15.5 Rank of elliptic curves

The questions concerning the rank of elliptic curves over $\mathbb{Q}$ are much more difficult than those which concern the torsion group, and satisfactory answers are still unknown. For a long time, it was believed that the rank can be arbitrarily large, i.e. that for any $M \in \mathbb{N}$, there is an elliptic curve E over $\mathbb{Q}$ such that $\text{rank}(E) \geq M$. However, some recent papers provide different heuristic arguments on why the rank might actually be bounded. Nowadays, we only know that there is an elliptic curve of rank ≥ 28. This curve was found in 2006 by Noam Elkies. Klagsbrun, Sherman and Weigandt [247] proved in 2019 that the rank of that curve is equal to 28, under the assumption that the generalized Riemann hypothesis holds. Its (minimal) equation is:

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

$$2006776241557552658503320820933854275093023031217895650 2x +$$

$$3448161179503055646703298569039072037485594435931918036126600829629193944873224342 9.$$

An overview of the record curves discoveries is given in the following table (details on the record curves can be found on the web page [128]).

rank $\geq$	year	authors
3	1938	Billing
4	1945	Wiman
6	1974	Penney & Pomerance
7	1975	Penney & Pomerance
8	1977	Grunewald & Zimmert
9	1977	Brumer & Kramer
12	1982	Mestre
14	1986	Mestre
15	1992	Mestre
17	1992	Nagao
19	1992	Fermigier
20	1993	Nagao
21	1994	Nagao & Kouya
22	1997	Fermigier
23	1998	Martin & McMillen
24	2000	Martin & McMillen
28	2006	Elkies

Strictly speaking, we do not know any algorithm for calculating the rank. Namely, for "algorithms" (we will still call them so) which are used for calculating the rank, out of which we will demonstrate a few, there is no guarantee that they will provide a result in all cases. An essential part of those algorithms involves the decision of whether there are rational points on a certain curve of genus 1 for which it is known that it has points everywhere locally (i.e. over $\mathbb{R}$ and over p-adic field $\mathbb{Q}_p$ for all prime numbers p). However, no algorithm is known which would answer that question. Furthermore, even if we ignore this problem (because maybe it will not appear for a particular curve), for curves which do not have rational points of order 2 and which have large coefficients, the known algorithms are not efficient enough for practical purposes.

Let us assume that E has a point of order 2. In that case, the calculation of the rank is usually easier than in the general case. We will describe the method for calculating the rank (according to [203, Chapter 13], [375, Chapter 3]), which is called the "descent by 2-isogeny". By the change of the coordinates, we can assume that the point of order 2 is exactly the point $(0,0)$ and that E has the equation

$$y^2 = x^3 + ax^2 + bx, \tag{15.29}$$

where $a, b \in \mathbb{Z}$. If the initial curve was given by the equation $y^2 = x^3 + a_2x^2 + a_4x + a_6$ and if x_0 is a root of the polynomial $x^3 + a_2x^2 + a_4x + a_6$, then we put $a = 3x_0 + a_2$, $b = (a + a_2)x_0 + a_4$. If the initial curve was given by the Weierstrass equation, then for x_0 we take a root of the cubic polynomial $x^3 + b_2x^2 + 8b_4x + 16b_6$ and put $a = 3x_0 + b_2$, $b = (a + b_2)x_0 + 8b_4$. The condition of non-singularity for the curve E is $\Delta = 16b^2(a^2 - 4b) \neq 0$.

We say that the curve E' which has the equation

$$y^2 = x^3 + a'x^2 + b'x, \tag{15.30}$$

where $a' = -2a$ and $b' = a^2 - 4b$, is 2-*isogenous* to the curve E. The condition of non-singularity for both curves E and E' is the same, and it can be written in the form $bb' \neq 0$. Generally, an *isogeny* is a homomorphism between two elliptic curves which is given by rational functions. In our case, we have the mapping $\phi : E \to E'$, $\phi(P) = (\frac{y^2}{x^2}, \frac{y(x^2-b)}{x^2})$ for $P = (x, y) \neq \mathcal{O}, (0,0)$, and $\phi(P) = \mathcal{O}$ otherwise. Analogously, we define $\psi : E' \to E$ by $\psi(P') = (\frac{y'^2}{4x'^2}, \frac{y'(x'^2-b')}{8x'^2})$ for $P' = (x', y') \neq \mathcal{O}, (0,0)$, and $\psi(P') = \mathcal{O}$ otherwise. We have $(\psi \circ \phi)(P) = 2P$ for any $P \in E$ and $(\phi \circ \psi)(P') = 2P'$ for any $P' \in E'$.

Let us also define the mappings $\alpha : E(\mathbb{Q}) \to \mathbb{Q}^*/\mathbb{Q}^{*2}$, $\beta : E'(\mathbb{Q}) \to \mathbb{Q}^*/\mathbb{Q}^{*2}$, by $\alpha(\mathcal{O}) = 1 \cdot \mathbb{Q}^{*2}$, $\alpha(0,0) = b \cdot \mathbb{Q}^{*2}$, $\alpha(x,y) = x \cdot \mathbb{Q}^{*2}$ for $P =$

$(x,y) \neq \mathcal{O}, (0,0)$, and analogously for β. It is clear that $\mathrm{Ker}(\phi) = \{\mathcal{O}, (0,0)\}$, $\mathrm{Ker}(\psi) = \{\mathcal{O}, (0,0)\}$, and it can be shown that $\mathrm{Im}(\phi) = \mathrm{Ker}(\beta)$ and $\mathrm{Im}(\psi) = \mathrm{Ker}(\alpha)$. The number 2 in the name 2-isogeny comes from the fact that the kernels of ϕ and ψ have two elements.

These mappings are used in the first step of the proof of the Mordell-Weil theorem, i.e. in the proof that the subgroup $2E(\mathbb{Q})$ has finite index in the group $E(\mathbb{Q})$. Namely, it is easy to see that the statement follows from the finiteness of the indices $[E(\mathbb{Q}) : \psi(E'(\mathbb{Q}))]$ and $[E'(\mathbb{Q}) : \phi(E(\mathbb{Q}))]$, and this, according to the group isomorphism theorem (see [267, Chapter 1.3], [397, Chapter 2]), follows from the finiteness of the groups $\mathrm{Im}(\alpha)$ and $\mathrm{Im}(\beta)$. In fact, the connection of these mappings with the rank is even more explicit. Namely, we have

$$2^r = \frac{[E(\mathbb{Q}) : \psi(E'(\mathbb{Q}))] \cdot [E'(\mathbb{Q}) : \phi(E(\mathbb{Q}))]}{4} = \frac{|\mathrm{Im}(\alpha)| \cdot |\mathrm{Im}(\beta)|}{4},$$

where $r = \mathrm{rank}(E(\mathbb{Q}))$. The details can be found in [375, Chapter 3].

We also have $r = \mathrm{rank}(E'(\mathbb{Q}))$, but the torsion groups of E and E' do not need to be isomorphic, and $|E(\mathbb{Q})_{\mathrm{tors}}| = 2^i |E'(\mathbb{Q})_{\mathrm{tors}}|$, where $i \in \{-1, 0, 1\}$.

We would like to have a description of the elements in $\mathrm{Im}(\alpha)$. We will denote by $\tilde{x}$ the class of x in $\mathbb{Q}/\mathbb{Q}^{*2}$.

Let $(x,y) \in E(\mathbb{Q})$. If $x = 0$, then $(x,y) = (0,0)$ and $\alpha(x,y) = \tilde{b}$. If $x \neq 0$, let us write x and y in the form $x = \frac{m}{e^2}$, $y = \frac{n}{e^3}$, $\gcd(m,e) = \gcd(n,e) = 1$ and put that into the equation of E. We obtain

$$n^2 = m(m^2 + ame^2 + be^4).$$

Let $b_1 = \pm \gcd(m,b)$, where the sign is chosen such that $mb_1 > 0$. Then $m = b_1 m_1$, $b = b_1 b_2$, $n = b_1 n_1$, so we obtain

$$n_1^2 = m_1(b_1 m_1^2 + am_1 e^2 + b_2 e^4).$$

Since the factors on the right-hand side of the last equation are relatively prime and $m_1 > 0$, we conclude that there are integers M and N such that $m_1 = M^2$, $b_1 m_1^2 + am_1 e^2 + b_2 e^4 = N^2$, and from this we finally obtain the equation

$$N^2 = b_1 M^4 + aM^2 e^2 + b_2 e^4, \tag{15.31}$$

in which M, e and N are unknowns. Now, $\alpha(x,y) = (\frac{b_1 M^2}{e^2}) \cdot \mathbb{Q}^{*2} = \tilde{b_1}$.

We conclude that $\mathrm{Im}(\alpha)$ consists of $\tilde{1}$, $\tilde{b}$ and of all $\tilde{b_1}$ where b_1 is a divisor of b for which equation (15.31), where $b_1 b_2 = b$, has solutions $N, M, e \in \mathbb{Z}$, $e \neq 0$. Then $(\frac{b_1 M^2}{e^2}, \frac{b_1 MN}{e^3}) \in E(\mathbb{Q})$. Note that equation (15.31) always has

a solution for $b_1 = 1$, which is $(M, e, N) = (1, 0, 1)$ and for $b_1 = b$, which is $(M, e, N) = (0, 1, 1)$.

When examining the solvability of equation (15.31), we can assume that $\gcd(M, e) = 1$. Also, there is no loss of generality in considering only those divisors of b_1 which are square-free. Alternatively, if we consider all divisors of b_1, then we can look only for those solutions which satisfy $\gcd(N, e) = \gcd(M, N) = 1$.

We have the following algorithm for calculating the rank of an elliptic curve E which has a rational point of order 2, i.e. it has an equation of the form (15.29). For every factorization $b = b_1 b_2$, where b_1 is a square-free integer, we write down equation (15.31). We try to determine whether that equation has non-trivial integer solutions (note that for such equations the local-global principle of Hasse and Minkowski does not necessarily hold, which means that we do not have an algorithm which can with certainty answer this question). Each solution (M, e, N) of equation (15.31) induces a point on the curve E with coordinates $x = \frac{b_1 M^2}{e^2}$, $y = \frac{b_1 MN}{e^3}$. Let r_1 be the number of factorizations for which equation (15.31) has solutions and let r_2 be the number defined analogously for the curve E'. Then there are non-negative integers e_1 and e_2 such that $r_1 = 2^{e_1}$, $r_2 = 2^{e_2}$ and

$$\text{rank}(E) = e_1 + e_2 - 2.$$

Example 15.9. *Let us calculate the rank of the elliptic curve*

$$E : \ y^2 = x^3 - 5x.$$

Solution: Here, the corresponding 2-isogenous curve is

$$E' : \ y^2 = x^3 + 20x.$$

For the curve E, possibilities for the number b_1 are ± 1, ± 5. For $b_1 = 1$ and $b_1 = -5$, we know that the corresponding equations are solvable. The cases $b_1 = -1$, $b_1 = 5$ and the corresponding Diophantine equations $N^2 = -M^4 + 5e^4$, $N^2 = 5M^4 - e^4$ are remaining. Since $2^2 = -1^4 + 5 \cdot 1^4$, we conclude that $r_1 = 4$ and $e_1 = 2$.

For E', we find that $b_1' \in \{\pm 1, \pm 2, \pm 4, \pm 5, \pm 10, \pm 20\}$. However, if we take into account that b_1' is square-free and that b_1' and b_2' cannot both be negative, we conclude that $b_1' \in \{1, 2, 5, 10\}$. For 1 and 5 we are done because $\tilde{5} = \tilde{20}$, so it only remains to determine whether the equation

$$N^2 = 2M^4 + 10e^4$$

has solutions. Since M and e are relatively prime, we can assume that $\gcd(M,5) = 1$. Then, by Fermat's little theorem, $M^4 \equiv 1 \pmod 5$ and $N^2 \equiv 2 \pmod 5$. However, this is impossible because the squares of integers are congruent to 0, 1 or 4 modulo 5. We conclude that $r_2 = 2$ and $e_2 = 1$. Finally, $\text{rank}(E) = 2 + 1 - 2 = 1$. $\diamondsuit$

Note that in the previous example, for eliminating b_1''s for which the corresponding Diophantine equation does not have solutions, we used facts that a negative number cannot be a square in $\mathbb{R}$ and that the number 2 is not a square in $\mathbb{Z}/5\mathbb{Z}$. However, with Diophantine equations of degree greater than 2 it can happen that they have solutions in $\mathbb{R}$ and that they have solutions in $\mathbb{Z}/m\mathbb{Z}$ for any integer m, but that they still do not have non-trivial solutions in $\mathbb{Q}$. One such example is the equation

$$N^2 = 17M^4 - 4e^4$$

which appears in the calculation of the rank of the elliptic curve $y^2 = x^3 + 17x$. In such cases, determining the rank is significantly more difficult.

Let $\omega(b)$ denote the number of different prime factors of b. Then b has $2^{\omega(b)+1}$ (positive or negative) square-free factors. Now from the formula $2^r = \frac{|\text{Im}(\alpha)|\cdot|\text{Im}(\beta)|}{4}$, it follows that $r \leq \omega(b) + \omega(b')$. However, from equation (15.31), it follows that if $a \leq 0$ and $b > 0$, then b_1 has to be positive. Analogously, if $a' \leq 0$ and $b' > 0$, then b_1' has to be positive. Similarly, from

$$N^2 = b_1\Big(M^2 + \frac{ae^2}{2b_1}\Big)^2 - \frac{b'e^4}{4b_1}$$

it follows that if $b' < 0$, then b_1 has to be positive and analogously if $b < 0$, then b_1' has to be positive. Note that b and b' cannot be both negative since $4b + b' = a^2$. It is clear that either $a \leq 0$ or $a' \leq 0$. Therefore, the negative divisors cannot appear in at least one of the sets $\text{Im}(\alpha)$, $\text{Im}(\beta)$. We conclude that

$$r \leq \omega(b) + \omega(b') - 1.$$

In the case when the rank is equal to 0 (and we manage to prove that), all rational points on that elliptic curve can be found by the Lutz-Nagell theorem.

Example 15.10. *Find all rational points on the elliptic curve*

$$E : y^2 = x^3 - 4x.$$

Solution: The possibilities for b_1 are ± 1, ± 2, and it is clear that all four obtained equations have solutions, so $e_1 = 2$. Here, the 2-isogenous curve is $y^2 = x^3 + 16x$, which is isomorphic to

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

The possibilities for b_1' are only ± 1, out of which, the equation for $b_1' = 1$ has solutions, while the one for $b_1' = -1$ does not have solutions. Hence, $e_2 = 0$, so $\operatorname{rank}(E) = 2 + 0 - 2 = 0$.

Therefore, the only rational points on E are torsion points. From $x^3 - 4x = x(x-2)(x+2)$, we see that E has three points of order two: $(0,0)$, $(2,0)$, $(-2,0)$. The discriminant of E is 2^{12}, so we can take $p = 3$. We obtain $|E(\mathbb{F}_3)| = 4$ and conclude that E does not have any other torsion point.

Hence, $E(\mathbb{Q}) = E(\mathbb{Q})_{\text{tors}} = \{\mathcal{O}, (0,0), (2,0), (-2,0)\}$. ♢

Let us now say something about local solvability of the equation

$$N^2 = b_1 M^4 + a M^2 e^2 + b_2 e^4 \tag{15.32}$$

and its corresponding affine equation

$$u^2 = b_1 v^4 + a v^2 + b_2. \tag{15.33}$$

Generally, the criterion for solvability over $\mathbb{R}$ (i.e. for $p = \infty$) of the equation $Y^2 = g(X)$ is very simple: the polynomial g has to assume a non-negative value at some point x. That will be certainly satisfied if g has real roots, and if g does not have real roots, then the leading coefficient of g has to be positive.

When it comes to solving equation (15.33) in $\mathbb{Q}_p$ (i.e. equation (15.32) modulo p^k for any $k \geq 1$), it is sufficient to consider only those primes p for which $p \mid 2\Delta$. Namely, it can be shown that for all other primes p, the equation is solvable.

We can write down equation (15.32) in the form

$$N^2 = b_1 \left(M^2 + \frac{a e^2}{2 b_1} \right)^2 - \frac{b' e^4}{4 b_1},$$

which gives the condition that for each odd prime divisor p of b' the Legendre symbol $(\frac{b_1}{p})$ has to be equal to 1. This is only a necessary but not a sufficient condition for the solvability in $\mathbb{Q}_p$. The general algorithm uses Hensel's lemma, so that for a given solution modulo p^k, it checks whether that solution can be "lifted" to the solution modulo p^{k+1}. As soon as k is large enough ($k > \nu_p(\Delta)$), the algorithm answers that question and solves the problem of solvability in $\mathbb{Q}_p$.

Let us assume that in the above-described algorithm of "descent by 2-isogeny" we came to the equation

$$u^2 = b_1 v^4 + a v^2 + b_2, \quad b_1 b_2 = b \tag{15.34}$$

which is everywhere locally solvable, but we did not manage to find a rational point on it. Then we can apply the method of "second descent" which can sometimes be used to find a rational point (u, v) on (15.34) or to prove that (15.34) does not have rational points. The idea is that since (15.34) is everywhere locally solvable, then also the corresponding conic

$$u^2 = b_1 w^2 + a w + b_2 \tag{15.35}$$

is everywhere locally solvable. However, for such quadratic equations, the local-global principle of Hasse and Minkowski holds, which implies that (15.35) is also globally solvable, i.e. it has a rational point (u_0, w_0). We can assume that $w_0 \neq 0$, because if $w_0 = 0$, then b_2 is a square so equation (15.34) certainly has a solution. All rational points on (15.35) can be obtained by the following parametric formulas:

$$w = \frac{w_0 t^2 - 2u_0 t + a + b_1 w_0}{t^2 - b_1},$$
$$u = \frac{-u_0 t^2 + (a + 2b_1 w_0)t - u_0 b_1}{t^2 - b_1}.$$

We would like to find (or prove that there does not exist) a rational number t such that $w = \frac{f(t)}{g(t)}$ is the square of a rational number. This condition leads to new quartics (for details, see [87, Chapter 3.6.6]). Now, we repeat with them the process of examining local solvability and searching for solutions with a relatively small height. Again, there are no guarantees that we will in each case get an answer.

The set of all $\tilde{b_1}$'s for which equation (15.31) is everywhere locally solvable also forms a group (and analogously for $\tilde{b_1'}$). If the corresponding group orders are 2^{f_1} and 2^{f_2}, then the number $s = f_1 + f_2 - 2$ is called the *2-Selmer rank* of E (see [373, Chapter 10.4]). It is clear that $r \leq s$. We noticed that it can be $r = s$, but also $r < s$ is possible. The conjecture is that $r \equiv s \pmod 2$.

The program MWRANK by John Cremona is an excellent freely available implementation of algorithms presented in this section. It is included in the program package SageMath. The algorithms are explained in detail in the book [94]. As of February 2021, the 2-descent algorithm is also implemented in PARI [331] through function **`ellrank`**.

For example, for the curve

$$y^2 + xy + y = x^3 + 343182146424416463624356325625799087 47x$$
$$+ 318437689581412719724488628468621484859945381164348693675 6$$

(Dujella, 2002) in less than a second, we obtain the result that the rank is equal to 15. In 2002, this curve was the curve with the largest rank for which the rank was exactly calculated (not only the lower bound for rank). Let us mention that in this example, the 2-Selmer rank is equal to the true rank, i.e. all corresponding quartics which are everywhere locally solvable are also globally solvable.

In the general case, when E does not have a point of order 2, the idea is again to assign to the curve E a family of quartics. In this case, they have the more general form

$$y^2 = g(x) = ax^4 + bx^3 + cx^2 + dx + e. \tag{15.36}$$

Here $a, b, c, d, e \in \mathbb{Q}$, such that

$$12ae - 3bd + c^2 = \lambda^4 c_4, \quad 72ace + 9bcd - 27ad^2 - 27eb^2 - 2c^3 = 2\lambda^6 c_6$$

for some $\lambda \in \mathbb{Q}$. A detailed description of the algorithm can be found in [94, Chapter 3.6]. The core of the algorithm is given in the paper by Birch and Swinnerton-Dyer [47] from 1963. This algorithm is also contained in MWRANK (although it works significantly less efficiently than the version for curves with a point of order 2).

If we choose an elliptic curve "randomly", it will, most likely, have a trivial torsion group and a very small rank (0 or 1). A conjecture is that the average rank is $1/2$ ("half" of curves have rank 0, and the other "half" rank 1, and rank ≥ 2 appears asymptotically for $0\,\%$ of all curves). From the results of Manjul Bhargava, winner of the Fields medal in 2014, and his collaborators, it follows that the average rank is strictly less than 1 (here, we assume that we ordered the elliptic curves $y^2 = x^3 + Ax + B$, $A, B \in \mathbb{Z}$, with respect to the size of $\max(4|A|^3, 27B^2)$). We saw before how we can ensure that a curve has in advance prescribed torsion subgroup. Now, we will consider the methods for finding elliptic curves of relatively large rank (even though a very large rank cannot be expected by having in mind that no elliptic curve with rank larger than 28 is known at the moment).

The general method for finding a curve with large rank consists of the following three phases:

- *Construction:* We generate a family of elliptic curves over $\mathbb{Q}$ (e.g. a curve over the field of rational functions $\mathbb{Q}(t)$) for which we believe (or know) that it contains elliptic curves of large rank, because the "generic" rank of the curve over $\mathbb{Q}(t)$ is relatively large. According to Silverman's specialization theorem [372, Chapter 3.11], for all except finitely many rational numbers t_0, the rank over $\mathbb{Q}$ of the curve which is obtained by inserting ("specializing") $t = t_0$, will be greater than or equal to the generic rank. Let us mention that an algorithm, whose authors are Gusić and Tadić [205, 206], for curves with at least one point of order 2 over $\mathbb{Q}(t)$, enables finding corresponding injective specializations $t = t_0$ and calculating the generic rank.

- *Sieve:* For each curve in the considered family (with not too huge coefficients), we calculate some data which gives us certain information about the rank (e.g. a lower and upper bound for the rank – perhaps under the assumption that certain widely accepted conjectures hold). Here, it is important that those (imprecise) information about the rank can be calculated much faster than the rank itself. Based on this information, we choose ("sieve") a small subset of the best candidates for the large rank in the considered family.

- *Calculating the rank:* For all curves from the (small) set of the best candidates, we try to calculate the rank exactly or at least to find a good lower bound for the rank to confirm that the curve indeed has a large rank.

Most of the methods which are still used, with some modifications, in the first two phases were introduced by Jean-François Mestre in the 1980s and 1990s.

We will demonstrate one of his constructions (from [300]) by which he obtained in 1991 infinitely many elliptic curves of rank ≥ 11. That construction is called the *Mestre polynomial method*. The initial point in the construction is the following fact (a special case of Lemma 11.17 for $r = 2$), which we could call "lemma on square rooting with a remainder".

Lemma 15.14. *Let $p(x) \in \mathbb{Q}[x]$ be a monic polynomial and $\deg p = 2n$. Then there are unique polynomials $q(x), r(x) \in \mathbb{Q}[x]$ such that $p = q^2 - r$ and $\deg r \leq n - 1$.*

The polynomial q can be found by successive computation of unknown coefficients of the polynomial q or from the asymptotic expansion of $\sqrt{p}$.

Let us now assume that $p(x) = \prod_{i=1}^{2n}(x - a_i)$, where $a_1, \ldots, a_{2n}$ are distinct rational numbers. Then the points $(a_i, \pm q(a_i))$, $i = 1, \ldots, 2n$ lie on the curve

$$C: \quad y^2 = r(x).$$

If $\deg r = 3$ or 4, and $r(x)$ does not have multiple roots, then C represents an elliptic curve. For $\deg r = 3$, that is clear. If $\deg r = 4$, then we choose one rational point on C (e.g. $(a_1, q(a_1))$) for the point at infinity and transform C into an elliptic curve (see Chapter 15.2).

For $n = 5$, almost all choices of a_i's give $\deg r = 4$. Then C has 10 rational points of the form $(a_i, q(a_i))$ and we can expect that we will obtain an elliptic curve of rank ≥ 9. Mestre constructed a family of elliptic curves (i.e. an elliptic curve over the field of rational functions $\mathbb{Q}(t)$) of rank ≥ 11, by taking $n = 6$ and $a_i = b_i + t$, $i = 1, \ldots, 6$; $a_i = b_{i-6} - t$, $i = 7, \ldots, 12$. In the general case, the polynomial $r(x)$ has degree 5. However, we can try to choose the numbers $b_1, \ldots, b_6$ such that the coefficient of x^5 is equal to 0, in order to obtain a polynomial of degree 4. In Mestre's example from 1991, these numbers were $b_1 = -17$, $b_2 = -16$, $b_3 = 10$, $b_4 = 11$, $b_5 = 14$, $b_6 = 17$.

Later on, Mestre, Nagao and Kihara, by using similar constructions improved this result and constructed curves over $\mathbb{Q}(t)$ of rank 14. In 2006, by using different methods, which originated in algebraic geometry, Elkies managed to construct a curve over $\mathbb{Q}(t)$ of rank 18 (see [172], [362, Chapter 13.1]). All these curves have a trivial torsion group. Fermigier, Kulesz and Lecacheux modified Mestre's method and obtained families of curves with (relatively) large rank and non-trivial torsion group. As we will see in Chapter 16.7, elliptic curves connected to Diophantine m-tuples can also be used for constructing elliptic curves (over $\mathbb{Q}$ and $\mathbb{Q}(t)$) with large rank for torsion groups $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/k\mathbb{Z}$, $k = 2, 4, 6, 8$.

In the second phase, sieving, the rough idea is that it is more likely that the curve will have "many" rational points (i.e. large rank) if it has many points in the reduction modulo p (i.e. if the number $N_p = |E(\mathbb{F}_p)|$ is large) for "most" p's. Let us note that according to Hasse's theorem, we have

$$p + 1 - 2\sqrt{p} \leq N_p \leq p + 1 + 2\sqrt{p},$$

so the condition that the number N_p is large, actually means that it is near the upper bound from Hasse's theorem.

A much more precise version of this rough idea is the famous *Birch and Swinnerton-Dyer (BSD) conjecture* which states that

$$\prod_{p \leq X,\, p \nmid 2\Delta} \frac{N_p}{p} \sim const \cdot (\ln X)^r,$$

where $r = \text{rank}(E)$. The BSD conjecture is usually stated in terms of the L-function which is defined by

$$L(E,s) = \prod_{p\nmid\Delta} \left(1 - a_p p^{-s} + p^{1-2s}\right)^{-1} \cdot \prod_{p|\Delta} \left(1 - a_p p^{-s}\right)^{-1},$$

where $a_p = p + 1 - N_p$ for p's at which E has good reduction, $a_p = 0$ in the case of additive reduction, $a_p = 1$ in the case of multiplicative split and $a_p = -1$ in the case of multiplicative non-split reduction. This function can be understood as an analogue of the Riemann zeta-function and the Dirichlet L-function if we recall Euler's formula $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p (1 - p^{-s})^{-1}$ (Theorem 7.15) and formula (7.24). The function $L(E,s)$ has an analytic continuation to the whole complex plane $\mathbb{C}$ and it satisfies the functional equation

$$\Lambda(s) = w_E \cdot \Lambda(2 - s),$$

where $w_E \in \{-1, 1\}$, while

$$\Lambda(s) = N^{s/2}(2\pi)^{-s}\Gamma(s)L(E,s),$$

where Γ is the gamma-function and N denotes the conductor of E.

Now, the BSD conjecture can be stated as follows: the order of the zero of $L(E,s)$ at $s = 1$ (the so-called *analytic rank* of E) is equal to the rank r, i.e.

$$L(E,s) = c \cdot (s-1)^r + \text{terms of higher order},$$

where $c \neq 0$ is a constant. It is known that the conjecture holds if the analytic rank is equal to 0 or 1 (Kolyvagin, 1989).

A conjecture (which follows from the BSD conjecture) is that the value w_E determines the parity of the rank: $w_E = (-1)^r$, i.e. if $w_E = 1$, then the rank is even, and if $w_E = -1$, then the rank is odd (this is called the "parity conjecture", and it enables to conditionally determine rank in the cases where, by other methods, we obtain the conclusion that $r \in \{r', r'+1\}$ for some r'). The value w_E can be calculated in PARI by using the function **`ellrootno`**.

Even though Birch and Swinnerton-Dyer conjecture is very important for understanding the rank of elliptic curves, it is not so useful for direct calculation (even the conditional) of the rank. Therefore, in the sieving phase, we usually use other variants of the above mentioned rough idea.

We can fix a finite set of primes $\mathcal{P}$, and for each $p \in \mathcal{P}$ find all values of parameters modulo p which maximize N_p. If we consider the curve of the form $y^2 = x^3 + ax + b$, parameters will be $(a,b) \in \mathbb{F}_p^2$, and the maximal N_p is

$p+1+\lfloor 2\sqrt{p}\rfloor$. If we look for curves of large rank with a given torsion group, then we use the corresponding parametrization from Chapter 15.3, and the maximal N_p is $|E(\mathbb{Q})_{\text{tors}}| \cdot \left\lfloor \frac{p+1+\lfloor 2\sqrt{p}\rfloor}{|E(\mathbb{Q})_{\text{tors}}|} \right\rfloor$. After that, by using the Chinese remainder theorem, we construct the list with parameters which maximize N_p for every $p \in \mathcal{P}$. This is called the finite field method.

Mestre and Nagao (see [299, 314]) gave heuristic arguments (motivated by the BSD conjecture) which suggest that for curves of large rank, certain sums should take large values (the largest in the considered family of curves). Some of those sums are

$$S_1(X) = \sum_{p \le X} \frac{N_p + 1 - p}{N_p} \ln p,$$
$$S_2(X) = \sum_{p \le X} \frac{N_p + 1 - p}{N_p},$$
$$S_3(X) = \sum_{p \le X} (N_p - p - 1) \ln p.$$

In the applications of this idea, we choose a few positive integers $X_1 < X_2 < \cdots < X_k$, and calculate $S_i(X_1)$, $S_i(X_2), \ldots$ but in each step, we discard, say 80 % of "the worst" curves, i.e. those with the smallest values of the corresponding sum. Note that for an efficient implementation of this method, X_k should not be too large (for instance, $X_k < 100000$) because we do not have a sufficiently efficient algorithm for calculating N_p for large primes p. In PARI, the number a_p can be calculated by the function **ellap**(E, p), so N_p is obtained as $N_p = p + 1 - a_p$.

We saw that in the case when E has a rational point of order 2, we have a very simple upper bound for the rank: $r \le \omega(b) + \omega(b') - 1$, and also $r \le s$, where s is the 2-Selmer rank. Generally, in the case when E has a point of finite order, it is possible to give a simple upper bound for the rank. If we are lucky enough, that upper bound might coincide with the lower bound obtained by searching for the points of small height. In such cases, we may obtain the exact value for the rank without applying the method of general 2-descent. The mentioned upper bound is called *Mazur's bound* [295]. Let E be an elliptic curve over $\mathbb{Q}$ given by its minimal Weierstrass equation and let E have a rational point of an odd prime order p. Then

$$r \le m_p = b + a - m - 1,$$

where

- b is the number of primes with bad reduction;
- a is the number of primes with additive reduction;
- m is the number of primes q with multiplicative reduction such that p does not divide the exponent of q in Δ and that $q \not\equiv 1 \pmod{p}$.

Example 15.11 (Dujella-Lecacheux, 2001)**.** *Let us try to calculate the rank of the curve E given by the equation*

$$y^2+y=x^3+x^2-1712371016075117860x+8857879575356913895129401 64.$$

Solution: We have

$$E(\mathbb{Q})_{\text{tors}} = \{\mathcal{O}, (888689186, 8116714362487), (-139719349, -33500922231893), (-139719349, 33500922231892), (888689186, -8116714362488)\} \cong \mathbb{Z}/5\mathbb{Z}.$$

Therefore, we can calculate Mazur's bound m_5. The discriminant is

$$\Delta = -3^{15} \cdot 5^5 \cdot 7^5 \cdot 11^5 \cdot 19^5 \cdot 41^5 \cdot 127^5 \cdot 1409 \cdot 10864429,$$

so we have $b = 9$, $a = 0$, $m = 2$ and we obtain $r \leq m_5 = 6$.

By searching for the points $P = (x, y)$ on E with integer coordinates and $|x| < 10^9$, we find the following six independent points modulo $E(\mathbb{Q})_{\text{tors}}$:

$$(624069446, 7758948474007), (763273511, 4842863582287)$$
$$(680848091, 5960986525147), (294497588, 20175238652299)$$
$$(-206499124, 35079702960532), (676477901, 6080971505482),$$

which shows that $\text{rank}(E) = 6$ (this was at the moment of discovery the curve of the largest known rank with the torsion group $\mathbb{Z}/5\mathbb{Z}$, and it was obtained by specializing parameters in a family of elliptic curves from [269]). ♢

Let G be one of 15 possible torsion groups for an elliptic curve over $\mathbb{Q}$ (according to Mazur's theorem). Let us define

$$B(G) = \sup\{\text{rank}(E(\mathbb{Q})) \,:\, E(\mathbb{Q})_{\text{tors}} = G\}.$$

There was a conjecture that $B(G)$ is unbounded for any G. However, as we already mentioned, there are recent papers which suggest that the rank is bounded, which means that the value $B(G)$ is also bounded for any G. At

present, we know that $B(G) \geq 3$ for any G. In the following table, the best known lower bounds for $B(G)$ are given. Most of the results from this table are obtained by a combination of the methods described in this section, with several improvements described in the recent paper by Elkies and Klagsbrun [173]. The details on record curves can be found on the web page [127].

G	$B(G) \geq$	authors
0	28	Elkies (2006)
$\mathbb{Z}/2\mathbb{Z}$	20	Elkies & Klagsbrun (2020)
$\mathbb{Z}/3\mathbb{Z}$	15	Elkies & Klagsbrun (2020)
$\mathbb{Z}/4\mathbb{Z}$	13	Elkies & Klagsbrun (2020)
$\mathbb{Z}/5\mathbb{Z}$	9	Klagsbrun (2020)
$\mathbb{Z}/6\mathbb{Z}$	9	Klagsbrun (2020), Voznyy (2020)
$\mathbb{Z}/7\mathbb{Z}$	6	Klagsbrung (2020)
$\mathbb{Z}/8\mathbb{Z}$	6	Elkies (2006), Dujella, MacLeod & Peral (2013)
$\mathbb{Z}/9\mathbb{Z}$	4	Fisher (2009), van Beek (2015), Dujella & Petričević (2021)
$\mathbb{Z}/10\mathbb{Z}$	4	Dujella (2005, 2008), Elkies (2006), Fisher (2016)
$\mathbb{Z}/12\mathbb{Z}$	4	Fisher (2008)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	15	Elkies (2009)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$	9	Dujella & Peral (2012, 2019), Klagsbrung (2020)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$	6	Elkies (2006), Dujella, Peral & Tadić (2015), Dujella & Peral (2020)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$	3	Connell (2000), Dujella (2000, 2001, 2006, 2008), Campbell & Goins (2003), Rathbun (2003, 2006), Dujella & Rathbun (2006), Flores, Jones, Rollick, Weigandt & Rathbun (2007), Fisher (2009)

There are also more precise predictions on how large the rank of an elliptic curve with given torsion group can be. It might be interesting to mention that in [332, Chapter 8.3], the prediction stated that only finitely many elliptic curves with torsion groups $\mathbb{Z}/8\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$ have rank ≥ 4. On the other hand, Dujella and Peral [153] proved that there are infinitely many elliptic curves with those torsion groups and rank ≥ 3, so if the above prediction is correct, this would be the best possible result for those torsion groups.

15.6 Finite fields

Before we move on to study elliptic curves over finite fields and their applications, let us provide a short introduction to the finite fields. More about