Elliptic Curves

In this Chapter we summarize the main aspects of the theory of elliptic curves[1]. Unfortunately, we will not be able to provide many of the proofs, because they are beyond the scope of this course.

2.1. Why elliptic curves?

A *Diophantine equation* is an equation given by a polynomial with integer coefficients, i.e.:

$$f(x_1, x_2, \ldots, x_r) = 0 \tag{2.1}$$

with $f(x_1, \ldots, x_r) \in \mathbb{Z}[x_1, \ldots, x_r]$. Since antiquity, many mathematicians have studied the solutions in integers of Diophantine equations that arise from a variety of problems in number theory, e.g. $y^2 = x^3 - n^2 x$ is the Diophantine equation related to the study of the congruent number problem (see Example 1.1.2).

Since we would like to systematically study the integer solutions of Diophantine equations, we ask ourselves three basic questions:

(a) Can we determine if Eq. (2.1) has any integral solutions, $x_i \in \mathbb{Z}$, or rational solutions, $x_i \in \mathbb{Q}$?

(b) If so, can we find any of the integral or rational solutions?

[1] The contents of this chapter are largely based on the article [**Loz05**], in Spanish.

(c) Finally, can we find *all* solutions and prove that we have found all of them?

The first question was proposed by David Hilbert: *to devise a process according to which it can be determined in a finite number of operations whether the equation is solvable in rational integers.* This was Hilbert's tenth problem, out of 23 fundamental questions that he proposed to the mathematical community during the Second International Congress of Mathematicians in Paris, in the year 1900. Surprisingly, in 1970, Matiyasevich, Putnam and Robinson discovered that there is no such general algorithm that decides whether equation (2.1) has integer solutions (see [**Mat93**]). However, if we restrict our attention to certain particular cases, then we can answer questions (a), (b) and (c) posed above. The most significant advances have been obtained in equations with one and two variables:

- *Polynomials in one variable*:

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n = 0$$

with $a_i \in \mathbb{Z}$. This case is fairly simple. The following criterion determines how to search for rational or integral roots of a polynomial: if $\frac{p}{q} \in \mathbb{Q}$ is a solution of $f(x) = 0$ then a_n is divisible by p and a_0 is divisible by q.

- *Linear equations in two variables*:

$$ax + by = d$$

with $a, b, d \in \mathbb{Z}$ and $ab \neq 0$. Clearly, this type of equation always has an infinite number of rational solutions. As for integral solutions, Euclid's algorithm (to find $\gcd(a, b)$) determines if there are solutions $x, y \in \mathbb{Z}$ and, if so, produces all solutions. In particular, the equation has integral solutions if and only if d is divisible by $\gcd(a, b)$.

- *Quadratic equations (conics)*:

$ax^2 + bxy + cy^2 + dx + ey = f$ with $a, b, c, d, e, f \in \mathbb{Z}$.

Finding integral and rational points on a conic is a classical problem. Legendre's criterion determines whether there are rational solutions: a conic C has rational solutions if and only if C has points over $\mathbb{Q}_p$, the p-adics, for all primes

$p \geq 2$ (see Appendix D for a brief introduction on the p-adics). Essentially, Legendre's criterion says that the conic has rational solutions if and only if there are solutions modulo p^n for all primes p and all $n \geq 1$ but, in practice, one only needs to check this for a finite number of primes that depends on the coefficients of the conic.

If C has rational points, and we have found at least one point, then we can find all the rational solutions using a *stereographic projection* (see Exercise 2.11.2). The integral points on C, however, are much more difficult to find. The problem is equivalent to finding integral solutions to *Pell's equation* $x^2 - Dy^2 = 1$. There are several methods to solve Pell's equation. For example, one can use continued fractions (certain convergents $\frac{x}{y}$ of the continued fraction for $\sqrt{D}$ are integral solutions (x, y) of Pell's equation; see Exercise 2.11.2).

- *Cubic equations*:

$$aX^3 + bX^2Y + cXY^2 + dY^3 + eX^2 + fXY + gY^2 + hX + jY + k = 0.$$

A cubic equation in two variables may have no rational solutions, only 1 rational solution, a finite number of solutions, or infinitely many solutions. Unfortunately, we do not know any algorithm that yields all rational solutions of a cubic equation although there are *conjectural* algorithms. In this chapter we will concentrate on this type of equation: a non-singular cubic, i.e. no self-intersections or pinches, with one rational point (which is, by definition, an elliptic curve).

- *Higher degree.* Typically, curves defined by an equation of degree ≥ 4 have a genus ≥ 2 (but some equations of degree 4 have genus 1, see Example 2.2.5 and Exercise 2.11.4). The genus is an invariant that classifies curves according to their topology. Briefly: if we consider a curve as defined over $\mathbb{C}$, then $C(\mathbb{C})$ may be considered as a surface over $\mathbb{R}$ and the genus of C counts the number of holes in the surface. For example $\mathbb{P}^1(\mathbb{C})$ has no holes and $g = 0$ (the projective plane is homeomorphic to a sphere), and an elliptic curve has genus

1 (homeomorphic to a torus, see Theorem 3.2.5). Surprisingly, the genus of a curve is intimately related with the arithmetic of its points. More precisely, Louis Mordell conjectured that a curve C of genus ≥ 2 can only have a finite number of rational solutions. The conjecture was proved by Faltings in 1983.

2.2. Definition

Definition 2.2.1. An *elliptic curve* over $\mathbb{Q}$ is a smooth cubic projective curve E defined over $\mathbb{Q}$, with at least one rational point $\mathcal{O} \in E(\mathbb{Q})$ that we call the *origin*.

In other words, an elliptic curve is a curve E in the projective plane (see Appendix C) given by a cubic polynomial $F(X, Y, Z) = 0$ with rational coefficients, i.e.

$$\begin{aligned} F(X,Y,Z) &= aX^3 + bX^2Y + cXY^2 + dY^3 \\ &\quad + eX^2Z + fXYZ + gY^2Z \\ &\quad + hXZ^2 + jYZ^2 + kZ^3 = 0, \end{aligned} \tag{2.2}$$

with coefficients $a, b, c, \ldots \in \mathbb{Q}$, and such that E is smooth, i.e. the tangent vector $\left(\frac{\partial F}{\partial X}(P), \frac{\partial F}{\partial Y}(P), \frac{\partial F}{\partial Z}(P)\right)$ does not vanish at any $P \in E$ (see Appendix C.5 for a brief introduction to singularities, and non-singular or smooth curves). If the coefficients $a, b, c, \ldots$ are in a field K, then we say that E is defined over K (and write E/K).

Even though the fact that E is a projective curve is crucial, we usually consider just affine charts of E, e.g. those points of the form $\{[X, Y, 1]\}$, and study instead the affine curve given by

$$\begin{aligned} &aX^3 + bX^2Y + cXY^2 + dY^3 \\ &+eX^2 + fXY + gY^2 + hX + jY + k = 0 \end{aligned} \tag{2.3}$$

but with the understanding that in this new model we may have left out some points of E *at infinity* (i.e. those points $[X, Y, 0]$ satisfying Eq. 2.2).

In general, one can find a change of coordinates that simplifies Eq. 2.3 enormously:

Proposition 2.2.2. *Let E be an elliptic curve, given by Eq. 2.2, defined over a field K of characteristic different from 2 or 3. Then there exists a curve $\widehat{E}$ given by*

$$zy^2 = x^3 + Axz^2 + Bz^3, \quad A, B \in K \quad \text{with} \quad 4A^3 + 27B^2 \neq 0$$

and an invertible change of variables $\psi : E \to \widehat{E}$ of the form:

$$\psi([X, Y, Z]) = \left[\frac{f_1(X, Y, Z)}{g_1(X, Y, Z)}, \frac{f_2(X, Y, Z)}{g_2(X, Y, Z)}, \frac{f_3(X, Y, Z)}{g_3(X, Y, Z)}\right]$$

where f_i and g_i are polynomials with coefficients in K, for $i = 1, 2, 3$, and the origin $\mathcal{O}$ is sent to the point $[0, 1, 0]$ of $\widehat{E}$, i.e. $\psi(\mathcal{O}) = [0, 1, 0]$.

The existence of such a change of variables is a consequence of the Riemann-Roch theorem of algebraic geometry (for a proof of the proposition see [Sil86], Chapter III.3). In [SiT92], Ch. I. 3, one can find an explicit method to find the change of variables $\psi : E \to \widehat{E}$. See also pages 46-49 of [Mil06].

A projective equation of the form $zy^2 = x^3 + Axz^2 + Bz^3$, or $y^2 = x^3 + Ax + B$ in affine coordinates, is called a *Weierstrass equation*. From now on, we will often work with an elliptic curve in this form. Notice that a curve E given by a Weierstrass equation $y^2 = x^3 + Ax + B$ is non-singular if and only if $4A^3 + 27B^2 \neq 0$, and it has a unique point at infinity, namely $[0, 1, 0]$, which we shall call the origin $\mathcal{O}$ or the point at infinity of E.

Sometimes we shall use a more general Weierstrass equation:

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

with $a_i \in \mathbb{Q}$ (we will explain the funky choice of notation for the coefficients later), but most of the time we will work with equations of the form $y^2 = x^3 + Ax + B$. It is easy to come up with a change of variables from one form to the other (see Exercise 2.11.3).

Example 2.2.3. Let $d \in \mathbb{Z}$, $d \neq 0$ and let E be the elliptic curve given by the cubic equation:

$$X^3 + Y^3 = dZ^3$$

with $\mathcal{O} = [1, -1, 0]$. The reader should verify that E is a smooth curve. We wish to find a Weierstrass equation for E and, indeed, one

can find a change of variables $\psi : E \to \widehat{E}$ given by:

$$\psi([X,Y,Z]) = [12dZ,\ 36d(X-Y),\ X+Y] = [x,y,z]$$

such that $zy^2 = x^3 - 432d^2z^3$. The map ψ is invertible, $\psi^{-1} : \widehat{E} \to E$ is:

$$\psi^{-1}([x,y,z]) = \left[\frac{36dz+y}{72d},\ \frac{36dz-y}{72d},\ \frac{x}{12d}\right].$$

In affine coordinates, the change of variables is going from $X^3+Y^3 = d$ to the curve $y^2 = x^3 - 432d^2$:

$$\begin{aligned}\psi(X,Y) &= \left(\frac{12d}{X+Y}, \frac{36d(X-Y)}{X+Y}\right),\\ \psi^{-1}(x,y) &= \left(\frac{36d+y}{6x}, \frac{36d-y}{6x}\right).\end{aligned}$$

■

Definition 2.2.4. Let $E : f(x,y) = 0$ be an elliptic curve with origin $\mathcal{O}$, and let $E' : g(X,Y) = 0$ be an elliptic curve with origin $\mathcal{O}'$. We say that E and E' are *isomorphic over* $\mathbb{Q}$ if there is an invertible change of variables $\psi : E \to E'$, defined by rational functions with coefficients in $\mathbb{Q}$, such that $\psi(\mathcal{O}) = \mathcal{O}'$.

Example 2.2.5. Sometimes, a curve given by a quartic polynomial can be isomorphic over $\mathbb{Q}$ to another curve given by a cubic polynomial. For instance, consider the curves

$$C/\mathbb{Q} : V^2 = U^4 + 1 \quad \text{and} \quad E/\mathbb{Q} : y^2 = x^3 - 4x.$$

The map $\psi : C \to E$ given by:

$$\psi(U,V) = \left(\frac{2(V+1)}{U^2}, \frac{4(V+1)}{U^3}\right)$$

is an invertible rational map, defined over $\mathbb{Q}$, that sends $(0,1)$ to $\mathcal{O}$, and $\psi(0,-1) = (0,0)$. See Exercise 2.11.4. More generally, any quartic

$$C : V^2 = aU^4 + bU^3 + cU^2 + dU + q^2,$$

for some $a,b,c,d,q \in \mathbb{Z}$, is isomorphic over $\mathbb{Q}$ to a curve of the form $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, also defined over $\mathbb{Q}$. The isomorphism is given in [**Was08**], Theorem 2.17, p. 37.

2.3. The group structure on $E(\mathbb{Q})$

Let E be an elliptic curve over $\mathbb{Q}$ given by a Weierstrass equation

$$E\colon y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad a_i \in \mathbb{Q}.$$

With a change of variables $(x, y) \mapsto (u^{-2}x,\ u^{-3}y)$ we can find the equation of an elliptic curve isomorphic to E given by

$$y^2 + (a_1u)xy + (a_3u^3)y = x^3 + (a_2u^2)x^2 + (a_4u^4)x + (a_6u^6)$$

with coefficients $a_iu^i \in \mathbb{Z}$, for $i = 1, 2, 3, 4, 6$. By the way, *this* is one of the reasons for the peculiar numbering of the coefficients a_i.

Example 2.3.1. Let E be given by $y^2 = x^3 + \frac{x}{2} + \frac{5}{3}$. We may change variables by $x = \frac{X}{6^2}$ and $y = \frac{Y}{6^3}$ to obtain a new equation $Y^2 = X^3 + 648X + 77760$ with integral coefficients. ■

In 1929, Siegel proved the following result about integral points, $E(\mathbb{Z})$, i.e. about those points on E with integer coordinates:

Theorem 2.3.2 (Siegel's theorem; [Sil86], Ch. IX, Thm. 3.1)**.** *Let $E/\mathbb{Q}$ be an elliptic curve given by $y^2 = x^3 + Ax + B$, with $A, B \in \mathbb{Z}$. Then E has only a finite number of integral points.*

Siegel's theorem is a consequence of a well-known theorem of Roth on diophantine approximation. Unfortunately, Siegel's theorem is not effective and does not provide neither a method to find the integral points on E, nor a bound on the number of integral points. However, in [Bak90], Alan Baker found an alternative proof that provides an explicit upper bound on the size of the coefficients of an integral solution. More concretely, if $x, y \in \mathbb{Z}$ satisfy $y^2 = x^3 + Ax + B$ then

$$\max(|x|, |y|) < \exp((10^6 \cdot \max(|A|, |B|))^{10^6}).$$

Obviously, Baker's bound is not a very sharp bound, but it is theoretically interesting nonetheless. From now on, we will concentrate on trying to find all rational points on a curve $E : y^2 = x^3 + Ax + B$. We will use the following notation for the rational points on E:

$$E(\mathbb{Q}) = \{(x, y) \in E \mid x, y \in \mathbb{Q}\} \cup \{\mathcal{O}\}$$

where $\mathcal{O} = [0, 1, 0]$ is the point at infinity.

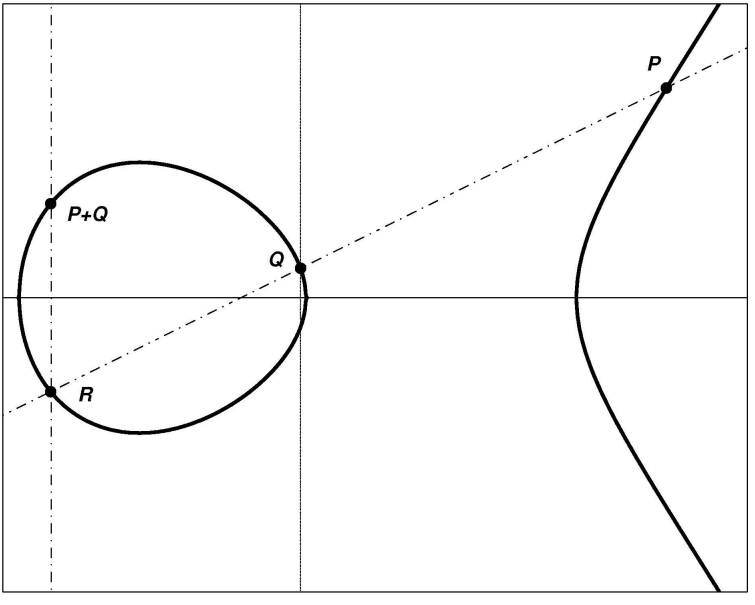

Figure 1. Addition of points on an elliptic curve

One of the aspects that makes the theory of elliptic curves so rich is that the set $E(\mathbb{Q})$ can be equipped with a group structure, geometric in nature. The (addition) operation on $E(\mathbb{Q})$ can be defined as follows (see Figure 1). Let E be given by a Weierstrass equation $y^2 = x^3 + Ax + B$ with $A, B \in \mathbb{Q}$. Let P and Q be two rational points in $E(\mathbb{Q})$ and let $\mathfrak{L} = \overline{PQ}$ be the line that goes through P and Q (if $P = Q$ then we define $\mathfrak{L}$ to be the tangent line to E at P). Since the curve E is defined by a cubic equation, and since we have defined $\mathfrak{L}$ so it already intersects E at two rational points, there must be a third point of intersection R in $\mathfrak{L} \cap E$, which is also defined over $\mathbb{Q}$, and

$$\mathfrak{L} \cap E(\mathbb{Q}) = \{P, Q, R\}.$$

The sum of P and Q, denoted by $P + Q$, is by definition the second point of intersection with E of the vertical line that goes through R, or in other words, the reflection of R across the x-axis.

Example 2.3.3. Let E be the elliptic curve $y^2 = x^3 - 25x$, as in Example 1.1.2. The points $P = (5, 0)$ and $Q = (-4, 6)$ belong to $E(\mathbb{Q})$. Let us find $P + Q$. First, we find the equation of the line $\mathfrak{L} = \overline{PQ}$. The slope must be

$$m = \frac{0-6}{5-(-4)} = -\frac{6}{9} = -\frac{2}{3}$$

and the line is $\mathfrak{L} : y = -\frac{2}{3}(x-5)$. Now we find the third point of intersection of $\mathfrak{L}$ and E by solving:

$$\begin{cases} y = -\frac{2}{3}(x-5) \\ y^2 = x^3 - 25x. \end{cases}$$

Plugging the first equation in the second one, we obtain an equation

$$x^3 - \frac{4}{9}x^2 - \frac{185}{9}x - \frac{100}{9} = 0$$

which factors as $(x-5)(x+4)(9x+5) = 0$. The first two factors are expected, since we already knew that $P = (5, 0)$ and $Q = (-4, 6)$ are in $\mathfrak{L} \cap E$. The third point of intersection must have $x = -\frac{5}{9}$, $y = -\frac{2}{3}(x-5) = \frac{100}{27}$ and, indeed, $R = (-\frac{5}{9}, \frac{100}{27})$ is a point in $\mathfrak{L} \cap E(\mathbb{Q})$. Thus, $P + Q$ is the reflection of R accross the x-axis, i.e. $P + Q = (-\frac{5}{9}, -\frac{100}{27})$.

Using Proposition 1.1.3, we may try to use the point $P + Q = (-\frac{5}{9}, -\frac{100}{27})$ to find a (new) right triangle with rational sides and area equal to 5, but this point corresponds to the triangle $(\frac{20}{3}, \frac{3}{2}, \frac{41}{6})$, the same triangle that corresponds to $Q = (-4, 6)$. In order to find a new triangle, let us find $Q + Q = 2Q$.

The line $\mathfrak{L}$ in this case is the tangent line to E at Q. The slope of $\mathfrak{L}$ can be found using implicit differentiation on $y^2 = x^3 - 25x$:

$$2y\frac{dy}{dx} = 3x^2 - 25, \quad \text{so} \quad \frac{dy}{dx} = \frac{3x^2 - 25}{2y}.$$

Hence, the slope of $\mathfrak{L}$ is $m = \frac{23}{12}$ and $\mathfrak{L} : y = \frac{23}{12}(x+4) + 6$. In order to find R we need to solve:

$$\begin{cases} y = \frac{23}{12}(x+4) + 6 \\ y^2 = x^3 - 25x. \end{cases}$$

Simplifying yields $x^3 - \frac{529}{144}x^2 - \frac{1393}{18}x - \frac{1681}{9} = 0$, which factors as

$$(x+4)^2(144x - 1681) = 0.$$

Once again, two factors were expected: $x = -4$ *needs* to be a double root because $\mathfrak{L}$ is *tangent* to E at $Q = (-4, 6)$. The third factors tells us that the x coordinate of R is $x = \frac{1681}{144}$, and $y = \frac{23}{12}(x+4) + 6 = \frac{62279}{1728}$. Thus, $Q + Q = 2Q = (\frac{1681}{144}, -\frac{62279}{1728})$. This point corresponds to the right triangle:

$$(a, b, c) = \left(\frac{1519}{492}, \frac{4920}{1519}, \frac{3344161}{747348}\right).$$

■

Example 2.3.4. Let $E : y^2 = x^3 + 1$ and put $P = (2, 3)$. Let us find P, $2P$, $3P$, etc:

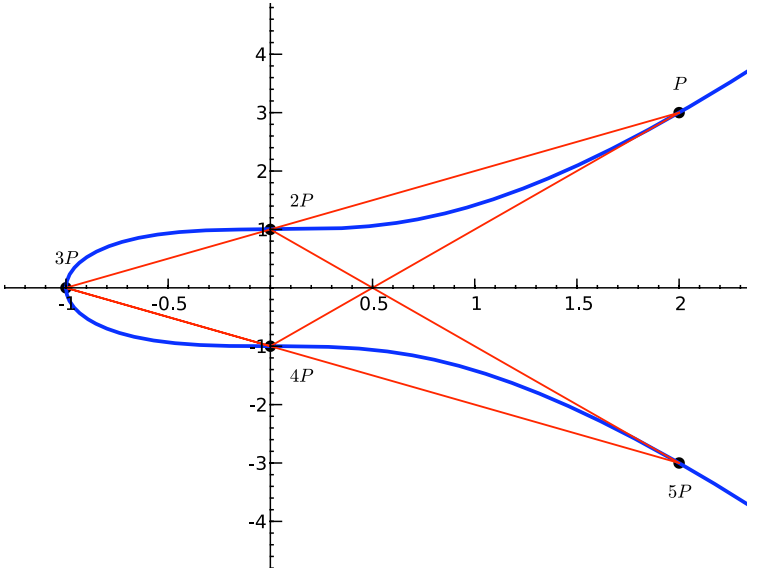

Figure 2. The rational points on $y^2 = x^3 + 1$, except the point at ∞.

- In order to find $2P$, first we need to find the tangent line to E at P, which is $y - 3 = 2(x - 2)$ or $y = 2x - 1$. The third point of intersection is $R = (0, -1)$ so $2P = (0, 1)$.

- To find $3P$, we add P and $2P$. The third point of intersection of E with the line that goes through P and $2P$ is $R' = (-1, 0)$, hence $3P = (-1, 0)$.
- The point $4P$ can be found by adding $3P$ and P. The third point of intersection of E and the line through P and $3P$ is $R'' = 2P = (0, 1)$, and so $4P = P + 3P = (0, -1)$.
- We find $5P$ by adding $4P$ and P. Notice that the line that goes through $4P = (0, -1)$ and $P = (2, 3)$ is tangent at $(2, 3)$, so the third point of intersection is P. Thus, $5P = 4P + P = (2, -3)$.
- Finally, $6P = P + 5P$ but $5P = (2, -3) = -P$. Hence, $6P = P + (-P) = \mathcal{O}$, the point at infinity.

This means that P is a point of finite order, and its order equals 6. See Figure 2 (the SAGE code for this graph can be found in the Appendix A.1.3). ■

The addition law can be defined more generally on any smooth projective cubic curve $E : f(X, Y, Z) = 0$, with a given rational point $\mathcal{O}$. Let $P, Q \in E(\mathbb{Q})$ and let $\mathfrak{L}$ be the line that goes through P and Q. Let R be the third point of intersection of $\mathfrak{L}$ and E. Then R is also a rational point in $E(\mathbb{Q})$. Let $\mathfrak{L}'$ be the line through R and $\mathcal{O}$. We define $P + Q$ to be the third point of intersection of $\mathfrak{L}'$ and E. Notice that any vertical line $x = a$ in the affine plane passes through $[0, 1, 0]$, because the same line in projective coordinates is given by $x = az$ and $[0, 1, 0]$ belongs to such line. Thus, if E is given by a model $y^2 = x^3 + Ax + B$ then $\mathfrak{L}'$ is always a vertical line, so $P + Q$ is always the reflection of R with respect to the x axis.

It is easy to verify that the addition operation that we have defined on points of $E(\mathbb{Q})$ is commutative. The origin $\mathcal{O}$ is the zero element, and for every $P \in E(\mathbb{Q})$ there exists a point $-P$ such that $P + (-P) = \mathcal{O}$. If E is given by $y^2 = x^3 + Ax + B$ and $P = (x_0, y_0)$ then $-P = (x_0, -y_0)$. The addition is also associative (but this is not obvious, and tedious to prove) and, therefore, $(E, +)$ is an abelian group.

The next step in the study of the structure of $E(\mathbb{Q})$ was proved by Mordell in 1922, and generalized by André Weil in his thesis, in 1928:

Theorem 2.3.5 (Mordell-Weil)**.** *$E(\mathbb{Q})$ is a finitely generated abelian group. In other words, there are points $P_1, \ldots, P_n$ such that any other point Q in $E(\mathbb{Q})$ can be expressed as a linear combination*

$$Q = a_1P_1 + a_2P_2 + \cdots + a_nP_n$$

for some $a_i \in \mathbb{Z}$.

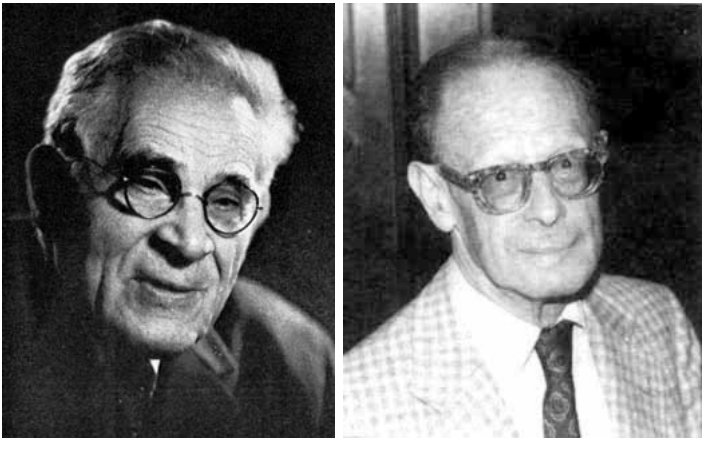

Figure 3. Louis Mordell (1888-1972) and André Weil (1906-1998).

The group $E(\mathbb{Q})$ is usually called the Mordell-Weil group of E, in honor of the two mathematicians that proved the theorem. The proof of the theorem has three fundamental ingredients: the so-called *weak* Mordell-Weil theorem ($E(\mathbb{Q})/mE(\mathbb{Q})$ is finite, for any $m \geq 2$; see below); the concept of height functions on abelian groups and the *descent theorem*, which establishes that an abelian group A with a height function h, such that A/mA is finite (for some $m \geq 2$), is finitely generated.

Theorem 2.3.6 (weak Mordell-Weil)**.** *$E(\mathbb{Q})/mE(\mathbb{Q})$ is a finite group for all $m \geq 2$.*

We will discuss the proof of a special case of the weak Mordell-Weil theorem in Section 2.8 (see Corollary 2.8.7).

It follows from the Mordell-Weil theorem and the general structure theory of finitely generated abelian groups that

$$E(\mathbb{Q}) \cong E(\mathbb{Q})_{\text{torsion}} \oplus \mathbb{Z}^{R_E}. \tag{2.4}$$

In other words, $E(\mathbb{Q})$ is isomorphic to the direct sum of two abelian groups (notice however that this decomposition *is not* canonical!). The first summand is a finite group formed by all *torsion* elements, i.e. those points on E of finite order:

$$E(\mathbb{Q})_{\text{torsion}} = \{P \in E(\mathbb{Q}) : \text{ there is } n \in \mathbb{N} \text{ such that } nP = \mathcal{O}\}.$$

The second summand of Eq. (2.4), sometimes called the *free part*, is $\mathbb{Z}^{R_E}$, i.e. R_E copies of $\mathbb{Z}$, for some integer $R_E \geq 0$. It is generated by R_E points of $E(\mathbb{Q})$ of infinite order (i.e. $P \in E(\mathbb{Q})$ such that $nP \neq \mathcal{O}$ for all non-zero $n \in \mathbb{Z}$). The number R_E is called the *rank* of the elliptic curve $E/\mathbb{Q}$. Notice, however, that the set

$$F = \{P \in E(\mathbb{Q}) : P \text{ is of infinite order}\} \cup \{\mathcal{O}\}$$

is not a subgroup of $E(\mathbb{Q})$ if the torsion subgroup is non-trivial. For instance, if T is a torsion point and P is of infinite order, then P and $P+T$ belong to F but $T = (P+T) - P$ does not belong to F. This fact makes the isomorphism of Eq. (2.4) not canonical because the subgroup of $E(\mathbb{Q})$ isomorphic to $\mathbb{Z}^{R_E}$ cannot be chosen, in general, in a unique way.

Example 2.3.7. The following are some examples of elliptic curves and their Mordell-Weil groups:

(1) The curve $E_1/\mathbb{Q} : y^2 = x^3 + 6$ has no rational points, other than the point at infinity $\mathcal{O}$. Therefore, there are no torsion points (other than $\mathcal{O}$) and no points of infinite order. In particular, the rank is 0, and $E_1(\mathbb{Q}) = \{\mathcal{O}\}$.

(2) The curve $E_2/\mathbb{Q} : y^2 = x^3 + 1$ has only 6 rational points. As we saw in Example 2.3.4, the point $P = (2, 3)$ has exact order 6. Therefore $E_2(\mathbb{Q}) \cong \mathbb{Z}/6\mathbb{Z}$ is an isomorphism of groups. Since there are no points of infinite order, the rank

of $E_2/\mathbb{Q}$ is 0, and

$$E_2(\mathbb{Q}) = \{\mathcal{O},\ P,\ 2P,\ 3P,\ 4P,\ 5P\} = \{\mathcal{O}, (2, \pm 3), (0, \pm 1), (-1, 0)\}.$$

(3) The curve $E_3/\mathbb{Q} : y^2 = x^3 - 2$ does not have any rational torsion points other than $\mathcal{O}$ (as we shall see in the next section). However, the point $P = (3, 5)$ is a rational point. Thus, P must be a point of infinite order and $E_3(\mathbb{Q})$ contains infinitely many distinct rational points. In fact, the rank of E_3 is equal to 1 and P is a generator of all of $E_3(\mathbb{Q})$, i.e.

$$E_3(\mathbb{Q}) = \{nP : n \in \mathbb{Z}\} \quad \text{and} \quad E_3(\mathbb{Q}) \cong \mathbb{Z}.$$

(4) The elliptic curve $E_4/\mathbb{Q} : y^2 = x^3 + 7105x^2 + 1327104x$ features both torsion and infinite order points. In fact, $E_4(\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}^3$. The torsion subgroup is generated by the point $T = (1152, 111744)$ of order 4. The free part is generated by three points of infinite order:

$$P_1 = (-6912, 6912),\ P_2 = (-5832, 188568),\ P_3 = (-5400, 206280).$$

Hence

$$E_4(\mathbb{Q}) = \{aT + bP_1 + cP_2 + dP_3 : a = 0, 1, 2 \text{ or } 3 \text{ and } b, c, d \in \mathbb{Z}\}.$$

As we mentioned above, the isomorphism $E_4(\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}^3$ is not canonical. For instance, $E_4(\mathbb{Q}) \cong \langle T \rangle \oplus \langle P_1, P_2, P_3 \rangle$ but also $E_4(\mathbb{Q}) \cong \langle T \rangle \oplus \langle P_1', P_2, P_3 \rangle$ with $P_1' = P_1 + T$.

■

The rank of $E/\mathbb{Q}$ is, in a sense, a measurement of the arithmetic complexity of the elliptic curve. It is not known if there is an upper bound for the possible values of R_E (the largest rank known is 28, discovered by Noam Elkies; see Andrej Dujella's website [**Duj09**] for up to date records and examples of curves with "high" ranks). It has been conjectured (with some controversy) that ranks can be arbitrarily large, i.e. for all $n \in \mathbb{N}$ there exists an elliptic curve E over $\mathbb{Q}$ with $R_E \geq n$. One of the key pieces of evidence in favor of such a conjecture was offered by Shafarevich and Tate, who proved that there exist elliptic curves defined over function fields $\mathbb{F}_p(T)$ and with arbitrarily large ranks ($\mathbb{F}_p(T)$ is a field that shares many similar properties with $\mathbb{Q}$; see [**ShT67**]). In any case, the problem of finding elliptic curves

of high rank is particularly interesting because of its arithmetic and computational complexity.

2.4. The torsion subgroup

In this section we concentrate on the torsion points of an elliptic curve:

$$E(\mathbb{Q})_{\text{torsion}} = \{P \in E(\mathbb{Q}) : \text{ there is } n \in \mathbb{N} \text{ such that } nP = \mathcal{O}\}.$$

Example 2.4.1. The curve $E_n : y^2 = x^3 - n^2x = x(x-n)(x+n)$ has three obvious rational points, namely $P = (0,0), Q = (-n,0), T = (n,0)$, and it is easy to check (see Exercise 2.11.6) that each one of these points is torsion of order 2, i.e. $2P = 2Q = 2T = \mathcal{O}$, and $P + Q = T$. In fact:

$$E_n(\mathbb{Q})_{\text{torsion}} = \{\mathcal{O}, P, Q, T\} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}.$$

■

Note that the Mordell-Weil theorem implies that $E(\mathbb{Q})_{\text{torsion}}$ is always finite. This fact prompts a natural question: *what abelian groups can appear in this context?* The answer was conjectured by Ogg and proven by Mazur:

Theorem 2.4.2 (Ogg's conjecture; Mazur, [Maz77], [Maz78])**.** *Let $E/\mathbb{Q}$ be an elliptic curve. Then, $E(\mathbb{Q})_{torsion}$ is isomorphic to exactly one of the following groups:*

$$\begin{aligned} &\mathbb{Z}/N\mathbb{Z} \quad \textit{with} \quad 1 \le N \le 10 \textit{ or } N = 12, \textit{ or} \\ &\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2M\mathbb{Z} \quad \textit{with} \quad 1 \le M \le 4. \end{aligned} \tag{2.5}$$

Example 2.4.3. For instance, the torsion subgroup of the elliptic curve with Weierstrass equation $y^2 + 43xy - 210y = x^3 - 210x^2$ is isomorphic to $\mathbb{Z}/12\mathbb{Z}$ and it is generated by the point $(0, 210)$. The elliptic curve $y^2 + 17xy - 120y = x^3 - 60x^2$ has a torsion subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/8\mathbb{Z}$, generated by the rational points $(30, -90)$ and $(-40, 400)$. See Figure 4 for a complete list of examples with each possible torsion subgroup. ■

Furthermore, it is known that, if G is any of the groups in Eq. 2.5, there are infinitely many elliptic curves whose torsion subgroup is

Curve	Torsion	Generators
$y^2 = x^3 - 2$	trivial	$\mathcal{O}$
$y^2 = x^3 + 8$	$\mathbb{Z}/2\mathbb{Z}$	$(-2, 0)$
$y^2 = x^3 + 4$	$\mathbb{Z}/3\mathbb{Z}$	$(0, 2)$
$y^2 = x^3 + 4x$	$\mathbb{Z}/4\mathbb{Z}$	$(2, 4)$
$y^2 - y = x^3 - x^2$	$\mathbb{Z}/5\mathbb{Z}$	$(0, 1)$
$y^2 = x^3 + 1$	$\mathbb{Z}/6\mathbb{Z}$	$(2, 3)$
$y^2 = x^3 - 43x + 166$	$\mathbb{Z}/7\mathbb{Z}$	$(3, 8)$
$y^2 + 7xy = x^3 + 16x$	$\mathbb{Z}/8\mathbb{Z}$	$(-2, 10)$
$y^2 + xy + y = x^3 - x^2 - 14x + 29$	$\mathbb{Z}/9\mathbb{Z}$	$(3, 1)$
$y^2 + xy = x^3 - 45x + 81$	$\mathbb{Z}/10\mathbb{Z}$	$(0, 9)$
$y^2 + 43xy - 210y = x^3 - 210x^2$	$\mathbb{Z}/12\mathbb{Z}$	$(0, 210)$
$y^2 = x^3 - 4x$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$	$\binom{(2,0)}{(0,0)}$
$y^2 = x^3 + 2x^2 - 3x$	$\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$	$\binom{(3,6)}{(0,0)}$
$y^2 + 5xy - 6y = x^3 - 3x^2$	$\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$	$\binom{(-3,18)}{(2,-2)}$
$y^2 + 17xy - 120y = x^3 - 60x^2$	$\mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$	$\binom{(30,-90)}{(-40,400)}$

Figure 4. Examples of each of the possible torsion subgroups over $\mathbb{Q}$.

isomorphic to G. See, for example, [**Kub76**], Table 3, p. 217. For the convenience of the reader, the table in Kubert's article is reproduced in Appendix E.

Example 2.4.4. Let $E_b : y^2 + (1-b)xy - by = x^3 - bx^2$ with $b \in \mathbb{Q}$ and $\Delta(b, c) = b^5(b^2 - 11b - 1) \neq 0$. Then, the torsion subgroup of $E_b(\mathbb{Q})$ contains a subgroup isomorphic to $\mathbb{Z}/5\mathbb{Z}$, and $(0, 0)$ is a point of exact order 5. Conversely, if $E : y^2 = x^3 + Ax + B$ is an elliptic curve with torsion subgroup equal to $\mathbb{Z}/5\mathbb{Z}$ then there is an invertible change of variables that takes E to an equation of the form E_b, for some $b \in \mathbb{Q}$. ■

A useful and simple consequence of Mazur's theorem is that if the order of a rational point $P \in E(\mathbb{Q})$ is larger than 12, then P must be a point of infinite order and, therefore, $E(\mathbb{Q})$ contains an infinite number of distinct rational points. Except for this criterion, Mazur's theorem is not very helpful in effectively computing the torsion subgroup of a given elliptic curve. However, the following result, proven

independently by E. Lutz and T. Nagell, provides a simple algorithm to determine $E(\mathbb{Q})_{\text{torsion}}$:

Theorem 2.4.5 (Nagell-Lutz, [Nag35], [Lut37]). *Let $E/\mathbb{Q}$ be an elliptic curve with Weierstrass equation*

$$y^2 = x^3 + Ax + B, \quad A, B \in \mathbb{Z}.$$

Then, every torsion point $P \neq \mathcal{O}$ of E satisfies:

(1) *The coordinates of P are integers, i.e. $x(P), y(P) \in \mathbb{Z}$.*

(2) *If P is a point of order $n \geq 3$ then $4A^3 + 27B^2$ is divisible by $y(P)^2$.*

(3) *If P is of order 2 then $y(P) = 0$ and $x(P)^3 + Ax(P) + B = 0$.*

For a proof, see [Sil86], Ch. VIII, Corollary 7.2, or [Mil06], Ch. II, Theorem 5.1.

Example 2.4.6. Let $E/\mathbb{Q} : y^2 = x^3 - 2$, so that $A = 0$ and $B = -2$. The polynomial $x^3 - 2$ does not have any rational roots, so $E(\mathbb{Q})$ does not contain any points of order 2. Also, $4A^3 + 27B^2 = 27 \cdot 4$. Thus, if $(x(P), y(P))$ are the coordinates of a torsion point in $E(\mathbb{Q})$ then $y(P)$ is an integer and $y(P)^2$ divides $27 \cdot 4$. This implies that $y(P) = \pm 1$, ± 2, ± 3, or ± 6. In turn, this implies that $x(P)^3 = 3$, 6, 11 or 38, respectively. However, $x(P)$ is an integer, and none of 3, 6, 11 or 38 is a perfect cube. Thus, $E(\mathbb{Q})_{\text{torsion}}$ is trivial (i.e. the only torsion point is $\mathcal{O}$).

Example 2.4.7. Let $p \geq 2$ be a prime number and let us define a curve $E_p : y^2 = x^3 + p^2$. Since $x^3 + p^2 = 0$ does not have any rational roots, $E_p(\mathbb{Q})$ does not contain points of order 2. Let P be a torsion point on $E_p(\mathbb{Q})$. The list of all squares dividing $4A^3 + 27B^2 = 27p^4$ is short, and by the Nagell-Lutz theorem the possible values for $y(P)$ are:

$$y = \pm 1, \ \pm p, \ \pm p^2, \ \pm 3p, \ \pm 3p^2, \text{ and } \pm 3.$$

Clearly, $(0, \pm p) \in E_p(\mathbb{Q})$ and one can show that those two points and $\mathcal{O}$ are the only torsion points - see Exercise 2.11.8. Thus, the torsion subgroup of $E_p(\mathbb{Q})$ is isomorphic to $\mathbb{Z}/3\mathbb{Z}$, for any prime $p \geq 2$. ■

2.5. Elliptic curves over finite fields

Let $p \geq 2$ be a prime and let $\mathbb{F}_p$ be the finite field with p elements, i.e.

$$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} = \{a \bmod p : a = 0, 1, 2, \ldots, p-1\}.$$

$\mathbb{F}_p$ is a field and we may consider elliptic curves defined over $\mathbb{F}_p$. As for elliptic curves over $\mathbb{Q}$, there are two conditions that need to be satisfied: the curve needs to be given by a cubic equation, and the curve needs to be smooth.

Example 2.5.1. For instance, $E : y^2 \equiv x^3 + 1 \bmod 5$ is an elliptic curve defined over $\mathbb{F}_5$. It is clearly given by a cubic equation ($zy^2 \equiv x^3 + z^3 \bmod 5$ in the projective plane $\mathbb{P}^2(\mathbb{F}_5)$) and it is smooth, because for $F \equiv zy^2 - x^3 - z^3 \bmod 5$ the partial derivatives are:

$$\frac{\partial F}{\partial x} \equiv -3x^2, \quad \frac{\partial F}{\partial y} \equiv 2yz, \quad \frac{\partial F}{\partial z} \equiv y^2 - 3z^2 \bmod 5.$$

Thus, if the partial derivatives are congruent to 0 modulo 5, then $x \equiv 0 \bmod 5$ and $yz \equiv 0 \bmod 5$. The latter congruence implies that y or $z \equiv 0 \bmod 5$, and $\partial F/\partial z \equiv 0$ implies that $y \equiv z \equiv 0 \bmod 5$. Since $[0, 0, 0]$ is not a point in the projective plane, we conclude that there are no singular points on $E/\mathbb{F}_5$.

However, $C/\mathbb{F}_3 : y^2 \equiv x^3 + 1 \bmod 3$ is not an elliptic curve because it is not smooth. Indeed, the point $P = (2 \bmod 3, 0 \bmod 3) \in C(\mathbb{F}_3)$ is a singular point:

$$\begin{aligned} \frac{\partial F}{\partial x}(P) &\equiv -3 \cdot 2^2 \equiv 0, \quad \frac{\partial F}{\partial y}(P) \equiv 2 \cdot 0 \cdot 1 \equiv 0, \quad \text{and} \\ \frac{\partial F}{\partial z}(P) &\equiv 0^2 - 3 \cdot 1^2 \equiv 0 \bmod 3. \end{aligned}$$

■

Let $E/\mathbb{Q}$ be an elliptic curve given by a Weierstrass equation $y^2 = x^3 + Ax + B$ with integer coefficients $A, B \in \mathbb{Z}$, and let $p \geq 2$ be a prime number. If we reduce A and B modulo p then we obtain the equation of a curve $\widetilde{E}$ given by a cubic curve and defined over the field $\mathbb{F}_p$. Even though E is smooth as a curve over $\mathbb{Q}$, the curve $\widetilde{E}$ may be singular over $\mathbb{F}_p$. In the previous example, we saw that $E/\mathbb{Q} : y^2 = x^3 + 1$ is smooth over $\mathbb{Q}$ and $\mathbb{F}_5$ but it has a singularity

over $\mathbb{F}_3$. If the reduction curve $\widetilde{E}$ is smooth, then it is an elliptic curve over $\mathbb{F}_p$.

Example 2.5.2. Sometimes the reduction of a model for an elliptic curve E modulo a prime p is not smooth, but it is smooth for some other models of E. For instance, consider the curve $E : y^2 = x^3 + 15625$. Then $\widetilde{E} \equiv E \bmod 5$ is not smooth over $\mathbb{F}_5$ because the point $(0, 0) \bmod 5$ is a singular point. However, using the invertible change of variables $(x, y) \mapsto (5^2X, 5^3Y)$ we obtain a new model over $\mathbb{Q}$ for E given by $E' : Y^2 = X^3 + 1$, which is smooth when we reduce it modulo 5. The problem here is that the model we chose for E is not *minimal*. We describe what we mean by minimal next. ■

Definition 2.5.3. Let E be an elliptic curve given by $y^2 = x^3 + Ax + B$, with $A, B \in \mathbb{Q}$.

(1) We define Δ_E, the *discriminant* of E, by

$$\Delta_E = -16(4A^3 + 27B^2).$$

For a definition of the discriminant for more general Weierstrass equations, see for example [Sil86], p. 46.

(2) Let S be the set of all elliptic curves E' that are isomorphic to E over $\mathbb{Q}$ (see Definition 2.2.4), and such that the discriminant of E' is an integer. The *minimal discriminant* of E is the integer $\Delta_{E'}$ that attains the minimum of the set $\{|\Delta_{E'}| : E' \in S\}$. In other words, the minimal discriminant is the smallest integral discriminant (in absolute value) of an elliptic curve that is isomorphic to E over $\mathbb{Q}$. If E' is the model for E with minimal discriminant, we say that E' is a *minimal model* for E.

Example 2.5.4. The curve $E : y^2 = x^3 + 5^6$ has discriminant $\Delta_E = -2^4 3^3 5^{12}$ and the curve $E' : y^2 = x^3 + 1$ has discriminant $\Delta_{E'} = -2^4 3^3$. Since E and E' are isomorphic (see Definition 2.2.4 and Example 2.5.2), then Δ_E cannot be the minimal discriminant for E and $y^2 = x^3 + 5^6$ is not a minimal model. In fact, the minimal discriminant is $\Delta_{E'} = -432$ and E' is a minimal model. ■

Before we go on to describe the types of reduction one can encounter, we need a little bit of background on types of singularities.

Let $\widetilde{E}$ be a cubic curve over a field K with Weierstrass equation $f(x,y)=0$, where:

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

and suppose that $\widetilde{E}$ has a singular point $P=(x_0,y_0)$, i.e. $\partial f/\partial x(P)=\partial f/\partial y(P)=0$. Thus, we can write the Taylor expansion of $f(x,y)$ around (x_0,y_0) as follows:

$$\begin{aligned} & f(x,y)-f(x_0,y_0) \\ = \;& \lambda_1(x-x_0)^2+\lambda_2(x-x_0)(y-y_0)+\lambda_3(y-y_0)^2-(x-x_0)^3 \\ = \;& ((y-y_0)-\alpha(x-x_0))\cdot((y-y_0)-\beta(x-x_0))-(x-x_0)^3 \end{aligned}$$

for some $\lambda_i\in K$ and $\alpha,\beta\in\bar{K}$ (an algebraic closure of K).

Definition 2.5.5. The singular point $P\in\widetilde{E}$ is a *node* if $\alpha\neq\beta$. In this case there are two different tangent lines to $\widetilde{E}$ at P, namely:

$$y-y_0=\alpha(x-x_0),\quad y-y_0=\beta(x-x_0)$$

If $\alpha=\beta$ then we say that P is a *cusp*, and there is a unique tangent line at P.

Definition 2.5.6. Let $E/\mathbb{Q}$ be an elliptic curve given by a minimal model, let $p\geq 2$ be a prime and let $\widetilde{E}$ be the reduction curve of E modulo p. We say that $E/\mathbb{Q}$ has *good reduction* modulo p if $\widetilde{E}$ is a smooth elliptic curve over $\mathbb{F}_p$. If $\widetilde{E}$ is singular at a point $P\in E(\mathbb{F}_p)$ then we say that $E/\mathbb{Q}$ has bad reduction at p and we distinguish two cases:

(1) If $\widetilde{E}$ has a cusp at P, then we say that E has *additive (or unstable) reduction.*

(2) If $\widetilde{E}$ has a node at P then we say that E has *multiplicative (or semistable) reduction.* If the slopes of the tangent lines (α and β as above) are in $\mathbb{F}_p$ then the reduction is said to be *split* multiplicative (and *non-split* otherwise).

Example 2.5.7. (1) $E_1\colon y^2=x^3+35x+5$ has good reduction at $p=7$, because $y^2\equiv x^3+5 \bmod 7$ is a non-singular curve over $\mathbb{F}_7$.

(2) However E_1 has bad reduction at $p = 5$, and the reduction is additive, since modulo 5 we can write the equation as $((y-0) - 0 \cdot (x-0))^2 - x^3$ and the unique slope is 0.

(3) The elliptic curve $E_2 \colon y^2 = x^3 - x^2 + 35$ has bad multiplicative reduction at 5 and 7. The reduction at 5 is split, while the reduction at 7 is non-split. Indeed, modulo 5 we can write the equation as

$$((y-0) - 2(x-0)) \cdot ((y-0) + 2(x-0)) - x^3,$$

the slopes being 2 and -2. However, for $p = 7$ the slopes are not in $\mathbb{F}_7$ (because -1 is not a quadratic residue in $\mathbb{F}_7$). Indeed, when we reduce the equation modulo 7 we obtain

$$y^2 + x^2 - x^3 \bmod 7$$

and $y^2 + x^2$ can only be factored in $\mathbb{F}_7[i]$ but not in $\mathbb{F}_7$.

(4) Let E_3 be an elliptic curve given by the model $y^2 + y = x^3 - x^2 - 10x - 20$. This is a miminal model for E_3 and its (minimal) discriminant is $\Delta_{E_3} = -11^5$. The prime 11 is the unique prime of bad reduction and the reduction is split multiplicative. Indeed, the point $(5, 5) \bmod 11$ is a singular point on $E_3(\mathbb{F}_{11})$ and

$$\begin{aligned} f(x,y) &= y^2 + y + x^2 + 10x + 20 - x^3 \\ &= (y - 5 - 5(x-5)) \cdot (y - 5 + 5(x-5)) - (x-5)^3. \end{aligned}$$

Hence, the slopes at $(5, 5)$ are 5 and -5, which are obviously in $\mathbb{F}_{11}$ and distinct.

■

Proposition 2.5.8. *Let K be a field and let E/K be a cubic curve given by $y^2 = f(x)$, where $f(x)$ is a monic cubic polynomial in $K[x]$. Suppose that $f(x) = (x-\alpha)(x-\beta)(x-\gamma)$ with $\alpha, \beta, \gamma \in \overline{K}$ (an algebraic closure of K) and put*

$$D = (\alpha - \beta)^2 (\alpha - \gamma)^2 (\beta - \gamma)^2.$$

Then E is non-singular if and only if $D \neq 0$.

The proof of the proposition is left as an exercise (see Exercise 2.11.9). Notice that the quantity D that appears in the previous

proposition is the *discriminant* of the polynomial $f(x)$. The discriminant of $E/\mathbb{Q}$, Δ_E as in Definition 2.5.3, is a multiple of D, in fact $\Delta_E = 16D$. This fact together with Proposition 2.5.8 yield the following corollary:

Corollary 2.5.9. *Let $E/\mathbb{Q}$ be an elliptic curve with coefficients in $\mathbb{Z}$. Let $p \geq 2$ be a prime. If E has bad reduction at p then $p \mid \Delta_E$. In fact, if E is given by a minimal model, then $p \mid \Delta_E$ if and only if E has bad reduction at p.*

Example 2.5.10. The discriminant of the elliptic curve $E_1 \colon y^2 = x^3 + 35x + 5$ of Example 2.5.7 is $\Delta_{E_1} = -2754800 = -2^4 \cdot 5^2 \cdot 71 \cdot 97$ (and, in fact, this is the minimal discriminant of E_1). Thus, E_1 has good reduction at 7 but it has bad reduction at 2, 5, 71 and 97. The reduction at 71 and 97 is multiplicative. ■

Let $\widetilde{E}$ be an elliptic curve defined over a finite field $\mathbb{F}_q$ with q elements, where $q = p^r$ and $p \geq 2$ is prime. Notice that $\widetilde{E}(\mathbb{F}_q) \subseteq \mathbb{P}^2(\mathbb{F}_q)$, and the projective plane over $\mathbb{F}_q$ only has a finite number of points (how many?). Thus, the number $N_q := |\widetilde{E}(\mathbb{F}_q)|$, i.e. the number of points on $\widetilde{E}$ over $\mathbb{F}_q$, is finite. The following theorem provides a bound for N_q. This result was conjectured by Emil Artin (in his thesis) and was proved by Helmut Hasse in the 1930's:

Theorem 2.5.11 (Hasse; [Sil86], Ch. V, Theorem 1.1)**.** *Let $\widetilde{E}$ be an elliptic curve defined over $\mathbb{F}_q$. Then:*

$$q + 1 - 2\sqrt{q} < N_q < q + 1 + 2\sqrt{q}$$

where $N_q = |\widetilde{E}(\mathbb{F}_q)|$.

Example 2.5.12. Let $E/\mathbb{Q}$ be the elliptic curve $y^2 = x^3 + 3$. Its minimal discriminant is $\Delta_E = -3888 = -2^4 \cdot 3^5$. Thus, the only primes of bad reduction are 2 and 3 and $\widetilde{E}/\mathbb{F}_p$ is smooth for all $p \geq 5$. For $p = 5$, there are precisely 6 points on $\widetilde{E}(\mathbb{F}_5)$ namely:

$$\widetilde{E}(\mathbb{F}_5) = \{\widetilde{O}, (1,2), (1,3), (2,1), (2,4), (3,0)\}$$

where all the coordinates should be regarded as congruences modulo 5. Thus, $N_5 = 6$ which is in the range given by Hasse's bound:

$$1.5278\ldots = 5 + 1 - 2\sqrt{5} < N_5 < 5 + 1 + 2\sqrt{5} = 10.4721\ldots$$

Figure 5. Helmut Hasse (1898-1979).

Similarly, one can verify that $N_7 = 13$. ■

The connections between the numbers N_p and the group $E(\mathbb{Q})$ are numerous and of great interest. The most surprising relationship is captured by the Birch and Swinnerton-Dyer conjecture (Conjecture 5.2.1), that relates the growth of N_p (as p varies) with the rank of the elliptic curve $E/\mathbb{Q}$. We shall discuss this conjecture in Section 5.2 in more detail. In the next proposition we describe a different connection between N_p and $E(\mathbb{Q})$. We shall use the following notation: if G is an abelian group and $m \geq 2$, then the points of G of order dividing m will be denoted by $G[m]$.

Proposition 2.5.13 ([Sil86], Ch. VII, Prop. 3.1)**.** *Let $E/\mathbb{Q}$ be an elliptic curve, p a prime number and m a natural number, not divisible by p. Suppose that $E/\mathbb{Q}$ has good reduction at p. Then the reduction map modulo p:*

$$E(\mathbb{Q})[m] \longrightarrow \widetilde{E}(\mathbb{F}_p)$$

is an injective homomorphism of abelian groups. In particular, the number of elements of $E(\mathbb{Q})[m]$ divides the number of elements of $\widetilde{E}(\mathbb{F}_p)$.

The previous proposition can be very useful when calculating the torsion subgroup of an elliptic curve. Let's see an application:

Example 2.5.14. Let $E/\mathbb{Q}\colon y^2 = x^3+3$. In Example 2.5.12 we have seen that $N_5 = 6$ and $N_7 = 13$, and $E/\mathbb{Q}$ has bad reduction only at 2 and 3.

If $q \neq 5, 7$ is a prime number, then $E(\mathbb{Q})[q]$ is trivial. Indeed, Proposition 2.5.13 implies that $|E(\mathbb{Q})[q]|$ divides $N_5 = 6$ and also $N_7 = 13$. Thus, $|E(\mathbb{Q})[q]|$ must divide $\gcd(6, 13) = 1$.

In the case of $q = 5$, we know that $|E(\mathbb{Q})[5]|$ divides $N_7 = 13$. Moreover, it is easy to show that, if $E(\mathbb{Q})[p]$ is non-trivial, then p divides $|E(\mathbb{Q})[p]|$ (later on we will see that $E(\mathbb{Q})[p]$ is always a subgroup of $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$; see Exercise 3.7.5). Since 5 does not divide 13, it follows that $E(\mathbb{Q})[5]$ must be trivial. Similarly, one can show that $E(\mathbb{Q})[7]$ is trivial, and we conclude that $E(\mathbb{Q})_{\text{torsion}}$ is trivial.

However, notice that $P = (1, 2) \in E(\mathbb{Q})$ is a point on the curve. Since we just proved that E does not have any points of finite order, it follows that P must be a point of *infinite* order, and, hence, we have shown that E has infinitely many rational points: $\pm P, \pm 2P, \pm 3P, \ldots$. In fact, $E(\mathbb{Q}) \cong \mathbb{Z}$ and $(1, 2)$ is a generator of its Mordell-Weil group. ■

In the previous example, the Nagell-Lutz theorem (Theorem 2.4.5) would have yielded the same result, i.e. the torsion is trivial, in an easier way. Indeed, for the curve $E : y^2 = x^3+3$ the quantity $4A^3+27B^2$ equals 3^5, so the possibilities for $y(P)^2$, where P is a torsion point of order ≥ 3, are 1, 9 or 81 (it is easy to see that there are no 2-torsion points). Therefore, the possibilities for $x(P)^3 = y(P)^2 - 3$ are -2, 6 or 78, respectively. Since $x(P)$ is an integer, we reach a contradiction. In the following example, the Nagell-Lutz theorem would be a lengthier and much more tedious alternative and Proposition 2.5.13 is much more effective.

Example 2.5.15. Let $E/\mathbb{Q} : y^2 = x^3 + 4249388$. In this case

$$4A^3 + 27B^2 = 2^4 \cdot 3^3 \cdot 11^2 \cdot 13^2 \cdot 17^2 \cdot 19^2 \cdot 23^2.$$

Therefore, $4A^3 + 27B^2$ is divisible by 192 distinct positive squares, which makes it very tedious to use the Nagell-Lutz theorem. The

(minimal) discriminant of $E/\mathbb{Q}$ is $\Delta_E = -16(4A^3 + 27B^2)$ and therefore E has good reduction at 5 and 7. Moreover, $B = 4249388 \equiv 3 \bmod 35$ and therefore, by our calculations in Example 2.5.14, $N_5 = 6$ and $N_7 = 13$. Thus, Proposition 2.5.13, and the same argument we used in Ex. 2.5.14, shows that the torsion of $E(\mathbb{Q})$ is trivial.

Incidentally, the curve $E/\mathbb{Q} : y^2 = x^3 + 4249388$ has a rational point $P = \left(\frac{25502}{169}, \frac{6090670}{2197}\right)$. Since the torsion of $E(\mathbb{Q})$ is trivial, P must be of infinite order. Another way to see this: since P has rational coordinates, which are not integral, the Nagell-Lutz theorem implies that the order of P is infinite. In fact, $E(\mathbb{Q})$ is isomorphic to $\mathbb{Z}$ and it is generated by P. ■

2.6. The rank and the free part of $E(\mathbb{Q})$

In the previous sections we have been able to describe efficient algorithms that determine the torsion subgroup of $E(\mathbb{Q})$. Recall that the Mordell-Weil theorem (Thm. 2.3.5) says that there is a (non-canonical) isomorphism

$$E(\mathbb{Q}) \cong E(\mathbb{Q})_{\text{torsion}} \oplus \mathbb{Z}^{R_E}.$$

Our next goal is to try to find R_E generators of the free part of the Mordell-Weil group. Unfortunately, no algorithm is known that will always yield such free points. We don't even have a way to determine R_E, the rank of the curve, although sometimes we can obtain upper bounds for the rank of a given curve $E/\mathbb{Q}$ (see, for instance, Theorem 2.6.4 below).

Naively, one could hope that if the coefficients of the (minimal) Weierstrass equation for $E/\mathbb{Q}$ are *small*, then the coordinates of the generators of $E(\mathbb{Q})$ should also be *small*, and perhaps a *brute force* computer search would yield these points. However, Bremner and Cassels found the following surprising example: the curve $y^2 = x^3 + 877x$ has rank equal to 1 and the x-coordinate of a generator P is

$$x(P) = (612776083187947368101/78841535860683900210)^2.$$

However, Serge Lang salvaged this idea and conjectured that for all $\epsilon > 0$ there is a constant C_ϵ such that there is a system of generators

$\{P_i : i = 1, \ldots, R_E\}$ of $E(\mathbb{Q})$ with

$$\widehat{h}(P_i) \leq C_\epsilon \cdot |\Delta_E|^{1/2+\epsilon}$$

where $\widehat{h}$ is the canonical height function of $E/\mathbb{Q}$, which we define next. Lang's conjecture says that the size of the coordinates of a generator may grow exponentially with the (minimal) discriminant of a curve $E/\mathbb{Q}$.

Definition 2.6.1. We define the *height* of $\frac{m}{n} \in \mathbb{Q}$, with $\gcd(m, n) = 1$, by:

$$h\left(\frac{m}{n}\right) = \log(\max\{|m|, |n|\}).$$

This can be used to define a height on a point $P = (x, y)$ on elliptic curve $E/\mathbb{Q}$, with $x, y \in \mathbb{Q}$ by:

$$H(P) = h(x).$$

Finally, we define the *canonical height* of $P \in E(\mathbb{Q})$ by

$$\widehat{h}(P) = \frac{1}{2} \lim_{N \to \infty} \frac{H(2^N \cdot P)}{4^N}.$$

Note: here $2^N \cdot P$ means multiplication in the curve, using the addition law defined in Section 2.3, i.e. $2 \cdot P = P + P$, $2^2 \cdot P = 2P + 2P$, etc.

Example 2.6.2. Let $E : y^2 = x^3 + 877x$ and let P be a generator of $E(\mathbb{Q})$. Here are some values of $\frac{1}{2} \cdot \frac{H(2^N \cdot P)}{4^N}$:

$$\begin{aligned}
\frac{1}{2} \cdot H(P) &= 47.8645312628\ldots \\
\frac{1}{2} \cdot \frac{H(2 \cdot P)}{4} &= 47.7958126219\ldots \\
\frac{1}{2} \cdot \frac{H(2^2 \cdot P)}{4^2} &= 47.9720107996\ldots \\
\frac{1}{2} \cdot \frac{H(2^3 \cdot P)}{4^3} &= 47.9636902383\ldots \\
\frac{1}{2} \cdot \frac{H(2^4 \cdot P)}{4^4} &= 47.9901607777\ldots \\
\frac{1}{2} \cdot \frac{H(2^5 \cdot P)}{4^5} &= 47.9901600133\ldots \\
\frac{1}{2} \cdot \frac{H(2^6 \cdot P)}{4^6} &= 47.9901569227\ldots \\
\frac{1}{2} \cdot \frac{H(2^7 \cdot P)}{4^7} &= 47.9901419861\ldots \\
\frac{1}{2} \cdot \frac{H(2^8 \cdot P)}{4^8} &= 47.9901807594\ldots
\end{aligned}$$

The limit is in fact equal to $\widehat{h}(P) = 47.9901859939...$, well below the value $|\Delta_E|^{1/2} = 207,773.12....$ ■

The canonical height enjoys the following properties and, in fact, the canonical height is defined so that it is (essentially) the *only* height that satisfies these properties:

Proposition 2.6.3 (Néron-Tate)**.** *Let $E/\mathbb{Q}$ be an elliptic curve and let $\widehat{h}$ be the canonical height on E.*

(1) *For all $P, Q \in E(\mathbb{Q})$, $\widehat{h}(P+Q)+\widehat{h}(P-Q) = 2\widehat{h}(P)+2\widehat{h}(Q)$. (Note: this is called the parallelogram law.)*

(2) *For all $P \in E(\mathbb{Q})$ and $m \in \mathbb{Z}$, $\widehat{h}(mP) = m^2 \cdot \widehat{h}(P)$. (Note: in particular, the height of mP is much larger height than the height of P, for any $m \neq 0, 1$.)*

(3) *Let $P \in E(\mathbb{Q})$. Then $\widehat{h}(P) \geq 0$, and $\widehat{h}(P) = 0$ if and only if P is a torsion point.*

For the proofs of these properties, see [Sil86], Ch. VIII, Thm. 9.3, or [Mil06], Ch. IV, Prop. 4.5 and Thm. 4.7.

As we mentioned at the beginning of this section, we can calculate upper bounds on the rank of a given elliptic curve (see [Sil86], p. 235, exercises 8.1, 8.2). Here is an example:

Theorem 2.6.4 ([Loz08], Prop. 1.1)**.** *Let $E/\mathbb{Q}$ be an elliptic curve given by a Weierstrass equation of the form*

$$E\colon y^2 = x^3 + Ax^2 + Bx, \text{ with } A, B \in \mathbb{Z}.$$

Let R_E be the rank of $E(\mathbb{Q})$. For an integer $N \geq 1$, let $\nu(N)$ be the number of distinct positive prime divisors of N. Then:

$$R_E \leq \nu(A^2 - 4B) + \nu(B) - 1.$$

More generally, let $E/\mathbb{Q}$ be any elliptic curve with a non-trivial point of 2-torsion and let a (resp. m) be the number of primes of additive (resp. multiplicative) bad reduction of $E/\mathbb{Q}$. Then:

$$R_E \leq m + 2a - 1.$$

Example 2.6.5. Pierre de Fermat proved that $n = 1$ is not a congruent number (see Example 1.1.2) by showing that $x^4 + y^4 = z^2$ has no rational solutions. As an application of the previous theorem, let us show that the curve

$$E_1\colon y^2 = x^3 - x = x(x-1)(x+1)$$

only has the trivial solutions $(0, 0)$, $(\pm 1, 0)$ which are torsion points of order 2. Indeed, the minimal discriminant of E_1 is $\Delta_{E_1} = 64$. Therefore $p = 2$ is the unique prime of bad reduction. Moreover, the reader can check that the reduction at $p = 2$ is multiplicative. Now thanks to Theorem 2.6.4 we conclude that $R_{E_1} = 0$ and E_1 only has torsion points. Finally, using Proposition 2.5.13 or Theorem 2.4.5, we can show that the only torsion points are the three trivial points named above. ■

Example 2.6.6. Let $E/\mathbb{Q}$ be the elliptic curve $y^2 = x(x+1)(x+2)$, which already appeared in Example 1.1.1. Since the equation of the Weierstrass equation is

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

it follows from Theorem 2.6.4 that the rank R_E satisfies:

$$R_E \leq \nu(A^2 - 4B) + \nu(B) - 1 = \nu(1) + \nu(2) - 1 = 0 + 1 - 1 = 0$$

and therefore the rank is 0. The reader can check that

$$E(\mathbb{Q})_{\text{torsion}} = \{\mathcal{O}, (0,0), (-1,0), (-2,0)\}.$$

Since the rank is zero, the four torsion points on $E/\mathbb{Q}$ are the only rational points on E. ■

Example 2.6.7. Let $E : y^2 = x^3 + 2308x^2 + 665858x$. The primes 2 and 577 are the only prime divisors of (both) B and $A^2 - 4B$. Thus

$$R_E \leq \nu(A^2 - 4B) + \nu(B) - 1 = 2 + 2 - 1 = 3.$$

The points $P_1 = (-1681, 25543)$, $P_2 = (-338, 26)$, and $P_3 = (577/16, 332929/64)$ are of infinite order and the subgroup of $E(\mathbb{Q})$ generated by P_1, P_2 and P_3 is isomorphic to $\mathbb{Z}^3$. Therefore, the rank of E is equal to 3. ■