}$, with $p \nmid c$. Thus,

$$\begin{aligned} y^2 = x^3 + Ax + B \;&\Rightarrow\; \frac{c^2}{p^2d^2} = \frac{a^3}{b^3} + A \cdot \frac{a}{b} + B \\ &\Rightarrow\; b^3c^2 = p^2d^2(a^3 + Aab^2 + Bb^3). \end{aligned}$$

If $p \nmid b$, we would have that $p|c$, but this is not possible by assumption again.

Let us now prove the second statement. Assume that $v_p(y) = -j$, i.e, p^j with $j > 0$ is the exact power of p dividing the denominator of y, then p^{2j} is the exact power of p dividing the denominator of y^2.

Similarly, assuming that $v_p(x) = -k$, if p^k with $k > 0$ is the exact power of p dividing the denominator of x, then the denominator of $x^3 + Ax + B$ is exactly divisible by p^{3k}. As $v_p(y^2) = v_p(x^3 + Ax + B)$, we have $3k = 2j$. It follows that there exists $r \in \mathbb{Z}$ with $j = 3r$ and $k = 2r$.

□

If we call

$$t = \frac{x}{y}, \quad s = \frac{1}{y},$$

dividing equation 5.1 by y^3 yields

$$\frac{1}{y} = \left(\frac{x}{y}\right)^3 + A\left(\frac{x}{y}\right)\left(\frac{1}{y}\right)^2 + B\left(\frac{1}{y}\right)^3,$$

which can be written as

$$s = t^3 + Ats^2 + Bs^3. \tag{5.2}$$

Moreover, if we have $P \in E(\mathbb{Q})$, we can choose (projective) coordinates for P, say x, y and z, with $x, y, z \in \mathbb{Z}$ such that $\gcd(x, y, z) = 1$.

With all this, we assume that every coefficient of the equations for E and every coordinate for a point $P \in E$ are integer numbers.

Definition 5.2.2 (E_r) Let $E/\mathbb{Q}$ be an elliptic curve given by $y^2 = x^3 + Ax + B$. Let $r \geq 1$ be an integer and let v_p be the p-adic valuation for some prime p. We define the set

$$E_r := \{(x, y) \in E(\mathbb{Q}) : \ v_p(x) \leq -2r \text{ and } v_p(y) \leq -3r\} \cup \{\mathcal{O}\}.$$

In other words, the set defined before is the set of points on E such that x has at least p^{2r} in its denominator and y has at least p^{3r} in its one. These should be thought as the points that are close to $\mathcal{O}$ modulo powers of p, i.e., p-adically close to $\mathcal{O}$.

We need to prove some results and set some notation to be used in the proof of the following proposition below.

Notation. If $z \in \mathbb{Q}$ is a rational number and $p \in \mathbb{N}$ is a prime such that p^j divides the numerator of z for some j, we write

$$p^j | z \quad \text{or} \quad z \equiv 0 \bmod(p^j).$$

Lemma 5.2.3 *Let $E/\mathbb{Q}$ be an elliptic curve given by the equation*

$$s = t^3 + Ats^2 + Bs^3,$$

as in equation (5.2)*. Then*

$$(x, y) \in E_r \quad \Longleftrightarrow \quad p^{3r}|s.$$

Further if $p^{3r}|s$, then $p^r|t$.

PROOF. ($\Rightarrow$) Let $(x, y) \in E_r$. As $v_p(y) \leq -3r$, p^{3r} divides the denominator of y, so p^{3r} divides the numerator of $s = 1/y$.

($\Leftarrow$) Suppose that $p^{3r}|s$. Then p^{3r} divides the denominator of y. Proposition 5.2.1 shows that p^{2r} divides the denominator of x. Therefore $(x, y) \in E_r$.

Suppose now that $p^{3r}|s$. Then the exact power of p dividing the denominator of y is p^{3k}, with $k \geq r$. Proposition 5.2.1 implies that the exact power of p dividing $t = x/y$ is p^k. Since $k \geq r$, we have $p^r|t$.

□

Lemma 5.2.4 *Let $E/\mathbb{Q}$ be an elliptic curve given by $s = t^3 + As^2t + Bs^3$, and let $p \in \mathbb{N}$ be a prime number. A line $L : t = c$, where $c \in \mathbb{Q}$ is a constant with $c \equiv 0$ mod(p), intersects the curve E in at most one point (s, t) with $s \equiv 0$ mod(p). The line is not tangent at such point of intersection.*

PROOF. Suppose we have two values of s, call them s_1 and s_2 with

$$s_1 \equiv s_2 \equiv 0 \bmod(p). \tag{5.3}$$

We are about to show that $s_1 - s_2 \equiv 0 \bmod(p^k)$ for all $k \geq 1$ by induction. The base case $k = 1$ is our assumption.

Suppose now that $s_1 \equiv s_2 \bmod(p^k)$ for some $k \geq 1$. As we supposed in equality (5.3), we can write $s_1 = ps_1'$ and $s_2 = ps_2'$ and then

$$s_1 - s_2 \equiv 0 \bmod(p^k) \;\Rightarrow\; p(s_1' - s_2') \equiv 0 \bmod(p^k) \;\Rightarrow\; s_1' \equiv s_2' \bmod(p^{k-1}).$$

so

$$\begin{aligned} s_1' \equiv s_2' \bmod(p^{k-1}) &\Rightarrow s_1' - s_2' \equiv 0 \bmod(p^{k-1}) \\ &\Rightarrow (s_1' + s_2')(s_1' - s_2') \equiv 0 \bmod(p^{k-1}) \\ &\Rightarrow (s_1')^2 - (s_2')^2 \equiv 0 \bmod(p^{k-1}) \\ &\Rightarrow p^2((s_1')^2 - (s_2')^2) \equiv 0 \bmod(p^{k+1}) \\ &\Rightarrow p^2(s_1')^2 \equiv p^2(s_2')^2 \bmod(p^{k+1}) \\ &\Rightarrow s_1^2 \equiv s_2^2 \bmod(p^{k+1}). \end{aligned}$$

Similary we can see that $s_1^3 \equiv s_2^3 \bmod(p^{k+2})$. Therefore,

$$s_1 = c^3 + Acs_1^2 + Bs_1^3 \equiv c^3 + Acs_2^2 + Bs_2^3 \equiv s_2 \bmod(p^{k+1}).$$

Then, we have $s_1 \equiv s_2 \bmod(p^k)$ for all $k \in \mathbb{Z}^+$. It follows that $s_1 = s_2$, so there is at most one point of intersection between the line $L : t = c$ and E with $s \equiv 0 \bmod(p)$.

The slope of the tangent line to the curve can be found by implicit differentiation

$$1 = 3t^2\frac{dt}{ds} + 2Ast + As\frac{dt}{ds} + 3Bs^2,$$

so,

$$\frac{dt}{ds} = \frac{1 - 2Ast - 3Bs^2}{3t^2 + As^2}.$$

If the line $L : t = c$ is tangent to the curve at (s, t), then $1 - 2Ast - 3Bs^2 = 0$. But $s \equiv t \equiv 0 \bmod(p)$ implies that

$$1 - 2Ast - 3Bs^2 \equiv 1 \not\equiv 0 \bmod(p).$$

Therefore, $L : t = c$ is not tangent to the curve.

□

Proposition 5.2.5 *Let $E/\mathbb{Q}$ be an elliptic curve given by $y^2 = x^3 + Ax + B$. Let $p, r \in \mathbb{Z}^+$ be two integers with p prime. We consider*

$$E_r = \{(x, y) \in E(\mathbb{Q}) : \ v_p(x) \leq -2r \text{ and } v_p(y) \leq -3r\} \cup \{\mathcal{O}\}.$$

Then

i) E_r is a subgroup of $E(\mathbb{Q})$.

ii) The map

$$\begin{aligned} \psi_r : E_r/E_{5r} &\to \mathbb{Z}_{p^{4r}} \\ (x, y) &\mapsto p^{-r}\frac{x}{y} \ mod(p^{4r}) \\ \mathcal{O} &\mapsto 0 \end{aligned}$$

is an injective homomorphism.

iii) If $(x, y) \in E_r$ but $(x, y) \notin E_{r+1}$, then $\psi_r(x, y) \not\equiv 0 \ mod(p)$.

Remark 5.2.6. The map ψ_r should be regarded as a logarithm for the group E_r/E_{5r} since it changes the law composition in the group to addition in $\mathbb{Z}_{p^{4r}}$, just as the classical logarithm changes the composition law in the multiplicative group of possitive real numbers to addition in $\mathbb{R}$.

PROOF.

(iii) To prove this, we have to show first that ψ_r is well-defined. If we have $(x, y) \in E_r$, Proposition 5.2.1 tells us that there exists $m \in \mathbb{Z}$, $m \geq r$ such that $v_p(x) = -2m$ and $v_p(y) = -3m$ or, in other words, $v(x/y) = m$. So we can assure that $v_p(p^{-m}x/y) = 0$.

Note now that by definition we have that $E_{r+1} \subsetneq E_r$. In fact

$$\begin{aligned} E_r/E_{r+1} &= \{(x, y) \in E_r : \ v_p(x) = -2r \text{ and } v_p(y) = -3r\} \\ &= \{(x, y) \in E(\mathbb{Q}) : \ v_p(x/y) = r\}. \end{aligned}$$

Let $(x, y) \in E_r/E_{r+1}$. Then $v_p\left(p^{-r}\dfrac{x}{y}\right) = 0$, so $\psi_r(x, y)$ is not a multiple of p, neither a multiple of p^{4r}.

(i) and (ii) If $\psi_r(x, y) \equiv 0 \bmod(p^{4r})$, then $v_p(x/y) \geq 5r$, so $(x, y) \in E_{5r}$. This proves that ψ_r is injective as soon as we prove that it is a homomorphism.

As E is given in a short Weierstrass form, if $P = (x, y) \in E$, then its opposite is given by $-P = (x, -y)$, so

$$\psi_r(-P) = \psi_r(x, -y) \equiv -p^{-r}x/y \bmod(p^{4r}) = -\psi_r(P).$$

We now claim that if $P_1 + P_2 + P_3 = \mathcal{O}$ then

$$\psi_r(P_1) + \psi_r(P_2) + \psi_r(P_3) \equiv 0 \bmod(p^{4r}).$$

Therefore

$$\psi_r(P_1 + P_2) = \psi_r(-P_3) = -\psi_r(P_3) = \psi_r(P_1) + \psi_r(P_2).$$

The proof of this claim also shows that if $P_1, P_2 \in E_r$ then $P_3 \in E_r$, hence E_r is a group.

We know that three points add to $\mathcal{O}$ if and only if thay are collinear. To prove the claim, let P_1, P_2 and P_3 lie on the line

$$ax + by + c = 0$$

and assume that $P_1, P_2 \in E_r$.

Let us show that we can use the variables s, t instead of x, y. Let $P_i' = (s_i, t_i)$ be the points $P_i = (x_i, y_i)$ written in terms of the s, t coordinates, where $s_i = 1/y_i$ and $t = x_i/y_i$. The points P_i', for $i = 1, 2, 3$, lies on the line

$$at + b + cs = 0.$$

Since $P_1, P_2 \in E_r$, lemma 5.2.3 implies that

$$p^{3r} | s_i, \quad p^r | t_i \ \text{ for } i = 1, 2.$$

As we know, the order of intersection of the line $ax + by + c = 0$ and the curve $y^2 = x^3+Ax+B$ can be calculated by using projective coordinates $x = X/Z, y = Y/Z$.

If we start with the line $at + b + cs = 0$ and the curve $s = t^3 + Ats^2 + Bs^3$ we can homogenize using $t = T/U, s = S/U$. If we let $Z = S$, $Y = U$ and $X = T$, we find that we are working with the same line and curve as above, where the point (x, y) corresponds to

$$t = T/U = X/Y = x/y \qquad \text{and} \qquad s = S/U = Z/Y = 1/y.$$

Since orders of intersection can be calculated using projective models, it follows that the order of intersection of the line and the curve in x, y coordinates is the same as the order of intersection in s, t coordinates. Particularly, the line and the curve are tangent in x, y coordinates if and only if it is tangent in s, t coordinates. This allows us to do the elliptic curve group calculations using the latter coordinates.

If $c = 0$, our line is of the form

$$at + b = 0 \ \Rightarrow t = \frac{-b}{a} = d,$$

so the line is of the form in the lemma 5.2.4, which tells us that this line intersects the curve in at most one point. But it passes through the points P_1' and P_2', so $P_1' = P_2'$ and the line is tangent to the curve. Changing back to x, y coordinates, we obtain $P_1 = P_2$. The definition of the group law says that since points P_1 and P_2 are equal, the line $ax + by + c = 0$ is tangent at (x, y). As pointed out above, this means that $at + b + cs = 0$ is tangent to the curve, but the Lemma 5.2.4 assures that this cannot happen, so $c \neq 0$.

Dividing the equation $at + b + cs = 0$ by c, we obtain

$$s = \alpha t + \beta$$

for some $\alpha, \beta \in \mathbb{Q}$. Then P_i' lies on the line $s = \alpha t + \beta$ for $i = 1, 2, 3$.

We claim that

$$\alpha = \frac{t_2^2 + t_1 t_2 + t_1^2 + As_2^2}{1 - A(s_1 + s_1)t_1 - B(s_2^2 + s_1 s_2 + s_2^2)} \tag{5.4}$$

This claim is easy to prove:

If $t_1 \neq t_2$, then $\alpha = (t_2 - t_1)/(s_2 - s_1)$. Since $s_i = t_i^3 + As_i^2 t_i + Bs_i^3$, we have

$$\begin{aligned}
&(s_2 - s_1)(1 - A(s_1 + s_1)t_1 - B(s_2^2 + s_1 s_2 + s_2^2)) \\
&\quad = (s_2 - s_1) - A(s_2^2 - s_1^2)t_1 + B(s_2^3 - s_1^3) \\
&\quad = (s_2 - As_2^2 t_2 - Bs_2^2) - (s_1 - As_1^2 t_1 - Bs_1^3) + As_2^2(t_2 - t_1) \\
&\quad = t_2^3 - t_1^3 + As_2^2(t_2 - t_1) \\
&\quad = (t_1 - t_2)(t_2^2 + t_1 t_2 + t_1^2 + As_2^2).
\end{aligned}$$

Now suppose that $t_1 = t_2$. As a line $t = c$ with $c \equiv 0 \bmod(p)$ intersects the curve $s = t^3 + As^2t + Bs^3$ only in one point with $s \equiv 0 \bmod(p)$, by lemma 5.2.4, the points (t_1, s_1) and (t_2, s_2) must be equal. The line $s = \alpha t + \beta$ is therefore the tangent line at this point, and the slope can be calculated by implicit differentiation of $s = t^3 + As^2t + Bs^3$.

$$1 = 3t^2\frac{dt}{ds} + 2Ast + As\frac{dt}{ds} + 3Bs^2,$$

Solving for dt/ds yields the expression (5.4) when $t_1 = t_2 = t$ and $s_1 = s_2 = s$.

As $(x_i, y_i) \in E_r$, by lemma 5.2.3, $p^{3r}|s_i$ and $p^r|t_i$, so $s_1 \equiv s_2 \equiv 0 \bmod(p)$, and then the denominator of α is

$$1 - A(s_1 + s_1)t_1 - B(s_2^2 + s_1s_2 + s_2^2) \equiv 1 \bmod(p);$$

and

$$t_2^2 + t_1t_2 + t_1^2 + As_2^2 \equiv 0 \bmod(p^{2r}).$$

Therefore $\alpha \equiv 0 \bmod(p^{2r})$. Since $p^{3r}|s_i$, we have

$$\beta = s_i - \alpha t_i \equiv 0 \bmod(p^{3r}).$$

The point P_3' is the third point of intersection of the line $s = \alpha t + \beta$ with $s = t^3 + As^2t + Bs^3$. Therefore, we need to solve for t:

$$\alpha t + \beta = t^3 + A(\alpha t + \beta)^2 t + B(\alpha t + \beta)^3.$$

This can be arranged to obtain

$$0 = t^3 + \frac{2A\alpha\beta + 3B\alpha^2\beta}{1 + B\alpha^3 + A\alpha^2}t^2 + \cdots.$$

But the sum of the three roots is the negative of the coefficient of t^2, so

$$t_1 + t_2 + t_3 = \frac{2A\alpha\beta + 3B\alpha^2\beta}{1 + B\alpha^3 + A\alpha^2} \equiv 0 \bmod(p^{5r}).$$

The last congruence holds because $p^{2r}|\alpha$ and $p^{3r}|\beta$. Since $t_1 \equiv t_2 \equiv 0 \bmod(p^r)$, we have that $t_3 \equiv 0 \bmod(p^{4r})$. Therefore, $s_3 = \alpha t_3 + \beta \equiv 0 \bmod(p^{3r})$. By lemma 5.2.3 $P_3 \in E_r$, which shows that E_r is a subgroup of $E(\mathbb{Q})$ and proves (i).

Moreover,

$$\psi_r(P_1) + \psi_r(P_2) + \psi_r(P_3) \equiv p^{-r}(t_1 + t_2 + t_3) \equiv 0 \bmod(p^{4r}),$$

so ψ_r is a homomorphism and this proves (ii).

□

Corollary 5.2.7 *Let $E/\mathbb{Q}$ be an elliptic curve given by $y^2 = x^3 + Ax + B$. Let $p, r \in \mathbb{Z}^+$ be two integers with p prime and let $m \in \mathbb{Z}^+$, $m > 1$ and m is not a power of p. Then E_1 contains no points of exact order m.*

PROOF. Suppose $P \in E_1$ has order m. Since m is not a power of p, we can multiply P by the largest power of p dividing m to obtain a point, not equal to $\mathcal{O}$, of order prime to p. Therefore, we may assume that P has order m with $p \nmid m$. Let r be the largest integer such that $P \in E_r$. Then

$$m\psi_r(P) = \psi_r(mP) = \psi_r(\mathcal{O}) \equiv 0 \bmod(p^{4r}).$$

Since $p \nmid m$, we have $\psi_r(P) \equiv 0 \bmod(p^{4r})$, so $P \in E_{5r}$. Since $5r > r$, this contadicts the choice of r.

□

The following theorem was proved independently by Lutz [47] and Nagell [57] in the 1930s. Quite often it allows a quick determination of the torsion points on an elliptic curve over $\mathbb{Q}$.

Theorem 5.2.8 (Lutz-Nagell) *Let E an elliptic curve given by $y^2 = x^3 + Ax + B$ with $A, B \in \mathbb{Z}$. Let $P = (x, y) \in E(\mathbb{Q})$. Suppose P has finite order. Then*

i) $x, y \in \mathbb{Z}$.

ii) $y^2 | \Delta$, where $\Delta = 4A^3 + 27B^2$.

PROOF.

i) Suppose x or y is not in $\mathbb{Z}$. Then there is some prime dividing the denominator of one of them. By proposition 5.2.1, $P \in E_r \subseteq E_1$ for some $r \geq 1$. Let q be a prime dividing the order m of P. Then $Q = (m/q)P \in E_r \subseteq E_1$ has order q. But by corollary 5.2.7, E_1 has no points of exact order q if q is not a power of p. As q is prime, therefore $q = p$, i.e, Q is a point of order the prime p.

Choose k such that $Q \in E_k$ but $Q \notin E_{k+1}$. Then, by proposition 5.2.5.iii, $\psi_k(Q) \not\equiv 0 \bmod(p)$, and

$$p\psi_k(Q) = \psi_k(pQ) = \psi_k(\mathcal{O}) \equiv 0 \bmod(p^{4r}).$$

Therefore,

$$\psi_k(Q) \equiv 0 \bmod(p^{4r-1}),$$

which contradicts th fact that $\psi_k(Q) \not\equiv 0 \bmod(p)$.

ii) Assume that $y \neq 0$. Then $2P = (x_2, y_2) \neq \mathcal{O}$. Since $2P$ has finite order, $x_2, y_2 \in \mathbb{Z}$. By the group law,

$$x_2 = \frac{x^4 - 2Ax^2 - 8Bx + A^2}{4y^2}.$$

Since $x_2 \in \mathbb{Z}$, this implies that

$$y^2 | (x^4 - 2Ax^2 - 8Bx + A^2).$$

A straightforward calculation shows that

$$(3x^2 + 4A)(x^4 - 2Ax^2 - 8Bx + A^2) - (3x^3 - 5Ax - 27B)(x^3 + Ax + B) = 4A^3 + 27B^2.$$

Since $y^2 = x^3 + Ax + B$, we see that y^2 divides both terms on the left, so

$$y^2 | (4A^3 + 27B^2).$$

□

Corollary 5.2.9 *Let $E/\mathbb{Q}$ be en elliptic curve. Then the torsion subgroup of $E(\mathbb{Q})$ is finite.*

Lutz-Nagell Algorithm

Algorithm 5.2.10 (Lutz-Nagell algorithm) *Let E be an elliptic curve defined over $\mathbb{Q}$ with equation $y^2 = x^3 + Ax + B$, for any $A, B \in \mathbb{Z}$. Using theorem 5.2.8 we can write an algorithm to find torsion subgroup.*

[Step 1] *(For $y = 0$)*
Solve $x^3 + Ax + B = 0$ to obtain x_1, x_2, x_3.
For $i = 1$ to 3:

If $x_i \in \mathbb{Z}$ then $(x_i, 0)$ is a possible torsion point.

[Step 2] $\Delta = 4A^3 + 27B^2$.
Factorize(Δ).

[Step 3] *(For $y \neq 0$)*
Obtain the possibilities for $y \in \mathbb{Z}$ such that $y^2 | \Delta$.
For each possibility, y_i, find the solutions for $y_i^2 = x^3 + Ax + B$, let them be x_{i1}, x_{i2}, x_{i3}.
For each i,

For $j = 1$ to 3:

If $x_{ij} \in \mathbb{Z}$ then (x_{ij}, y_i) is a possible torsion point.

[Step 4] $\mathcal{T} = \emptyset$ *(Inicialize the set of torsion points).*

For every possible torsion point P*,*

If $P = \mathcal{O}$ *then:*

$\mathcal{T} \leftarrow P$.

m=1;

$(x_Q, y_Q) = Q = mP$*;*

While $x_Q, y_Q \in \mathbb{Z}$*:*

$m = m+1$*;*

$(x_Q, y_Q) = Q = mP$

If $Q = \mathcal{O}$ *then:*

$\mathcal{T} \leftarrow P$.

[Step 5] *Now we use Mazur's Theorem (theorem 4.1.1)to find the group structure.*

$n = \#\mathcal{T}$.

If $n = 1, 2, 3, 5, 6, 7, 9, 10$ *then* $E(\mathbb{Q})_{tors} = \mathbb{Z}/n\mathbb{Z}$.

If $n = 16$*, then* $E(\mathbb{Q})_{tors} = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$.

Else

If any element has order n,

$E(\mathbb{Q})_{tors} = \mathbb{Z}/n\mathbb{Z}$*;*

Else,

$E(\mathbb{Q})_{tors} = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}$.

Why does the step 4 of the algorithm give us a finite loop?

The Lutz-Nagell theorem gives a finite list of possibilities for torsion points. If P is a torsion point then, for every n, the point nP must either be $\mathcal{O}$ or be on that list. Since there are only finitely many points on the list, either we will have $nP = mP$ for some $m \neq n$, in which case P is torsion and $(m-n)P = \mathcal{O}$; or some nP is not on the list and P is not torsion.

Another critial point in the algorithm is step 2. If Δ is too large, it is difficult to fatorize. So to have a good algorithm to find torsion points we need a good algorithm to factorize numbers as well.

Some examples

Example 5.2.11 Let E be an elliptic curve given by $y^2 = x^3 + 4$. Then $\Delta = 432$. Let $P = (x, y)$ be a point of finite order in $E(\mathbb{Q})$. Since $0 = x^3 + 4$ has no rational solutions, we have $y \neq 0$. Therefore, $y^2|432 = 2^4 \cdot 3^3$, i.e., $y|12$. The posibilities are

$$y = \pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12.$$

We have to check which values of y give an integer value for x. Doing this, we have that only $y = \pm 2$ fits this. So the *possible* torsion points are $(0, 2)$ and $(0, -2)$. If we do the calculations, we have $3(0, \pm 2) = \mathcal{O}$, so

$$E(\mathbb{Q})_{tors} = \{\mathcal{O}, (0, 2), (0, -2)\} \simeq \mathbb{Z}/3\mathbb{Z}.$$

Example 5.2.12 Let E be given by $y^2 = x^3 + 8$. If $y = 0$, then $x = -2$ gives us a possible torsion point $(-2, 0)$.

Now, $\Delta = 4A^3 + 27B^2 = 1728 = 2^6 \cdot 3^3$.

If $y \neq 0$, then $y^2|1728$, wich means that $y|24$, i.e.,

$$y = \pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 8, \pm 12, \pm 24.$$

Trying the posibilities, we find that $(1, \pm 3)$ and $(2, \pm 4)$ are four possible torsion points.

We can see that

$$2(-2, 0) = \mathcal{O},$$

so $(-2, 0)$ is torsion. More over

$$2(1, 3) = (-7/4, -13/8) \text{ and } 2(2, 4) = (-7/4, 13/8).$$

Since these points do not have integer coordinates, they cannot have finite order. It follows that

$$E_{tors} = \{\mathcal{O}, (-2, 0)\} \simeq \mathbb{Z}/2\mathbb{Z}.$$

5.3 Division polynomials algorithm

Division polynomials are a tool for searching torsion points on elliptic curves. As we are only interested in the case in which the elliptic curve E is defined over $\mathbb{Q}$, we define here division polynomials within this restriction, but they can be defined for a general field K, see ([5], chap. III, sc. 4).

Definition 5.3.1 (Division polynomials) Let E be an elliptic curve defined over $\mathbb{Q}$ given in the Weierstrass short normal form

$$E : y^2 = x^3 + Ax + B, \quad \text{with } A, B \in \mathbb{Z}.$$

We define the **division polynomials** Ψ_m recursively as follows:

$$\begin{aligned}
\Psi_1 &= 1,\\
\Psi_2 &= 2y,\\
\Psi_3 &= 3x^4 + 6Ax^2 + 12Bx - A^2,\\
\Psi_4 &= 2\Psi_2(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - A^3 - 8B^2),\\
\Psi_{2k+1} &= \Psi_{k+2}\Psi_k - \Psi_{k-1}\Psi_{k+1}^3, && k \geq 2;\\
\Psi_{2k} &= \Psi_k(\Psi_{k+2}\Psi_{k-1}^2 - \Psi_{k-2}\Psi_{k+1}^2)/\Psi_2, && k \geq 3.
\end{aligned}$$

It is easy to see that Ψ_{2k} are polynomials indeed, proving recursively that the numerator in the expression for Ψ_{2k} is divisible by Ψ_2.

We also define polynomials ϕ_m and ω_m for $m \geq 2$ as follows:

$$\begin{aligned}
\phi_m &= x\Psi_m^2 - \Psi_{m-1}\Psi_{m+1},\\
\omega_m &= (\Psi_{m+2}\Psi_{m-1}^2 - \Psi_{m-2}\Psi_{m+1}^2)/2\Psi_2.
\end{aligned}$$

The most useful properties of division polynomials are summarized in the following theorem

Theorem 5.3.2 *Let $m \in \mathbb{Z}^+$. Then*

i) Polynomials Ψ_m, ϕ_m and $y^{-1}\omega_m$ if m is odd; and $(2y)^{-1}\Psi_m$, ϕ_m and ω_m if m is even, are polynomials in $\mathbb{Z}[x, y^2]$. Substituting $y^2 = x^3 + Ax + B$, we may consider them as polynomials in $\mathbb{Z}[x]$.

ii) Considering $\Psi_m, \phi_m \in \mathbb{Z}[x]$, we have

$$\begin{aligned}
\phi_m(x) &= x^{m^2} + \text{ lower degree terms},\\
\Psi_m^2(x) &= m^2x^{m^2-1} + \text{ lower degree terms}.
\end{aligned}$$

iii) If $P \in E(\mathbb{Q})$, then

$$mP = \left(\frac{\phi_m(P)}{\Psi_m^2(P)}, \frac{\omega_m(P)}{\Psi_m^3(P)}\right).$$

We omit here the proof of this theorem, but we give the ideas for doing it. Assertions (i) and (ii) are easy to prove by induction, but involve rather long calculations. It is possible to prove assertion (iii) in an elementary way; however, it envolves extensive computer calculations. Other proofs, using more advanced methods, can be found in [21] and [44].

It turns out that the characterization of m-torsion points can be achieved if we define polynomials f_m as follows. Let $m \in \mathbb{Z}^+$, $m > 2$, the polynomials f_m are defined as:

$$f_m = \begin{cases} \Psi_m, & \text{if } m \text{ is odd;}\\ \Psi_m/\Psi_2, & \text{if } m \text{ is even.}\end{cases}$$

Note that, like polynomials ϕ_m and ω_m, we also have $f_m \in \mathbb{Z}[x]$. Moreover, by contruction,

$$f_m = \begin{cases} mx^{(m^2-1)/2} + \text{lower degree terms}, & \text{if } m \text{ is odd;} \\ \\ \dfrac{1}{m}x^{(m^2-4)/2} + \text{lower degree terms}, & \text{if } m \text{ is even.} \end{cases}$$

The following statement gives a way of looking for m-torsion points:

Theorem 5.3.3 *Let E be an elliptic curve defined over $\mathbb{Q}$, let $m \in \mathbb{Z}^+$ and let $P \in E(\mathbb{Q})$ such that P is not a 2-torsion point. Then*

$$P \in E(\mathbb{Q})[m] \iff f_m(x(P)) = 0.$$

We could derive a "brute force" method for serching torsion points of order m, since we know that all possible torsion subgroups of $E(\mathbb{Q})$ from Mazur's theorem 4.1.1:

Algorithm 5.3.4 (Division polynomials algorithm) *Let*

$$E : y^2 = x^3 + Ax + B, \quad \text{with } A, B \in \mathbb{Z}$$

be an elliptic curve defined over $\mathbb{Q}$ given in Weierstrass short normal form. In order to find its torsion subgroup we proceed as follows:

[Step 1] *(Inicialize the set of torsion points)* $\mathcal{T} = \emptyset$.

[Step 2] *(Look for possible 2-torsion points)*

Solve $x^3 + Ax + B = 0$ *to obtain* x_1, x_2, x_3.
For $i = 1$ *to* 3*:*

If $x_i \in \mathbb{Z}$*:*

$P = (x_i, 0)$*;*

If $2P = \mathcal{O}$ *then* $\mathcal{T} \leftarrow P$*;*

[Step 2] *For* $m = 3, \ldots, 10, 12$*:*

Look for integer solutions of $f_m(x) = 0$.

For every integer solution x*:*

If $\sqrt{x^2 + Ax + B} \in \mathbb{Z}$*:*

$P = (x, \sqrt{x^2 + Ax + B})$*;*

$Q = (x, -\sqrt{x^2 + Ax + B})$*;*

$\mathcal{T} \leftarrow P, Q$*;*

[Step 4] *(Use Mazur's Theorem to find the group structure).*

$n = \#\mathcal{T}$.

If $n = 1, 2, 3, 5, 6, 7, 9, 10$ *then* $E(\mathbb{Q})_{tors} = \mathbb{Z}/n\mathbb{Z}$.

If $n = 16$, *then* $E(\mathbb{Q})_{tors} = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$.

Else

If any element has order n,

$E(\mathbb{Q})_{tors} = \mathbb{Z}/n\mathbb{Z}$;

Else,

$E(\mathbb{Q})_{tors} = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}$.

One advantage of using this algorithm is that we do not need to factorize Δ, as in Lutz-Nagell algorithm 5.2.10. But instead, we have to compute f_m for $m = 3, \ldots, 10, 12$ and calculate its integer roots.

5.4 Tate's Algorithm

In this section, we address the problem of searching torsion points of an elliptic curve by using another classical important result (apparently due to Tate): all elliptic curves with a torsion point of order n (with $4 \leq n \leq 10$ or 12) lie in a one-parameter family. We base our study in [26].

5.4.1 Tate's normal form

In this subsection we find the one-parameter families in which an elliptic curve with a torsion point of order n (with $4 \leq n \leq 10$ or 12) can be writen. The theory developed here is based in [32].

Proposition 5.4.1 *Let E be an elliptic curve defined over $\mathbb{Q}$ with a torsion point P of order $n = 4, \ldots, 10, 12$. Then E can be written in the following form:*

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2,$$

for some $a_1, a_2, a_3 \in \mathbb{Q}$.

PROOF. Let E be an elliptic curve given in a Weierstrass normal form

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

and let $P = (x_0, y_0)$ be a torsion point of order n. We can assume that $O = (0, 0)$ taking the linear change of variables

$$x = x' + x_0, \qquad y = y' + y_0,$$

which gives us the equation

$$y^2 + \alpha_1 xy + \alpha_3 y = x^3 + \alpha_2 x^2 + \alpha_4 x,$$

where

$$\begin{aligned}
\alpha_1 &= a_1, \\
\alpha_2 &= a_2 + 3x_0, \\
\alpha_3 &= a_3 + 2y_0 + a_1 x_0, \\
\alpha_4 &= a_4 + 2a_2 x_0 + 3x_0^2 - a_1 y_0.
\end{aligned}$$

In other words, $O \in E$ if, and only if, $a_6 = 0$. We assume then that the curve has the form

$$E_0 : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x.$$

If we compute y' by using implicit derivation yields

$$(2y + a_1 x + a_3)y' = 3x^2 + 2a_2 x + a_4 - a_1 y.$$

We see that the slope of the tangent line at O is $\dfrac{a_4}{a_3}$ on E_0.

Note that, for the curve E_0 in normal form with O on it, we have:

i) The point O is singular if, and only if, $a_3 = a_4 = 0$, by definition 1.2.10.

ii) The point O is nonsigular and has order 2 in the group E_0 if, and only if, $a_3 = 0$ and $a_4 \neq 0$, which is the case of vertical tangent at O.

The family of these curves reduces to

$$E_{00} : y^2 + a_1 xy = x^3 + a_2 x^2 + a_4 x.$$

Now we assume that O is a nonsingular point which is not of order 2, i.e., $a_3 \neq 0$. By a change of variables of the form

$$x = x', \qquad y = y' + \frac{a_4}{a_3} x',$$

the equation for E_0 becomes

$$E' : y^2 + \alpha_1 xy + \alpha_3 y = x^3 + \alpha_2 x^2,$$

where

$$\alpha_1 = \frac{2a_4}{a_3}, \qquad \alpha_2 = a_2 - \frac{a_4^2}{a_3^2} - a_1 \frac{a_4}{a_3}, \qquad \alpha_3 = a_3.$$

Renaming $a_i = \alpha_i$ for $i = 1, 2, 3$, we have again

$$E' : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2.$$

And calculating y',

$$(2y + a_1x + a_3)y' = 3x^2 + 2a_2x - a_1y.$$

we see that the tangent line at O has slope equal to 0, i.e., it is horizontal.

Note now that the point O on E' has order 3 if, and only if, $a_2 = 0$ and $a_3 \neq 0$ since this is the condition for the curve E' to have a third-order intersection with the tangent line $y = 0$ at O.

The family reduces, in this case, to

$$E' : y^2 + a_1xy + a_3y = x^3.$$

To sum up, if we assume that O is not a torsion point of order 2 or 3, we can write

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2.$$

□

Theorem 5.4.2 (Tate's Normal Form) *Let E be an elliptic curve defined over a field K with $O = (0, 0)$ a torsion point of order $n > 3$. Then there exist parameters $b, c \in K$ such that*

$$E \equiv E(b, c) : y^2 + (1 - c)xy - by = x^3 - bx^2$$

This equation is known as the **Tate's normal form** *of E.*

PROOF. First, we consider the equation for E given by

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2, \tag{5.5}$$

where $a_2, a_3 \neq 0$ since O is a a torsion point of order $n > 3$, by proposition 5.4.1.

Now, if we consider the following (birrational) change of variables

$$x \mapsto \left(\frac{a_3}{a_2}\right)^2 x, \qquad y \mapsto \left(\frac{a_3}{a_2}\right)^3 y.$$

and rewrite the equation for E, we obtain

$$E : y^2 + \frac{a_1a_2}{a_3}xy + \frac{a_2^3}{a_3^2}y = x^3 + \frac{a_2^3}{a_3^2}x^2.$$

Using the abbreviating notation

$$1 - c = \frac{a_1a_2}{a_3}, \qquad -b = \frac{a_2^3}{a_3^2},$$

we end up with the Tate's normal form of E,

$$E \equiv E(b, c) : y^2 + (1 - c)xy - by = x^3 - bx^2.$$

□

Further calculation, using the relations in definition 2.1, yields the following formula for the discriminant $\Delta \equiv \Delta(b,c)$ of $E(b,c)$

$$\Delta(b,c) = (1-c)^4b^3 - (1-c)^3b^3 - 8(1-c)^2b^4 + 36(1-c)b^4 - 27b^4 + 16b^5.$$

Note that as E is an elliptic curve, $b \neq 0$, since otherwise $\Delta = 0$.

The previous theorem tells us that all the curves E with a torsion point of order $n > 3$ belong to a family of curves in two parameters: b and c. In other words, the Tate's normal form gives a description, in terms of equations for the set of pairs (E, P), consisting on an elliptic curve E together with a point P on E such that P, $2P$ and $3P$ are all unequal to $\mathcal{O}$. These pairs correspond to pairs (b,c) such that $b \neq 0$ and $\Delta(b,c) \neq 0$. The curve in the family corresponding to (b,c) is $E(b,c)$ and the point is $P = (0,0)$.

If we require that $nP = \mathcal{O}$ for any $n > 3$, we will get restrictions that, in practise, can be translate to a polynomial equation depending on b and c of the form $f_n(b,c) = 0$.

Proposition 5.4.3 (Multiplication Formulas of $E(b,c)$) *In order to derive the equations for $f_n(b,c) = 0$ for special cases, we can make use of the following formulas, which are been obtained from proposition 2.2.3:*

$$\begin{array}{ll} P = (0,0), & -P = (0,b), \\ 2P = (b,bc), & -2P = (b,0), \\ 3P = (c,b-c), & -3P = (c,c^2), \\ 4P = (d(d-1), d^2(c-d+1)), & -4P = (d(d-1), d(d-1)^2), \end{array}$$

where $d = b/c$ in the formulas for $4P$ and $-4P$. Finally, introducing $e = c/(d-1)$, we have

$$5P = (de(e-1), d^2e(e-1^2)), \qquad -5P = (de(e-1), d^2e^2(d-e)).$$

All of these formulas are also easily obtained using SAGE:

```
sage: K.<b,c>=FractionField(PolynomialRing(QQ,'b,c'));
sage: E = EllipticCurve(K,[1-c, -b, -b,0,0]);
sage: P=E(0,0);
sage: print 2*P
sage: print -2*P
sage: print 3*P
sage: print -3*P
sage: print 4*P
sage: print -4*P
(b : b*c : 1)
(b : 0 : 1)
(c : b - c : 1)
(c : c^2 : 1)
((b^2 - b*c)/c^2 : (b^2*c^2 - b^3 + b^2*c)/c^3 : 1)
((b^2 - b*c)/c^2 : (-b^3 + 2*b^2*c - b*c^2)/(-c^3) : 1)
```

Example 5.4.4 Which is the condition that b and c must satisfy for $E(b,c)$ to have the point $P=(0,0)$ of order 4? When does it have a 2-torsion point?

We look for the formula for $f_4(b,c)$. If P has order 4, then $4P=\mathcal{O}$ or, in other words, $2P=-2P$. Using the formulas from proposition 5.4.3, we have

$$2P=-2P \;\Rightarrow\; (b,bc)=(b,0) \;\Rightarrow\; bc=0 \;\Rightarrow\; c=0,$$

because $b\neq 0$. Thus the condition is $f_4(c,b)=c$, which is the equation of a projective line. Moreover, the equation for the family becomes

$$E(b,0): y^2+xy-by=x^3-bx^2,$$

with discriminant $\Delta(b,0)=b^4(1+16b)\neq 0$.

Moreover, for a given x the y-coordinate satisfies the equation

$$y^2+(x-b)y+(bx^2-x^3)=0.$$

The point $P=(x,y)$ has order 2 if, and only if, this equation in y has a double root, or, in other words, if the discriminant of the quadratic equation equals zero,

$$(x-b)^2-4x^2(b-x)=0 \iff (x-b)(x-b+4x^2)=0.$$

One solution is $x=b$, that gives us $2P=(b,bc)=(b,0)=-2P$ for $c=0$. The other solutions are the points which x-coordinate satisfies

$$4x^2+x-b=0 \iff 4x^2+x+\frac{1}{16}-\left(b+\frac{1}{16}\right)=0 \iff \left(2x+\frac{1}{4}\right)^2=\left(b+\frac{1}{16}\right).$$

This fact tells us that there are two other 2-torsion points on $E(b,0)$ over $\mathbb{Q}$, other that coming from $2P=-2P$, if and only if $b+1/16$ is a perfect square, v^2, over $\mathbb{Q}$. Moreover, v can take any value except 0, $1/4$ and $-1/4$. The x values for these two points are

$$x=-\frac{1}{8}\pm\frac{v}{2}.$$

Example 5.4.5 *W*hich is the condition that b and c must satisfy for $E(b,c)$ to have the point $P=(0,0)$ of order 5?

Following an analogue argument as in previous example, the condition $5P=\mathcal{O}$ is equivalent to $3P=-2P$, and using again the formulas from proposition 5.4.3, we have

$$3P=-2P \;\Rightarrow\; (c,b-c)=(b,0) \;\Rightarrow\; b=c.$$

Thus the condition is $f_5(c,b)=b-c$, which is the equation of a projective line. Moreover, the equation for the family becomes

$$E(b,b): y^2+(1-b)xy-by=x^3-bx^2,$$

with discriminant $\Delta(b,b)=b^5(b^2-11b-1)\neq 0$.

If we keep on using this kind of arguments, we can reach the following result. (Most cases are proved -quite straightforwardly- in [32]).

Theorem 5.4.6 (Tate's Parametrizations) *Every elliptic curve E with a point P of order $n = 4, \ldots, 10, 12$ can be written in the following Tate normal form*

$$E \equiv E(b,c) : y^2 + (1-c)xy - by = x^3 - bx^2,$$

with the following relations:

i) If $n = 4$, then $b = \alpha$, $c = 0$.

ii) If $n = 5$, then $b = \alpha$, $c = \alpha$.

iii) If $n = 6$, then $b = \alpha + \alpha^2$, $c = \alpha$.

iv) If $n = 7$, then $b = \alpha^3 - \alpha$, $c = \alpha^2 - \alpha$.

v) If $n = 8$, then $b = (2\alpha - 1)(\alpha - 1)$, $c = b/\alpha$.

vi) If $n = 9$, then $c = \alpha^2(\alpha - 1)$, $b = c(\alpha(\alpha - 1) + 1)$.

vii) If $n = 10$, then $c = (2\alpha^3 - 3\alpha^2 + \alpha)/[\alpha - (\alpha - 1)^2]$, $b = c\alpha^2/[\alpha - (\alpha - 1)^2]$.

viii) If $n = 12$, then $c = (3\alpha^2 - 3\alpha + 1)/(\alpha - 1)^3$, $b = c(-2\alpha^2 + 2\alpha - 1)/(\alpha - 1)$.

Example 5.4.7 *Find the torsion points of order 5 of the elliptic curve*

$$E : y^2 = x^3 + 12933x - 2285226.$$

If we suppose that E has a point of order 5, theorem 5.4.6 tells us that E must be isomorphic, by a linear change of variables, to one curve lying in the family

$$y^2 + (1-\alpha)xy - \alpha y = x^3 - \alpha x^2.$$

If we take this general equation to Weierstrass short normal form, we obtain an equation which we will note

$$y^2 = x^3 + A_5(\alpha)x + B_5(\alpha).$$

where, using the following sequence of instruction in SAGE,

```
sage: var('a');
sage: E = EllipticCurve([1-a, -a,-a,0,0]);
sage: E
Elliptic Curve defined by
y^2 + (-a+1)*x*y + (-a)*y = x^3 + (-a)*x^2
over Symbolic Ring
```

```
sage: F = E.short_weierstrass_model();
sage: F
Elliptic Curve defined by
y^2 = x^3 + (648*(a-1)*a-27*((a-1)^2-4*a)^2)*x
          + (-1944*(a-1)*((a-1)^2-4*a)*a
          +54*((a-1)^2-4*a)^3+11664*a^2)
over Symbolic Ring
```

we obtain

$$A_5(\alpha) = 648\alpha(\alpha-1) - 27((\alpha-1)^2 - 4\alpha)^2,$$
$$B_5(\alpha) = -1944\alpha(\alpha-1)\cdot((\alpha-1)^2 - 4\alpha) + 54((\alpha-1)^2 - 4\alpha)^3 + 11664\alpha^2.$$

By remark 2.1.4, as this curve should be isomorphic to ours, it must hold

$$\frac{A_5(\alpha)^3}{B_5(\alpha)^2} = \frac{12933^3}{2285226^2},$$

which sums up to an equation in the variable α, in our case, of degree 12. This equation will be called the **final polynomial** for $n = 5$.

```
sage: x = polygen(QQ);
sage: f = ((648*(x-1)*x-27*((x-1)^2-4*x)^2)^3)*(2285226^2)
             -((-1944*(x-1)*((x-1)^2-4*x)*x
                +54*((x-1)^2-4*x)^3+11664*x^2)^2)*(12933^3);
sage: f.roots()
[(10, 1), (-1/10, 1)]
```

We can see that the only rational roots of our final polynomial are $-1/10$ and 10.

Now, by theorem 2.1.5, for every root α_0 of the final polynomial, we have to check if there exists some $u \in \mathbb{Q}$ verifying

$$\begin{cases} u^4 = \dfrac{A}{A(\alpha_0)}, \\ \\ u^6 = \dfrac{B}{B(\alpha_0)}. \end{cases}$$

If there is a solution of the system above for some root, we have a point of order 5; if not, then there are no points of order 5 in E.

Using SAGE one more time, for $\alpha_0 = 10$, we have

```
sage: A1 = 12933;
sage: B1 = -2285226;
sage: A(a) = 648*(a-1)*a-27*((a-1)^2-4*a)^2;
```

```
sage: B(a) = -1944*(a-1)*((a-1)^2-4*a)*a
 +54*((a-1)^2-4*a)^3+11664*a^2;
sage: var('u')
sage: solve([u^4 == A1/A(10), u^6 == B1/B(10)], u)
[[u == 1], [u == -1]]
```

Hence there is a point of order 5 in E, which corresponds to $(0,0)$ in the Tate's normal form. Tracing back the changes of variables a point of order 5 turns out to be $(123, 1080)$.

5.4.2 Torsion points of order 3

The only case remaining is $n = 3$. We could use the Tate's normal form showed above for this case, but it has some inconveniences, being the heaviest one that the family of curves depends on two parameters in this case. However, we can use theorem 5.3.3 and the divisor polynomial f_3 for searching possible 3-torsion points. This particular case is summed up in the following proposition.

Proposition 5.4.8 *Let E be an elliptic curve defined over $\mathbb{Q}$ given by a Weierstrass short normal form $E : y^2 = x^3 + Ax + B$. Then E has a torsion point P of order 3 if and only if there is an integral solution to the equation*

$$f_3(x) = 3x^4 + 6Ax^2 + 12Bx - A^2 = 0.$$

PROOF. Suppose that $P = (x, y)$ is a torsion point of order 3. This means that $3P = \mathcal{O}$ or, in other words, that $2P = -P$. As E is given by the Weierstrass short normal form, taking $a_1 = a_3 = a_2 = 0$, $a_4 = A$ and $a_6 = B$, the group law (proposition 2.2.3) gives us $-P = (x, -y)$. Recalling the duplicaction formula from proposition 2.2.3 too, we have

$$x(2P) = \frac{x^4 - 2Ax^2 - 8Bx + A^2}{4x^3 + 4Ax + 4B},$$

so, if we impose $2P = -P$, then it must hold

$$\begin{aligned} \frac{x^4 - 2Ax^2 - 8Bx + A^2}{4x^3 + 4Ax + 4B} = x \;&\Rightarrow\; x^4 - 2Ax^2 - 8Bx + A^2 = 4x^4 + 4Ax^2 + 4Bx \\ &\Rightarrow\; 3x^4 + 6Ax^2 + 12Bx - A^2 = 0. \end{aligned}$$

□

5.4.3 Tate's Algorithm

We sum up here the steps in the algorithm.

Algorithm 5.4.9 (Tate's algorithm) *Let*

$$E : y^2 = x^3 + Ax + B, \quad \text{with } A, B \in \mathbb{Z}$$

be an elliptic curve defined over $\mathbb{Q}$ given in a Weierstrass short normal form. In order to find its torsion subgroup we proceed as follows:

[Step 1] *Compute the number of points with order* 2*, that is, the solutions for*

$$x^3 + Ax + B = 0, \tag{5.6}$$

namely x_1, x_2, x_3*. For* $i = 1, 2, 3$*, if* $x_i \in \mathbb{Q}$*, define* $P_i = (x_i, 0)$*.*

If $2P_i = \mathcal{O}$*, then* P_i *is a 2-torsion point.*

[Step 2] *Pick the smaller five (for instance) good primes for* E *and compute a bound* M *for the torsion subgroup order as explained above (section 5.1).*

[Step 3] *If the number of rational divisors for equation* (5.6) *is either 0 or 1, then for every divisor* d *of* M*, apply the procedure described in previous subsection to check if there is a point of order* d*. If this is done in decreasing order, the first affirmative answer gives us the group (which should be isomorphic to* C_d*) and one generator: either the point which comes from point* $(0, 0)$ *in Tate's normal form for* $n = 4, \ldots, 10, 12$ *or the point directly obtained for* $n = 3$*.*

[Step 4] *If the number of rational solutions for equation* (5.6) *is 3, then apply the same procedure as above for every divisor* d *of* $M/2$*. Now the first affirmative answer gives us the group (which is isomorphic to* $C_2 \times C_d$*) and a set of generators, a point of order 2 and the point which comes from point* $(0, 0)$ *in Tate's normal form.*

5.5 Dude's algorithm

In this last section, we find the torsion subgroup by using an algorithm due to Dude, based in the analytic parametrization of elliptic curves. To manage this, we first need some theory about elliptic curves defined over $\mathbb{C}$, which can be found in [53]. Then, we develop the algorithm based in Dude's results [18].

5.5.1 Elliptic curves over $\mathbb{C}$

Lattices and basis

Definition 5.5.1 (Lattice) A **lattice** Λ in $\mathbb{C}$ is the subgroup generated by two complex numbers that are linearly independent over $\mathbb{R}$. Thus,

$$\Lambda = w_1\mathbb{Z} + w_2\mathbb{Z}, \qquad \text{for some } w_1, w_2 \in \mathbb{C}.$$

Since either w_1 nor w_2 is a real multiple of the other, we can order them so that $\Im(w_1/w_2) > 0$. Let $\{w_1', w_2'\}$ be a second pair of elements of Λ, then

$$w_1' = aw_1 + bw_2, \qquad w_2' = cw_1 + dw_2,$$

for some $a, b, c, d \in \mathbb{Z}$. In other words,

$$\begin{pmatrix} w_1' \\ w_2' \end{pmatrix} = A \begin{pmatrix} w_1 \\ w_2 \end{pmatrix},$$

where $A \in \mathcal{M}_2(\mathbb{Z})$.

Definition 5.5.2 ($\mathbb{Z}$-basis) The pair (w_1', w_2') is a **$\mathbb{Z}$-basis** of the lattice Λ above if the matrix A is invertible, i.e., if its determinant is ± 1.

We can say the same as above in other way: (w_1', w_2') is a $\mathbb{Z}$-basis of Λ if $A \in GL_2(\mathbb{Z})$.

Let us now write $z = w_1/w_2$ and $z' = w_1'/w_2'$, then

$$\Im(z') = \Im\left(\frac{az+b}{cz+d}\right) = \frac{(ad-bc)\Im(z)}{|cz+d|^2}.$$

We can deduce from this that $\Im(z') > 0$ if, and only if, $\det A = 1$. Therefore, the group $SL_2(\mathbb{Z})$ of matrices with integer coefficients and determinant 1 acts transitively on the set of basis (w_1, w_2) of Λ with $\Im(w_1/w_2) > 0$.

Notation. We will call

$$M = \{(w_1, w_1) \in \mathbb{C}^2 : \Im(w_1/w_2) > 0\};$$

and

$$\mathcal{L} = \{\Lambda \in \mathbb{C} : \Lambda \text{ is a lattice}\}.$$

We have proved the following statement:

Proposition 5.5.3 *The map*

$$(w_1, w_2) \mapsto w_1\mathbb{Z} + w_2\mathbb{Z}$$

induces a bijection

$$SL_2(\mathbb{Z})\backslash M \to \mathcal{L},$$

where $SL_2(\mathbb{Z})\backslash M$ means the set of orbits in M for the action

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} w_1 \\ w_2 \end{pmatrix} = \begin{pmatrix} aw_1 + bw_2 \\ cw_1 + dw_2 \end{pmatrix}.$$

Notation. We denote the invertible elements in $\mathbb{C}$ as

$$\mathbb{C}^* = \{z \in \mathbb{C} : \exists w \in \mathbb{C} \text{ such that } zw = 1\} = \mathbb{C} \setminus \{0\}.$$

Note that $(\mathbb{C}^*, \cdot)$ is a subgroup of $(\mathbb{C}, \cdot)$. We also denote

$$\mathbb{H} = \{z \in \mathbb{C} : \Im(z) > 0\},$$

which is the complex upper half-plane.

If $z \in \mathbb{C}^*$, we define the following actions on M and $\mathcal{L}$

$$\begin{aligned} \mathbb{C}^* \times M &\longrightarrow M, \qquad & z \cdot (w_1, w_2) &\mapsto (zw_1, zw_2); \\ \mathbb{C}^* \times \mathcal{L} &\longrightarrow \mathcal{L}, \qquad & z \cdot \Lambda &\mapsto z\Lambda, \end{aligned}$$

where

$$z\Lambda = \{z\lambda : \lambda \in \Lambda\}.$$

The map $(w_1, w_2) \mapsto w_1/w_2$ induces a bijection between $M \setminus \mathbb{C}^* \to \mathbb{H}$. Subjectivity is trivial from definition of M. To see the injectivity, we consider $(w_1, w_2), (w_1', w_2') \in M$ with the same image and we have to prove that they are in the same orbit.

$$\begin{aligned} \frac{w_1}{w_2} = \frac{w_1'}{w_2'} &\iff w_1 w_2' = w_1' w_2 \\ &\iff \frac{w_1}{w_1'} = \frac{w_2}{w_2'} = z \\ &\iff \begin{cases} w_1' = zw_1 \\ w_2' = zw_2 \end{cases} \\ &\iff (w_1', w_2') = z \cdot (w_1, w_2). \end{aligned}$$

We want to deduce now the action of $SL_2(\mathbb{Z})$ on $\mathbb{H}$ from the action of $SL_2(\mathbb{Z})$ on $M \setminus \mathbb{C}^*$. We consider the following diagram

$$\begin{array}{ccc} SL_2(\mathbb{Z}) \times (M \setminus \mathbb{C}^*) & \xrightarrow{\sigma_2} & M \setminus \mathbb{C}^* \\ \uparrow{\scriptstyle \sigma_1} & & \downarrow{\scriptstyle \sigma_3} \\ SL_2(\mathbb{Z}) \times \mathbb{H} & \dashrightarrow & \mathbb{H} \end{array}$$

where

$$\begin{aligned} \sigma_1\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \tau\right) &= \left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \begin{pmatrix} \tau \\ 1 \end{pmatrix}\right), \\ \sigma_2\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \begin{pmatrix} \tau \\ \rho \end{pmatrix}\right) &= \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \tau \\ \rho \end{pmatrix} = \begin{pmatrix} a\tau + b\rho \\ c\tau + d\rho \end{pmatrix}, \\ \sigma_3(\tau, \rho) &= \frac{a\tau + b\rho}{c\tau + d\rho}. \end{aligned}$$

So, by the commutativity of the diagram, we can assure that the action of $SL_2(\mathbb{Z})$ on $\mathbb{H}$ is

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \tau = \frac{a\tau + b}{c\tau + d}$$

Summing up, we have the bijections

$$\begin{array}{ccccc} \mathcal{L} \setminus \mathbb{C}^* & \overset{1:1}{\longleftrightarrow} & (SL_2(\mathbb{Z}) \setminus M) \setminus \mathbb{C}^* & \overset{1:1}{\longleftrightarrow} & SL_2(\mathbb{Z}) \setminus \mathbb{H} \\ (\mathbb{Z}w_1 + \mathbb{Z}w_2) \cdot \mathbb{C}^* & \longleftrightarrow & SL_2(\mathbb{Z}) \cdot (w_1, w_2) \cdot \mathbb{C}^* & \longleftrightarrow & SL_2(\mathbb{Z}) \cdot \dfrac{w_1}{w_2} \end{array}$$

Definition 5.5.4 (Fundamental domain) Let Λ be a lattice with basis $\{w_1, w_2\}$. If we choose $z_0 \in \Lambda$ and consider the parallelogram with vertices z_0, z_0+w_1, z_0+w_2, $z_0+w_1+w_2$, then its interior is called a **fundamental domain** D for Λ.

We usually choose z_0 so that D to contain 0.

Doubly periodic functions

Let Λ be a lattice on $\mathbb{C}$. To give a function on $\mathbb{C}/\Lambda$ amounts to giving a function on $\mathbb{C}$ such that

$$f(z+w) = f(z), \quad \text{(as a function on } \mathbb{C}\text{), for all } w \in \Lambda.$$

Proposition 5.5.5 *Let Λ be a lattice on $\mathbb{C}$ with basis $\{w_1, w_2\}$. Then*

$$f(z+w) = f(z), \quad \textit{for all } w \in \Lambda \iff \begin{cases} f(z+w_1) = f(z) \\ f(z+w_2) = f(z) \end{cases}$$

PROOF. ($\Rightarrow$) This direction is trivial. It suffices to set $w = w_1$ and $w = w_2$ in the hypothesis.
($\Leftarrow$) Let $w \in \Lambda$. Then there exists $a, b \in \mathbb{Z}$ such that $w = aw_1 + bw_2$.

$$\begin{aligned} f(z+w) &= f(z+aw_1+bw_2) = f(z+aw_1+(b-1)w_2+w_2) = f(z+aw_1+(b-1)w_2) \\ &= f(z+aw_1+(b-2)w_2+w_2) = f(z+aw_1+(b-2)w_2) \\ &\vdots\ b-2 \text{ steps} \\ &= f(z+aw_1) \\ &\vdots\ a \text{ steps} \\ &= f(z). \end{aligned}$$

□

Definition 5.5.6 (Doubly periodic function) Let Λ be a lattice on $\mathbb{C}$ with basis $\{w_1, w_2\}$. A function on $\mathbb{C}$ such that

$$f(z+w) = f(z), \quad \text{for all } w \in \Lambda.$$

is called a **doubly periodic function** for Λ.

The two following results will be useful in the next section. Their proofs have to do with basic complex analysis and they can be found in [53, Prop.2.1] and [53, Col.2.2] repectively.

Proposition 5.5.7 *Let $f(z)$ be a doubly periodic function for Λ, not identically zero, and let D be a fundamental domain for Λ such that f has no zeros or poles on the boundary of D.*

i) $\sum_{P\in D} Res_P(f) = 0$,

ii) $\sum_{P\in D} ord_P(f) = 0$,

iii) $\sum_{P\in D} ord_P(f)\cdot P \equiv 0 \mod \Lambda$.

Lemma 5.5.8 *A nonconstant doubly periodic function has at least two poles (or one double pole).*

We will consider in this section one meromorphic and doubly periodic function on a lattice Λ: the Weierstrass $\wp$-function.

The Weierstrass $\wp$-function

Let Λ be a lattice. The Riemann-Roch theorem 1.7.4 applied to the quotient $\mathbb{C}/\Lambda$ proves the existence of nonconstant doubly periodic meromorphic functions for Λ, but we are going to construct them explicity.

Let G be a finite group acting on a set S. It is easy to construct functions invariant under the action of G: it suffices to take f to be a any function $f : S \to \mathbb{C}$ and define

$$F(s) = \sum_{g\in G} f(gs).$$

This way we have

$$F(g's) = \sum_{g\in G} f(gg's) = F(s),$$

because, as g runs over G, so does $g'g$. Thus F is invariant under the action of G. Reciprocally all invariant functions are given in this form.

When G is not finite, one has to verify that the series above converges. In order to be able to change the order of sumation, we need -at least- absolute convergence. Recall how normal convergence is defined:

Definition 5.5.9 (Normal convergence) Let D be an open subset of $\mathbb{C}$ and let $\{f_n\}_{n\in\mathbb{N}}$ be a sequence of holomorphic functions on D. The series $\sum f_n$ is said to **converge normally** on a subset $A \subseteq D$ if the series of positive terms $\sum ||f_n||$ converges, where $||f_n|| = \sup_{z\in A} |f_n(z)|$

This definition tells us that $\sum f_n$ is both uniformly convergent and absolutely convergent on A. When $\{f_n\}_{n\in\mathbb{N}}$ is a sequence of meromorphic functions, the series is said to **converge normally** on A if, after a finite number of terms f_n have been removed, it becomes a normally convergent series of holomorphic functions. If D is a compact subset of $\mathbb{C}$ and the series of meromorphic functions $f = \sum f_n$ converges normally on D, then f is a meromorphic function too. Moreover, the series of derivatives converges normally on compact subsets of D and its sum is the derivative of f.

Now let $f(z)$ be a meromorphic function on $\mathbb{C}$ and let

$$\varphi(z) = \sum_{w \in \Lambda} f(z + w).$$

Assume that as $|z| \to \infty$, $f(z) \to 0$ so fast that the series for $\varphi(z)$ is normally convergent on compact subsets. Then $\varphi(z)$ is doubly periodic with respect to Λ because replacing z by $z + w_0$ for some $w_0 \in \Lambda$ merely rearranges the terms in the sum.

To prove the normal convergence for the functions we are interested in, we need the following lemma:

Lemma 5.5.10 *For any lattice $\Lambda \in \mathbb{C}$, the series*

$$\sum_{\substack{w \in \Lambda \\ w \neq 0}} \frac{1}{|w|^3}$$

converges.

PROOF. Let $\{w_1, w_2\}$ be a basis for Λ and, for each integer $n \geq 1$, consider the parallelogram

$$P(n) = \{a_1 w_1 + a_2 w_2 : a_1, a_2 \in \mathbb{R}, \max\{|a_1|, |a_2|\} = n\}.$$

We can see the family of parallelograms in the following figure:

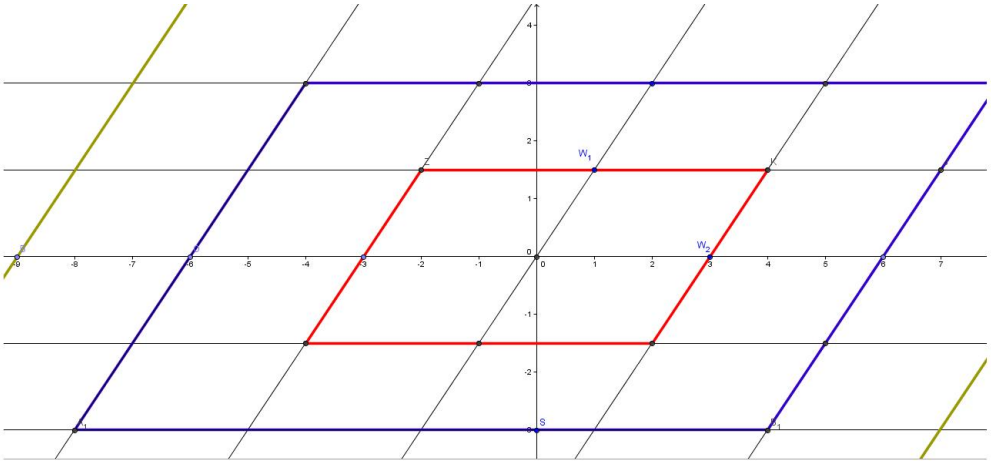


Figure 5.1: $P(n)$ parallelograms.

This way, every parallelogram $P(n)$ has exactly $8n$ points of Λ and the distance between 0 and any of them is at least kn, where

$$k = \min_{w \in P(1) \cap \Lambda} d(0, w).$$

Therefore, the contribution of the points on $P(n)$ to the sum is bounded by $\frac{8n}{k^3n^3}$, and so

$$\sum_{\substack{w\in\Lambda\\ w\neq 0}} \frac{1}{|w|^3} \leq \frac{8}{k^3}\sum_{n=1}^{\infty}\frac{1}{n^2} < \infty$$

□

We know from lemma 5.5.8 that the simplest possible nonconstant doubly periodic function is one with a double pole at each point of Λ and no other poles. Suppose $f(z)$ is such a function. Then $f(z) - f(-z)$ is a doubly periodic function with no poles except perhaps simple ones at the points of Λ. Hence it must be constant, and since it is an odd function it must vanish. Thus $f(z)$ is even and we can make it unique by imposing the normalization condition

$$f(z) = z^{-2} + 0 + z^2 g(z)$$

with $g(z)$ a holomorphic function near $z = 0$. There is such a function, namely Weierstrass $\wp$-function, but we cannot define it directly from $1/z^2$ by the method at the start of this subsection because

$$\sum_{w\in\Lambda}\frac{1}{(z-w)^2}$$

is not normally convergent. Instead, set the following definition:

Definition 5.5.11 (Weierstrass $\wp$-function) Given a lattice $\Lambda \in \mathbb{C}$, we define the **Weierstrass $\wp$-function** as

$$\wp(z) = \frac{1}{z^2} + \sum_{\substack{w\in\Lambda\\ w\neq 0}}\left(\frac{1}{(z-w)^2} - \frac{1}{w^2}\right),$$

and

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

Proposition 5.5.12 *The two series above converge normally on compact subsets of $\mathbb{C}$ and their sums $\wp$ and $\wp'$ are doubly periodic meromorphic functions on $\mathbb{C}$ with $\wp' = d\wp/dz$.*

PROOF. Let

$$\varphi(z) = \frac{-2}{z^3} = \frac{d}{dz}\left(\frac{1}{z^2}\right).$$

We note that $\sum_{w\in\Lambda}\varphi(z+w)$ converges normally on any compact disk $|z| \leq r$ by comparison with $\sum_{w\in\Lambda} 1/|w|^3$ and so does $\wp'(z) = \sum_{w\in\Lambda}\varphi(z)$. Thus, $\wp'(z)$ is a doubly periodic meromorphic function on $\mathbb{C}$.

For $|z| \leq r$, for all but finitely many w with $|w| \leq 2r$, we have that

$$\left|\frac{1}{(z-w)^2} - \frac{1}{w^2}\right| = \left|\frac{-z^2+2zw}{w^2(z-w)^2}\right| = \frac{\left|zw\left(2-\frac{z}{w}\right)\right|}{|w^4|\left|1-\frac{z}{w}\right|^2} \leq \frac{z\frac{3}{2}}{|w|^{3\frac{1}{4}}} \leq \frac{6r}{|w^3|}$$

and so $\wp(z)$ converges normally on the compact disk $|z| \leq r$. Because its derivative is doubly periodic with period lattice Λ, so also is $\wp(z)$.

□

Einsestein series

Let Λ be a lattice in $\mathbb{C}$ and consider the following sum

$$\sum_{\substack{w\in\Lambda \\ w\neq 0}} \frac{1}{w^n}.$$

As the map

$$\Lambda \longrightarrow \Lambda; \qquad w \mapsto -w$$

has order 2 and its only fixed point is 0, then $\Lambda \setminus \{0\}$ is a disjoint union of its orbits . It follows that the sum above is zero if n is odd. Otherwise, we write

$$G_{2k}(\Lambda) = \sum_{\substack{w\in\Lambda \\ w\neq 0}} \frac{1}{w^{2k}}. \tag{5.7}$$

Remark 5.5.13. If $\Lambda = w_1\mathbb{Z} + w_2\mathbb{Z}$, we can always find $c \in \mathbb{C}^*$ and $z \in \mathbb{H}$ such that $G_{2k}(\Lambda) = c \cdot G_{2k}(z\mathbb{Z} + \mathbb{Z})$. We denote

$$G_{2k}(z) := G_{2k}(z\mathbb{Z} + \mathbb{Z}).$$

PROOF. The remark is easy to prove from one easy fact: if $c \in \mathbb{C}^*$ then

$$G_{2k}(c\Lambda) = \sum_{\substack{w\in\Lambda \\ w\neq 0}} \frac{1}{(cw)^{2k}} = c^{-2k} \sum_{\substack{w\in\Lambda \\ w\neq 0}} \frac{1}{w^{2k}} = c^{-2k} G_{2k}(\Lambda).$$

Then, if $\{w_1, w_2\}$ is a basis for Λ, then

$$G_{2k}(w_1\mathbb{Z} + w_2\mathbb{Z}) = G_{2k}(w_2(\frac{w_1}{w_2}\mathbb{Z} + \mathbb{Z})) = w_2^{-2k} G_{2k}(\frac{w_1}{w_2}\mathbb{Z} + \mathbb{Z}) = w_2^{-2k} G_{2k}(z),$$

with $z = w_1/w_2 \in \mathbb{H}$.

□

Definition 5.5.14 (Einsestein series) The series $G_{2k}(\Lambda)$ and $G_{2k}(z)$ are called **Einsestein series**.

We check now that Einsestein series converge in the complex plane:

Proposition 5.5.15 *Let $\Lambda = z\mathbb{Z}+\mathbb{Z}$. Then for all integers $k \geq 2$, $G_{2k}(z)$ converges to a holomorphic function on $\mathbb{H}$.*

PROOF. Let

$$D = \{z \in \mathbb{C} : |z| \geq 1, |\Re(z)| \leq 1/2\}.$$

We consider first $z \in D$ and $\Lambda = z\mathbb{Z}+\mathbb{Z}$. If $w \in \Lambda$, we can write $w = mz+n$ with $m, n \in \mathbb{Z}$. Then

$$|w|^2 = |mz+n|^2 = (mz+n)(m\overline{z}+n) = m^2 z\overline{z} + 2\Re(z)mn + n^2 \geq m^2 - mn + n^2 = |m\rho - n|^2$$

with $\rho = e^{2\pi i/3}$. Hence, for all lattices $\Lambda = z\mathbb{Z}+\mathbb{Z}$ with $z \in D$, there exists a lattice $\Lambda' = \rho\mathbb{Z}+\mathbb{Z}$ which every element $w \in \Lambda$ is bounded by an element of $w' \in \Lambda'$ in the following way

$$|w|^2 \geq |w'|^2 \;\Rightarrow\; |w|^{2k} \geq |w'|^{2k} \overset{k\geq 2}{>} |w'|^3.$$

This leads us to

$$\frac{1}{|w|^{2k}} < \frac{1}{|w'|^3} \;\Rightarrow\; G_{2k}(z) = \sum_{\substack{w\in\Lambda \\ w\neq 0}} \frac{1}{|w|^{2k}} < \sum_{\substack{w'\in\Lambda' \\ w'\neq 0}} \frac{1}{|w'|^3}.$$

Therefore, lemma 5.5.10 shows that for $k \geq 2$, $G_{2k}(z)$ converges normally on D.

Now, for any matrix $A \in SL_2(\mathbb{Z})$, $G_{2k}(A^{-1}z)$ also converges normally on D, because $A^{-1}z \in D$ when $z \in D$. This shows that $G_{2k}(z)$ converges normally on AD. It can be proved that the sets AD cover $\mathbb{H}$, and so this shows that $G_{2k}(z)$ is holomorphic on the whole $\mathbb{H}$.

□

The relation between $\wp$ and $\wp'$

The following result is fundamental in Dude's algorithm:

Proposition 5.5.16 *Let Λ be a lattice in $\mathbb{C}$. The following relation between $\wp$ and $\wp'$ holds:*

$$\wp'(z)^2 = 4\wp(z)^3 - g_4(\Lambda)\wp(z) - g_6(\Lambda),$$

where $g_4(\Lambda) = 60G_4(\Lambda)$ and $g_6(\Lambda) = 140G_6(\Lambda)$.

PROOF. We compute the Laurent expansion of $\wp(z)$ near 0. Recall that for $|t| < 1$,

$$\frac{1}{1-t} = 1 + t + t^2 + t^3 + \cdots = \sum_{n=0}^{\infty} t^n,$$

and differentiating this expresion we obtain

$$\frac{1}{(1-t)^2} = \sum_{n=1}^{\infty} n t^{n-1} = \sum_{n=0}^{\infty} (n+1) t^n,$$

Hence, for $|z| < |w|$ we have

$$\begin{aligned}
\frac{1}{(z-w)^2} - \frac{1}{w^2} &= \frac{1}{w^2}\left(\frac{1}{(1-z/w)^2} - 1\right) \\
&= \frac{1}{w^2}\left(\sum_{n=0}^{\infty}(n+1)\frac{z^n}{w^n} - 1\right) \\
&= \frac{1}{w^2}\sum_{n=1}^{\infty}(n+1)\frac{z^n}{w^n} \\
&= \sum_{n=1}^{\infty}(n+1)\frac{z^n}{w^{n+2}}
\end{aligned}$$

Putting this into the definition of $\wp(z)$ and changing the order of summation, we find that for $|z| < |w|$,

$$\begin{aligned}
\wp(z) &= \frac{1}{z^2} + \sum_{\substack{w\in\Lambda \\ w\neq 0}} \left(\frac{1}{(z-w)^2} - \frac{1}{w^2}\right) \\
&= \frac{1}{z^2} + \sum_{\substack{w\in\Lambda \\ w\neq 0}} \sum_{n=1}^{\infty}(n+1)\frac{z^n}{w^{n+2}} \\
&= \frac{1}{z^2} + \sum_{n=1}^{\infty}(n+1)z^n \sum_{\substack{w\in\Lambda \\ w\neq 0}} \frac{1}{w^{n+2}} \\
&\overset{n=2k}{=} \frac{1}{z^2} + \sum_{k=1}^{\infty}(2k+1)G_{2k+2}(\Lambda)z^{2k},
\end{aligned}$$

where in the latter equality we have used that $\sum 1/w^{n+2}$ is zero if n is odd, so the only terms which 'survive' are the even ones. We have then

$$\begin{aligned}
\wp(z) &= \frac{1}{z^2} + 3G_4(\Lambda)z^2 + 5G_6(\Lambda)z^4 + \cdots, \\
\wp'(z) &= -\frac{2}{z^3} + 6G_4(\Lambda)z + 20G_6(\Lambda)z^3 + \cdots.
\end{aligned}$$

Now consider

$$\begin{aligned}
\wp'(z)^2 &= \frac{4}{z^6} - 2\frac{2}{z^3}(6G_4 z + 20G_6 z^3 + \cdots) + (6G_4 z + 20G_6 z^3 + \cdots)^2 \\
&= \frac{4}{z^6} - \frac{24G_4}{z^2} - 80G_6 + \text{ higher order terms}, \\
\wp(z)^3 &= \frac{1}{z^6} + 3\frac{1}{z^4}(3G_4 z^2 + 5G_6 z^4 + \cdots) + 3\frac{1}{z^2}(3G_4 z^2 + 5G_6 z^4 + \cdots)^2 \\
&\quad + (3G_4 z^2 + 5G_6 z^4 + \cdots)^3 \\
&= \frac{1}{z^6} + \frac{9G_4}{z^2} + 15G_6 + \text{ higher order terms}, \\
-4\wp(z)^3 &= -\frac{4}{z^6} - \frac{36G_4}{z^2} - 60G_6 + \text{ higher order terms}, \\
60G_4\wp(z) &= \frac{60G_4}{z^2} + 180G_4^2 z^2 + 300G_4 G_6 z^4 + \text{ higher order terms}.
\end{aligned}$$

We now use these expressions to calculate the following Laurent expansion:

$$\begin{aligned}
&\wp'(z)^2 - 4\wp(z)^3 + 60G_4\wp(z) + 140G_6 \\
&\qquad = \frac{4}{z^6} - \frac{24G_4}{z^2} - 80G_6 - \frac{4}{z^6} - \frac{36G_4}{z^2} - 60G_6 \\
&\qquad + \frac{60G_4}{z^2} + 180G_4^2 z^2 + 300G_4 G_6 z^4 + 140G_6 + \text{ higher order terms} \\
&\qquad = 180G_4^2 z^2 + \text{ terms of order higher or equal to 2}.
\end{aligned}$$

We can conclude that the Laurent expansion of

$$\wp'(z)^2 - 4\wp(z)^3 + 60G_4(\Lambda)\wp(z) + 140G_6(\Lambda)$$

has no nonzero term in z^n with $n \leq 0$. Therefore this function is holomorphic at 0 and takes the value 0 there. Since it is doubly periodic and has no poles in a suitable fundamental domain containing 0, then, by lemma 5.5.8, it is periodic and in fact zero.

□

Lattices and elliptic curves

As we have just seen in the previous subsection that, given a lattice Λ in $\mathbb{C}$, there exists a narrow relation between the Weierstrass $\wp$-function and its derivative:

$$\wp'(z)^2 = 4\wp(z)^3 + g_4(\Lambda)\wp(z) + g_6(\Lambda).$$

If we consider an elliptic curve $E(\mathbb{C})$ with Weierstrass short equation

$$y^2 = 4x^3 + Ax + B, \quad \text{with } A, B \in \mathbb{Z},$$

we can see the analogy between both expressions above.

In this section we will see how a lattice in $\mathbb{C}$ is related to an elliptic curve over Λ. This will give us a way of finding rational torsion points of the elliptic curve from the lattice and the Weierstrass $\wp$-function. This is the 'soul' of Dude's algorithm.

Lemma 5.5.17 *Let Λ be a lattice in $\mathbb{C}$. The polynomial*

$$f(x) = 4x^3 - g_4(\Lambda)x - g_6(\Lambda)$$

has dinstinct roots.

PROOF. Let $\{w_1, w_2\}$ be a basis for the lattice Λ. The function $\wp'(z)$ is odd, so $\wp'(w_1/2) = -\wp'(-w_1/2)$ and doubly periodic, so $\wp'(w_1/2) = \wp'(-w_1/2)$. We can deduce then that $\wp'(w_1/2) = 0$ and proposition 5.5.16 shows that $\wp(w_1/2)$ is a root of $f(x)$. The same argument shows that $\wp(w_2/2)$ and $\wp((w_1 + w_2)/2)$ are also roots of $f(x)$. It remains to prove that these three complex numbers are dinstinct.

The function $\wp(z) - \wp(w_1/2)$ has a zero at $w_1/2$, which must be a double zero because its derivative is also 0 there. Since $\wp(z) - \wp(w_1/2)$ has only one (double) pole in a fundamental domain D containing 0, by proposition 5.5.7, $w_1/2$ is the only zero of $\wp(z) - \wp(w_1/2)$ in D, i.e., $\wp(z)$ takes the value $\wp(w_1/2)$ only at the point $z = w_1/2$ within D. In particular $\wp(w_1/2)$ is not equal to $\wp(w_2/2)$ or $\wp((w_1+w_2)/2)$. The same argument shows that $\wp(w_2/2)$ is not equal to $\wp((w_1 + w_2)/2)$.

□

From the latter lemma, we see that

$$E(\Lambda) : y^2 = 4x^3 + g_4(\Lambda)x + g_6(\Lambda)$$

is an elliptic curve. Moreover, as $c^4 g_4(c\Lambda) = g_4(\Lambda)$ and $c^6 g_6(c\Lambda) = g_6(\Lambda)$ for $c \in \mathbb{C}^*$, the lattice $c\Lambda$ defines essentially the same elliptic curve as Λ.

Reciprocally, for any elliptic curve

$$E : y^2 z = x^3 + Axz^2 + Bz^3,$$

the closed space $E(\mathbb{C})$ of $\mathbb{P}^2(\mathbb{C})$ has a natural complex structure: for example in a neighbourhood of a point $P \in E(\mathbb{C})$ such that $y(P) \neq 0 \neq z(P)$, the function x/z provides a local coordinate.

Proposition 5.5.18 *If E is an elliptic curve given by $E : y^2 z = 4x^3 + Axz^2 + Bz^3$, then we have a map*

$$\varphi : \mathbb{C}/\Lambda \to E(\Lambda)(\mathbb{C}); \qquad z \mapsto (\wp(z), \wp'(z), 1), \quad 0 \mapsto \mathcal{O}$$

which is an isomorphism (of Riemann surfaces).

PROOF. It is certainly a well-defined map because $\wp(z)$ and $\wp'(z)$ are doubly periodic functions. The function

$$\wp(z) : \mathbb{C}/\Lambda \longrightarrow \mathbb{P}^1(\mathbb{C})$$

is 2:1 in a fundamental domain containing 0, except at the points $w_1/2$, $w_2/2$ and $(w_1 + w_2)/2$, where is one-to-one. Therefore, $\wp$ realizes $\mathbb{C}/\Lambda$ as a covering of degree 2 of the Riemann sphere and it is a local isomorphism except in 0, $w_1/2$, $w_2/2$ and $(w_1+w_2)/2$. Similary, x/z realizes $E(\Lambda)(\mathbb{C})$ as a covering of degree 2 of the Riemann sphere, and it is a local isomorphism except at $\mathcal{O}$ and the three points where $y = 0$. It follows that $\mathbb{C}/\Lambda \to E(\Lambda)(\mathbb{C})$ is an isomorphism outside the two sets of four points. A similar argument shows that it is local isomorphism at the remaining four points.

□

Consider now $\wp(z + z')$. For $z' \in \mathbb{C}$ fixed, it is a doubly periodic function of z and therefore it is rational function of $\wp$ and $\wp'$ as we are going to see in the following result:

Proposition 5.5.19 (Addition formula) *The following formula holds:*

$$\wp(z + z') = \frac{1}{4}\left(\frac{\wp'(z) - \wp'(z')}{\wp(z) - \wp(z')}\right) - \wp(z) - \wp(z').$$

PROOF. Let $f(z)$ be the difference between the right and the left sides. Its only possible poles in a fundamental domain of Λ are at 0 or $\pm z'$. By examining the Laurent expansion of $f(z)$ near these points one sees that it has no pole at 0 or $-z'$, and at worst a simple pole at z'. Since f is doubly periodic, it must be constant, and as $f(0) = 0$, it must be identically 0.

□

Corollary 5.5.20 *The map*

$$\varphi : \mathbb{C}/\Lambda \to E(\Lambda)(\mathbb{C}); \qquad z \mapsto (\wp(z), \wp'(z)), \quad 0 \mapsto \mathcal{O}$$

is a group homomorphism.

PROOF. Let $y = mx + b$ be the line through the points $P = (x, y)$ and $P' = (x', y')$ on the curve $y^2 = 4x^3 - g_4x - g_6$. Then x, x' and $x(P + P')$ are roots of the polynomial

$$(mx + b)^2 - 4x^3 + g_4x + g_6$$

and so

$$x(P + P') + x + x' = \frac{m^2}{4} = \frac{1}{4}\left(\frac{y - y'}{x - x'}\right).$$

The formula in latter proposition agrees with this one for the x-coordinate of the sum of two points in $E(\Lambda)$, so this proves that the homomorphism holds.

□

Theorem 5.5.21 *Every elliptic curve E over $\mathbb{C}$ is isomorphic to $E(\Lambda)$ for some lattice Λ.*

PROOF. Recall from proposition 2.1.8 that over an algebraically closed field, the elliptic curves are classified (up to isomorphism) by their j-invariants. For any lattice $\Lambda \in \mathbb{C}$, the curve

$$E(\Lambda) : y^2 = 4x^3 - g_4(\Lambda)x - g_6(\Lambda)$$

has discriminant and j-invariant given by

$$\Delta = g_4(\Lambda)^3 - 27g_6(\Lambda)^2, \qquad j(\Lambda) = \frac{1728g_4(\Lambda)^3}{g_4(\Lambda)^3 - 27g_6(\Lambda)^2}.$$

Furthermore, for $c \in \mathbb{C}^*$, $g_4(c\lambda) = c^{-4}g_4(\Lambda)$ and $g_6(c\Lambda) = c^{-6}g_6(\Lambda)$, and so the isomorphism class of $E(\Lambda)$ depends only on Λ up to scaling. Define

$$j(\tau) = j(\tau\mathbb{Z} + \mathbb{Z}).$$

Then for every $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$,

$$j(\frac{a\tau + b}{c\tau + d}) = j(\tau).$$

Moreover, it can be proved that $j : \mathbb{H} \to \mathbb{C}$ is surjective, which completes the proof.

□

5.5.2 Two useful algorithms

Two problems appear now:

1) How to compute, given a basis $\{w_1, w_2\}$ of the lattice Λ associated to E, the values for $\wp(z)$ and $\wp'(z)$.

2) Given an elliptic curve E, how to compute a basis $\{w_1, w_2\}$ of the lattice associated.

Some algorithms can be used to solve this problems. For further explanation see [10, pp. 395-398].

Reduction algorithm

Let $\{w_1, w_2\}$ be a basis for the lattice Λ such that $\Im(w_1/w_2) > 0$. As we have done so far, we consider $\tau = w_1/w_2 \in \mathbb{H}$. The problem is that in practice using this τ for computing certain quantities could be inneficient. Because of this one should first find the complex number τ' belonging to the fundamental domain D of Λ which is equivalent to τ under the action of $SL_2(\mathbb{Z})$.

Algorithm 5.5.22 (Reduction algorithm) *Given $\tau \in \mathbb{H}$ this algorithm outputs the unique τ' equivalent to τ under the action of $SL_2(\mathbb{Z})$ and which belongs to the fundamental domain D of Λ, as well as the matrix $A \in SL_2(\mathbb{Z})$ such that $\tau' = A\tau$.*

1. [**Initialize**]
   $A \leftarrow \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.
2. [**Reduce real part**]
   $n \leftarrow \lfloor \Re(\tau) \rfloor$,
   $\tau \leftarrow \tau - n$,
   $A \leftarrow \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix} A$.
3. [**Finished**]
   $m \leftarrow \tau\overline{\tau}$.
   If $m \geq 1$
   output τ and A and terminate the algorithm;
   else:
   $\tau \leftarrow -\tau/m$,
   $A \leftarrow \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} A$,
   Go to step 2.

The $\wp$ and $\wp'$ algorithm

We can use power series expansions to compute $\wp$ and $\wp'$:

Proposition 5.5.23 *Let $\{w_1, w_2\}$ be a basis for the lattice Λ. Set*

$$\tau := \frac{w_1}{w_2} \in \mathbb{H}, \qquad q := e^{2\pi i \tau}, \qquad u := e^{2\pi i z/w_2},$$

then

$$\wp(z) = \left(\frac{2\pi i}{w_2}\right)^2 \left(\frac{1}{12} + \frac{u}{(1-u)^2} + \sum_{n=1}^{\infty} q^n \left(u\left(\frac{1}{(1-q^n u)^2} + \frac{1}{(q^n - u)^2}\right) - \frac{2}{(1-q^n)^2}\right)\right)$$

and

$$\wp'(z) = \left(\frac{2\pi i}{w_2}\right)^3 u \left(\frac{1+u}{(1-u)^3} + \sum_{n=1}^{\infty} q^n \left(\frac{1+q^n u}{(1-q^n u)^3} + \frac{q^n + u}{(q^n - u)^3}\right)\right)$$

Algorithm 5.5.24 ($\wp$ and $\wp'$ algorithm) *Let $\{w_1, w_2\}$ be a basis for the lattice Λ and let $z \in \mathbb{C}$. This algorithm computes $\wp(z)$ and $\wp'(z)$.*

1. [**Initialize and reduction**]
   If $\Im(w_1/w_2) < 0$
   swap(w_1,w_2).
   $\tau \leftarrow w_1/w_2$.
   Using the algorithm 5.5.22, find a matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ *such that* $A\tau$ *is in the fundamental domain* D,
   $\tau \leftarrow A\tau$,
   $w_2 \leftarrow cw_1 + dw_2$.
2. [**Reduce** z]
   $z \leftarrow z/w_2$,
   $n \leftarrow \lfloor \Im(z)/\Im(\tau) \rfloor$,
   $z \leftarrow z - n\tau$,
   $z \leftarrow z - \lfloor \Re(z) \rfloor$.
3. [**Compute**]
   If $z = 0$,
   Output a message saying that $z \in \Lambda$;
   else,
   Compute $\wp(z)$ and $\wp'(z)$ using the formulas given in proposition 5.5.23 and terminate the algorithm.

The w_1 and w_2 algorithm

Now given g_4 and g_6 defining a Weierstrass short equation for an elliptic curve E, we want to compute a basis $\{w_1, w_2\}$ of the corresponding lattice Λ.

We need a definition before: the Arithmetic-Geometric Mean (AGM) of two numbers.

Definition 5.5.25 (AGM) Let $a, b \in \mathbb{R}^+$. The **Arithmetic-Geometric Mean** of a and b, denoted by $AGM(a, b)$, is defined as the common limit of the two sequences $\{a_n\}$ and $\{b_n\}$ defined by

$$\begin{cases} a_0 = a, \\ b_0 = b, \\ a_{n+1} = \dfrac{a_n + b_n}{2}, \\ b_{n+1} = \sqrt{a_n b_n}. \end{cases}$$

It is easy to see that the set of real points on an elliptic curve with real coefficients has either one or two components in the standard topology of $\mathbb{R}^2$. The component which is unbounded is called the **identity component** because it can be considered to contain the point at infinity which is the identity for the group law. The following algorithm gives a basis of a lattice Λ of an elliptic curve with real coefficients using the AGM. Since elliptic curves are usually given by the generalized Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

instead of

$$y^2 = 4x^3 + g_4x + g_6,$$

the algorithm is given in that context.

Algorithm 5.5.26 (Periods of an elliptic curve over $\mathbb{R}$) *Given $a_1, \ldots, a_6 \in \mathbb{R}$, this algorithm computes the basis $\{w_1, w_2\}$ of the period lattice Λ of E such that w_2 is a positive real number and w_1/w_2 has positive imaginary part and real part equal to 0 or $-1/2$.*

1. [**Initialize**]

   Using formulas in definition 2.1, compute b_2, b_4, b_6 and Δ;

   If $\Delta < 0$, go to step 3.

2. [**Disconnected case**] *Let e_1, e_2 and e_3 be the three real roots of the polynomial*

   $$4x^3 + b_2x^2 + 2b_4x + b_6 = 0,$$

   with $e_1 > e_2 > e_3$.

   $w_2 \leftarrow \dfrac{\pi}{AGM(\sqrt{e_1 - e_3}, \sqrt{e_1 - e_2})}$,

   $w_1 \leftarrow \dfrac{i\pi}{AGM(\sqrt{e_1 - e_3}, \sqrt{e_2 - e_3})}$.

   Terminate the algorithm.

3. [**Connected case**]

   Let e_1 be the unique real root of $4x^3 + b_2x^2 + 2b_4x + b_6 = 0$,

   $a \leftarrow 3e_1 + b_2/4$,

   $b \leftarrow \sqrt{3e_1^2 + (b_2/2)e_1 + b_4/2}$

   $w_2 \leftarrow \dfrac{2\pi}{AGM(2\sqrt{b}, \sqrt{2b + a})}$,

   $w_1 \leftarrow -\dfrac{w_2}{2} + \dfrac{i\pi}{AGM(2\sqrt{b}, \sqrt{2b - a})}$.

   Terminate the algorithm.

5.5.3 Dude's analytic algorithm

All the work we have done so far reduces the problem of finding rational torsion points of E to that of finding complex torsion points in $\mathbb{C}/\Lambda$ and checking whether their images $(\wp(z), \wp'(z))$ by the map $\mathbb{C}/\Lambda \to E(\mathbb{C})$ are rational.

However, we are interested on finding the n-torsion points of $\mathbb{C}/\Lambda$, but they are trivially given by the isomorphism

$$E(\mathbb{C})[n] \simeq \frac{1}{n}\Lambda/\Lambda = \left\{ \frac{a}{n}w_1 + \frac{b}{n}w_2 : a, b \in \mathbb{Z} \right\} / (w_1\mathbb{Z} + w_2\mathbb{Z}).$$

So we only need to check the rationality of the images of $\mathbb{C}/\Lambda \to E(\mathbb{C})$.

The basis obtained with the w_1 and w_2 algorithm of the previous section has the property that the multiples of w_1 correspond to points on the identity component of the curve, and the translates of these multiples by $w_2/2$ correspond to points on the bounded component (if any).

Algorithm 5.5.27 *Let*

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

be an elliptic curve given in Weierstrass short normal form. The following algorithm returns the torsion subgroup of E, its order and a set of generators.

[Step 1] *Pick the smaller five (for instance) good primes for E and compute a bound M for the torsion subgroup order using proposition 3.1.20.*

[Step 2] *If $M = 1$:*

return $(\{e\}, 1, \{\mathcal{O}\})$.

[Step 3] *We use the w_1 and w_2 algorithm 5.5.26, to calculate w_1 and w_2.*

[Step 4] *If $4 \nmid M$, then by Mazur's theorem we know that the torsion subgroup is cyclic of order at most 10.*

For n from 10 to 2:

If $n|M$:

If $w_1/n \in \mathbb{Q}$:

return $(C_n, n, \{w_1/n\})$.

Else if n is even and $w_1/n + w_2/2 \in \mathbb{Q}$:

return $(C_n, n, \{w_1/n + w_2/2\})$.

return $(\{e\}, 1, \{\mathcal{O}\})$.

[Step 5] *If $4 \mid M$, the torsion subgroup may not be cyclic.*

Let $\mathcal{D}$ the set of 2-torsion points of E over $\mathbb{C}$, i.e.,

$$\mathcal{D} = \{z \in \mathbb{C} : z^3 + Az + B = 0\}.$$

If $\mathcal{D} = \emptyset$, then the torsion subgroup is cyclic of odd order and contained within the identity component of E.

For n from 11 to 3:

If $n|M$ and n is odd:

If $w_1/n \in \mathbb{Q}$:

return $(C_n, n, \{w_1/n\})$.

return $(\{e\}, 1, \{\mathcal{O}\})$.

Else if $|\mathcal{D}| = 1$, the torsion subgroup is cyclic, and we proceed as in the case where $4 \nmid M$, but only checking the odd cases:

For n from 11 to 3:

If $n|M$ and n is odd:

If $w_1/n \in \mathbb{Q}$:

return $(C_n, n, \{w_1/n\})$.

Else if n is even and $w_1/n + w_2/2 \in \mathbb{Q}$:

return $(C_n, n, \{w_1/n + w_2/2\})$.

Else, the torsion subgroup is non-cyclic.

We take $P_1 \in \mathcal{D} \cap \mathbb{Q}$ as the first generator.

If $w_1/8 \in \mathbb{Q}$:

return $(C_2 \times C_8, 16, \{P_1, w_1/8\})$.

Else If $w_1/6 \in \mathbb{Q}$:

return $(C_2 \times C_6, 12, \{P_1, w_1/6\})$.

If $w_1/4 \in \mathbb{Q}$:

return $(C_2 \times C_4, 8, \{P_1, w_1/4\})$.

Else, we take $P_2 \in \mathcal{D} \cap \mathbb{Q}$, $P_2 \neq P_1$ as the second generator.

return $(C_2 \times C_2, 4, \{P_1, P_2\})$.

Appendix A

Applications of elliptic curves

A.1 Proof of Fermat's Last Theorem

Elliptic curves played a crucial role to prove Fermat's Last Theorem:

Theorem (Fermat's Last Theorem) *No three possitive integers $a, b, c \in \mathbb{Z}$ can satisfy the equation*

$$a^n + b^n = c^n$$

for $n \in \mathbb{N}$, $n \geq 3$.

Some particular cases were proven by Fermat ($n = 4$, 1660s), Euler ($n = 3$, 1753), Dirichlet ($n = 5$, 1825), Lame ($n = 7$, 1839) and Kummer ($n \leq 1000$, 1857). We give here the main ideas of the prove of the theorem in general.

A first naive approach shows that finding rational points on curves gives a way to tackle the problem: if we define the curve $F_n(x, y) = x^n + y^n - 1 = 0$ and (α, β) is a rational point of F_n, i.e., $F(\alpha, \beta) = 0$ with $\alpha = a/c$ and $\beta = b/c$, then (a, b, c) gives an integer solution for $x^n + y^n = z^n$, since

$$\frac{a^n}{c^n} + \frac{b^n}{c^n} - 1 = 0 \iff a^n + b^n = c^n.$$

Conversely, any integer solution to Fermat's equation yields a rational point of the curve $F_n(x, y) = 0$.

In 1983, Faltings [23] proved the following theorem, that was conjectured by Mordell in 1922:

Theorem (Faltings) *Let C be an algebraic curve defined over $\mathbb{Q}$ of genus g. If $g > 2$, then C has only finitely rational points.*

This theorem means that for any curve except for lines, conics ($g = 0$) and elliptic curves ($g = 1$), the number of rational points on the curve is finite. This implies that

the equation $x^n + y^n = z^n$ will have at most finitely many solutions for any $n > 4$, since equations for $n = 3, 4$ can be transformed to elliptic curves. So this result is not strong enough.

Using a different approach, one idea is to "transform", using some kind of isomorphism, the curves $x^n + y^n = 1$ to a family of curves that have no rational points on it. And this family is a family of elliptic curves.

Assume that an elliptic curve E defined over $\mathbb{Q}$ can be written as

$$E : y^2 = x^3 + Ax + B, \quad \text{with } A, B \in \mathbb{Q},$$

(this fact is proven in section 2.1 of this text). We define the *discriminant* of E as $\Delta = 4A^3 + 27B^2$. We require that $\Delta \neq 0$, condition which is equivalent to the condition that the three roots of $x^3 + Ax + B$ are distinct. In this case, if $x^3 + Ax + B = (x-\alpha)(x-\beta)(x-\gamma)$ then,

$$\Delta = (\alpha - \beta)^2(\beta - \gamma)^2(\gamma - \alpha)^2.$$

Now let (a, b, c) be an integer solution of the equation $x^n + y^n = z^n$ for some $n > 2$. De define an elliptic curve E_n by the equation

$$y^2 = x(x - a^n)(x + b^n).$$

The discriminant of this curve is

$$\Delta = (a^n)^2(b^n)^2(a^n + b^n)^2 = (abc)^{2n}.$$

So the discriminant is the $2n$-th power of an integer. We aim to show that no elliptic curve exists whose discriminant is a 6th or higher power.

We have said that $(E, +)$ have group structure with a special point $\mathcal{O}$. Now, for each prime p, define $E(\mathbb{F}_p)$ to be the set of points $(u, v) \in \mathbb{F}_p^2$ such that

$$v^2 = u^3 + Au + B \bmod(p).$$

Then a point in $E(\mathbb{Q})$ yields a point in $E(\mathbb{F}_p)$ and the set $E(\mathbb{F}_p)$ is clearly finite, $\#E(\mathbb{F}_p) \leq p^2$.

A theorem due to Hasse gives a better bound:

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

It was proven by Hasse [29] in 1933, with the proof published in a series of papers in 1936.

We define now a sequence given by $a_p = \#E(\mathbb{F}_p) - (p + 1)$. Then we get an infinite sequence $a_2, a_3, a_5, a_7, \ldots$. For the sake of completeness, we define a's for non-prime indices too:

$$a_n = \begin{cases} \#E(\mathbb{F}_n) - (n + 1), & \text{if } n = p, prime; \\ \prod_{i=1}^{k} a_{p_i}^{e_i}, & \text{if } n = \prod_{i=1}^{k} p_i^{e_i}. \end{cases}$$

For example,

$$a_1 = 1, \qquad a_2 = \#E(\mathbb{F}_2) - 3, \qquad a_3 = \#E(\mathbb{F}_2) - 4, \qquad a_4 = a_2^2 = (\#E(\mathbb{F}_2) - 3)^2 \ldots$$

We can now define a generating function for this sequence:

$$G_E(z) = \sum_{n \geq 1} a_n z^n.$$

By studying properties of $G_E(z)$ we can infer properties of E. We have to define the last concept we need to prove Fermat's Last Theorem:

Definition. *A function f defined over complex numbers is modular of level ℓ and contundance N if for every $M \in GL_2(\mathbb{Z})$ with*

$$M = \begin{pmatrix} a & b \\ kN & d \end{pmatrix}$$

then

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^{\ell} \cdot f(z)$$

for all $z \in \mathbb{C}$ with $\Im(z) > 0$.

We define now a special generating function

$$SG_E(z) = G_E(e^{2\pi i z}) = \sum_{n \geq 1} a_n e^{2\pi 1 z}.$$

In 1990, Ribet [67, 68] proved the so called epsilon conjecture. An important consequence of this theorem is the following one:

Theorem (Ribet) *Functions SG_{E_n} are not modular for $n > 2$.*

Finally in 1995, Wiles [80], proved the following theorem:

Theorem (Wiles) *Function SG_E for any elliptic curve E is modular.*

This contradicts the fact that E_n is an elliptic curve for $n \geq 3$, and proves Fermat's Last Theorem.

A.2 Elliptic curve cryptography

Elliptic curves are nowadays used in cryptography, specifically in public key (or asymmetric) cryptography. In a public key cryptosystem there are two keys. The public

key, which is published in a directory and allows encryption; and the private key which is kept secret and allows decryption. The first public key cryptosystem was invented by Diffie and Helman in 1976. We describe it over a general finite group G:

Algorithm (Diffie-Hellman key exchange, DH) *This algorithm allows two people, A and B, to generate a shared piece of secret information over an insecure communications channel.*

i) (Setup). A and B publicly select a finite group G and an element $\alpha \in G$.

ii) A generates a random integer a, computes α^a in G, and transmits it to B over a public communications channel.

iii) B generates a random integer b, computes α^b in G, and transmits it to A over a public communications channel.

iv) A receives α^b and computes $(\alpha^b)^a$.

v) B receives α^a and computes $(\alpha^a)^b$.

Now A and B both know the element α^{ab} which can be used as a private key for further communication.

If an opponent O listens in on this process he knows G, α, α^a and α^b. Finding α^{ab} from this information is the Diffie-Hellman problem. If O could find a from α and α^a then he could simply compute $(\alpha^b)^a$ and solve the Diffie-Hellman problem.

Given a finite group G an $\alpha \in G$ and α^a, with $\alpha \in \mathbb{Z}$, the problem of computing a is called the *discreet logarithm problem.* No efficient algorithm is known for computing discrete logarithms.

Going back to public key cryptosystems, on one hand, we have the classical asymetric cryptosystem: RSA, published in 1978 by Rivest, Shamir, and Adleman. It is based on the presumed difficulty of factoring large integers, the factoring problem. On the other hand, we have elliptic curve cryptography (ECC) which relies on the believed difficulty of the elliptic curve discrete logarithm for its security, where the group G is a cyclic subgroup of a given elliptic curve. Elliptic curves were proposed for use as the basis for discrete logarithm-based cryptosystems in 1985, independently by Miller of IBM and Koblitz of the University of Washington [52, 42]. Elliptic curve groups were proposed as a substitute for the multiplicative groups mod p usually used in DH.

Applications in a lot of sectors depend nowadays on the underlying security already available in the wired computing environment. Both for secure (authenticated, private) Web transactions and for secure (signed, encrypted) messaging. As we have mentioned, three alternatives are available for these applications: RSA, Diffie-Hellman Key Exchange and ECC. We are going to compare RSA and ECC in the area of wireless technologies

because the first one has been the most used and the second one is the topic of study of the present text. Moreover, wireless technologies are the most extended technologies in use today.

For the same level of security per best currently known attacks, elliptic curve-based systems can be implemented with much smaller parameters, leading to significant performance advantages. Such performance improvements are particularly important in the wireless arena where computing power, memory, and battery life of devices are more constrained. There are various standards bodies guiding the implementation of security protocols for the industry. More specifically, to ECC is the IEEE P1363 published standard for describing implementation of elliptic curve operations. NIST provides a list of curves to be used, specified in FIPS 186-2, Digital Signature Standard.

Since elliptic curve discrete logbased cryptosystems appeared, many of the top mathematicians in algorithmic number theory have tried their hand at attacking them. Successful attacks have been found only for a few very special families of curves (e.g., the Menezes-Okomoto-Vanstone attack using the Weil pairing on supersingular elliptic curves). By comparison, much more efficient attacks are known for both RSA and mod p discrete log-based cryptosystems. Therefore, for the same level of resistance against the best known attacks, the system parameters for an elliptic-curve-based system can be chosen to be much smaller than the parameters for RSA or mod p systems. Table A.2 shows the size of equivalent security levels in bits for symmetric cryptosystems, ECC and DH/RSA systems.

Symmetric	ECC	DH/RSA
80	163	1024
128	283	3072
192	409	7680
256	571	15360

Table A.1: Key sizes for equivalent security levels (in bits).

At the 163-bit ECC/1024-bit RSA security level, an elliptic curve exponentiation for general curves over arbitrary prime fields is roughly 5 to 15 times as fast as an RSA private key operation, depending on the platform and optimizations. At the 256-bit ECC/3072-bit RSA security level the ratio has already increased to between 20 and 60, depending on optimizations.

This growing difference in key bit length for equivalent security levels accounts for the performance advantages to be obtained from substituting ECC for RSA/DH in public key cryptographic protocols.

As an simple example of cryptography with elliptic curves we present the ElGamal

cryptosystem. This has never been standardised for use with elliptic curves because is vulnerable to chosen ciphertext attack. We have chosen this cryptosystem becasuse it is an easy understandable example of using elliptic curves in cryptography. For cryptographic use we recommend Elliptic Curve Integrated Encryption Scheme (ECIES), see [71].

We can consider an elliptic curve E defined over a finite field $\mathbb{F}_q$, i.e., $E(\mathbb{F}_q)$, which will turn out to have a finite number of points, which we can in fact bound by Hasse's theorem above. To do cryptography on $E(\mathbb{F}_q)$ it is usual to take either $q = p$, for some prime $p > 3$ or $q = 2^n$, for fome $n \geq 2$.

Algorithm (ElGamal for elliptic curves)

i) (Setup). An elliptic curve over a finite field is chosen, namely $E(\mathbb{F}_q)$, together with a point $P \in E(\mathbb{F}_q)$. The point P generates a cyclic subgroup $G = \langle P \rangle = \{\mathcal{O}, P, 2P, \ldots (n-1)P\}$ of order n. Each user picks a random integer $0 \leq l \leq n-1$ (the private key) and publics lP (the public key). We suppose that messages are elements of G and that a user A wishes to send a plain message $M \in G$ to user B.

ii) A generates a random integer $0 \leq k \leq n-1$ and computes kP.

iii) A looks up B's public key lP and computes $k(lP)$, then $M + klP$.

iv) A sends to B the pair of group elements $(kP, M + klP)$.

v) B computes $(M + klP) - l(kP) = M$ and recovers the plain message.

Once again being able to find l from P and lP (solving the elliptic curve discrete logarithm problem) would allow us to crack this cryptosystem.

Another use of public key cryptography is in *digital signature algorithms*. On a physical document a signature is (ideally) proof that you wrote the document. A digital signature is a similar proof that you are who you claim to be that can be sent electronically. We present a simplified version of the ElGamal digital signature algorithm from [79].

Algorithm (ElGamal Elliptic Curve Digital Signatures) *This algorithm allows a user A to send a message m, represented as an integer, to B such that B can be sure that A sent it. We choose an elliptic curve defined over a finite field, $E(\mathbb{F}_p)$, with p a prime, and a point $P \in E(\mathbb{F}_p)$. Let $G = \langle P \rangle = \{\mathcal{O}, P, 2P, ..., (n-1)P\}$.*

i) (Setup). A chooses an integer $0 \leq l \leq n-1$ and calculates lP. A's public key is $(E, \mathbb{F}_p, lP, P)$ and A's private key is l.

ii) A sends the message (m, kP, s). We can think of m as the message and (kP, s) as the signature.

iii) B receives (m, kP, s) and calculates $V_1 = x(lP) + s(kP)$ and $V_2 = mP$.

iv) If $V_1 = V_2$, B accepts the message from A. Otherwise he rejects it.

First we check that this algorithm will accept messages coming from A as valid. If it is a valid signature then

$$V_1 = x(lP) + s(kP) = xlP + k^{-1}(m - lx)kP = xlP + mP - lxP = mP = V_2,$$

as the algorithm checks for. Now we note that being able to crack the elliptic curve discrete log problem would allow you to impersonate A since you could find l from P and lP and then send any message m signed with A's signature (since could calculate the correct s)

To sum up, we can say that over the last years, elliptic curve cryptography has moved from being an interesting theoretical alternative to being a cutting edge technology adopted by an increasing number of companies. There are two reasons for this new development: one is that ECC is no longer new, and has withstood a generation of attacks; second, in the growing wireless industry, its advantages over RSA have made it an attractive security alternative.

Wireless Internet mail industry leaders such as Qualcomm have embraced ECC, as well as other major companies in the wireless industry such as Motorola, Docomo, and RIM. Major computer companies such as IBM, Sun Microsystems, Microsoft, and Hewlett-Packard are all investing in ECC. The U.S. government is backing the use of ECC as well, with NSA creating the security requirements for wireless devices connecting to the military, and NIST providing standardized curves for use in a range of applications of ECC.

Wireless devices are rapidly becoming more dependent on security features such as the ability to do secure email, secure Web browsing, and virtual private networking to corporate networks, and ECC allows more efficient implementation of all of these features.

Bibliography

[1] D. Abramovich, *Formal finiteness and the torsion conjecture on elliptic curves. A footnote to a paper: "Rational torsion of prime order in elliptic curves over number fields".* Asterisque 228 3 (1995), 5-17.

[2] M. Atiyah, I.G. Macdonald, *Introducción el Álgebra Conmutativa.* Reverté (1980).

[3] A. Baker and J. Coates, *Integer points on curves of genus 1.* Proc. Cambridge Philos. Soc. 67 (1970), 595-602.

[4] M. Bhargava, A. Shankar, *Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank 0.* Preprint (2010).

[5] I. F. Blake, *Elliptic curves in cryptography.* London Mathematical Society Lecture Note Series, 265. Cambridge University Press, Cambridge, 1999.

[6] A. Bremner, J.W.S. Cassels, *On the equation* $y^2 = x(x^2 + p)$. Math Comp., 42(1984), 257- 264.

[7] A. Brumer *The average rank of elliptic curves. I.* Inventiones Mathematicae 109 (1992), 445-472.

[8] I. A. Burhanuddin, M. A. Huang, *Elliptic curve torsion points and division polynomials.* Department of Computer Science, University of Southern California, Los Angeles, 2005.

[9] P. L. Clark, *Dirichlet Theorem on Primes in Arithmetic Progressions.* `http://math.uga.edu/~pete/4400DT.pdf`

[10] H. Cohen, *A Course in Computational Algebraic Number Theory* Berlin Heidelberg New York: Springer 1993.

[11] H. Cohen, *Number Theory. Volume I: Tools and Diophntine Equations.* Springer-Verlag, New York, 2007. Graduate Texts in Mathematic, No. 239.

[12] J. E. Cremona, *Algorithms for modular elliptic curves.* Cambridge University Press 1992.

[13] J. E. Cremona, *Elliptic curve data.* `http://www.warwick.ac.uk/~masgaj/ftp/data/`.

[14] Dalemöller, *Elliptic Curves*, 2nd edition. Springer-Verlag, New York, 2004. Graduate Texts in Mathematic, No. 111.

[15] M. Derickx, *Torsion points on elliptic curves and gonalities of modular curves.* Master thesis. Mathematisch Instituut, Universiteit Leiden, 2012.

[16] M. Derickx, S. Kamienny, W. Stein, M. Stoll. *Torsion points on elliptic curves over number fields of small degree.* In preparation, 2013.

[17] Diophantus, *Arithmetica.* `http://archive.org/stream/diophantusofalex00heatiala#page/2/mode/2up`

[18] D. Dude, *A procedure to calculate torsion of elliptic curves over* $\mathbb{Q}$. Manuscripta Mathematica, Vol. 95, Issue 1 (1998), 463-469.

[19] A. Dujella, *Rank records history, Rank = 19.* `http://web.math.pmf.unizg.hr/~duje/tors/rkeq19.html`

[20] N. D. Elkies, $\mathbb{Z}^{28}$ *in* $E(\mathbb{Q})$*, etc.*. Number Theory Listserver, May 2006.

[21] A. Enge, *Elliptic Curves and Their Applications to Cryptography, An Introduction.* Kluwer Academic Publishers, 1998.

[22] G. Faltings, *The general case of S. Lang's conjecture.* Proccedings of the Barsotti symposium in algebraic geometry, Academic Press, San Diego, 1994.

[23] G. Faltings, *Finiteness theorems for abelian varieties over number fields.* Arithmetic geometry (Storrs, Conn., 1984) (1986): 9-27.

[24] G. Frey, *Curves with manitely many points of fixed degree.* Israel J. Math. 85 (1994), 79-83.

[25] W. Fulton, *Algebraic curves. An introduction to Algebraic Geometry.* Addison-Wesley, (1989). `http://www.math.lsa.umich.edu/~wfulton/CurveBook.pdf`

[26] I. García,M. A. Olalla, J. M. Tornero, *Computing the Rational Torsion of an Elliptic Curve Using Tate Normal Form.* Journal of Number Theory, Vol. 96, Issue 1 (2002), 76-88.

[27] J. Harris, *Algebraic geometry, a first curse.* Springer (1992).

[28] R. Hartshorne, *Algebraic Geometry.* Springer-Verlag (1977). Graduate Texts in Mathematic, No. 52.

[29] H. Hasse, *Zur Theorie der abstrakten elliptischen Funktionenkörper. I, II & III.* Crelle's Journal (1936) (175)

[30] D. R. Heath-Brown, *The Average Analytic Rank of Elliptic Curves.* Duke Math. J. Volume 122, Number 3 (2004), 591-623.

[31] Historical data on elliptic curve rank records.
`http://web.math.pmf.unizg.hr/~duje/tors/rankhist.html`

[32] D. Husemoller , *Elliptic curves.* Springer Verlag, New York (1987), pp 88-93.

[33] C. Ivorra Castillo, *Teoría de Números.*
`http://www.uv.es/~ivorra/Libros/Numeros.pdf`

[34] D. Jeon, CH. Kim, E. Park , *On the Torsion of Elliptic Curves Over Quartic Number Fields.* J. London Math. Soc. (2006) 74 (1): 1-12.

[35] D. Jeon, C.H. Kim, A. Schweizer, *On the torsion of elliptic curves over cubic number fields.* Acta Arith. 113 (2004), 291-301.

[36] S. Kamienny, *Torsion points on elliptic curves and q-coefficients of modular forms* Math. 109 (1992), 221-229.

[37] S. Kamienny, B. Mazur, *Rational Torsion of prime orden in elliptic curves over number fields.* Asterisque 228, 3 (1995), 81-100.

[38] S. Kamienny, F. Najman *Torsion groups of elliptic curves over quadratic fields.* Acta Arith. 152 (2012), 291-305.

[39] K. Kato, N. Kurokawa, T. Saito, *Number Theory 2: Introduction to Class Field Theory, Volumen 2.* The American mathematical Society, USA, 2011. Translations of Mathematical Monographs, volume 240.

[40] M. Kenku, F. Momose, *Torsion points on elliptic curves defined over quadratic fields.* Nagoya Mathematical Journal 109 (1988), 125-149.

[41] A.W. Knapp, *Elliptic Curves.* Princeton U. P., 1992.

[42] N. Koblitz, *Elliptic Curve Cryptosystems*, Mathematics of Computation, vol. 48, 1987, pp. 203-9.

[43] D. S. Kubert, *Universal bounds on the torsion of elliptic curves.* Compositio Mathematica, 38 no. 1 (1979), 121-128.

[44] S. Lang, *Elliptic curves: Diophantine analysis.* Volume 231 of Grundlehren der Mathematischen Wissenschaften. Springer-Verlag, Berlin, 1978.

[45] S. Lang, *Algebraic Number Theory*. Graduate Text in Mathematics, vol. 110. 3rd edition. Springer-Verlag, New York, 2002.

[46] B. Levi, *Sull'equazione indeterminata del 3^o ordine*. Atti del Congresso Internazionale dei matematici. Roma 2 (1908), 175-177.

[47] E. Lutz, *Sur léquation $y^2 = x^3 - Ax - B$ dans les corps p-adiques*. J. Reine Angew. Math.,1937, 177: 237-247.

[48] B. Mazur, *Modular curves and the Einsenstein Ideal*. I.H.E.S. Publ. Math. 47 (1977), 33-186.

[49] B. Mazur, *Rational Isogenies of Prime degree*. Invent. Math. 44 No. 2 (1978), 129-162.

[50] L. Merel, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres*. Invent. Math. 124 (1996), 437-449.

[51] J. F. Mestre, *Construction d'une courbe elliptique de rang* > 12. C. R. Acad. Sei. Paris, v. 295, 1982, pp. 643-644.

[52] V. S. Miller, *Use of Elliptic Curves in Cryptography*. H. C. Williams, Ed., Advances in Cryptology - CRYPTO, LNCS, vol. 218, 1985, Springer-Verlag, 1986, pp. 417-26.

[53] J. Milne, *Elliptic curves*. BookSurge Publishers (2006).

[54] J. Milne, *Algebraic Number Theory*, Curse notes (2011).
`http://www.jmilne.org/math/CourseNotes/ANTe6.pdf`

[55] L.J. Mordell, *On the rational solutions of the indeterminate equations of the third and fourth degrees*. Proc Cam. Phil. Soc. 21, (1922) p. 179.

[56] L. J. Mordell, *Diophantine equations. Volume 30*. Acedemic Press (1967).

[57] T. Nagell, *Solution de quelque problemes dans la theorie arithmetique des cubiques planes du premier genre*. Wid. Akad. Skrifter Oslo I, 1935, Nr. 1.

[58] F. Najman, *Complete classification of torsion of elliptic curves over quadratic cyclotomic fields*. J. Number Theory 130 (2010), 1964-1968.

[59] F. Najman, *Torsion of rational elliptic curves over cubic fields and sporadic points on* $X_1(n)$. Preprint, 2012

[60] A. Néron, *Problèmes arithmétiques et géometriques rattachés à la notion de rang d'une courbe algébraique dans un corps*. Bull. Soc. Math. France, v. 80, 1952, pp. 101-166.

[61] J. Oesterlé, *Torsion des courbes elliptiques sur les corps de nombres*. Unpublished.

[62] A. Ogg, *Rational point of finite order on elliptic curves*. Invent. Math. 12 (1971), 33-186.

[63] P. Parent, *Bornes effectives pour la torsion des courbes elliptiques sur les corps des nombres,* J. Reine Angrew. Math. 506 (1999), 85-116.

[64] P. Parent, *Torsion des courbes elliptiques sur les corps cubiques.* Ann. Inst. Fourier 50, 3 (2000), 723-749.

[65] P. Parent, *No 17-torsion on elliptic curves over cubic number fields.* J. Théor. Nombres Bordeaux 15 (2003), no. 3, 831-838.

[66] H. Poincar é, *Sur les propiétés arithmétiques des courbes algébriques.* Journal de mathématiques pures et appliquées 5e série, tome 7 (1901), p. 161-234.

[67] K. Ribet, *On modular representations of* $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ *arising from modular forms.* Inventiones mathematicae 100, (1990), (2): 431-471.

[68] K. Ribet, *From the Taniyama-Shimura conjecture to Fermat's last theorem.* Annales de la facultÃ© des sciences de Toulouse Sér. 5, 11 no. 1 (1990), p. 116-139.

[69] I. R. Shafarevich, J. Tate, *The rank of elliptic curves.* In Amer. Math. Soc. Transl., vol. 8, pgs. 917-920. Amer. Math. Soc., 1967.

[70] T. Shioda *An explicit algorithm for computing Picard number of certain algebraic surfaces.* Amer. J. Math., 108(2): 415-432, 1986.

[71] V. Shoup, *A Proposal for an ISO Standard for Public Key Encryption.* `http://www.shoup.net/papers/iso-2_1.pdf`, 2001

[72] C. L. Siegel, *Uber einige Anwendungen diophantischer Approximationen*, Abh. Preuss. Akad. Wiss. 1 (1929).

[73] J. H. Silverman, *The Arithmetic of Elliptic Curves*, 2nd edition. Graduate Texts in Mathematic, No. 106. Springer-Verlag, 2009.

[74] Joseph H. Silverman (1994), *Advanced Topics in the Arithmetic of Elliptic Curves.* Graduate Texts in Mathematics. 151. Springer-Verlag, 2009.

[75] W. A. Stein, *The Birch and Swinnerton-Dyer Conjecture, a Computational Approach.* Preliminar version. `http://modular.math.washington.edu/books/bsd/bsd.pdf`

[76] Y. Taguchi, *Discriminants and finiteness thorems in number theory.* `http://www2.math.kyushu-u.ac.jp/~taguchi/bib/taegu-var.pdf`

[77] M. Ulas, *On torsion points on an elliptic curve via division polynomials.* Universitatis Iagellonicae Acta Mathematica, Fasciculus XLIII, 2005.

[78] D. Ulmer, *Elliptic curves with large rank over function fields.* Ann. of Math.(2), 155(1): 295-315, 2002.

[79] L. C. Washington, *Elliptic Curves - Number Theory and Cryptography*. Chapman and Hall, 2003.

[80] A. Wiles, *Modular elliptic curves and Fermat's Last Theorem*. Annals of Mathematics 141, (1995), no. 3: 443-551

[81] M. P. Young, *Low-lying zeros of families of elliptic curves*. J. Amer. Math. Soc. 19 (2006), no. 1, 205-250.

[82] L. Z. Zhao, *Lecture notes on Local Fields*.
`http://www.srcf.ucam.org/~lzz20/local\_fields.pdf`