Their discriminants are -11, -11^5, -11, respectively. The first two curves have points of order 5, while the third curve does not have non-trivial rational points.

The further possibilities for the conductor are $N = 14, 15, 17, 19, 20, 21, 24, 26, 27, 30, \ldots$ All curves with the conductor less than 37 have only finitely many rational points (their rank is equal to 0). One of the curves with conductor 37,

$$y^2 + y = x^3 - x,$$

has a point of infinite order $(0, 0)$ (and the rank equal to 1).

15.3 Torsion group

The most important fact about elliptic curves over $\mathbb{Q}$ is the Mordell-Weil theorem.

Theorem 15.3 (Mordell-Weil)**.** *The group $E(\mathbb{Q})$ is a finitely generated Abelian group.*

In 1922, this theorem was proved by the British mathematician Louis Joel Mordell (1888 – 1972), while in 1928, the French mathematician André Weil (1906 – 1998) generalized it to Abelian varieties over number fields.

In other words, the Mordell-Weil theorem states that there is a finite set of rational points $\{P_1, \ldots, P_k\}$ on E from which all other rational points on E can be obtained by the secant-tangent construction. Since each finitely generated Abelian group is isomorphic to the product of cyclic groups (more precisely, to the product of the form $\mathbb{Z}^n \times \mathbb{Z}_{k_1} \times \cdots \times \mathbb{Z}_{k_m}$ with $k_1 \mid k_2 \mid \cdots \mid k_m$, where we denoted by $\mathbb{Z}_k$ the quotient ring $\mathbb{Z}/k\mathbb{Z}$; see [224, Chapter 2.2]), we obtain the following consequence of the Mordell-Weil theorem.

Corollary 15.4.

$$E(\mathbb{Q}) \cong E(\mathbb{Q})_{\text{tors}} \times \mathbb{Z}^r$$

The subgroup $E(\mathbb{Q})_{\text{tors}}$ of $E(\mathbb{Q})$ which consists of all points of finite order is called the *torsion group* of E, and the non-negative integer r is called the *rank* of E, and it is denoted by $\text{rank}(E)$ (or, more precisely, by $\text{rank}(E(\mathbb{Q}))$). The corollary states that there are r rational points $P_1, \ldots, P_r$ of infinite order on the curve E such that any rational point P on E can be written in the form

$$P = T + m_1 P_1 + \cdots + m_r P_r,$$

where T is a point of finite order and $m_1, \ldots, m_r$ are integers. Here, $m_1 P_1$ denotes the sum $P_1 + \cdots + P_1$ of m_1 summands, which is often also denoted by $[m_1]P_1$.

A natural question arises: which are possible values of $E(\mathbb{Q})_{\text{tors}}$ and $\text{rank}(E)$. Furthermore, we may also ask how to calculate them for a given curve E. It appears that it is much easier to give the answers to these questions for the torsion group than for the rank.

Let us, for a moment, consider points of finite order over $\mathbb{C}$ and $\mathbb{R}$. We saw that an elliptic curve over $\mathbb{C}$ can be identified with the quotient group $\mathbb{C}/L$, where $L = \{m_1\omega_1 + m_2\omega_2 \,:\, m_1, m_2 \in \mathbb{Z}\}$. Hence, $nP = \mathcal{O}$ if and only if the parameter of P (z from fundamental parallelogram such that $\wp(z) = x(P)$) is of the form $\frac{m_1}{n}\omega_1 + \frac{m_2}{n}\omega_2$, $0 \le m_1, m_2 < n$. Therefore, the solutions of the equation $nP = \mathcal{O}$ form a group isomorphic to $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

In the case of a curve with real coefficients, the lattice L has a basis in which one of the periods, say ω_1, is real, and if $\Delta > 0$ (i.e. the graph of E has two components), the other period, ω_2, is purely imaginary (hence, then the fundamental parallelogram is, in fact, a rectangle). For the case when $\Delta < 0$, a detailed description can be found in [404, Chapter 3.4]. The points in $E(\mathbb{R})$ correspond to the parameters $t \in [0, \omega_1)$ (the lower base of the parallelogram) and in the case when the graph of E has two components, also to $t - \frac{1}{2}\omega_2 \in [0, \omega_1)$ (the midsegment of the rectangle parallel to the base). Hence, the group $E(\mathbb{R})$ is isomorphic either to the circle group S^1 (when $\Delta < 0$) or to $\mathbb{Z}/2\mathbb{Z} \times S^1$ (when $\Delta > 0$). The solutions of the equation $nP = \mathcal{O}$ form a group isomorphic to $\mathbb{Z}/n\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

Let us now return to curves over $\mathbb{Q}$. From what we have already said, it follows that the group $E(\mathbb{Q})_{\text{tors}}$ should be a finite subgroup of S^1 or $\mathbb{Z}/2\mathbb{Z} \times S^1$. It is known that all finite subgroups of S^1 are cyclic. Therefore, $E(\mathbb{Q})_{\text{tors}}$ is isomorphic to a group of the form $\mathbb{Z}/k\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2k\mathbb{Z}$ (note that if k is odd, then $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/k\mathbb{Z} \cong \mathbb{Z}/2k\mathbb{Z}$).

In 1978, Mazur [296] proved that there are exactly 15 possible torsion groups for elliptic curves over $\mathbb{Q}$:

$$\begin{aligned} \mathbb{Z}/k\mathbb{Z}, &\quad \text{for } k = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/k\mathbb{Z}, &\quad \text{for } k = 2, 4, 6, 8. \end{aligned}$$

Points of order 2 on the curve $y^2 = x^3 + ax^2 + bx + c$ are precisely the points with y-coordinate equal to 0. We can have 0, 1 or 3 such points, depending on the number of rational roots of the polynomial $x^3 + ax^2 + bx + c$. These points, together with $\mathcal{O}$, form a subgroup of $E(\mathbb{Q})_{\text{tors}}$ which is either trivial or isomorphic to $\mathbb{Z}/2\mathbb{Z}$ or isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. The remaining

points of finite order can be found by using the Lutz-Nagell theorem. The idea is to find a model of the curve in which all torsion points will have integer coordinates. This is precisely the model $y^2 = x^3 + ax^2 + bx + c$, which is obtained from the general Weierstrass equation (15.1) by eliminating terms with xy and y (by substitutions (15.10) with $u = 2$, if needed). If $a_1 = a_3 = 0$, then Weierstrass equation already has the required form; otherwise, we put $a = b_2$, $b = 8b_4$, $c = 16b_6$. Then for a torsion point $P = (x, y)$, we use the fact that both P and $2P$ have integer coordinates, to obtain an estimate for y. The Lutz-Nagell theorem is often stated for an equation of the form $y^2 = x^3 + ax + b$, which is no loss of generality because the term with x^2 can be eliminated by completing the cube; however, this elimination involves additional scaling of coordinates and results with an (unnecessary) larger estimate for y. Let us mention that for a curve in the general Weierstrass form, a point $P(x, y)$ of finite order satisfies that $4x$ and $8y$ are integers.

Theorem 15.5 (Lutz-Nagell)**.** *Let E be an elliptic curve given by the equation*

$$y^2 = f(x) = x^3 + ax^2 + bx + c, \tag{15.14}$$

where $a, b, c \in \mathbb{Z}$. If $P = (x_1, y_1)$ is a point of finite order in $E(\mathbb{Q})$, then $x_1, y_1 \in \mathbb{Z}$.

A proof of the Lutz-Nagell theorem can be found in [203, Chapter 9] and [415, Chapter 8.1]. It is named after the French mathematician Élisabeth Lutz (1914 – 2008) and the Norwegian mathematician Trygve Nagell (1895 – 1988) who both published it in the 1930s.

Proposition 15.6. *Let E be an elliptic curve given by equation (15.14), where $a, b, c \in \mathbb{Z}$. If $P = (x_1, y_1)$ is a point of finite order in $E(\mathbb{Q})$, then either $y_1 = 0$ or $y_1^2 \mid \Delta_0$, where $\Delta_0 = -\Delta/16 = 27c^2 + 4a^3c + 4b^3 - a^2b^2 - 18abc$.*

Proof: If $2P = \mathcal{O}$, then $P = -P = (x_1, -y_1)$, so $y_1 = 0$. Otherwise, $2P = (x_2, y_2)$, where, according to the Lutz-Nagell theorem, $x_2, y_2 \in \mathbb{Z}$. From the formula for addition on E, we have $2x_1 + x_2 = \lambda^2 - a$, where $\lambda = \frac{f'(x_1)}{2y_1}$ is the slope of the tangent line at the point P. We see that $\lambda \in \mathbb{Z}$, which implies that $y_1 \mid f'(x_1)$. Now, from the formula

$$\Delta_0 = (-27f(x) + 54c + 4a^3 - 18ab)f(x) + (f'(x) + 3b - a^2)f'(x)^2 \tag{15.15}$$

and $y_1^2 = f(x_1)$, it follows that $y_1^2 \mid \Delta_0$. Formula (15.15) can be obtained by applying (extended) Euclid's algorithm to the polynomials $f(x)$ and $(f'(x))^2$. □

The Lutz-Nagell theorem gives us a finite list of candidates for torsion points. More precisely, it gives candidates for y-coordinates of points. However, for a given y, it is not difficult to find integer solutions of the equation $x^3 + ax^2 + bx + c - y^2 = 0$ (either by examining factors of $y^2 - c$ or by Cardano's formula for solving a cubic equation). If P is a torsion point, then for any positive integer n, the point nP has to be either $\mathcal{O}$ or one of the points from the list. Since the list is finite, we will either obtain that $nP = mP$ for $m \neq n$, in which case $(n-m)P = \mathcal{O}$ and the point P is a torsion point, or a multiple nP will be outside of the list, so P is not a torsion point. Alternatively, we can use Mazur's theorem, according to which the order of each torsion point is ≤ 12. Thus, if $nP \neq \mathcal{O}$ for all $n \leq 12$, then P is not a torsion point.

Suppose that we found all torsion points and that after that we want to determine the structure of the torsion group. According to Mazur's theorem, the only cases when the order of the group does not completely determine the structure of the group are the cases $|E(\mathbb{Q})_{\text{tors}}| = 4$, 8 and 12, when we have two possibilities: $\mathbb{Z}/4k\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2k\mathbb{Z}$, $k = 1, 2, 3$. If we have one point of order 2, then $E(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/4k\mathbb{Z}$, and if we have three points of order two, then $E(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2k\mathbb{Z}$.

Example 15.3. *Determine the torsion group of the elliptic curve*

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

Solution: We have $\Delta_0 = 4$. Therefore, any torsion point $P = (x, y)$ has to satisfy either $y = 0$ or $y \mid 2$. Hence, $y \in \{0, 1, -1, 2, -2\}$. It is clear that the equations $x^3 + x = 1$ and $x^3 + x = 4$ do not have integer solutions, while $x = 0$ is the only integer solution of the equation $x^3 + x = 0$. This means that $E(\mathbb{Q})_{\text{tors}} = \{\mathcal{O}, (0, 0)\} \cong \mathbb{Z}/2\mathbb{Z}$. ♢

Example 15.4. *Determine the torsion group of the elliptic curve*

$$E : y^2 = x^3 + 8.$$

Solution: Here, $\Delta_0 = 1728$. If $y = 0$, then $x = -2$, so we have the point $(-2, 0)$ of order 2. If $y \neq 0$, then $y^2 \mid 1728$, i.e. $y \mid 24$. By testing all possibilities, we find the following points with integer coordinates: $P_1 = (1, 3)$, $P_2 = (2, 4)$, $-P_1 = (1, -3)$, $-P_2 = (2, -4)$. By calculating multiples, we obtain

$$2P_1 = \Big(-\frac{7}{4}, -\frac{13}{8}\Big), \quad 2P_2 = \Big(-\frac{7}{4}, \frac{13}{8}\Big).$$

Since the coordinates of points $2P_1$ and $2P_2$ are not integers, we conclude that points P_1 and P_2 are of infinite order. Hence, $E(\mathbb{Q})_{\text{tors}} = \{\mathcal{O}, (-2, 0)\} \cong \mathbb{Z}/2\mathbb{Z}$. ♢

The problem with the application of the Lutz-Nagell theorem can emerge if it is difficult to factorize the discriminant Δ or if it has a lot of square factors.

In those cases, the following fact can be used.

Proposition 15.7. *Let E be the elliptic curve given by the equation*

$$y^2 = f(x) = x^3 + ax^2 + bx + c,$$

where $a, b, c \in \mathbb{Z}$. Let p be an odd prime number such that $p \nmid \Delta_0$ and let

$$\rho_p : E(\mathbb{Q}) \to E(\mathbb{F}_p)$$

be the reduction modulo p. If the point $P \in E(\mathbb{Q})$ is of finite order and $\rho_p(P) = \mathcal{O}$, then $P = \mathcal{O}$.

Proof: By the Lutz-Nagell theorem, all torsion points (except $\mathcal{O}$) have integer coordinates, so with the reduction modulo p they do not reduce to $\mathcal{O}$. □

According to Proposition 15.7, the kernel (the set of all elements of the domain that map to the neutral element of the codomain) of the restriction of the mapping ρ_p to $E(\mathbb{Q})_{\text{tors}}$ is trivial. The image of that restriction is a subgroup of $E(\mathbb{F}_p)$, so, since the order of a subgroup divides the order of the group (see [223, Chapter 3.7], [267, Chapter 1.2]), we conclude that $|E(\mathbb{Q})_{\text{tors}}|$ divides $|E(\mathbb{F}_p)|$. If we take a few values of p, then the greatest common divisor g of the corresponding values of $|E(\mathbb{F}_p)|$ has to be a multiple of $|E(\mathbb{Q})_{\text{tors}}|$.

Computing the order of $E(\mathbb{F}_p)$ for large p's is not a simple task. However, in applications for calculating the torsion group, p's are usually very small (we choose the smallest odd p's which do not divide discriminant), so that for computing $|E(\mathbb{F}_p)|$, the following formula with the Legendre symbol is sufficient

$$|E(\mathbb{F}_p)| = p + 1 + \sum_{x \in \mathbb{F}_p} \Big(\frac{x^3 + ax^2 + bx + c}{p}\Big).$$

Let us note that we will provide more information on elliptic curves over finite fields in Chapter 15.7.

Example 15.5. *Determine the torsion group of the elliptic curve*

$$E\ :\ y^2 = x^3 + 18x + 72.$$

Solution: Here, $\Delta_0 = 4 \cdot 18^3 + 27 \cdot 72^2 = 163296 = 2^5 \cdot 3^6 \cdot 7$. By using the Lutz-Nagell theorem, we should check all divisors $y \mid 108$. Instead, we can use that $|E(\mathbb{F}_5)| = 5$ and $|E(\mathbb{F}_{11})| = 8$, from where, since $\gcd(5, 8) = 1$, it follows that the torsion group of $E(\mathbb{Q})$ is trivial. $\diamondsuit$

In the previous example, for the greatest common divisor g of the obtained values of $|E(\mathbb{F}_p)|$, we got $g = 1$, so we did not have to search for torsion points. If there are non-trivial torsion points, can we find them without using the Lutz-Nagell theorem (and the corresponding factorization)? We consider the divisors n of g, starting from the largest to the smallest one, and we search for a point of order n on E (by taking into account which n's are possible by Mazur's theorem).

Here, we can use the connection with complex and real points of E. We have already mentioned that we can choose the basis for L such that points in the fundamental parallelogram which correspond to the real ones, and then also to the rational ones, lie in the interval $[0, \omega_1)$ and, in the case when the graph of E has two components, also in the interval $\frac{1}{2}\omega_2 + [0, \omega_1)$. By doubling a point from the second interval, we obtain a point from the first interval. Hence, if n is odd, all points P of order n come from parameters from the interval $[0, \omega_1)$. More precisely, their parameter is of the form $\frac{m}{n}\omega_1$, where $\gcd(m, n) = 1$. Let $mm' \equiv 1 \pmod{n}$. Then $m'P$ is also a point of order n, and its parameter is $\frac{1}{n}\omega_1$. Therefore, the value $\wp(\frac{1}{n}\omega_1)$ has to be an integer.

If n is even, then similarly as above, we conclude that one of the numbers $\wp(\frac{1}{n}\omega_1)$, $\wp(\frac{1}{n}\omega_1 + \frac{1}{2}\omega_2)$ or $\wp(\frac{1}{n}\omega_1 + \frac{1}{2}\omega_1 + \frac{1}{2}\omega_2)$ has to be an integer.

Therefore, the algorithm (*Doud's algorithm* from 1998) is the following: we calculate

- $\wp(\frac{1}{n}\omega_1)$ if n is odd or $\Delta < 0$;
- $\wp(\frac{1}{n}\omega_1)$, $\wp(\frac{1}{n}\omega_1 + \frac{1}{2}\omega_2)$, $\wp(\frac{1}{n}\omega_1 + \frac{1}{2}\omega_1 + \frac{1}{2}\omega_2)$ if n is even and $\Delta > 0$

for all divisors n of g. The value of the function $\wp$ cannot be calculated exactly but can be approximated numerically with a certain precision. If we find that a value of $\wp$-function is very close to an integer, then we test whether that integer x will give an integer value y which satisfies the equation of the elliptic curve. For a point $P = (x, y)$, obtained in that way, we calculate nP to check whether P is indeed a point of order n. If it is so,

then we obtained the largest cyclic subgroup of the torsion group and it remains to see whether there exists a point of order 2 which is not contained in that cyclic subgroup. If we obtain $nP \neq \mathcal{O}$, then we continue with smaller divisors of g. With this process, we obtain all torsion points of $E(\mathbb{Q})$.

For calculating the periods ω_1, ω_2 and values of the function $\wp$, one can use the program package PARI [331], in which many functions on elliptic curves over $\mathbb{Q}$ are implemented. Before using those functions, the elliptic function needs to be "initialized" by $E = \texttt{ellinit}(e)$, where $e = [a_1, a_2, a_3, a_4, a_6]$ is the vector of coefficients of the Weierstrass equation of E. Now, $E.\texttt{omega}[1]$ is the real and $E.\texttt{omega}[2]$ the complex period of E, while $\texttt{ellwp}(E, z)$ gives the value of the Weierstrass $\wp$ function associated to E at z.

Example 15.6. *Determine the torsion group of the elliptic curve*

$$E : \ y^2 = x^3 - 58347x + 3954150.$$

Solution: We have $4a^3 + 27b^2 = -372386507784192 = -2^{18} \cdot 3^{17} \cdot 11$. Note that in our solution, we will not use this factorization. We first take $p = 5$. We obtain $|E(\mathbb{F}_5)| = 10$. Then we obtain $|E(\mathbb{F}_7)| = 10$. Even without knowing the complete factorization, we could easily check that 11 divides the discriminant. Therefore, we continue with $p = 13$. We obtain $|E(\mathbb{F}_{13})| = 10$. Then we take $p = 17$ and we obtain $|E(\mathbb{F}_{17})| = 20$. We conclude that the order of the torsion group divides 10. The periods are

$$\omega_1 = 0.198602\ldots \quad \omega_2 = 0.156713\ldots i.$$

We calculate

$$\wp\Big(\frac{1}{10}\omega_1\Big) = 2539.825532\ldots$$

which is not close to an integer. However,

$$\wp\Big(\frac{1}{10}\omega_1 + \frac{1}{2}\omega_2\Big) = -213.000000\ldots$$

has the required property and it gives the rational point

$$(x, y) = (-213, 2592)$$

on curve E (for $\wp\big(\frac{1}{10}\omega_1 + \frac{1}{2}\omega_1 + \frac{1}{2}\omega_2\big)$ it is obtained $58.174468\ldots$). Now, it is easily checked that this point has order 10.

Since we already know that the order of the torsion group divides 10, we conclude that the torsion group is isomorphic to $\mathbb{Z}/10\mathbb{Z}$ with a generator $(-213, 2592)$. Finally, we calculate the multiples of this point and obtain

$$E(\mathbb{Q})_{\text{tors}} = \{\mathcal{O}, (-213, 2592), (651, -15552), (3, 1944), (219, -1296), (75, 0), \\ (219, 1296), (3, -1944), (651, 15552), (-213, -2592)\}. \qquad \diamondsuit$$

The methods for determining the torsion group for elliptic curves over $\mathbb{Q}$, which we described in this section, are implemented in the program package PARI through function **elltors**. The version **elltors**$(E, 1)$ uses the Lutz-Nagell theorem, while **elltors**$(E, 0)$ or **elltors**(E) uses Doud's algorithm. The result is a 3-component vector $[t, v_1, v_2]$, where t is the order of the torsion group, v_1 gives the structure of the torsion group as a product of cyclic groups, while v_2 gives generators of those cyclic groups.

We have already mentioned that in 1978, Mazur proved the following theorem.

Theorem 15.8. *There are exactly 15 possible torsion groups for elliptic curves over $\mathbb{Q}$. These are the following groups:*

$$\mathbb{Z}/k\mathbb{Z}, \quad \textit{for } k = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/k\mathbb{Z}, \quad \textit{for } k = 2, 4, 6, 8.$$

The harder part in the proof of this result lies in proving that groups which are not listed in the theorem cannot appear as a torsion group of an elliptic curve over $\mathbb{Q}$.

We will now demonstrate how, for each of the 15 groups listed in Mazur's theorem, we can construct infinitely many elliptic curves with that torsion (sub)group. We will follow the approach from [261]. First, we will consider the cyclic case, i.e. torsion groups of the form $\mathbb{Z}/k\mathbb{Z}$.

Elliptic curves will be sought in the (long) Weierstrass form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{15.16}$$

Therefore, let us give the formulas for addition of points on the curve given by (15.16): if $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$, then $P_1 + P_2 = (x_3, y_3)$, where

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

$$\lambda = \begin{cases} \frac{y_2-y_1}{x_2-x_1}, & \text{if } x_2 \neq x_1, \\ \frac{3x_1^2+2a_2x_1+a_4-a_1y_1}{2y_1+a_1x_1+a_3}, & \text{if } P_2 = P_1, \end{cases}$$

$$\mu = \begin{cases} \frac{y_1x_2-y_2x_1}{x_2-x_1}, & \text{if } x_2 \neq x_1, \\ \frac{-x_1^3+a_4x_1+2a_6-a_3y_1}{2y_1+a_1x_1+a_3}, & \text{if } P_2 = P_1. \end{cases}$$

Furthermore, $-P_1 = (x_1, -y_1 - a_1x_1 - a_3)$.

Let P be a point in $E(\mathbb{Q})$ of order k. Without loss of generality, we can assume that $P = (0,0)$ (by the substitution, i.e. translation $(x,y) \mapsto (x - x_P, y - y_P)$). Then in equation (15.16), we have $a_6 = 0$, and due to non-singularity, one of the numbers a_3 and a_4 is non-zero.

Let us first assume that P is a point of order 2. This means that $P = -P = (0, -a_3)$, so $a_3 = 0$. Hence, for curves with the equation

$$y^2 + a_1xy = x^3 + a_2x^2 + a_4x,$$

$P = (0,0)$ is a point of order 2.

If the point P is not of order 2, then we can assume that $a_4 = 0$ (so it has to be $a_3 \neq 0$), by the substitution $(x,y) \mapsto (x, y + a_3^{-1}a_4x)$ which preserves the point $(0,0)$. Hence, from now on, we will consider curves of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2.$$

Assume that P is a point on that curve of order 3. Then $-P = 2P$, so from $-P = (0, -a_3)$ and $2P = (-a_2, a_1a_2 - a_3)$, we conclude that $3P = \mathcal{O}$ if and only if $a_2 = 0$. Hence, the curves with the equation

$$y^2 + a_1xy + a_3y = x^3$$

have torsion subgroup isomorphic to $\mathbb{Z}/3\mathbb{Z}$.

In the remaining cases, we can assume that a_2 and a_3 are non-zero. Let us put $u = a_3^{-1}a_2$. The substitution $(x,y) \mapsto \left(\frac{x}{u^2}, \frac{y}{u^3}\right)$ preserves the point $P = (0,0)$, while the equation of the curve becomes

$$y^2 + a_3^{-1}a_1a_2xy + a_3^{-2}a_2^3y = x^3 + a_3^{-2}a_2^3x^2.$$

Let us introduce the notation $b = -a_3^{-2}a_2^3$, $c = 1 - a_3^{-1}a_1a_2$. We obtain the equation of the curve in the *Tate normal form*

$$y^2 + (1-c)xy - by = x^3 - bx^2, \tag{15.17}$$

named after the American mathematician John Tate (1925 – 2019) (note that the coefficients b and c are of weight 0). With this equation, the first

few multiples of the point P have very simple coordinates. We will need the coordinates of points $\pm P, \pm 2P, \ldots, \pm 6P$ (to express conditions $kP = \mathcal{O}$ for $k = 4, 5, 6, 7, 8, 9, 10, 12$). We obtain:

$$-P = (0, b),\ \ 2P = (b, bc),\ \ -2P = (b, 0),\ \ 3P = (c, b - c),\ \ -3P = (c, c^2),$$

$$4P = \left(\frac{b(b-c)}{c^2}, \frac{-b^2(b-c-c^2)}{c^3} \right), \quad -4P = \left(\frac{b(b-c)}{c^2}, \frac{b(b-c)^2}{c^3} \right),$$

$$5P = \left(\frac{-bc(b-c-c^2)}{(b-c)^2}, \frac{bc^2(b^2-bc-c^3)}{(b-c)^3} \right),$$

$$-5P = \left(\frac{-bc(b-c-c^2)}{(b-c)^2}, \frac{b^2(b-c-c^2)^2}{(b-c)^3} \right),$$

$$6P = \left(\frac{(c-b)(c^3+bc-b^2)}{(c-b+c^2)^2}, \frac{c(c-b)^2(bc^2-c^2+3bc-2b^2)}{(c-b+c^2)^3} \right),$$

$$-6P = \left(\frac{(c-b)(c^3+bc-b^2)}{(c-b+c^2)^2}, \frac{c(c^3+bc-b^2)^2}{(c-b+c^2)^3} \right).$$

From the coordinates of these points, we conclude:

- The point P is of order 4, i.e. $2P = -2P$, if and only if $c = 0$. Hence, the general form of the curve with torsion subgroup $\mathbb{Z}/4\mathbb{Z}$ is

  $$y^2 + xy - by = x^3 - bx^2, \quad b \in \mathbb{Q} \setminus \{-\tfrac{1}{16}, 0\}.$$

  We excluded values $b = -1/16$ and $b = 0$ (and similarly will happen with exceptions in the following formulas) because for them we obtain singular curves.

- The point P is of order 5, i.e. $3P = -2P$, if and only if $b = c$. Hence, the general form of the curve with torsion subgroup $\mathbb{Z}/5\mathbb{Z}$ is

  $$y^2 + (1-b)xy - by = x^3 - bx^2, \quad b \in \mathbb{Q} \setminus \{0\}.$$

- The point P is of order 6, i.e. $3P = -3P$, if and only if $b = c + c^2$. Hence, the general form of the curve with torsion subgroup $\mathbb{Z}/6\mathbb{Z}$ is

  $$y^2 + (1-c)xy - (c+c^2)y = x^3 - (c+c^2)x^2, \quad c \in \mathbb{Q} \setminus \{-\tfrac{1}{9}, -1, 0\}.$$

- The point P is of order 7, i.e. $4P = -3P$, if and only if $b(b-c) = c^3$. The equation $b^2 - bc = c^3$ can be understood as an equation of a singular cubic, with a singularity at $(b, c) = (0, 0)$. Let us put $b = cd$ in the equation to obtain the parametrization $c = d^2 - d$, $b = d^3 - d^2$. Hence, the general form of the curve with torsion group $\mathbb{Z}/7\mathbb{Z}$ is

$$y^2 + (1-c)xy - by = x^3 - bx^2,$$
$$b = d^3 - d^2, \;\; c = d^2 - d, \;\; d \in \mathbb{Q} \setminus \{0, 1\}.$$

- The point P is of order 8, i.e. $4P = -4P$, if and only if $-b(b-c-c^2) = (b-c)^2$. We again obtained a singular equation with a singularity at $(b, c) = (0, 0)$. By putting $b = cd$, we obtain $cd = 2d^2 - 3d + 1 = (2d-1)(d-1)$, so $c = \frac{(2d-1)(d-1)}{d}$, $b = (2d-1)(d-1)$. Hence, the general form of the curve with torsion group $\mathbb{Z}/8\mathbb{Z}$ is

$$y^2 + (1-c)xy - by = x^3 - bx^2,$$
$$b = (2d-1)(d-1), \;\; c = \tfrac{(2d-1)(d-1)}{d}, \;\; d \in \mathbb{Q} \setminus \{0, \tfrac{1}{2}, 1\}.$$

- The point P is of order 9, i.e. $5P = -4P$, if and only if $-c^3(b-c-c^2) = (b-c)^3$. By putting $b = cd$, we obtain $c^2 - (d-1)c = (d-1)^3$. It is a singular cubic with a singularity at $(c, d) = (0, 1)$. Let us put $c = (d-1)f$ and insert this in the last equation. We obtain $d = f^2 - f + 1$. Hence, the general form of the curve with torsion group $\mathbb{Z}/9\mathbb{Z}$ is

$$y^2 + (1-c)xy - by = x^3 - bx^2,$$
$$b = cd, \;\; c = (d-1)f, \;\; d = f^2 - f + 1, \;\; f \in \mathbb{Q} \setminus \{0, 1\}.$$

- The point P is of order 10, i.e. $5P = -5P$, if and only if $bc^2(b^2 - bc - c^3) = b^2(b - c - c^2)^2$. We again make substitutions $b = cd$ and $c = (d-1)f$ and obtain that $d = \frac{-f^2}{f^2-3f+1}$. Hence, the general form of the curve with torsion group $\mathbb{Z}/10\mathbb{Z}$ is

$$y^2 + (1-c)xy - by = x^3 - bx^2,$$
$$b = cd, \;\; c = (d-1)f, \;\; d = \tfrac{-f^2}{f^2-3f+1}, \;\; f \in \mathbb{Q} \setminus \{0, \tfrac{1}{2}, 1\}.$$

- Finally, the point P is of order 12, i.e. $6P = -6P$, if and only $(c - b)^2(bc^2 - c^2 + 3bc - 2b^2) = (c^3 + bc - b^2)^2$. After substitutions $b = cd$ and $c = (d-1)f$, we obtain $3d^2 - fd^2 - 3d - fd + f^2 + 1 = 0$. The discriminant of this quadratic equation, $(4f - 3)(f - 1)^2$, has to be

a square. Hence, we again encounter a singular cubic. From this, we have $f = \frac{t^2+3}{4}$, so we obtain $d = \frac{t^2+2t+5}{2(t+3)}$. We conclude that the general form of the curve with torsion group $\mathbb{Z}/12\mathbb{Z}$ is

$$y^2 + (1-c)xy - by = x^3 - bx^2,$$
$$b = cd,\ \ c = (d-1)f,\ \ d = \tfrac{t^2+2t+5}{2(t+3)},\ \ f = \tfrac{t^2+3}{4},\ \ t \in \mathbb{Q} \setminus \{-3, -1, 1\}.$$

We will now consider the torsion groups $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/k\mathbb{Z}$ for $k = 2, 4, 6, 8$. All such curves have three points of order 2. Therefore, here we will consider curves with the equation

$$y^2 = (x-\alpha)(x-\beta)(x-\gamma), \tag{15.18}$$

where α, β, γ are three distinct rational numbers. The curve given by equation (15.18) has three rational points of order 2, so it has a torsion subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

While constructing curves with the torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ we will use the following fact.

Theorem 15.9. *Let E be an elliptic curve over a field K, $\mathrm{char}(K) \neq 2, 3$. Let*

$$E:\ y^2 = (x-\alpha)(x-\beta)(x-\gamma), \quad \alpha, \beta, \gamma \in K.$$

For a point $Q = (x_2, y_2) \in E(K)$, there is a point $P = (x_1, y_1) \in E(K)$ such that $2P = Q$ if and only if $x_2 - \alpha$, $x_2 - \beta$ and $x_2 - \gamma$ are perfect squares in K.

Proof: We will prove one direction of this theorem, namely, that if there is a point P such that $2P = Q$, then $x_2 - \alpha$, $x_2 - \beta$ and $x_2 - \gamma$ are squares. The proof of the other direction of the theorem can be found in [248, Chapter 4.2].

Let $P = (x_1, y_1)$ be a point with the required property and let $y = \lambda x + \mu$ be the tangent line at P. Consider the polynomial

$$(x-\alpha)(x-\beta)(x-\gamma) - (\lambda x + \mu)^2.$$

Its roots are x_1 (the root of multiplicity 2) and x_2 (because the point $-Q = (x_2, -y_2)$ lies on the tangent line). Hence,

$$(x-\alpha)(x-\beta)(x-\gamma) - (\lambda x + \mu)^2 = (x-x_1)^2(x-x_2). \tag{15.19}$$

Putting $x = \alpha$ in (15.19), we obtain

$$-(\lambda\alpha + \mu)^2 = (\alpha - x_1)^2(\alpha - x_2),$$

from where we conclude that $x_2 - \alpha$ is a square. By inserting $x = \beta$ and $x = \gamma$, respectively, we conclude that both $x_2 - \beta$ and $x_2 - \gamma$ are squares. □

Let us now go back to the construction of curves with the torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. Without loss of generality, we can assume that the point $P = (0, 0)$ is one of the points of order 2, and exactly the one for which there is $Q \in E(\mathbb{Q})$ such that $2Q = P$. This means that the curve has the equation

$$y^2 = x(x - \alpha)(x - \beta)$$

and that the numbers $-\alpha$ and $-\beta$ are squares in $\mathbb{Q}$. Hence, the general form of the curve with torsion subgroup $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ is

$$y^2 = x(x + r^2)(x + s^2), \quad r, s \in \mathbb{Q} \setminus \{0\},\ r \neq \pm s. \tag{15.20}$$

A point of order 4 on (15.20) is the point $Q = (rs, rs(r + s))$. In order to obtain a curve with the torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$, there should be a point R (of order 8) such that $2R = Q$. According to Theorem 15.9, a necessary and sufficient condition for the existence of such a point is that rs, $r(r + s)$ and $s(r + s)$ are squares of rational numbers. Hence, we have: $rs = u^2$ and $r^2 + u^2 = v^2$. From this, we have $r = (t^2 - 1)w$, $u = 2tw$ for $t, w \in \mathbb{Q}$. We may take $w = 1$. Therefore, the general form of the curve with torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ is

$$y^2 = x(x + r^2)(x + s^2), \quad r = t^2 - 1,\ \ s = \frac{4t^2}{t^2 - 1},\ \ t \in \mathbb{Q} \setminus \{-1, 0, 1\}.$$

The remaining case is the torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. To obtain it, we should have a point P of order 3 on the curve (without loss of generality, we can assume that its first coordinate is equal to 0) for which there is a point Q of order 6 such that $2Q = P$. According to Theorem 15.9, then in (15.18) we should have $\alpha = -r^2$, $\beta = -s^2$, $\gamma = -t^2$. Hence, we obtain the curve

$$y^2 = (x + r^2)(x + s^2)(x + t^2), \tag{15.21}$$

which, apart from three points of the order 2, has another obvious rational point $P = (0, rst)$. If the point P is of order 3, we will obtain the required torsion group. Thus, we have to satisfy the condition $-P = 2P$, which gives

$$\frac{(r^2s^2 + r^2t^2 + s^2t^2)^2}{4r^2s^2t^2} - r^2 - s^2 - t^2 = 0,$$

i.e.

$$(sr + ts + tr)(-sr + ts + tr)(-sr + ts - tr)(sr + ts - tr) = 0.$$

We can take that $t = \frac{rs}{r-s}$, and we conclude that the general form of the curve with torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ is

$$y^2 = (x + r^2)(x + s^2)\left(x + \frac{r^2 s^2}{(r-s)^2}\right), \quad r, s \in \mathbb{Q} \setminus \{0\},\ r \neq \pm s, \frac{1}{2}s, 2s.$$

15.4 Canonical height and Mordell-Weil theorem

The two main steps in the proof of the Mordell-Weil theorem are:

- the proof that the index $[E(\mathbb{Q}) : 2E(\mathbb{Q})]$ is finite;
- properties of the *height* h, defined by $h(P) = \ln H(x)$, where $P = (x, y)$ and $H(\frac{m}{n}) = \max(|m|, |n|)$, while $h(\mathcal{O}) = 0$.

The function H is sometimes also called the "naïve" height and h the logarithmic height. It is obvious that, for any constant C, the set

$$\{P \in E(\mathbb{Q}) \,:\, h(P) \leq C\}$$

is finite (it has no more than $2(2e^C + 1)^2$ elements).

We want to find a relation between the heights of points P and $2P$ (roughly speaking, how the number of digits grows when doubling a point). Let a curve E be given by the equation $y^2 = x^3 + ax + b$ and let $P = (x, y) \in E(\mathbb{Q})$. Then the x-coordinate of the point $2P$ is

$$x(2P) = \frac{x^4 - 2ax^2 - 8bx + a^2}{4(x^3 + ax + b)}.$$

Since by squaring a number, its height doubles, and the largest power of x which appears in the expression of $x(2P)$ is x^4, we conclude that $h(2P) \approx 4h(P)$.

Example 15.7. For the curve

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

and the point $P = (0, 0)$, we have:

$$2P = (1, 0),\ \ 4P = (2, -3),\ \ 8P = \left(\tfrac{21}{25}, -\tfrac{69}{125}\right),\ \ 16P = \left(\tfrac{480106}{4225}, \tfrac{332513754}{274625}\right),$$
$$32P = \left(\tfrac{53139223644814624290821}{18700987715366274360 25}, \tfrac{12201668323950325956888219182513256}{8087174560555986485289398018 6125}\right). \qquad \diamondsuit$$

Similarly, if we look at the formula for the addition of points, we conclude that if we fix the point P_0, then $h(P + P_0) \approx 2h(P)$. This observation is stated more precisely in the following proposition (for a proof, see [415, Chapter 8.3]).