Chapter 2

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. If the reader is not familiar with projective geometry or needs to refresh the memory, it is a good time to look at Appendix C or another reference (for example, [**SK52**] is a beautiful book on projective geometry).

2.1. Why elliptic curves?

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

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

with $f(x_1, \dots, x_r) \in \mathbb{Z}[x_1, \dots, x_r]$. 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. $y^2 = x^3 - n^2x$ 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:

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

(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?

(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, Davis, 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)*:

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

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 $\mathbb{R}$ and over $\mathbb{Q}_p$, the p-adics, for all primes $p \geq 2$ (see Appendix D for a brief introduction to 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 2.12.2). 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 2.12.2).

- *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 at least one rational point (which will be our definition of 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 2.12.4). 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, the projective line $\mathbb{P}^1(\mathbb{C})$ has no holes and $g = 0$ (the projective plane is homeomorphic to a sphere; see Appendix C for a quick introduction to projective geometry), 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.

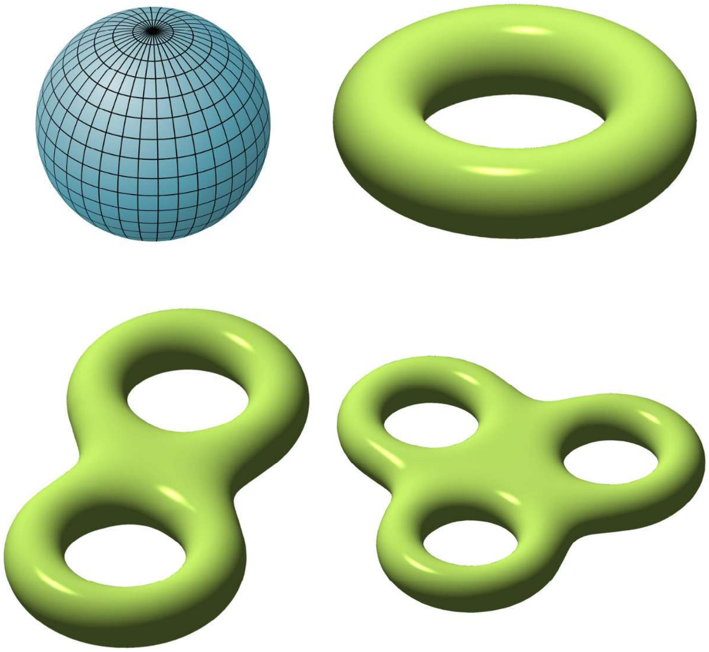

Figure 1. A surface of genus 0 (a sphere), and surfaces of genus 1, 2, and 3 (with 1, 2, and 3 holes, respectively).

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*

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

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). The reference [**SiT92**], Ch. I. 3, gives 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 2.12.3).

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. Note that if we change $X = U+V$, $Y = -V$, $Z = W$, then we obtain a new equation

$$U^3 + 3U^2V + 3UV^2 = dW^3. \tag{2.4}$$

Since this equation is quadratic in V, and cubic in W, with no other cubic monomials that involve W, the variable W will end up playing the role of x, and the variable V will play the role of y in our Weierstrass model. Next, we change variables to obtain a coefficient of 1 in front of V^2 and W^3. If we multiply Eq. (2.4) through by d^2, we obtain

$$d^2U^3 + 3d^2U^2V + 3d^2UV^2 = d^3W^3, \tag{2.5}$$

and now we change variables $x = 3dW$, $y = 9dV$, and $z = U$. Then, Eq. (2.5) becomes

$$d^2z + \frac{dyz}{3} + \frac{y^2z}{27} = \frac{x^3}{27}, \tag{2.6}$$

or, equivalently, $y^2z + 9dyz = x^3 - 27d^2z$, which is a Weierstrass equation. Thus, $[x, y, z] = [3dW, 9dV, U] = [3dZ, -9dY, X + Y]$ and we have found a change of variables $\psi : E \to \widehat{E}$ given by

$$\psi([X, Y, Z]) = [3dZ, -9dY, X + Y]$$

such that the image lands on the curve in Weierstrass equation $\widehat{E} : y^2z + 9dyz = x^3 - 27d^2z$. The map ψ is invertible; the inverse map $\psi^{-1} : \widehat{E} \to E$ is

$$\psi^{-1}([x, y, z]) = \left[\frac{9dz + y}{9d}, -\frac{y}{9d}, \frac{x}{3d}\right].$$

In affine coordinates, the change of variables is going from $X^3+Y^3 = d$ to the curve $y^2 + 9dy = x^3 - 27d^2$ via the maps:

$$\begin{aligned} \psi(X, Y) &= \left(\frac{3d}{X + Y}, -\frac{9dY}{X + Y}\right), \\ \psi^{-1}(x, y) &= \left(\frac{9d + y}{3x}, -\frac{y}{3x}\right). \end{aligned}$$

We leave it as an exercise for the reader to verify that the model can be further simplified to the form $y^2 = x^3 - 432d^2$. ■

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 2.12.4. 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.

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 2.2.6. 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. ■

2.3. Integral points

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

Theorem 2.3.1 (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 provides 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.

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

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.

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 2). 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.

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 it is tedious to prove) and, therefore, $(E, +)$ is an abelian group.

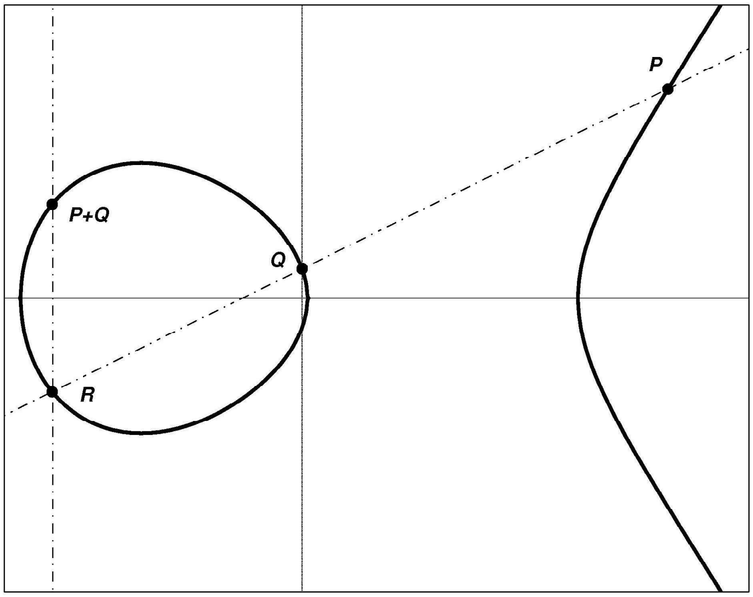

Figure 2. Addition of points on an elliptic curve

Example 2.4.1. 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 into 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 across 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 factor 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 2.4.2. Let $E : y^2 = x^3 + 1$ and put $P = (2, 3)$. Let us find P, $2P$, $3P$, etc.

- 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 $2P = (0, 1)$.

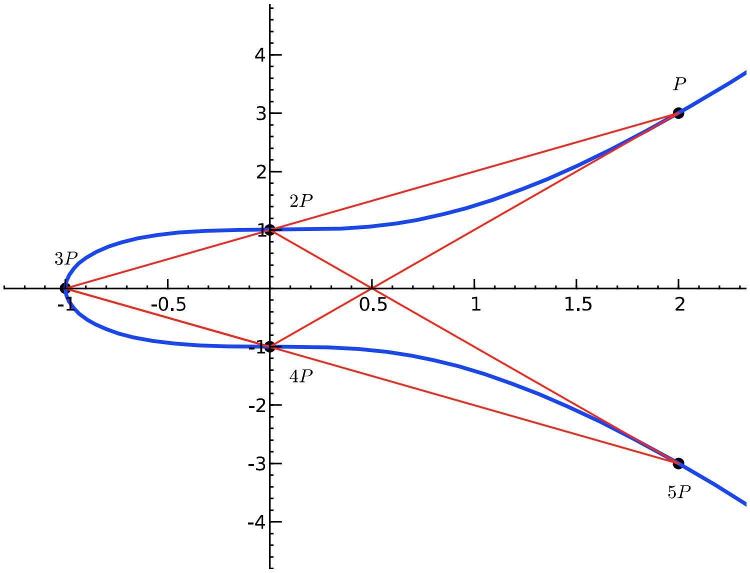

Figure 3. The rational points on $y^2 = x^3 + 1$, except the point at ∞.

- 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 3 (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 $y^2 = x^3 + Ax + B$, and $\mathcal{O}$ is chosen to be the point $[0, 1, 0]$, then $\mathfrak{L}'$ is always a vertical line, so $P + Q$ is always the reflection of R with respect to the x axis.

The next step in the study of the structure of $E(\mathbb{Q})$ was conjectured by Henri Poincaré in 1908, proved by Louis Mordell in 1922 and generalized by André Weil in his thesis in 1928:

Theorem 2.4.3 (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 $a_i \in \mathbb{Z}$.

The group $E(\mathbb{Q})$ is usually called the Mordell-Weil group of E, in honor of the two mathematicians who proved the theorem.

Example 2.4.4. Consider the elliptic curve $E/\mathbb{Q}$ given by the Weierstrass equation

$$y^2 + y = x^3 - 7x + 6.$$

The set of rational points $E(\mathbb{Q})$ for this elliptic curve is infinite. For instance, the following points are on the curve:

$$(1, 0),\ (2, 0),\ (0, -3),\ (-3, -1),\ (8, -22),\ (-2, -4),\ (3, -4),$$
$$(3, 3),\ (-1, -4),\ (1, -1),\ (0, 2),\ (2, -1),\ (-2, 3),\ (-1, 3),$$
$$\left(\frac{1}{4}, \frac{13}{8}\right),\ \left(\frac{25}{9}, -\frac{91}{27}\right),\ \left(-\frac{26}{9}, \frac{28}{27}\right),\ \left(\frac{7}{9}, \frac{17}{27}\right), \ldots.$$

At a first glance, it may seem very difficult to describe all the points on $E(\mathbb{Q})$, including those listed above, in a succinct manner. However,

Figure 4. Louis Mordell (1888-1972) and André Weil (1906-1998).

the Mordell-Weil theorem tells us that there must be a finite set of points that generate the whole group. Indeed, it can be proved that the three points

$$P = (1, 0),\ Q = (2, 0), \text{ and } R = (0, -3)$$

are generators of $E(\mathbb{Q})$. This means that *any other point* on $E(\mathbb{Q})$ can be expressed as a $\mathbb{Z}$-linear combination of P, Q and R. In other words,

$$E(\mathbb{Q}) = \{a \cdot P + b \cdot Q + c \cdot R : a, b, c \in \mathbb{Z}\}.$$

For instance,

$$(-3, -1) = P + Q,\ (8, -22) = P + R,\ (-2, -4) = P - Q,$$

$$(-1, -4) = Q - R \text{ and } (3, 3) = P - R.$$

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 2.4.5 (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 2.9 (see Corollary 2.9.7).

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

$$E(\mathbb{Q}) \cong E(\mathbb{Q})_{\text{torsion}} \oplus \mathbb{Z}^{R_E}. \tag{2.7}$$

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. (2.7), 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. (2.7) 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 2.4.6. 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 2.4.2, 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 $R_E \geq n$. We state this as a conjecture for future reference:

Conjecture 2.4.7 (Conjecture of the rank)**.** *Let $N \geq 0$ be a natural number. Then there exists an elliptic curve E defined over $\mathbb{Q}$ with rank $R_E \geq N$.*

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.

2.5. 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 2.5.1. 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 2.12.6) 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 2.5.2 (Ogg's conjecture; Mazur, [**Maz77**], [**Maz78**])**.** *Let $E/\mathbb{Q}$ be an elliptic curve. Then $E(\mathbb{Q})_{torsion}$ is isomorphic to one of the following groups:*

$$\begin{aligned} &\mathbb{Z}/N\mathbb{Z} \quad \textit{with} \quad 1 \leq N \leq 10 \textit{ or } N = 12, \textit{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus &\mathbb{Z}/2M\mathbb{Z} \quad \textit{with} \quad 1 \leq M \leq 4. \end{aligned} \tag{2.8}$$

Example 2.5.3. 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

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

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 5 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. 2.8, there are infinitely many elliptic curves whose torsion subgroup is 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 2.5.4. Let $E_t : y^2 + (1 - t)xy - ty = x^3 - tx^2$ with $t \in \mathbb{Q}$ and $\Delta_t = t^5(t^2 - 11t - 1) \neq 0$. Then, the torsion subgroup of $E_t(\mathbb{Q})$ 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_t for some $t \in \mathbb{Q}$. See also Examples E.1.1 and E.1.2. ■

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 2.5.5 (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 2.5.6. 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 are a perfect cube. Thus, $E(\mathbb{Q})_{\text{torsion}}$ is trivial (i.e., the only torsion point is $\mathcal{O}$).

Example 2.5.7. Let $p \geq 2$ be a prime number and let us define a curve $E_p \colon y^2 = x^3 + p^2$. 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 2.12.8. Thus, the torsion subgroup of $E_p(\mathbb{Q})$ is isomorphic to $\mathbb{Z}/3\mathbb{Z}$ for any prime $p \geq 2$. ■

2.6. 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 2.6.1. 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 2.6.2. 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 2.6.3. 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 2.6.4. 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 2.6.2), 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 modulo p that 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:

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

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

Definition 2.6.5. 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.

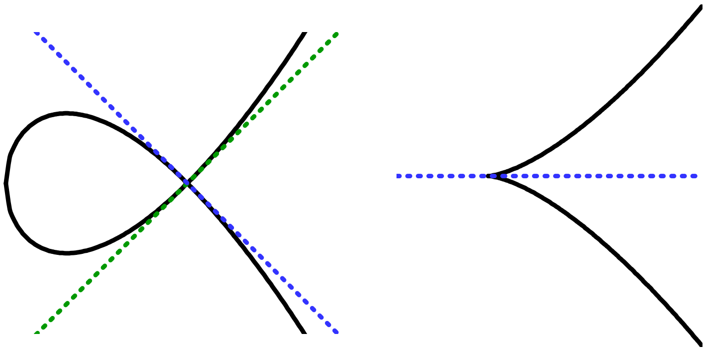

Figure 6. A node (left) with two tangent lines, and a cusp (right) with only one tangent line.

Definition 2.6.6. 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 smooth and hence is an 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 2.6.7. Let us see some examples of elliptic curves with different types of reduction:

(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 minimal 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 $(5,5)$ mod 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 2.6.8. *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 2.12.9). 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 2.6.3, is a multiple of D; in fact, $\Delta_E=16D$. This fact together with Proposition 2.6.8 yield the following corollary:

Corollary 2.6.9. *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 2.6.10. The discriminant of the elliptic curve $E_1\colon y^2=x^3+35x+5$ of Example 2.6.7 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 2.6.11 (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 $N_q = |\widetilde{E}(\mathbb{F}_q)|$.

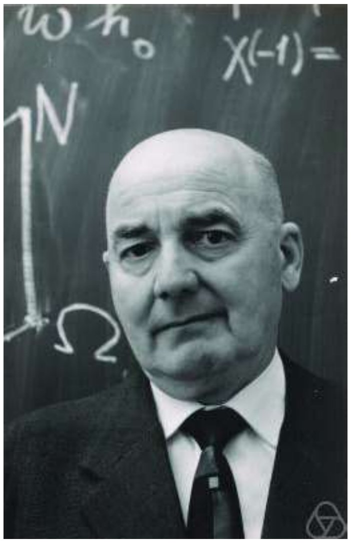

Figure 7. Helmut Hasse (1898-1979).

Remark 2.6.12. Heuristically, we expect that N_q is approximately $q+1$, in agreement with Hasse's bound. Indeed, let $E/\mathbb{Q}$ be an elliptic curve given by $y^2 = x^3 + Ax + B$, with $A, B \in \mathbb{Z}$, and let $q = p$ be a prime for simplicity. There are p choices of x in $\mathbb{F}_p$. For each value x_0, the polynomial $f(x) = x^3 + Ax + B$ gives a value $f(x_0) \in \mathbb{F}_p$. The probability that a random element in $\mathbb{F}_p$ is a perfect square in $\mathbb{F}_p$ is $1/2$ (notice, however, that $f(x_0)$ is not random; this is just a heuristic argument). If $f(x_0)$ is a square modulo p, i.e., if there is a $y_0 \in \mathbb{F}_p$ such that $f(x_0) \equiv y_0^2 \bmod p$, then there are two points $(x_0, \pm y_0)$ in

$\widetilde{E}(\mathbb{F}_p)$. If $f(x_0)$ is not a square modulo p, then there are no points in $\widetilde{E}(\mathbb{F}_p)$ with x-coordinate equal to x_0. Hence:

$$N_p \approx p \cdot \left(\frac{1}{2} \cdot 2 + \frac{1}{2} \cdot 0\right) + 1 = p + 1.$$

Notice that we have added 1 in order to account for the point at infinity.

Remark 2.6.13. Suppose that $E/\mathbb{Q}$ is an elliptic curve that has bad reduction at a prime p. How many points does the singular curve $\widetilde{E}$ have over $\mathbb{F}_p$? The reader can find the answer to this question in Exercise 5.7.1.

Example 2.6.14. 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:

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

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 2.6.15 ([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 2.6.16. Let $E/\mathbb{Q}$: $y^2 = x^3 + 3$. In Example 2.6.14 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 2.6.15 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, by Lagrange's theorem from group theory, 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 2.5.5) 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 2.6.15 is much more effective.

Example 2.6.17. 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 2.6.16, $N_5 = 6$ and $N_7 = 13$. Thus, Proposition 2.6.15 and the same argument we used in Ex. 2.6.16 show 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 that 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. ■

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

In the previous sections we have described simple algorithms that determine the torsion subgroup of $E(\mathbb{Q})$. Recall that the Mordell-Weil theorem (Thm. 2.4.3) 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 2.7.4 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

$$x(P) = (612776083187947368101/7884153586068390021 0)^2.$$

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 2.7.1. 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 an 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 2.4, i.e., $2 \cdot P = P + P$, $2^2 \cdot P = 2P + 2P$, etc.

Example 2.7.2. 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 2.7.3 (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 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 2.7.4 ([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 2.7.5. 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 2.7.4 we conclude that $R_{E_1} = 0$ and E_1 only has torsion points. Finally, using Proposition 2.6.15 or Theorem 2.5.5, we can show that the only torsion points are the three trivial points named above. ■

Example 2.7.6. 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 Weierstrass equation of E is

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

it follows from Theorem 2.7.4 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 2.7.7. 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. ■

2.8. Linear independence of rational points

Let $E/\mathbb{Q}$ be the curve defined in Example 2.7.7. We claimed that the subgroup generated by the points $P_1=(-1681,25543)$, $P_2=(-338,26)$, and $P_3=(577/16,332929/64)$ is isomorphic to $\mathbb{Z}^3$. But how can we show that? In particular, why is P_3 not a linear combination of P_1 and P_2? In other words, are there integers n_1 and n_2 such that $P_3=n_1P_1+n_2P_2$? In fact, $E/\mathbb{Q}$ has a rational torsion point $T=(0,0)$ of order 2, so could some combination of P_1, P_2 and P_3 equal T? This example motivates the need for a notion of linear dependence and independence of points over $\mathbb{Z}$.

Definition 2.8.1. Let $E/\mathbb{Q}$ be an elliptic curve. We say that the rational points $P_1,\ldots,P_m \in E(\mathbb{Q})$ are *linearly dependent over* $\mathbb{Z}$ if there are integers $n_1,\ldots,n_m \in \mathbb{Z}$ such that

$$n_1P_1+n_2P_2+\cdots+n_mP_m=T,$$

where T is a torsion point. Otherwise, if no such relation exists, we say that the points are *linearly independent* over $\mathbb{Z}$.

Example 2.8.2. Let $E/\mathbb{Q} : y^2 = x^3 + x^2 - 25x + 39$ and let

$$P_1 = \left(\frac{61}{4}, -\frac{469}{8}\right),\ P_2 = \left(-\frac{335}{81}, -\frac{6868}{729}\right),\ P_3 = (21, 96).$$

The points P_1, P_2 and P_3 are rational points on E and linearly dependent over $\mathbb{Z}$ because

$$-3P_1 - 2P_2 + 6P_3 = \mathcal{O}.$$

■

Example 2.8.3. Let $E/\mathbb{Q} : y^2 + y = x^3 - x^2 - 26790x + 1696662$ and put

$$\begin{aligned} P_1 &= \left(\frac{59584}{625}, \frac{71573}{15625}\right), \\ P_2 &= \left(\frac{101307506181}{210337009}, \frac{30548385002405573}{3050517641527}\right). \end{aligned}$$

The points P_1 and P_2 are rational points on E, and they are linearly dependent over $\mathbb{Z}$ because

$$-3P_1 + 2P_2 = (133, -685),$$

and $(133, -685)$ is a torsion point of order 5. ■

Now that we have defined linear independence over $\mathbb{Z}$, we need a method to prove that a number of points are linearly independent. The existence of the Néron-Tate pairing provides a way to prove independence.

Definition 2.8.4. The *Néron-Tate pairing* attached to an elliptic curve is defined by

$$\langle \cdot, \cdot \rangle : E(\mathbb{Q}) \times E(\mathbb{Q}) \to \mathbb{R}, \quad \langle P, Q \rangle = \widehat{h}(P + Q) - \widehat{h}(P) - \widehat{h}(Q),$$

where $\widehat{h}$ is the canonical height on E. Let $P_1, P_2, \ldots, P_r$ be r rational points on $E(\mathbb{Q})$. The *elliptic height matrix* associated to $\{P_i\}_{i=1}^r$ is

$$\mathcal{H} = \mathcal{H}(\{P_i\}_{i=1}^r) := (\langle P_i, P_j \rangle)_{1 \le i \le r,\ 1 \le j \le r}.$$

The determinant of $\mathcal{H}$ is called the *elliptic regulator* of the set of points $\{P_i\}_{i=1}^r$. If $\{P_i\}_{i=1}^r$ is a complete set of generators of the free part of $E(\mathbb{Q})$, then the determinant of $\mathcal{H}(\{P_i\}_{i=1}^r)$ is called the *elliptic regulator of* $E/\mathbb{Q}$.

Theorem 2.8.5. *Let $E/\mathbb{Q}$ be an elliptic curve. Then the Néron-Tate pairing $\langle \cdot, \cdot \rangle$ associated to E is a non-degenerate symmetric bilinear form on $E(\mathbb{Q})/E(\mathbb{Q})_{torsion}$, i.e.,*

(1) *For all $P, Q \in E(\mathbb{Q})$, $\langle P, Q\rangle = \langle Q, P\rangle$.*

(2) *For all $P, Q, R \in E(\mathbb{Q})$ and all $m, n \in \mathbb{Z}$,*

$$\langle P, mQ + nR\rangle = m\langle P, Q\rangle + n\langle P, R\rangle.$$

(3) *Suppose $P \in E(\mathbb{Q})$ and $\langle P, Q\rangle = 0$ for all $Q \in E(\mathbb{Q})$. Then $P \in E(\mathbb{Q})_{torsion}$. In particular, P is a torsion point if and only if $\langle P, P\rangle = 0$.*

The properties of the Néron-Tate pairing follow from those of the canonical height in Proposition 2.7.3 (see Exercise 2.12.12). Theorem 2.8.5 has the following important corollary:

Corollary 2.8.6. *Let $E/\mathbb{Q}$ be an elliptic curve and let $P_1, P_2, \ldots, P_r \in E(\mathbb{Q})$ be rational points. Let $\mathcal{H}$ be the elliptic height matrix associated to $\{P_i\}_{i=1}^r$. Then:*

(1) *Suppose $\det(\mathcal{H}) = 0$ and $u = (n_1, \ldots, n_r) \in \mathrm{Ker}(\mathcal{H})$, with $n_i \in \mathbb{Z}$. Then the points $\{P_i\}_{i=1}^r$ are linearly dependent and $\sum_{k=1}^r n_k P_k = T$, where T is a torsion point on $E(\mathbb{Q})$.*

(2) *If $\det(\mathcal{H}) \neq 0$, then the points $\{P_i\}_{i=1}^r$ are linearly independent and the rank of $E(\mathbb{Q})$ is $\geq r$.*

Here is an example of how the Néron-Tate pairing is used in practice:

Example 2.8.7. Let $E/\mathbb{Q}$ be the elliptic curve $y^2 = x^3 + 2308x^2 + 665858x$. Put

$$\begin{aligned} P &= (-1681, 25543), \quad Q = (-338, 26), \quad \text{and} \\ R &= \left(\frac{332929}{36}, -\frac{215405063}{216}\right). \end{aligned}$$

Are P, Q and R independent? In order to find out, we find the elliptic height matrix associated to $\{P, Q, R\}$, using PARI or Sage:

$$\begin{aligned}\mathcal{H} &= \begin{pmatrix} \langle P,P\rangle & \langle Q,P\rangle & \langle R,P\rangle \\ \langle P,Q\rangle & \langle Q,Q\rangle & \langle R,Q\rangle \\ \langle P,R\rangle & \langle Q,R\rangle & \langle R,R\rangle \end{pmatrix}\\ &= \begin{pmatrix} 7.397\ldots & -3.601\ldots & 3.795\ldots \\ -3.601\ldots & 6.263\ldots & 2.661\ldots \\ 3.795\ldots & 2.661\ldots & 6.457\ldots \end{pmatrix}.\end{aligned}$$

The determinant of $\mathcal{H}$ seems to be *very* close to 0 (PARI returns $3.368 \cdot 10^{-27}$). Hence Cor. 2.8.6 suggests that P, Q and R are not independent. If we find the (approximate) kernel of $\mathcal{H}$ with PARI, we discover that the (column) vector $(1, 1, -1)$ is approximately in the kernel, and therefore, $P + Q - R$ may be a torsion point. Indeed, the point $P + Q - R = (0, 0)$ is a torsion point of order 2 on $E(\mathbb{Q})$. Hence, P, Q and R are linearly *dependent* over $\mathbb{Z}$.

Instead, let $P_1 = (-1681, 25543)$, $P_2 = (-338, 26)$, a third point $P_3 = (577/16, 332929/64)$ and let $\mathcal{H}'$ be the elliptic height matrix associated to $\{P_i\}_{i=1}^3$. Then $\det(\mathcal{H}') = 101.87727\ldots$ is non-zero and, therefore, $\{P_i\}_{i=1}^3$ are linearly independent and the rank of $E/\mathbb{Q}$ is at least 3. ■

2.9. Descent and the weak Mordell-Weil theorem

In the previous sections we have seen methods to calculate the torsion subgroup of an elliptic curve $E/\mathbb{Q}$, and also methods to check if a collection of points are independent modulo torsion. However, we have not discussed any method to find points of infinite order. In this section, we briefly explain the *method of descent*, which facilitates the search for generators of the free part of $E(\mathbb{Q})$. Unfortunately, the method of descent is not always successful! We will try to measure the failure of the method in the following section. The method of descent (as explained here) is mostly due to Cassels. For a more detailed treatment, see [**Was08**] or [**Sil86**]. A more general descent algorithm was laid out by Birch and Swinnerton-Dyer in [**BSD63**].

The current implementation of the algorithm is more fully explained in Cremona's book [**Cre97**].

Let $E/\mathbb{Q}$ be a curve given by $y^2 = x^3 + Ax + B$, with $A, B \in \mathbb{Z}$. The most general case of the method of descent is quite involved, so we will concentrate on a particular case where the calculations are much easier: we will assume that $E(\mathbb{Q})$ has 4 distinct rational points of 2-torsion (including $\mathcal{O}$). As we saw before (Theorem 2.5.5, or Exercise 2.12.6), a point $P = (x, y) \in E(\mathbb{Q})$ is of 2-torsion if and only if $y = 0$ and $x^3 + Ax + B = 0$ (or $P = \mathcal{O}$). Thus, if $E(\mathbb{Q})$ has 4 distinct rational points of order 2, that means that $x^3 + Ax + B$ has three (integral) roots and it factors completely over $\mathbb{Z}$:

$$x^3 + Ax + B = (x - e_1)(x - e_2)(x - e_3)$$

with $e_i \in \mathbb{Z}$. Since $x^3 + Ax + B$ does not have an x^2 term, we conclude that $e_1 + e_2 + e_3 = 0$.

Suppose, then, that $E : y^2 = (x - e_1)(x - e_2)(x - e_3)$, where the roots satisfy $e_i \in \mathbb{Z}$ and $e_1 + e_2 + e_3 = 0$. We would like to find a solution $(x_0, y_0) \in E$ with $x_0, y_0 \in \mathbb{Q}$, i.e.,

$$y_0^2 = (x_0 - e_1)(x_0 - e_2)(x_0 - e_3).$$

Thus, each term $(x_0 - e_i)$ must be *almost* a square, and we can make this precise by writing

$$(x_0 - e_1) = au^2,\ (x_0 - e_2) = bv^2,\ (x_0 - e_3) = cw^2,\ y_0^2 = abc(uvw)^2,$$

where $a, b, c, u, v, w \in \mathbb{Q}$, the numbers $a, b, c \in \mathbb{Q}$ are square-free, and abc is a square (in $\mathbb{Q}$).

Example 2.9.1. Let

$$E : y^2 = x^3 - 556x + 3120 = (x - 6)(x - 20)(x + 26)$$

so that $e_1 = 6$, $e_2 = 20$ and $e_3 = -26$. The point $(x_0, y_0) = (\frac{164184}{289}, \frac{66469980}{4913})$ is rational and on E. We can write

$$x_0 - e_1 = \frac{164184}{289} - 6 = 2 \cdot \left(\frac{285}{17}\right)^2$$

and, similarly, $x_0 - e_2 = (\frac{398}{17})^2$ and $x_0 - e_3 = 2 \cdot (\frac{293}{17})^2$. Thus, following the notation of the preceeding paragraphs

$$a = 2,\ b = 1,\ c = 2,\ u = \frac{285}{17},\ v = \frac{398}{17},\ w = \frac{293}{17}.$$

Notice that abc is a square and $y_0^2 = (\frac{66469980}{4913})^2 = abc(uvw)^2$. ■

Example 2.9.2. Let $E : y^2 = x^3 - 556x + 3120$ as before, with $e_1 = 6$, $e_2 = 20$ and $e_3 = -26$. Let $P = (-8, 84)$, $Q = (24, 60)$ and $S = P+Q = (-\frac{247}{16}, -\frac{5733}{64})$. The points P, Q and S are in $E(\mathbb{Q})$. We would like to calculate the aforementioned numbers a, b, c for each of the points P, Q and S. For instance

$$\begin{aligned} x(P) - e_1 &= -8 - 6 = -14 = -14 \cdot 1^2, \\ x(P) - e_2 &= -7 \cdot 4^2, \quad \text{and} \quad x(P) - e_3 = 2 \cdot 3^2. \end{aligned}$$

Thus, $a_P = -14$, $b_P = -7$ and $c_P = 2$. Similarly, we calculate

$$\begin{aligned} x(Q) - 6 &= 2 \cdot 3^2, \quad x(Q) - 20 = 2^2, \quad x(Q) + 26 = 2 \cdot 5^2, \\ x(S) - 6 &= -7 \cdot \left(\frac{7}{4}\right)^2, \\ x(S) - 20 &= -7 \cdot \left(\frac{9}{4}\right)^2, \; x(S) + 26 = \left(\frac{13}{4}\right)^2. \end{aligned}$$

Thus $a_Q = 2$, $b_Q = 1$, $c_Q = 2$, and $a_S = -7$, $b_S = -7$, $c_S = 1$. Notice the following interesting fact:

$$a_P \cdot a_Q = -28 = -7 \cdot 2^2, \quad b_P \cdot b_Q = -7, \quad c_P \cdot c_Q = 4.$$

Therefore, the square-free part of $a_P \cdot a_Q$ equals $a_S = a_{P+Q} = -7$. And similarly, the square-free parts of $b_P \cdot b_Q$ and $c_P \cdot c_Q$ equal $b_S = -7$ and $c_S = 1$, respectively. Also, the reader can check that $a_{2P} = b_{2P} = c_{2P} = 1$ and $a_{2Q} = b_{2Q} = c_{2Q} = 1$. ■

The previous example points to the fact that there may be a homomorphism between points on $E(\mathbb{Q})$ and triples (a, b, c) of rational numbers modulo squares, or square-free parts of rational numbers; formally, we are talking about $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2 \times \mathbb{Q}^\times/(\mathbb{Q}^\times)^2 \times \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$. Here, the group $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ is the multiplicative group of non-zero rational numbers, with the extra relation that two non-zero rational numbers are equivalent if their square-free parts are equal (or, equivalently, if their quotient is a perfect square). For instance, 3 and $\frac{12}{25}$ represent the same element of $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ because $\frac{12}{25} = 3 \cdot \left(\frac{2}{5}\right)^2$. The following theorem constructs such a homomorphism. Here we have adapted the proof that appears in [**Was08**], Theorem 8.14.

Theorem 2.9.3. *Let $E/\mathbb{Q}$ be an elliptic curve*

$$y^2 = x^3 + Ax + B = (x - e_1)(x - e_2)(x - e_3)$$

with distinct $e_1, e_2, e_3 \in \mathbb{Z}$ and $e_1 + e_2 + e_3 = 0$. There is a homomorphism of groups

$$\delta : E(\mathbb{Q}) \to \mathbb{Q}^\times/(\mathbb{Q}^\times)^2 \times \mathbb{Q}^\times/(\mathbb{Q}^\times)^2 \times \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$$

defined for $P = (x_0, y_0)$ by

$$\delta(P) = \begin{cases} (1,1,1) & \text{if } P = \mathcal{O}; \\ (x_0 - e_1, x_0 - e_2, x_0 - e_3) & \text{if } y_0 \neq 0; \\ ((e_1 - e_2)(e_1 - e_3), e_1 - e_2, e_1 - e_3) & \text{if } P = (e_1, 0); \\ (e_2 - e_1, (e_2 - e_1)(e_2 - e_3), e_2 - e_3) & \text{if } P = (e_2, 0); \\ (e_3 - e_1, e_3 - e_2, (e_3 - e_1)(e_3 - e_2)) & \text{if } P = (e_3, 0). \end{cases}$$

If $\delta(P) = (\delta_1, \delta_2, \delta_3)$, then $\delta_1 \cdot \delta_2 \cdot \delta_3 = 1$ in $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$. Moreover, the kernel of δ is precisely $2E(\mathbb{Q})$; i.e., if $\delta(Q) = (1,1,1)$, then $Q = 2P$ for some $P \in E(\mathbb{Q})$.

Proof. Let δ be the function defined in the statement of the theorem. Let us show that δ is a homomorphism of (abelian) groups; i.e., we want to show that $\delta(P) \cdot \delta(Q) = \delta(P + Q)$. Notice first of all that $\delta(P) = \delta(x_0, y_0) = \delta(x_0, -y_0) = \delta(-P)$, because the definition of δ does not depend on the sign of the y coordinate of P (in fact, it only depends on whether $y(P) = 0$). Thus, it suffices to prove that $\delta(P) \cdot \delta(Q) = \delta(-(P + Q))$ for all $P, Q \in E(\mathbb{Q})$.

Let $P = (x_0, y_0)$, $Q = (x_1, y_1)$ and $R = -(P + Q) = (x_2, y_2)$, and let us assume, for simplicity, that $y_i \neq 0$ for $i = 1, 2, 3$. By the definition of the addition rule on an elliptic curve (see Figure 2), the points P, Q and R are collinear. Let $\mathcal{L} = \overline{PQ}$ be the line that goes through all three points, and suppose it has equation $\mathcal{L} : y = ax + b$. Therefore, if we substitute y in the equation of $E/\mathbb{Q}$, we obtain a polynomial

$$p(x) = (ax + b)^2 - (x - e_1)(x - e_2)(x - e_3).$$

The polynomial $p(x)$ is cubic, its leading term is -1, and it has precisely three rational roots, namely x_0, x_1 and x_2. Hence, it factors:

$$p(x) = (ax+b)^2 - (x-e_1)(x-e_2)(x-e_3) = -(x-x_0)(x-x_1)(x-x_2).$$

If we evaluate $p(x)$ at $x = e_i$, we obtain

$$p(e_i) = (ae_i + b)^2 = -(e_i - x_0)(e_i - x_1)(e_i - x_2)$$

or, equivalently, $(x_0 - e_i)(x_1 - e_i)(x_2 - e_i) = (ae_i + b)^2$. Thus, the product $\delta(P) \cdot \delta(Q) \cdot \delta(R)$ equals

$$\begin{aligned}
\delta(P) \cdot \delta(Q) \cdot \delta(R) &= (x_0 - e_1, x_0 - e_2, x_0 - e_3) \\
&\quad \cdot (x_1 - e_1, x_1 - e_2, x_1 - e_3) \\
&\quad \cdot (x_2 - e_1, x_2 - e_2, x_2 - e_3) \\
&= ((x_0 - e_1)(x_1 - e_1)(x_2 - e_1), \\
&\quad (x_0 - e_2)(x_1 - e_2)(x_2 - e_2), \\
&\quad (x_0 - e_3)(x_1 - e_3)(x_2 - e_3)) \\
&= ((ae_1 + b)^2, (ae_2 + b)^2, (ae_3 + b)^2) \\
&= (1, 1, 1) \in (\mathbb{Q}^\times/(\mathbb{Q}^\times)^2)^3.
\end{aligned}$$

Hence, $\delta(P) \cdot \delta(Q) \cdot \delta(R) = 1$. If we multiply both sides by $\delta(R)$ and notice that $a^2 = 1$ for any $a \in \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$, we conclude that

$$\delta(P) \cdot \delta(Q) = \delta(R) = \delta(-(P + Q)) = \delta(P + Q),$$

as desired. In order to completely prove that δ is a homomorphism, we would need to check the cases when P, Q or R is one of the points $(e_i, 0)$ or $\mathcal{O}$, but we leave those special cases for the reader to check (Exercise 2.12.15).

If $\delta(P) = (\delta_1, \delta_2, \delta_3)$, then it follows directly from the definition of δ that $\delta_1 \cdot \delta_2 \cdot \delta_3 = 1$ in $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$. Indeed, this is clear for $P = \mathcal{O}$ or $P = (e_i, 0)$, and if $P = (x_0, y_0)$ with $y_0 \neq 0$, then $(x_0 - e_1)(x_0 - e_2)(x_0 - e_3) = y_0^2$, which is a square, and is therefore trivial in $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$.

Next, let us show that the kernel of δ is $2E(\mathbb{Q})$. Clearly, $2E(\mathbb{Q})$ is in the kernel of δ, because δ is a homomorphism with image in $(\mathbb{Q}^\times/(\mathbb{Q}^\times)^2)^3$, as we just proved. Indeed, if $P \in E(\mathbb{Q})$, then

$$\delta(2P) = \delta(P) \cdot \delta(P) = \delta(P)^2 = (\delta_1^2, \delta_2^2, \delta_3^2) = (1, 1, 1),$$

because squares are trivial in $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$.

Now let us show the reverse inclusion, i.e., that the kernel of δ is contained in $2E(\mathbb{Q})$. Let $Q = (x_1, y_1) \in E(\mathbb{Q})$ such that $\delta(Q) = (1, 1, 1)$. We want to find $P = (x_0, y_0)$ such that $2P = Q$. Notice that it is enough to show that $x(2P) = x_1$, because $2P$ is a point on $E(\mathbb{Q})$ and if $x(2P) = x(Q)$, then $Q = 2(\pm P)$. Hence, our goal will be to construct $(x_0, y_0) \in E(\mathbb{Q})$ such that

$$x(2P) = \frac{x_0^4 - 2Ax_0^2 - 8Bx_0 + A^2}{4y_0^2} = x_1.$$

The formula for $x(2P)$ above is given in Exercise 2.12.16.

Once again, for simplicity, let us assume $y(Q) = y_1 \neq 0$ and, as stated above, we assume $\delta(Q) = (1, 1, 1)$. Hence, $x_1 - e_i$ is a square in $\mathbb{Q}$ for $i = 1, 2, 3$. Let us write

$$x_1 - e_i = t_i^2, \qquad \text{for some } t_i \in \mathbb{Q}^\times. \tag{2.9}$$

We define a new auxiliary polynomial $p(x)$ by

$$t_1\frac{(x-e_2)(x-e_3)}{(e_1-e_2)(e_1-e_3)} + t_2\frac{(x-e_1)(x-e_3)}{(e_2-e_1)(e_2-e_3)} + t_3\frac{(x-e_1)(x-e_2)}{(e_3-e_1)(e_3-e_2)}.$$

The polynomial $p(x)$ is an interpolating polynomial (or Lagrange polynomial) which was defined so that $p(e_i) = t_i$. Notice that $p(x)$ is a quadratic polynomial, say $p(x) = a + bx + cx^2$. Also define another polynomial $q(x) = x_1 - x - p(x)^2$ and notice that

$$q(e_i) = x_1 - e_i - p(e_i)^2 = x_1 - e_i - t_i^2 = 0$$

from the definition of t_i in Eq. (2.9). Since $q(e_i) = 0$, it follows that $(x - e_i)$ divides $q(x)$ for $i = 1, 2, 3$. Thus, $(x - e_1)(x - e_2)(x - e_3) = x^3 + Ax + B$ divides $q(x)$. In other words, $q(x) \equiv 0 \bmod x^3 + Ax + B$. Since $q(x) = x_1 - x - p(x)^2$, we can also write

$$x_1 - x \equiv p(x)^2 \equiv (a + bx + cx^2)^2 \bmod (x^3 + Ax + B).$$

We shall expand the square on the right-hand side, modulo $f(x) = x^3 + Ax + B$. Notice that $x^3 \equiv -Ax - B$, and $x^4 \equiv -Ax^2 - Bx$ modulo $f(x)$:

$$\begin{aligned} x_1 - x &\equiv p(x)^2 \equiv (a + bx + cx^2)^2 \\ &\equiv c^2x^4 + 2bcx^3 + (2ac + b^2)x^2 + 2abx + a^2 \\ &\equiv c^2(-Ax^2 - Bx) + 2bc(-Ax - B) \\ &\quad +(2ac + b^2)x^2 + 2abx + a^2 \\ &\equiv (2ac + b^2 - Ac^2)x^2 \\ &\quad +(2ab - Bc^2 - 2Abc)x + (a^2 - 2bcB), \end{aligned}$$

where all the congruences are modulo $f(x) = x^3 + Ax + B$. The congruences in the previous equation say that a polynomial of degree 1, call it $g(x) = x_1 - x$, is congruent to a polynomial of degree $\leq$ 2, call the last line $h(x)$, modulo a polynomial of degree 3, namely $f(x)$. Then $h(x) - g(x)$ is a polynomial of degree ≤ 2, divisible by a polynomial of degree 3. This implies that $h(x) - g(x)$ must be zero and $h(x) = g(x)$, i.e.,

$$x_1 - x = (2ac + b^2 - Ac^2)x^2 + (2ab - Bc^2 - 2Abc)x + (a^2 - 2bcB).$$

If we match coefficients, we obtain the following equalities:

$$2ac + b^2 - Ac^2 = 0, \tag{2.10}$$

$$2ab - Bc^2 - 2Abc = -1, \tag{2.11}$$

$$a^2 - 2bcB = x_1. \tag{2.12}$$

If $c = 0$, then $b = 0$ by Eq. (2.10); therefore, $p(x) = a + bx + cx^2 = a$ is a constant function, and so $t_1 = t_2 = t_3$. By Eq. (2.9), it follows that $e_1 = e_2 = e_3$, which is a contradiction with our assumptions. Hence, c must be non-zero. We multiply Eq. (2.11) by $\frac{1}{c^2}$ and Eq. (2.10) by $\frac{b}{c^3}$ to obtain

$$\frac{2ab}{c^2} - B - \frac{2Ab}{c} = -\frac{1}{c^2}, \tag{2.13}$$

$$\frac{2ab}{c^2} + \frac{b^3}{c^3} - \frac{Ab}{c} = 0. \tag{2.14}$$

We subtract Eq. (2.13) from Eq. (2.14) to get:

$$\left(\frac{b}{c}\right)^3 + A\left(\frac{b}{c}\right) + B = \left(\frac{1}{c}\right)^2.$$

Hence, the point $P = (x_0, y_0) = (\frac{b}{c}, \frac{1}{c})$ is a rational point on $E(\mathbb{Q})$. It remains to show that $x(2P) = x(Q)$. From Eq. (2.14) we deduce that

$$a = \frac{\frac{Ab}{c} - \frac{b^3}{c^3}}{\frac{2b}{c^2}} = \frac{A - \left(\frac{b}{c}\right)^2}{2 \cdot \frac{1}{c}} = \frac{A - x_0^2}{2y_0},$$

and, therefore, substituting a in Eq. (2.12) yields

$$\begin{aligned} x(Q) = x_1 = a^2 - 2bcB &= \left(\frac{A - x_0^2}{2y_0}\right)^2 - 2bcB \\ &= \frac{(A^2 - 2Ax_0^2 + x_0^4) - (2bcB)(4y_0^2)}{4y_0^2} \\ &= \frac{(A^2 - 2Ax_0^2 + x_0^4) - (2bcB)(\frac{4}{c^2})}{4y_0^2} \\ &= \frac{(A^2 - 2Ax_0^2 + x_0^4) - 8Bx_0}{4y_0^2} \\ &= \frac{x_0^4 - 2Ax_0^2 - 8Bx_0 + A^2}{4y_0^2} = x(2P) \end{aligned}$$

as desired. In order to complete the proof of the fact that the kernel of δ is $2E(\mathbb{Q})$, we would need to consider the case when $y(Q) = y_1 = 0$, but we leave this special case to the reader (Exercise 2.12.18). ■

Thus, the previous proposition shows that there is a homomorphism $\delta : E(\mathbb{Q}) \to (\mathbb{Q}^\times/(\mathbb{Q}^\times)^2)^3$ with kernel equal to $2E(\mathbb{Q})$. In fact, the theorem shows that there is a homomorphism from $E(\mathbb{Q})$ into

$$\Gamma = \{(\delta_1, \delta_2, \delta_3) \in (\mathbb{Q}^\times/(\mathbb{Q}^\times)^2)^3 : \delta_1 \cdot \delta_2 \cdot \delta_3 = 1 \in \mathbb{Q}^\times/(\mathbb{Q}^\times)^2\}.$$

Hence, δ induces an injection

$$E(\mathbb{Q})/2E(\mathbb{Q}) \hookrightarrow \Gamma \subset (\mathbb{Q}^\times/(\mathbb{Q}^\times)^2)^3.$$

The groups $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ and Γ are infinite, so such an injection does not tell us much about the size of $E(\mathbb{Q})/2E(\mathbb{Q})$. However, the image of $E(\mathbb{Q})/2E(\mathbb{Q})$ is much smaller than Γ.

Example 2.9.4. Let $E : y^2 = x^3 - 556x + 3120$ as in Example 2.9.2. It turns out that $E(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}^2$. The generators of the torsion part are $T_1 = (6, 0)$ and $T_2 = (20, 0)$, and the generators of the free part are $P = (-8, 84)$ and $Q = (24, 60)$. The image of the map δ in this case is, therefore, generated by the images of T_1, T_2, P and Q.

$$\begin{aligned} \delta(T_1) &= (-7, -14, 2), \quad \delta(T_2) = (14, 161, 46), \\ \delta(P) &= (-14, -7, 2), \quad \delta(Q) = (2, 1, 2). \end{aligned}$$

Thus, the image of δ is formed by the 16 elements that one obtains by multiplying out $\delta(T_1)$, $\delta(T_2)$, $\delta(P)$ and $\delta(Q)$, in all possible ways. Thus, $\delta(E(\mathbb{Q})/2E(\mathbb{Q}))$ is the group:

$$\begin{aligned}&\{(1,1,1),\ (-7,-14,2),\ (14,161,46),\ (-2,-46,23),\\ &(-14,-7,2),\ (2,2,1),\ (-1,-23,23),\ (7,322,46),\\ &(2,1,2),\ (-14,-14,1),\ (7,161,23),\ (-1,-46,46),\\ &(-7,-7,1),\ (1,2,2),\ (-2,-23,46),\ (14,322,23)\}.\end{aligned}$$

(Exercise: Check that the elements listed above form a group under multiplication.) We see that the only primes that appear in the factorization of the coordinates of elements in the image of δ are: $2, 7$ and 23. Therefore, the coordinates of δ are not just in $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ but in a much smaller subgroup of 16 elements:

$$\Gamma' = \{\pm 1,\ \pm 2,\ \pm 7,\ \pm 23,\ \pm 14,\ \pm 46,\ \pm 161,\ \pm 322\} \subset \mathbb{Q}^\times/(\mathbb{Q}^\times)^2.$$

And the image of $E(\mathbb{Q})/2E(\mathbb{Q})$ embeds into

$$\begin{aligned}\Gamma_\Delta &= \{(\delta_1,\delta_2,\delta_3) \in \Gamma' \times \Gamma' \times \Gamma' : \delta_1 \cdot \delta_2 \cdot \delta_3 = 1 \in \mathbb{Q}^\times/(\mathbb{Q}^\times)^2\}\\ &\subset \Gamma' \times \Gamma' \times \Gamma'.\end{aligned}$$

Since Γ' has 16 elements and $E(\mathbb{Q})/2E(\mathbb{Q})$ embeds into $(\Gamma')^3$, we conclude that $E(\mathbb{Q})/2E(\mathbb{Q})$ has at most $(16)^3 = 2^{12}$ elements. In fact, Γ_Δ has only 16^2 elements, so $E(\mathbb{Q})/2E(\mathbb{Q})$ has at most 2^8 elements. Notice also the following interesting "coincidence": the prime divisors that appear in Γ_Δ coincide with the prime divisors of the discriminant of E, which is $\Delta_E = 6795034624 = 2^{18}\cdot 7^2\cdot 23^2$. In the next proposition we explain that, in fact, this is always the case. ■

Proposition 2.9.5. *Let $E : y^2 = (x-e_1)(x-e_2)(x-e_3)$, with $e_i \in \mathbb{Z}$. Let $P = (x_0, y_0) \in E(\mathbb{Q})$ and write*

$$(x_0 - e_1) = au^2,\ (x_0 - e_2) = bv^2,\ (x_0 - e_3) = cw^2,\ y_0^2 = abc(uvw)^2,$$

where $a, b, c, u, v, w \in \mathbb{Q}$, the numbers $a, b, c \in \mathbb{Z}$ are square-free, and abc is a square (in $\mathbb{Z}$). Then, if p divides $a \cdot b \cdot c$, then p also divides the quantity $\Delta = (e_1 - e_2)(e_2 - e_3)(e_1 - e_3)$.

Note: the discriminant of E equals $\Delta_E = 16(e_1 - e_2)^2(e_2 - e_3)^2(e_1 - e_3)^2$. So a prime p divides Δ if and only if p divides Δ_E. If $p > 2$, then this is clear (see Exercise 2.12.19 for $p = 2$).

Proof. Suppose a prime p divides abc. Then p divides a, b or c. Let us assume that $p \mid a$ (the same argument works if p divides b or c). Let p^k be the exact power of p that appears in the factorization of the rational number $x_0 - e_1 = au^2$. Notice that k may be positive or negative, depending on whether p divides the numerator or denominator of au^2. Notice, however, that k must be odd, because $p \mid a$, and a is square-free.

Suppose first that $k < 0$, i.e., $p^{|k|}$ is the exact power of p that divides the denominator of $x_0 - e_1$. Since $e_i \in \mathbb{Z}$, it follows that $p^{|k|}$ must divide the denominator of x_0 too, and therefore $p^{|k|}$ is the exact power that divides the denominators of $x_0 - e_2$ and $x_0 - e_3$ as well. Hence, $p^{3|k|}$ is the exact power of p dividing the denominator of $y_0^2 = \prod(x_0 - e_i)$, but this is impossible because y_0^2 is a square and $3|k|$ is odd. Thus, k must be positive.

If $k > 0$ and p divides $x_0 - e_1$, then the denominator of x_0 is not divisible by p, so it makes sense to consider $x_0 \bmod p$, and $x_0 \equiv e_1 \bmod p$. Similarly, the denominators of $x_0 - e_2$ and $x_0 - e_3$ are not divisible by p and

$$bv^2 \equiv x_0 - e_2 \equiv e_1 - e_2, \qquad \text{and} \qquad cw^2 \equiv x_0 - e_3 \equiv e_1 - e_3 \bmod p.$$

Since $y_0^2 = abc(uvw)^2$ and p divides a, then p must also divide one of b or c. Let's suppose it also divides b. Then $0 \equiv bv^2 \equiv x_0 - e_2 \equiv e_1 - e_2 \bmod p$ and $\Delta = (e_1 - e_2)(e_2 - e_3)(e_1 - e_3) \equiv 0 \bmod p$, as claimed. ■

The definition of the map δ and the previous proposition yield the following immediate corollary:

Corollary 2.9.6. *With notation as in the previous Theorem and Proposition, define a subgroup Γ' of $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ by*

$$\Gamma' = \{n \in \mathbb{Z} : 0 \neq n \text{ is square-free and if } p \mid n, \text{ then } p \mid \Delta\}/(\mathbb{Z}^\times)^2.$$

Then, δ induces an injection of $E(\mathbb{Q})/2E(\mathbb{Q})$ into

$$\begin{aligned}\Gamma_\Delta &= \{(\delta_1, \delta_2, \delta_3) \in \Gamma' \times \Gamma' \times \Gamma' : \delta_1 \cdot \delta_2 \cdot \delta_3 = 1 \in \mathbb{Q}^\times/(\mathbb{Q}^\times)^2\} \\ &\subset \Gamma' \times \Gamma' \times \Gamma'.\end{aligned}$$

We are ready to prove the weak Mordell-Weil theorem (Thm. 2.4.5), at least in our restricted case:

Corollary 2.9.7 (Weak Mordell-Weil theorem)**.** *Let $E : y^2 = (x - e_1)(x-e_2)(x-e_3)$ be an elliptic curve, with $e_i \in \mathbb{Z}$. Then $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite.*

Proof. By Cor. 2.9.6, $E(\mathbb{Q})/2E(\mathbb{Q})$ injects into $\Gamma_\Delta \subset \Gamma' \times \Gamma' \times \Gamma'$. Since Γ' is finite, $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite as well. ■

2.10. Homogeneous spaces

In this section we want to make the weak Mordell-Weil theorem explicit, i.e., we want:

- explicit bounds on the size of $E(\mathbb{Q})/2E(\mathbb{Q})$, and
- a method to find generators of $E(\mathbb{Q})/2E(\mathbb{Q})$ (see Exercise 2.12.25, though).

Before we discuss bounds, we need to understand the structure of the quotient $E(\mathbb{Q})/2E(\mathbb{Q})$. Remember that, from the Mordell-Weil theorem (Thm. 2.4.3), $E(\mathbb{Q}) \cong T \oplus \mathbb{Z}^{R_E}$ where $T = E(\mathbb{Q})_{\text{torsion}}$ is a finite abelian group. Therefore,

$$E(\mathbb{Q})/2E(\mathbb{Q}) \cong T/2T \oplus (\mathbb{Z}/2\mathbb{Z})^{R_E}.$$

In our restricted case, we have assumed all along that $E(\mathbb{Q})$ contains 4 points of 2-torsion, namely $\mathcal{O}$ and $(e_i, 0)$, for $i = 1, 2, 3$. And, by Exercise 2.12.6, $E(\mathbb{Q})$ cannot have more points of order 2. Thus, $T/2T \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ (see Exercise 2.12.20).

Hence, the size of $E(\mathbb{Q})/2E(\mathbb{Q})$ is exactly 2^{R_E+2}, under our assumptions. Recall that we defined $\nu(N)$ to be the number of distinct prime divisors of an integer N. We prove our first bound:

Proposition 2.10.1. *Let $E : y^2 = (x - e_1)(x - e_2)(x - e_3)$ be an elliptic curve, with $e_i \in \mathbb{Z}$. Then the rank of $E(\mathbb{Q})$ is $R_E \leq 2\nu(\Delta_E)$.*

Proof. If the quantity Δ_E has $\nu = \nu(\Delta_E)$ distinct (positive) prime divisors, then we claim that the set

$$\Gamma' = \{n \in \mathbb{Z} : 0 \neq n \text{ is square-free and if } p \mid n, \text{ then } p \mid \Delta\}/(\mathbb{Z}^\times)^2$$

has precisely $2^{\nu(\Delta_E)+1}$ elements. Indeed, if $\Delta_E = p_1^{s_1} \cdots p_\nu^{s_\nu}$, then

$$\Gamma' = \{(-1)^{t_0} p_1^{t_1} \cdots p_\nu^{t_\nu} : t_i = 0 \text{ or } 1 \text{ for } i = 0, \ldots, \nu\}.$$

Thus, Γ' has as many elements as $\{(t_0, \ldots, t_\nu) : t_i = 0 \text{ or } 1\}$, which clearly has $2^{\nu+1}$ elements. Moreover, the set Γ_Δ, as defined in Corollary 2.9.6, has as many elements as $\Gamma' \times \Gamma'$, i.e., $2^{2\nu+2}$ elements. Since $E(\mathbb{Q})/2E(\mathbb{Q})$ injects into Γ_Δ, we conclude that it also has at most $2^{2\nu+2}$ elements. Since the size of $E(\mathbb{Q})/2E(\mathbb{Q})$ is 2^{R_E+2}, we conclude that $R_E + 2 \leq 2\nu + 2$ and $R_E \leq 2\nu$, as claimed. ■

Example 2.10.2. Let

$$E : y^2 = x^3 - 1156x = x(x-34)(x+34).$$

The discriminant of $E/\mathbb{Q}$ is $\Delta_E = 98867482624 = 2^{12} \cdot 17^6$. Hence, $\nu(\Delta_E) = 2$ and the rank of E is at most 4. (The rank is in fact 2; see Example 2.10.4 below.) ■

The bound $R_E \leq 2\nu(\Delta_E)$ is, in general, not very sharp (Theorem 2.7.4 is an improvement). However, the method we followed to come up with the bound yields a strategy to find generators for $E(\mathbb{Q})/2E(\mathbb{Q})$ as follows. Recall that $E(\mathbb{Q})/2E(\mathbb{Q})$ embeds into Γ_Δ via the map δ, so we want to identify which elements of Γ_Δ may belong to the image of δ. Suppose $(\delta_1, \delta_2, \delta_3) \in \Gamma_\Delta$ belongs to the image of δ and it is not the image of a torsion point. Then there exists $P = (x_0, y_0) \in E(\mathbb{Q})$ such that:

$$\begin{cases} y_0^2 = (x_0 - e_1)(x_0 - e_2)(x_0 - e_3), \\ x_0 - e_1 = \delta_1 u^2, \\ x_0 - e_2 = \delta_2 v^2, \\ x_0 - e_3 = \delta_3 w^2 \end{cases}$$

for some rational numbers u, v, w. We may substitute the last equation in the previous two, and obtain

$$\begin{cases} e_3 - e_1 = \delta_1 u^2 - \delta_3 w^2, \\ e_3 - e_2 = \delta_2 v^2 - \delta_3 w^2. \end{cases}$$

Recall that the elements $(\delta_1, \delta_2, \delta_3)$ that are in the image of δ satisfy $\delta_1 \cdot \delta_2 \cdot \delta_3 = 1$ modulo squares. Thus, $\delta_3 = \delta_1 \cdot \delta_2 \cdot \lambda^2$ and if we do a change of variables $(u, v, w) \mapsto (X, Y, \frac{Z}{\lambda})$, we obtain a system

$$C(\delta_1, \delta_2) : \begin{cases} e_3 - e_1 = \delta_1 X^2 - \delta_1\delta_2 Z^2, \\ e_3 - e_2 = \delta_2 Y^2 - \delta_1\delta_2 Z^2, \end{cases}$$

or, equivalently, one can subtract both equations to get

$$C(\delta_1,\delta_2):\begin{cases} e_1-e_2=\delta_2Y^2-\delta_1X^2,\\ e_3-e_2=\delta_2Y^2-\delta_1\delta_2Z^2.\end{cases}$$

The space $C(\delta_1,\delta_2)$ is the intersection of two conics, and it may have rational points or not. If $(\delta_1,\delta_2,\delta_3)$ is in the image of δ, however, then the space $C(\delta_1,\delta_2)$ must have a rational point; i.e., there are $X,Y,Z\in\mathbb{Q}$ that satisfy the equations of $C(\delta_1,\delta_2)$. Moreover, if $X_0,Y_0,Z_0\in\mathbb{Q}$ are the coordinates of a point in $C(\delta_1,\delta_2)$, then

$$P=(e_1+\delta_1X_0^2,\ \delta_1\delta_2X_0Y_0Z_0) \tag{2.15}$$

is a rational point on $E(\mathbb{Q})$ such that $\delta(P)=(\delta_1,\delta_2,\delta_3)$. The spaces $C(\delta_1,\delta_2)$ are called *homogeneous spaces* and are extremely helpful when we try to calculate the Mordell-Weil group of an elliptic curve. We record our findings in the form of a proposition, for later use:

Proposition 2.10.3. *Let $E/\mathbb{Q}$ be an elliptic curve with Weierstrass equation $y^2=(x-e_1)(x-e_2)(x-e_3)$, with $e_i\in\mathbb{Z}$ and $e_1+e_2+e_3=0$. Let $\delta:E(\mathbb{Q})/2E(\mathbb{Q})\hookrightarrow\Gamma_\Delta$ be the injection given by Corollary 2.9.7, and let $\delta(E):=\delta(E(\mathbb{Q})/2E(\mathbb{Q}))$ be the image of δ in Γ_Δ. Then:*

1. *If $(\delta_1,\delta_2,\delta_3)\in\delta(E)$, then the space $C(\delta_1,\delta_2)$ has a point (X_0,Y_0,Z_0) with rational coordinates, $X_0,Y_0,Z_0\in\mathbb{Q}$.*
2. *Conversely, if $C(\delta_1,\delta_2)$ has a rational point (X_0,Y_0,Z_0), then $E(\mathbb{Q})$ has a rational point*

$$P=(e_1+\delta_1X_0^2,\ \delta_1\delta_2X_0Y_0Z_0).$$

3. *Since δ is a homomorphism and $\delta(E)$ is the image of δ, it follows that $\delta(E)$ is a subgroup of Γ_Δ. In particular:*
   - *If $(\delta_1,\delta_2,\delta_3)$ and $(\delta_1',\delta_2',\delta_3')$ are elements of the image, then their product $(\delta_1\cdot\delta_1',\ \delta_2\cdot\delta_2',\ \delta_3\cdot\delta_3')$ is also in the image;*
   - *If $(\delta_1,\delta_2,\delta_3)\in\delta(E)$ but $(\delta_1',\delta_2',\delta_3')\in\Gamma_\Delta$* **is not** *in the image, then their product $(\delta_1\cdot\delta_1',\ \delta_2\cdot\delta_2',\ \delta_3\cdot\delta_3')$* **is not** *in the image $\delta(E)$;*
   - *If $C(\delta_1,\delta_2)$ and $C(\delta_1',\delta_2')$ have rational points, then $C(\delta_1\cdot\delta_1',\ \delta_2\cdot\delta_2')$ also has a rational point;*

- *If* $C(\delta_1, \delta_2)$ *has a rational point but* $C(\delta_1', \delta_2')$ **does not have** *a rational point, then* $C(\delta_1 \cdot \delta_1',\ \delta_2 \cdot \delta_2')$ **does not have** *a rational point.*

Example 2.10.4. Let $E : y^2 = x^3 - 1156x = x(x-34)(x+34)$. The only divisors of Δ_E are 2 and 17. Thus, $\Gamma' = \{\pm 1, \pm 2, \pm 17, \pm 34\}$. Let us choose $e_1 = 0$, $e_2 = -34$ and $e_3 = 34$. Therefore, the homogeneous spaces for this curve are all of the form

$$C(\delta_1, \delta_2) : \begin{cases} \delta_2 Y^2 - \delta_1 X^2 = 34, \\ \delta_2 Y^2 - \delta_1 \delta_2 Z^2 = 68 \end{cases}$$

with $\delta_1, \delta_2 \in \Gamma'$. We analyze these spaces, case by case. There are 64 pairs (δ_1, δ_2) to take care of:

(1) $((\delta_1, \delta_2, \delta_3) = (1,1,1))$. The point at infinity (i.e., the origin) is sent to $(1,1,1)$ via δ, i.e., $\delta(\mathcal{O}) = (1,1,1)$.

(2) $(\delta_1 < 0$ and $\delta_2 < 0)$. The equation $\delta_2 Y^2 - \delta_1 \delta_2 Z^2 = 68$ cannot have solutions (in $\mathbb{Q}$ or $\mathbb{R}$) because the left-hand side is always negative for any $X, Z \in \mathbb{Q}$.

(3) $(\delta_1 > 0$ and $\delta_2 < 0)$. The equation $\delta_2 Y^2 - \delta_1 X^2 = 34$ cannot have solutions (in $\mathbb{Q}$ or $\mathbb{R}$), because the left-hand side is always negative.

(4) $(\delta_1 = -1,\ \delta_2 = 34)$. The space $C(-1, 34)$ has a rational point $(X, Y, Z) = (0, 1, 1)$, which maps to $T_1 = (0, 0)$ on $E(\mathbb{Q})$ via Eq. (2.15).

(5) $(\delta_1 = -34,\ \delta_2 = 2)$. The space $C(-34, 2)$ has the rational point $(X, Y, Z) = (1, 0, 1)$, which maps to $T_2 = (-34, 0)$ on $E(\mathbb{Q})$ via Eq. (2.15).

(6) $(\delta_1 = 34,\ \delta_2 = 17)$. If $\delta(T_1) = \delta((0,0))$ equals $(-1, 34, -34)$, and $\delta(T_2) = (-34, 2, -17)$, then

$$\delta(T_1 + T_2) = \delta(T_1) \cdot \delta(T_2) = (-1, 34, -34) \cdot (-34, 2, -17) = (34, 17, 2).$$

Thus, the space $C(34, 17)$ must have a point that maps back to $T_1 + T_2 = (34, 0)$. Indeed, $C(34, 17)$ has a point $(X, Y, Z) = (1, 2, 0)$ that maps to $(34, 0)$ via Eq. (2.15).

(7) ($\delta_1 = -1,\ \delta_2 = 2$). The space $C(-1,2)$ has a rational point $(X,Y,Z) = (4,3,5)$, which maps to $P = (-16,-120)$ on $E(\mathbb{Q})$ via Eq. (2.15). P is a point of infinite order.

(8) ($(\delta_1,\delta_2) = (1,17)$, $(34,1)$, or $(-34,34)$). These are the pairs that correspond to $(-1,2)\cdot\gamma$, with $\gamma = (-1,34)$, $(-34,2)$ or $(34,17)$. Therefore, the corresponding spaces $C(\delta_1,\delta_2)$ must have rational points that map to $P+T_1$, $P+T_2$ and $P+T_1+T_2$, respectively.

(9) ($\delta_1 = -2,\ \delta_2 = 2$). The space $C(-2,2)$ has a rational point $(X,Y,Z) = (1,4,3)$, which maps to $Q = (-2,-48)$ on $E(\mathbb{Q})$ via Eq. (2.15). Q is a point of infinite order.

(10) ($(\delta_1,\delta_2) = (2,17)$, $(17,1)$, or $(-17,34)$). These are the pairs that correspond to $(-2,2)\cdot\gamma$, with $\gamma = (-1,34)$, $(-34,2)$ or $(34,17)$. Therefore, the corresponding spaces $C(\delta_1,\delta_2)$ must have rational points that map to $Q+T_1$, $Q+T_2$ and $Q+T_1+T_2$, respectively.

(11) ($(\delta_1,\delta_2) = (2,1)$, and $(-2,34)$, $(-17,2)$, or $(17,17)$). Since $(-1,2)$ and $(-2,2)$ correspond to P and Q, respectively, then $(-1,2)\cdot(-2,2) = (2,1)$ corresponds to $P+Q$. The other pairs correspond to $(-2,2)\cdot\gamma$, with $\gamma = (-1,34)$, $(-34,2)$ or $(34,17)$. Therefore, the corresponding spaces $C(\delta_1,\delta_2)$ must have rational points that map to $P+Q+T_1$, $P+Q+T_2$ and $P+Q+T_1+T_2$, respectively.

(12) ($\delta_1 = 1,\ \delta_2 = 2$). The space $C(1,2)$ does not have rational points (see Exercise 2.12.21). In fact, it does not have solutions in $\mathbb{Q}_2$, the field of 2-adic numbers.

(13) ($(\delta_1,\delta_2) = (2,2)$, $(17,2)$, $(34,2)$, $(-1,1)$, $(-2,1)$, $(-17,1)$, $(-34,1)$, $(-1,17)$, $(-2,17)$, $(-17,17)$, $(-34,17)$, $(1,34)$, $(2,34)$, $(17,34)$, $(34,34)$). The corresponding spaces $C(\delta_1,\delta_2)$ do not have rational points. For instance, suppose $C(2,2)$ had a point. Then $(2,2,1)$ would be in the image of δ. Since $(2,1,2)$ *is* in the image of δ (we already saw above that $C(2,1)$ has a point), then $(2,1,2)\cdot(2,2,1) = (1,2,2)$ would also be in the image of δ, but we just saw (in the previous item) that $(1,2,2)$ is *not* in the image of δ. Therefore,

we have reached a contradiction and $C(2,2)$ cannot have a rational point. One can rule out all the other (δ_1, δ_2) in the list similarly.

We have analyzed all 64 possible pairs (δ_1, δ_2) and have found that the image of $E(\mathbb{Q})/2E(\mathbb{Q})$ via δ has order 2^4. Therefore, $2^{R_E+2} = 2^4$ and $R_E = 2$. The rank of the curve is exactly 2 and T_1, T_2, P and Q (as found above) are generators of $E(\mathbb{Q})/2E(\mathbb{Q})$. (In fact, they are generators of $E(\mathbb{Q})$ as well.) ■

Example 2.10.5. Let $E : y^2 = x^3 - 6724x = x(x-82)(x+82)$. Let $e_1 = 0$, $e_2 = -82$ and $e_3 = 82$. The only divisors of Δ_E are 2 and 41, hence $\Gamma' = \{\pm 1, \pm 2, \pm 41, \pm 82\}$. Let us analyze the homogeneous spaces

$$C(\delta_1, \delta_2) : \begin{cases} \delta_2 Y^2 - \delta_1 X^2 = 82, \\ \delta_2 Y^2 - \delta_1 \delta_2 Z^2 = 164 \end{cases}$$

as we did in the previous example. Once again, there are 64 pairs to check:

(1) $((\delta_1, \delta_2, \delta_3) = (1,1,1))$. The point at infinity (i.e., the origin) is sent to $(1,1,1)$ via δ, i.e., $\delta(\mathcal{O}) = (1,1,1)$.

(2) ($\delta_1 < 0$ and $\delta_2 < 0$). The equation $\delta_2 Y^2 - \delta_1 \delta_2 Z^2 = 164$ cannot have rational solutions because the left-hand side is always negative for any $X, Z \in \mathbb{Q}$.

(3) ($\delta_1 > 0$ and $\delta_2 < 0$). The equation $\delta_2 Y^2 - \delta_1 X^2 = 82$ cannot have rational solutions, because the left-hand side is always negative.

(4) $((\delta_1, \delta_2) = (-1, 82), (-82, 2), (82, 41))$. The corresponding spaces have (trivial) rational points that map, respectively, to $T_1 = (0,0)$, $T_2 = (-82, 0)$ and $T_3 = T_1 + T_2 = (82, 0)$ via Eq. (2.15).

(5) $((\delta_1, \delta_2) = (1, 2))$. The space $C(1,2)$ does not have rational points (same reason as for Exercise 2.12.21). In fact, it does not have any solutions over $\mathbb{Q}_2$.

(6) $((\delta_1, \delta_2) = (-1, 41), (-82, 1), (82, 82))$. The corresponding spaces cannot have rational points, because these elements of Γ_Δ are the product of $(1,2,2)$, with no points,

times $(-1, 82, -82)$, $(-82, 2, -41)$, $(82, 41, 2)$, which do have points by a previous item in this list.

How about all the other possible pairs (δ_1, δ_2)? Consider $(-1, 2, -2)$ and its homogeneous space:

$$C(-1,2) : \begin{cases} 2Y^2 + X^2 = 82, \\ 2Y^2 + 2Z^2 = 164. \end{cases}$$

Let us show that there are solutions to $C(-1, 2)$ over $\mathbb{R}$, $\mathbb{Q}_2$ and $\mathbb{Q}_{41}$:

- (Over $\mathbb{R}$). The point $(0, \sqrt{41}, \sqrt{41})$ is a point on $C(-1, 2)$ defined over $\mathbb{R}$.
- (Over $\mathbb{Q}_{41}$). Let $Y_0 = 1$ and put $f(X) = X^2 - 80$, $g(Z) = Z^2 - 81$. By Hensel's Lemma (see Appendix D.1 and Corollary D.1.2), it suffices to show that there are $\alpha_0, \beta_0 \in \mathbb{F}_{41}$ such that

$$f(\alpha_0) = g(\beta_0) \equiv 0 \bmod 41 \quad \text{and} \quad f'(\alpha_0),\ g'(\beta_0) \not\equiv 0 \bmod 41.$$

  The reader can check that the congruences $\alpha_0 \equiv 11 \bmod 41$ and $\beta_0 \equiv 9 \bmod 41$ work. Thus, there are $\alpha, \beta \in \mathbb{Q}_{41}$ such that $f(\alpha) = 0 = g(\beta)$. Hence, $(X_0, Y_0, Z_0) = (\alpha, 1, \beta)$ is a point on $C(-1, 2)$ defined over $\mathbb{Q}_{41}$, as desired.

- (Over $\mathbb{Q}_2$). Let $X_0 = 0$ and put $f(Y) = Y^2 - 41$. Let $\alpha_0 = 1$. Then $f(\alpha_0) = -40$, $f'(\alpha_0) = 82$ and

$$3 = \nu_2(-40) > \nu_2(82^2) = \nu_2(2^2 \cdot 41^2) = 2.$$

  Thus, by Hensel's Lemma (Theorem D.1.1; see also Example D.1.4), there is $\alpha \in \mathbb{Q}_2$ such that $f(\alpha) = 0$, or $\alpha^2 = 41$. Hence, the point $(X_0, Y_0, Z_0) = (0, \alpha, \alpha)$ is a point on $C(-1, 2)$ defined over $\mathbb{Q}_2$, as desired.

One can also show that, in fact, $C(-1, 2)$ has a point over $\mathbb{Q}_p$ *for all* $p \geq 2$. Therefore, we cannot deduce any contradictions working locally about whether $C(-1, 2)$ has a point over $\mathbb{Q}$. A computer search does not yield any $\mathbb{Q}$-points on $C(-1, 2)$. Therefore, our method breaks at this point, and we cannot determine whether there is a point on $E(\mathbb{Q})$ that comes from $C(-1, 2)$.

It turns out that $C(-1, 2)$ *does not* have rational points (but this is difficult to show). This type of space, a space that has solutions everywhere locally ($\mathbb{Q}_p$, $\mathbb{R}$) but not globally ($\mathbb{Q}$) is the main obstacle for the descent method to fully work. ■

2.11. Selmer and Sha

In Example 2.10.5, we found a type of homogeneous space that made our approach to finding generators of $E(\mathbb{Q})/2E(\mathbb{Q})$ break down. In this section, we study everywhere locally solvable spaces in detail.

Let $E : y^2 = (x - e_1)(x - e_2)(x - e_3)$ be an elliptic curve with $e_i \in \mathbb{Z}$ and $e_1 + e_2 + e_3 = 0$. Let Γ' be defined as in Corollary 2.9.7, i.e.:

$$\Gamma' = \{n \in \mathbb{Z} : 0 \neq n \text{ is square-free and if } p \mid n, \text{ then } p \mid \Delta\}/(\mathbb{Z}^\times)^2$$

where $\Delta = (e_1 - e_2)(e_2 - e_3)(e_1 - e_3)$. We define $\mathcal{H}$ as the following set of homogeneous spaces:

$$\mathcal{H} := \{C(\delta_1, \delta_2) : \delta_1, \delta_2 \in \Gamma'\}.$$

Some homogeneous spaces in $\mathcal{H}$ have rational points that correspond to rational points on $E(\mathbb{Q})$; see Prop. 2.10.3. Other homogeneous spaces do not have points (e.g. $C(1, 2)$ in Example 2.10.4, or $C(-1, 2)$ in Example 2.10.5). For each elliptic curve, we define two different sets of homogeneous spaces, the Selmer group and the Shafarevich-Tate group, as follows. The *Selmer group* is

$$\mathrm{Sel}_2(E/\mathbb{Q}) := \{C(\delta_1, \delta_2) \text{ with points over } \mathbb{R} \text{ and } \mathbb{Q}_p \text{ for all primes } p\}.$$

In other words, the Selmer group is the set of all homogeneous spaces that are solvable everywhere *locally*, i.e., over $\mathbb{R}$ and over all fields of p-adic numbers. The group operation on $\mathrm{Sel}_2(E/\mathbb{Q})$ is defined by

$$C(\delta_1, \delta_2) \cdot C(\gamma_1, \gamma_2) = C(\delta_1\gamma_1, \delta_2\gamma_2).$$

Notice that, due to Prop. 2.10.3, $E(\mathbb{Q})/2E(\mathbb{Q})$ injects into $\mathcal{H}$ via δ and the homogeneous spaces in the image of δ, i.e. $\delta(E) \subseteq \mathcal{H}$, have rational points. Since $\mathbb{Q} \subseteq \mathbb{Q}_p$ for all primes $p \geq 2$, the spaces in the image of δ belong to $\mathrm{Sel}_2(E/\mathbb{Q})$. Hence, $\mathrm{Sel}_2(E/\mathbb{Q})$ has a subgroup formed by those homogeneous spaces in $\mathrm{Sel}_2(E/\mathbb{Q})$ that have rational points as well (i.e., over $\mathbb{Q}$), and this subgroup is isomorphic to $E(\mathbb{Q})/2E(\mathbb{Q})$:

$$E(\mathbb{Q})/2E(\mathbb{Q}) = \{C(\delta_1, \delta_2) \text{ with points defined over } \mathbb{Q}\}.$$

Finally, the *Shafarevich-Tate group* is the *quotient* of the Selmer group by its subgroup $E(\mathbb{Q})/2E(\mathbb{Q})$. Thus, each element of the Shafarevich-Tate group is represented by $C(1,1)$ or by a homogeneous space that is solvable everywhere locally but *does not* have a rational point:

$$\begin{aligned} Ш_2(E/\mathbb{Q}) \quad = \quad & \{C(1,1)\} \\ & \cup \{C(\delta_1,\delta_2) \in \mathrm{Sel}_2(E/\mathbb{Q}) \text{ without points over } \mathbb{Q}\}. \end{aligned}$$

These three groups, Selmer, Ш (or "Sha") and $E/2E$, fit in a *short exact sequence*

$$0 \longrightarrow E(\mathbb{Q})/2E(\mathbb{Q}) \longrightarrow \mathrm{Sel}_2(E/\mathbb{Q}) \longrightarrow Ш_2(E/\mathbb{Q}) \longrightarrow 0.$$

In other words, the map $\psi : E(\mathbb{Q})/2E(\mathbb{Q}) \to \mathrm{Sel}_2(E/\mathbb{Q})$ is injective, the map $\phi : \mathrm{Sel}_2(E/\mathbb{Q}) \to Ш_2(E/\mathbb{Q})$ is surjective, and the kernel of ϕ is the image of ψ.

Remark 2.11.1. Here for simplicity we have defined what number theorists would usually refer to as the 2-part of the Selmer group ($\mathrm{Sel}_2(E/\mathbb{Q})$ above) and the 2-torsion of Ш (the group $Ш_2$ as defined above). For the definition of the full Selmer and Ш groups, see [**Sil86**], Ch. X, §4.

Example 2.11.2. Let $E : y^2 = x^3 - 1156x$, as in Example 2.10.4. The full group of homogeneous spaces $\mathcal{H}$ has 64 elements:

$$\mathcal{H} = \{C(\delta_1,\delta_2) : \delta_i = \pm1, \pm2, \pm17, \pm34\}.$$

The spaces in $\mathcal{H}$ with $\delta_2 < 0$ do not have points over $\mathbb{R}$, so they do not belong to $\mathrm{Sel}_2(E/\mathbb{Q})$. Moreover, we showed that the spaces $(\delta_1,\delta_2) = (2,2)$, $(17,2)$, $(34,2)$, $(-1,1)$, $(-2,1)$, $(-17,1)$, $(-34,1)$, $(-1,17)$, $(-2,17)$, $(-17,17)$, $(-34,17)$, $(1,34)$, $(2,34)$, $(17,34)$, and $(34,34)$ do not have points over $\mathbb{Q}_2$. Therefore, they do not belong to $\mathrm{Sel}_2(E/\mathbb{Q})$ either. All other spaces have rational points; therefore, they are everywhere locally solvable, so they all belong to $\mathrm{Sel}_2(E/\mathbb{Q})$. Hence,

$$\begin{aligned} \mathrm{Sel}_2(E/\mathbb{Q}) \quad = \quad & \{C(\delta_1,\delta_2) : (\delta_1,\delta_2) = \\ & \quad (1,1), (-1,34), (-34,2), (34,17), \\ & \quad (1,17), (34,1), (-34,34), (-2,2), \\ & \quad (17,1), (-17,34), (2,1), (-2,34), \\ & \quad (-17,2), (17,17), (-1,2), (2,17)\}. \end{aligned}$$

Notice that, indeed, the elements of $\mathrm{Sel}_2(E/\mathbb{Q})$ listed above form a subgroup of $\Gamma' \times \Gamma' \subset (\mathbb{Q}^\times/(\mathbb{Q}^\times)^2)^2$. Since all the elements of $\mathrm{Sel}_2(E/\mathbb{Q})$ have rational points, we conclude that $\mathrm{Sel}_2(E/\mathbb{Q})$ equals $E(\mathbb{Q})/2E(\mathbb{Q})$ and

$$Ш_2(E/\mathbb{Q}) = \mathrm{Sel}_2(E/\mathbb{Q})/(E(\mathbb{Q})/2E(\mathbb{Q})) = \{C(1,1)\},$$

i.e., $Ш_2$ is the trivial subgroup in this case. ■

Example 2.11.3. Let $E : y^2 = x^3 - 6724x$, as in Example 2.10.5. The full group of homogeneous spaces $\mathcal{H}$ has 64 elements:

$$\mathcal{H} = \{C(\delta_1, \delta_2) : \delta_i = \pm 1, \pm 2, \pm 41, \pm 82\}.$$

The spaces in $\mathcal{H}$ with $\delta_2 < 0$ do not have points over $\mathbb{R}$, so they do not belong to $\mathrm{Sel}_2(E/\mathbb{Q})$. Moreover, the spaces $(\delta_1, \delta_2) = (2,2)$, $(41,2)$, $(82,2)$, $(-1,1)$, $(-2,1)$, $(-41,1)$, $(-82,1)$, $(-1,41)$, $(-2,41)$, $(-41,41)$, $(-82,41)$, $(1,82)$, $(2,82)$, $(41,82)$, and $(82,82)$ do not have points over $\mathbb{Q}_2$. Therefore, they do not belong to $\mathrm{Sel}_2(E/\mathbb{Q})$ either. It turns out that the rest of the spaces (such as $C(-1,2)$) are everywhere locally solvable (we showed this for $C(-1,2)$). Therefore they all belong to $\mathrm{Sel}_2(E/\mathbb{Q})$. Hence,

$$\begin{aligned} \mathrm{Sel}_2(E/\mathbb{Q}) \quad = \quad & \{C(\delta_1,\delta_2) : (\delta_1,\delta_2) = \\ & (1,1), (-1,82), (-82,2), (82,41), \\ & (1,41), (82,1), (-82,82), (-2,2), \\ & (41,1), (-41,82), (2,1), (-2,82), \\ & (-41,2), (41,41), (-1,2), (2,41)\}. \end{aligned}$$

The spaces $(1,1)$, $(-1,82)$, $(-82,2)$ and $(82,41)$ have rational points that correspond to (torsion) points on $E(\mathbb{Q})$. However, *none* of the other spaces have rational solutions! Thus, the rest are representative of non-trivial elements of Sha, and we conclude that

$$E(\mathbb{Q})/2E(\mathbb{Q}) = \{C(1,1), C(-1,82), C(-82,2), C(82,41)\}$$

and $Ш_2(E/\mathbb{Q}) = \{C(\delta_1,\delta_2) : (\delta_1,\delta_2) = (1,1),\ (-1,2),\ (-2,2),\ (2,1)\}$.

Notice that the elements of $Ш_2$ listed above are representatives of all the classes in the quotient of $\mathrm{Sel}_2(E/\mathbb{Q})$ by $E(\mathbb{Q})/2E(\mathbb{Q})$. For instance, $(-1,2) \cdot (1,41) = (-1,82) \in E(\mathbb{Q})/2E(\mathbb{Q})$. Thus, $(-1,2) \cdot (1,41)$ is trivial in $Ш_2$. ■

2.12. Exercises

Exercise 2.12.1. Let $f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n$, with $a_i \in \mathbb{Z}$. Prove that if $x = \frac{p}{q} \in \mathbb{Q}$, with $\gcd(p, q) = 1$, is a solution of $f(x) = 0$, then a_n is divisible by p and a_0 is divisible by q.

Exercise 2.12.2. Let C be the conic defined by $x^2 - 2y^2 = 1$.

(1) Find all the rational points on C. (Hint: the point $O = (1, 0)$ belongs to C. Let $L(t)$ be the line that goes through O and has slope t. Since C is a quadratic and $L(t) \cap C$ contains at least one rational point, there must be a second point of intersection Q. Find the coordinates of Q in terms of t.)

(2) Let $\alpha = 1 + \sqrt{2}$. Calculate $\alpha^2 = a + b\sqrt{2}$ and $\alpha^4 = c + d\sqrt{2}$ and verify that (a, b) and (c, d) are integral points on C : $x^2 - 2y^2 = 1$. (Note: in fact, if $\alpha^{2n} = e + f\sqrt{2}$, then $(e, f) \in C$ and the coefficients of α^{2n+1} are a solution of $x^2 - 2y^2 = -1$.)

(3) (This problem is only for those who already know about continued fractions.) Find the continued fraction of $\sqrt{2}$ and find the first 6 convergents. Use the convergents to find three distinct (positive) integral solutions of $x^2 - 2y^2 = 1$, other than $(1, 0)$. (Note: the reader should remind herself or himself how to find the continued fraction and convergents *by hand*, then check his or her answer using Sage; see Appendix A.4.)

Exercise 2.12.3. Let $C/\mathbb{Q}$ be an affine curve.

(1) Suppose that $C/\mathbb{Q}$ is given by an equation of the form

$$C : xy^2 + ax^2 + bxy + cy^2 + dx + ey + f = 0. \tag{2.16}$$

Find an invertible change of variables that takes the equation of C onto one of the form $xy^2+gx^2+hxy+jx+ky+l = 0$. (Hint: consider a change of variables $X = x + \lambda$, $Y = y$).

(2) Suppose that $C'/\mathbb{Q}$ is given by an equation of the form

$$C' : xy^2 + ax^2 + bxy + cx + dy + e = 0. \tag{2.17}$$

Find an invertible change of variables that takes the equation of C' onto one of the form $y^2 + \alpha xy + \beta y = x^3 + \gamma x^2 +$

$\delta x + \eta$. (Hint: multiply (2.17) by x and consider the change of variables $X = x$ and $Y = xy$. Make sure that, at the end, the coefficients of y^2 and x^3 equal 1.)

(3) Suppose that $C''/\mathbb{Q}$ is a curve given by an equation of the form

$$C'' : y^2 + axy + by = x^3 + cx^2 + dx + e. \tag{2.18}$$

Find an invertible change of variables that takes the equation of C'' onto one of the form $y^2 = x^3 + Ax + B$. (Hint: do it in two steps. First eliminate the xy and y terms. Then eliminate the x^2 term.)

(4) Let $E/\mathbb{Q} : y^2 + 43xy - 210y = x^3 - 210x^2$. Find an invertible change of variables that takes the equation of E to one of the form $y^2 = x^3 + Ax + B$.

Exercise 2.12.4. Let C and E be curves defined, respectively, by $C : V^2 = U^4 + 1$ and $E : y^2 = x^3 - 4x$. Let ψ be the map defined by

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

(1) Show that if $U \neq 0$ and $(U, V) \in C(\mathbb{Q})$, then $\psi(U, V) \in E(\mathbb{Q})$.

(2) Find an inverse function for ψ; i.e., find $\varphi : E \to C$ such that $\varphi(\psi(U, V)) = (U, V)$.

Next, we work in projective coordinates. Let $C : W^2V^2 = U^4 + W^4$ and $E : zy^2 = x^3 + z^3$.

(3) Write down the definition of ψ in projective coordinates; i.e., what is $\psi([U, V, W])$?

(4) Show that $\psi([0, 1, 1]) = [0, 1, 0] = \mathcal{O}$.

(5) Show that $\psi([0, -1, 1]) = [0, 0, 1]$. (*Hint: Show that*

$$\psi([U, V, W]) = [2U^2, 4UW, W(V - W)].)$$

Exercise 2.12.5. Use Sage to solve the following problems:

(1) Find $3Q$, where $E : y^2 = x^3 - 25x$ and $Q = (-4, 6)$. Use $3Q$ to find a new right triangle with rational sides and area equal to 5. (Hint: Examples 1.1.2 and 2.4.1.)

(2) Let $y^2 = x(x+5)(x+10)$ and $P = (-9, 6)$. Find nP for $n = 1, \ldots, 12$. Compare the x-coordinates of nP with the list given at the end of Example 1.1.1, and write down the next three numbers that belong in the list.

Exercise 2.12.6. Let $E/\mathbb{Q}$ be an elliptic curve given by a Weierstrass equation of the form $y^2 = f(x)$, where $f(x) \in \mathbb{Z}[x]$ is a monic cubic polynomial with distinct roots (over $\mathbb{C}$).

(1) Show that $P = (x, y) \in E$ is a torsion point of exact order 2 if and only if $y = 0$ and $f(x) = 0$.

(2) Let $E(\mathbb{Q})[2]$ be the subgroup of $E(\mathbb{Q})$ formed by those rational points $P \in E(\mathbb{Q})$ such that $2P = \mathcal{O}$. Show that the size of $E(\mathbb{Q})[2]$ may be 1, 2 or 4.

(3) Give examples of three elliptic curves defined over $\mathbb{Q}$ where the size of $E(\mathbb{Q})[2]$ is 1, 2 and 4, respectively.

Exercise 2.12.7. Let $E_t : y^2 + (1-t)xy - ty = x^3 - tx^2$ with $t \in \mathbb{Q}$ and $\Delta_t = t^5(t^2 - 11t - 1) \neq 0$. As we saw in Example 2.5.4 (or Appendix E), every curve E_t has a subgroup isomorphic to $\mathbb{Z}/5\mathbb{Z}$. Use Sage to find elliptic curves with torsion $\mathbb{Z}/5\mathbb{Z}$ and rank 0, 1 and 2. Also, try to find an elliptic curve E_t with rank r, as high as possible. (Note: the highest rank known — as of 6/1/2009 — for an elliptic curve with $\mathbb{Z}/5\mathbb{Z}$ torsion is 6, discovered by Dujella and Lecacheux in 2001; see [**Duj09**].)

Exercise 2.12.8. Let $p \geq 2$ be a prime and $E_p : y^2 = x^3 + p^2$. Show that there is no torsion point $P \in E_p(\mathbb{Q})$ with $y(P)$ equal to

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

Prove that $Q = (0, p)$ is a torsion point of exact order 3. Conclude that $\{\mathcal{O}, Q, 2Q\}$ are the only torsion points on $E_p(\mathbb{Q})$. (Note: for $p = 3$, the point $(-2, 1) \in E_3(\mathbb{Q})$. Show that it is *not* a torsion point.)

Exercise 2.12.9. Prove Proposition 2.6.8, as follows:

(1) First show that if $f(x)$ is a polynomial, $f'(x)$ its derivative, and $f(\delta) = f'(\delta) = 0$, then $f(x)$ has a double root at δ.

(2) Show that if $y^2 = f(x)$ is singular, where $f(x) \in K[x]$ is a monic cubic polynomial, then the singularity must occur at $(\delta, 0)$, where δ is a root of $f(x)$.

(3) Show that $(\delta, 0)$ is singular if and only if δ is a double root of $f(x)$. Therefore $D = 0$ if and only if E is singular.

Exercise 2.12.10. Let $E/\mathbb{Q} : y^2 = x^3 + 3$. Find all the points of $\widetilde{E}(\mathbb{F}_7)$ and verify that N_7 satisfies Hasse's bound.

Exercise 2.12.11. Let $E/\mathbb{Q} : y^2 = x^3 + Ax + B$ and let $p \geq 3$ be a prime of bad reduction for $E/\mathbb{Q}$. Show that $E(\mathbb{F}_p)$ has a unique singular point.

Exercise 2.12.12. Prove parts (1) and (3) of Theorem 2.8.5. (Hint: use Definition 2.8.4 and Proposition 2.7.3.)

Exercise 2.12.13. Prove Corollary 2.8.6.

Exercise 2.12.14. Let $E : y^2 = x^3 - 10081x$. Use Sage (or PARI) to find a minimal set of generators for the subgroup that is spanned by all these points on E:

$$(0,0),\ (-100,90),\ \left(\frac{10081}{100}, \frac{90729}{1000}\right),\ (-17,408)$$

$$\left(\frac{907137}{6889}, -\frac{559000596}{571787}\right),\ \left(\frac{1681}{16}, \frac{20295}{64}\right), \left(\frac{833}{4}, \frac{21063}{8}\right)$$

$$\left(-\frac{161296}{1681}, \frac{19960380}{68921}\right), \left(-\frac{6790208}{168921}, -\frac{40498852616}{69426531}\right).$$

(Hint: use Theorem 2.7.4 to determine the rank of $E/\mathbb{Q}$.)

Exercise 2.12.15. Let E and δ be defined as in Theorem 2.9.3, and suppose $P = (x_0, y_0)$ is a point on E with $y_0 \neq 0$. Show:

- $\delta(P) \cdot \delta(\mathcal{O}) = \delta(P)$.
- $\delta((e_1, 0)) \cdot \delta((e_2, 0)) = \delta((e_1, 0) + (e_2, 0))$.
- $\delta(P) \cdot \delta((e_1, 0)) = \delta(P + (e_1, 0))$.

Exercise 2.12.16. Let $E : y^2 = x^3 + Ax + B$ be an elliptic curve with $A, B \in \mathbb{Q}$, and suppose $P = (x_0, y_0)$ is a point on E, with $y_0 \neq 0$.

(1) Prove that the x-coordinate of $2P$ is given by

$$x(2P) = \frac{x_0^4 - 2Ax_0^2 - 8Bx_0 + A^2}{4y_0^2}.$$

(2) Find a formula for $y(2P)$ in terms of x_0 and y_0.

Exercise 2.12.17. The curve $E/\mathbb{Q} : y^2 = x^3 - 157^2 x$ has a rational point Q with x-coordinate $x = x(Q)$ given by

$$x = \left(\frac{224403517704336969924557513090674863160948472041}{17824664537857719176051070357934327140032961660}\right)^2.$$

Show that there exists a point $P \in E(\mathbb{Q})$ such that $2P = Q$. Find the coordinates of P. (Hint: use PARI or Sage and Exercise 2.12.16.)

Exercise 2.12.18. Let $E : y^2 = (x - e_1)(x - e_2)(x - e_3)$ with $e_i \in \mathbb{Q}$, distinct, and such that $e_1 + e_2 + e_3 = 0$. Additionally, suppose that $e_1 - e_2 = n^2$ and $e_1 - e_3 = m^2$ are squares. This exercise shows that, under these assumptions, there is a point $P = (x_0, y_0)$ such that $2P = (e_1, 0)$, i.e., P is a point of exact order 4.

(1) Show that $e_1 = \frac{n^2+m^2}{3}$, $e_2 = \frac{m^2-2n^2}{3}$, $e_3 = \frac{n^2-2m^2}{3}$.

(2) Find A and B, in terms of n and m, such that $x^3 + Ax + B = (x - e_1)(x - e_2)(x - e_3)$. (Hint: Sage or PARI can be of great help here.)

(3) Let $p(x) = x^4 - 2Ax^2 - 8Bx + A^2 - 4(x^3 + Ax + B)e_1$. Show that $p(x_0) = 0$ if and only if $x(2P) = e_1$, and therefore $2P = (e_1, 0)$. (Hint: use Exercise 2.12.16.)

(4) Express all the coefficients of $p(x)$ in terms of n and m. (Hint: use Sage or PARI.)

(5) Factor $p(x)$ for $(n, m) = (3, 6),\ (3, 12),\ (9, 12), \ldots$.

(6) Guess that $p(x) = (x - a)^2(x - b)^2$ for some a and b. Express all the coefficients of $p(x)$ in terms of a and b.

(7) Finally, compare the coefficients of $p(x)$ in terms of a, b and n, m and find the roots of $p(x)$ in terms of n, m. (Hint: compare first the coefficient of x^3 and then the coefficient of x^2.)

(8) Write $P = (x_0, y_0)$ in terms of n and m.

Exercise 2.12.19. Let e_1, e_2, e_3 be three distinct integers. Show that $\Delta = (e_1 - e_2)(e_2 - e_3)(e_1 - e_3)$ is always even.

Exercise 2.12.20. In this exercise we study the structure of the quotient $G/2G$, where G is a finite abelian group.

(1) Let $p \geq 2$ be a prime and let $G = \mathbb{Z}/p^e\mathbb{Z}$, with $e \geq 1$. Prove that $G/2G$ is trivial if and only if $p > 2$.

(2) Prove that, if $G = \mathbb{Z}/2^e\mathbb{Z}$ and $e \geq 1$, then $G/2G \cong \mathbb{Z}/2\mathbb{Z}$.

(3) Finally, let G be an arbitrary finite abelian group. We define $G[2^\infty]$ to be the 2-primary component of G, i.e.,

$$G[2^\infty] = \{g \in G : 2^n \cdot g = 0 \text{ for some } n \geq 1\}.$$

In other words, $G[2^\infty]$ is the subgroup of G formed by those elements of G whose order is a power of 2. Prove that

$$G[2^\infty] \cong \mathbb{Z}/2^{e_1}\mathbb{Z} \oplus \mathbb{Z}/2^{e_2}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/2^{e_r}\mathbb{Z}$$

for some $r \geq 0$ and $e_i \geq 1$ (here $r = 0$ means $G[2^\infty]$ is trivial). Also show that $G/2G \cong (\mathbb{Z}/2\mathbb{Z})^r$.

Exercise 2.12.21. Show that the space

$$C : \begin{cases} 2Y^2 - X^2 = 34, \\ Y^2 - Z^2 = 34 \end{cases}$$

does not have any rational solutions with $X, Y, Z \in \mathbb{Q}$. (Hint: modify the system so there are no powers of 2 in any of the denominators, then work modulo 8.)

Exercise 2.12.22. For the following elliptic curves, use the method of 2-descent (as in Proposition 2.10.3 and Example 2.10.4) to find the rank of $E/\mathbb{Q}$ and generators of $E(\mathbb{Q})/2E(\mathbb{Q})$. **Do not** use Sage:

(1) $E : y^2 = x^3 - 14931x + 220590$.

(2) $E : y^2 = x^3 - x^2 - 6x$.

(3) $E : y^2 = x^3 - 37636x$.

(4) $E : y^2 = x^3 - 962x^2 + 148417x$. (Hint: use Theorem 2.7.4 first to find a bound on the rank.)

Exercise 2.12.23. Find the rank and generators for the rational points on the elliptic curve $y^2 = x(x + 5)(x + 10)$.

Exercise 2.12.24. (Elliptic curves with non-trivial rank.) The goal here is a systematic way to find curves of rank at least $r \geq 0$ without using tables of elliptic curves:

(1) (Easy) Find 3 non-isomorphic elliptic curves over $\mathbb{Q}$ with rank ≥ 2. You must prove that the rank is at least 2. (To show linear independence, you may use PARI or Sage to calculate the height matrix).

(2) (Fair) Find 3 non-isomorphic elliptic curves over $\mathbb{Q}$ with rank ≥ 3.

(3) (Medium difficulty) Find 3 non-isomorphic elliptic curves over $\mathbb{Q}$ with rank ≥ 6. If so, then you can probably find 3 curves of rank ≥ 8 as well.

(4) (Significantly harder) Find 3 non-isomorphic elliptic curves over $\mathbb{Q}$ of rank ≥ 10.

(5) (You would be famous!) Find an elliptic curve over $\mathbb{Q}$ of rank ≥ 29.

Exercise 2.12.25. Let E be an elliptic curve and suppose that the images of the points $P_1, P_2, \ldots, P_n \in E(\mathbb{Q})$ in $E(\mathbb{Q})/2E(\mathbb{Q})$ generate the group $E(\mathbb{Q})/2E(\mathbb{Q})$. Let G be the subgroup of $E(\mathbb{Q})$ generated by $P_1, P_2, \ldots, P_n$.

(1) Prove that the index of G in $E(\mathbb{Q})$ is finite, i.e., the quotient group $E(\mathbb{Q})/G$ is finite.

(2) Show that, depending on the choice of generators $\{P_i\}$ of the quotient $E(\mathbb{Q})/2E(\mathbb{Q})$, the size of $E(\mathbb{Q})/G$ may be arbitrarily large.

Exercise 2.12.26. Fermat's last theorem shows that $x^3 + y^3 = z^3$ has no integer solutions with $xyz \neq 0$. Find the first $d \geq 1$ such that $x^3 + y^3 = dz^3$ has infinitely many non-trivial solutions, find a generator for the solutions and write down a few examples. (Hint: Example 2.2.3.)