Elliptic equations

Andrej Dujella

Winter School on Explicit Methods in Number Theory,
Debrecen, January 26-30, 2009.

1 Introduction

Let $\mathbb{K}$ be a field. In general, an *elliptic curve* over $\mathbb{K}$ is a nonsingular projective cubic curve over $\mathbb{K}$ with at least one $\mathbb{K}$-rational point. Hence, it has the equation of the form

$$F(x,y) = ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0,$$

where $a, b, c, \ldots, j \in \mathbb{K}$, and the nonsingularity means that in every point on the curve, considered in the projective plane $\mathbb{P}^2(\overline{\mathbb{K}})$ over the algebraic clusure of $\mathbb{K}$, at least one partial derivative of F is non-zero. Each such equation can be transformed by birational transformations to the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{1}$$

which is called the *Weierstrass form*.

Program packages which deal with elliptic curves (PARI/GP, APECS, KANT/KASH, SAGE, MAGMA) usually initialize an elliptic curve as the vector $[a_1, a_2, a_3, a_4, a_6]$. Note that there is no a_5. An explanation is that if we give the weight i to a_i, the weight 2 to x and the weight 3 to y, then all summands in (1) have the weight 6.

If $\mathrm{char}(\mathbb{K}) \neq 2, 3$, then the equation (1) can be transformed to the form

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

which is called the *short Weierstrass form*. Now the nonsingularity means that the cubic polynomial $f(x) = x^3 + ax + b$ has no multiple roots (in algebraic closure $\overline{\mathbb{K}}$), or equivalently that the *discriminant* $\Delta = -4a^3 - 27b^2$ in nonzero.

Thus, if $\mathrm{char}(\mathbb{K}) \neq 2, 3$, it is often convenient to define an elliptic curve $E(\mathbb{K})$ over $\mathbb{K}$ as the set of points $(x, y) \in \mathbb{K} \times \mathbb{K}$ which satisfy an equation

$$E : \; y^2 = x^3 + ax + b,$$

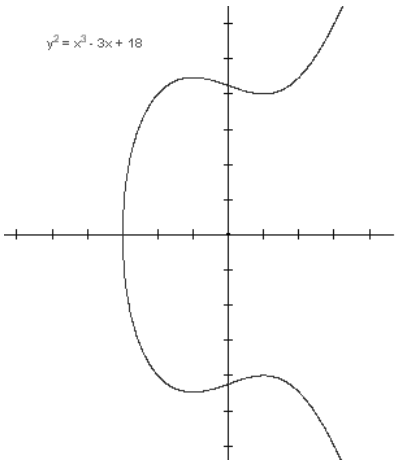
where $a, b \in \mathbb{K}$ and $4a^3 + 27b^2 \neq 0$, together with a single element denoted by $\mathcal{O}$ and called the "point in infinity".

The point in infinity appears naturally if we represent the curve in projective plane $\mathbb{P}^2(\mathbb{K})$, i.e. the set of equivalence classes of triples $(X, Y, Z) \in \mathbb{K}^3 \setminus \{(0,0,0)\}$, where $(X, Y, Z) \sim (kX, kY, kZ)$, $k \in \mathbb{K}$, $k \neq 0$. Replacing x by $\frac{X}{Z}$ and y by $\frac{Y}{Z}$, we obtain the projective equation of elliptic curve

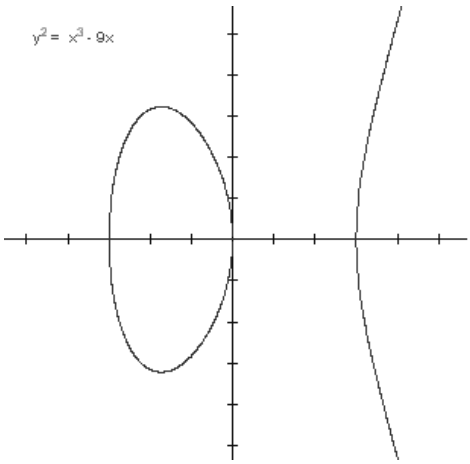
$$Y^2Z = X^3 + aXZ^2 + bZ^3.$$

If $Z \neq 0$, then (X, Y, Z) has representative of the form $(x, y, 1)$ and it may be identified by (x, y). But there is one equivalence class with $Z = 0$. It has a representative $(0, 1, 0)$, and this point we identify with $\mathcal{O}$.

One of the most important facts about elliptic curves is that the set of points on an elliptic curve forms an abelian group (Poincaré, 1908). In order to visualize the group operation, assume for the moment that $\mathbb{K} = \mathbb{R}$. Then we have an ordinary curve in the plane. It has one or two components, depending on the number of real roots of the cubic polynomial $f(x) = x^3 + ax + b$.

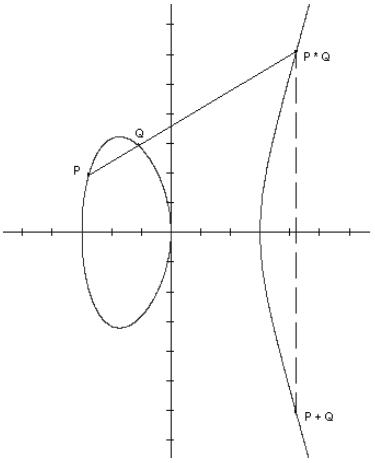


1 root – 1 component

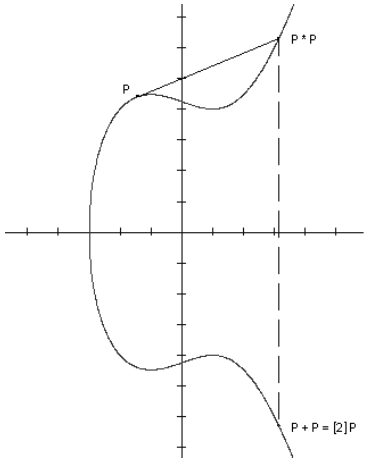


3 roots – 2 components

Let E be an elliptic curve over $\mathbb{R}$, and let P and Q be to two points on E. We define $-P$ as the point with the same x-coordinate but negative y-coordinate of P. If P and Q have different x-coordinates, then the straight line though P and Q intersects the curve in exactly one more point, denoted by $P * Q$. We define $P + Q$ as $-(P * Q)$. If $P = Q$, then we replace the secant line by the tangent line at the point P. We also define $P + \mathcal{O} = \mathcal{O} + P = P$ for all $P \in E(\mathbb{R})$.



secant line



tangent line

Using this geometric definition, we can determine explicit algebraic formulas for this group law. Such formulas make sense over any field (with

small modification for fields of characteristic 2 or 3).

Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$. Then

1) $-\mathcal{O} = \mathcal{O}$;

2) $-P = (x_1, -y_1)$;

3) $\mathcal{O} + P = P$;

4) if $Q = -P$, then $P + Q = \mathcal{O}$;

5) if $Q \neq -P$, then $P + Q = (x_3, y_3)$, where

$$x_3 = \lambda^2 - x_1 - x_2, \quad y_3 = -y_1 + \lambda(x_1 - x_3),$$

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1}, \text{ if } x_2 \neq x_1, \\ \frac{3x_1^2 + a}{2y_1}, \text{ if } x_2 = x_1. \end{cases}$$

The number λ is the slope of the straight line through the points P and Q in the case $P \neq Q$, and the slope of the tangent line at the point P in the case $P = Q$.

It can be shown that these formulas give an abelian group law on an elliptic curve over any field $\mathbb{K}$. All properties of an abelian group are evident, except the associative law.

In this lecture notes, we will mainly consider elliptic curves over $\mathbb{Q}$.

Let us just mention that elliptic curves over finite fields $\mathbb{F}_q$, in particular for $q = p$ (prime fields) and $q = 2^k$ (fields of characteristic 2), are very important for the application in cryptography.

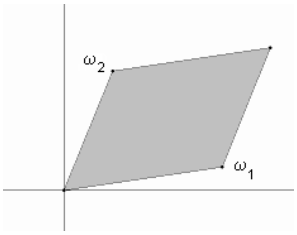
We will briefly mention some facts on elliptic curves over $\mathbb{C}$. In computing the arc-length of an ellipse, one integrates a function involving square root of a cubic or quartic polynomial. Such integrals are called *elliptic integrals*. They cannot be expressed by elementary functions, but they can be expressed in terms of *Weierstrass $\wp$-function*. It satisfies the differential equation of the form

$$\left(\frac{\wp'}{2}\right)^2 = \wp^3 + a\wp + b.$$

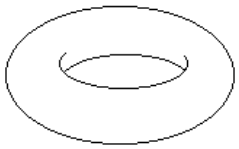
We can parametrize points on an elliptic curve $y^2 = x^3 + ax + b$ over $\mathbb{C}$ by $(\wp(t), \frac{1}{2}\wp'(t))$. Moreover, this is a homomorphism, i.e. if $P = (\wp(t), \frac{1}{2}\wp'(t))$ and $Q = (\wp(u), \frac{1}{2}\wp'(u))$, then $P + Q = (\wp(t+u), \frac{1}{2}\wp'(t+u))$. This gives an elegant proof of the associativity low on an elliptic curve.

Using the function $\wp$ we can visualize an elliptic curve over $\mathbb{C}$. The function $\wp$ is doubly periodic, i.e. there exist $\omega_1, \omega_2 \in \mathbb{C}$ ($\omega_1/\omega_2 \notin \mathbb{R}$) such that $\wp(z + m\omega_1 + n\omega_2) = \wp(z)$ for all $m, n \in \mathbb{Z}$. Denote by L the lattice of all points of the form $m\omega_1 + n\omega_2$. The the above parametrization is a complex analytic isomorphism between $\mathbb{C}/L$ and $E(\mathbb{C})$. So we can consider $E(\mathbb{C})$ as the fundamental parallelogram $m\omega_1 + n\omega_2$, $0 \leq m, n < 1$, in which we

"glue" the opposite sides: first we obtain a cylinder, and when we "glue" its bases, we obtain a *torus* (a sphere with one "hole" – so elliptic curves have genus 1).



fundamental parallelogram



torus

2 Rational points on elliptic curves

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

Theorem 2.1 (Mordell-Weil)**.** *$E(\mathbb{Q})$ is a finitely generated abelian group.*

In the other words, there is always a finite set of points $P_1, \ldots, P_k$ on E which generates all points in $E(\mathbb{Q})$ by the secant-tangent process. There are two basic steps in the proof of Mordell-Weil theorem:

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

Any finitely generated abelian group is isomorphic to a direct product of cyclic groups. Thus we have the following corollary of Theorem 2.1

Corollary 2.1.

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

The subgroup $E(\mathbb{Q})_{\text{tors}}$ of points of finite order is called the *torsion group* of E, and the integer $r \geq 0$ is called the *rank* of E and it is denoted by $\text{rank}(E)$. By Corollary 2.1, there exist r rational points $P_1, \ldots, P_r$ on E such that any rational point P on E can be represented 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.

We may ask which values are possible for $E(\mathbb{Q})_{\text{tors}}$ and $\text{rank}(E)$ for general E, and also how we can compute them for a given E. It appears that these questions are much easier for the torsion group.

Theorem 2.2 (Mazur)**.** *If E is an elliptic over over $\mathbb{Q}$, then $E(\mathbb{Q})_{tors}$ is one of the following* 15 *groups:*

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

Let us now discuss the problem of finding the torsion points on an elliptic curve

$$E : \ y^2 = x^3 + ax + b$$

over $\mathbb{Q}$. First, let $P = (x, y)$ be a point of order 2. From $2P = \mathcal{O}$ it follows $P = -P$, i.e. $(x, y) = (x, -y)$, which implies $y = 0$. Hence, the points of order 2 are exactly the points with y-coordinate equal to 0. We may have 0, 1 or 3 such points, depending on the number of rational roots of the polynomial $x^3 + ax + b$. These points, with the point in infinity $\mathcal{O}$, form a subgroup of $E(\mathbb{Q})_{\text{tors}}$ which is trivial or isomorphic to $\mathbb{Z}/2\mathbb{Z}$ or to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Other point of finite order can be found by the following theorem.

Theorem 2.3 (Lutz-Nagell)**.** *Let E be an elliptic curve given by the equation*

$$y^2 = x^3 + ax + b, \quad a, b \in \mathbb{Z}.$$

If $P = (x, y) \in E(\mathbb{Q})_{tors}$, then x, y are integers. (If E is given by the (long) Weierstrass equation with integer coefficients, then $4x$ and $8y$ are integers.)

Corollary 2.2. *If $P = (x, y) \in E(\mathbb{Q})_{tors}$, then either $y = 0$ (and P has order 2) or $y^2 | \Delta$, where $\Delta = -4a^3 - 27b^2$.*

Example 2.1. *Find the torsion group for the elliptic curve*

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

Solution: We have $\Delta = -1728$. If $y = 0$, then $x = -2$ and we have the point $(0, -2)$ of order 2. If $y \neq 0$, then $y^2 | 1728$, i.e. $y | 24$. By testing all possibilities, we find the following points with integer coordinates: $P_1 = (1, 3)$, $P_2 = (2, 4)$, $-P_1 = (1, -3)$, $-P_2 = (2, -4)$. We compute

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

and since the points $2P_1$ and $2P_2$ do not have integer coordinates, we conclude that P_1 and P_2 are points of infinite order. Hence, $E(\mathbb{Q})_{\text{tors}} = \{\mathcal{O}, (0, -2)\} \cong \mathbb{Z}_2$. ♢

A problem with the application of Lutz-Nagell theorem appears if it is hard to factorize the discriminant, or if the discriminant has many quadratic factors.

An alternative approach is to consider $|E(\mathbb{F}_p)|$ for few small primes p such that $p \nmid 2\Delta$, and use the fact that $|E(\mathbb{Q})_{\text{tors}}|$ divides $|E(\mathbb{F}_p)|$. This give us good candidate n for the order of group $E(\mathbb{Q})_{\text{tors}}$. It remains to find a point of order n. Doud's algorithm from 1998 uses the Weierstrass $\wp$-function. We may assume that its period ω_1 is real. If n is odd, then a point P of order n corresponds to a parameter of the form $\frac{m}{n}\omega_1$, where $\gcd(m,n) = 1$. Let $mm' \equiv 1 \pmod{n}$. Then the point $m'P$ also has order n, and its parameter is $\frac{1}{n}\omega_1$. Hence, we conclude that $\wp(\frac{1}{n}\omega_1)$ has to be an integers. If n is even, then similar arguments show that one of the numbers $\wp(\frac{1}{n}\omega_1)$, $\wp(\frac{1}{n}\omega_1 + \frac{1}{2}\omega_2)$ or $\wp(\frac{1}{n}\omega_1 + \frac{1}{2}\omega_1 + \frac{1}{2}\omega_2)$ have to be an integer.

Example 2.2. *Find the torsion group for the elliptic curve*

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

Solution: We have $4a^2 + 27b^3 = -372386507784192 = -2^{18} \cdot 3^{17} \cdot 11$ (but we will not use this factorization in our solution). We take first $p = 5$, and we find that $|E(\mathbb{F}_5)| = 10$. For $p = 7$ we also obtain $|E(\mathbb{F}_7)| = 10$. We conclude that $|E(\mathbb{Q})_{\text{tors}}|$ divides 10. We have (e.g. using arithmetic-geometric mean)

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

We compute

$$\wp(\frac{1}{10}\omega_1) = 2539.825532\ldots, \quad \wp(\frac{1}{10}\omega_1 + \frac{1}{2}\omega_2) = -213.000000\ldots,$$

so we find a rational point

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

of order 10. Hence, $E(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}_{10}$, and by computing the multiplies of P we obtain that

$$E(\mathbb{Q})_{\text{tors}} = \{\mathcal{O}, (-213, 2592), (651, -15552), (3, 1944), (219, -1296), (75, 0), \\ (219, 1296), (3, -1944), (641, 15552), (-213, -2592)\}.$$

$\diamondsuit$

The questions concerning the rank are much harder, and at present we don't have satisfactory answers. It is a folklore conjecture that the rank can be arbitrary large, i.e. that for any positive integer M there exist a curve E over $\mathbb{Q}$ such that $\text{rank}(E) \geq M$. However, the current record is the curve with rank ≥ 28 found by Elkies in 2006. There is a stronger version of this conjecture which says that for any admissible torsion group G, there exist an elliptic curve E with $E(\mathbb{Q})_{\text{tors}} \cong G$ and $\text{rank}(E) \geq M$. Let us define

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

The current records for $B(G)$ for each of 15 admissible torsion groups are given in the following table:

G	$B(G) \geq$	Author(s)
0	28	Elkies (2006)
$\mathbb{Z}/2\mathbb{Z}$	18	Elkies (2006)
$\mathbb{Z}/3\mathbb{Z}$	13	Eroshkin (2007,2008)
$\mathbb{Z}/4\mathbb{Z}$	12	Elkies (2006)
$\mathbb{Z}/5\mathbb{Z}$	6	Dujella & Lecacheux (2001)
$\mathbb{Z}/6\mathbb{Z}$	8	Eroshkin (2008), Dujella & Eroshkin (2008), Elkies (2008), Dujella (2008)
$\mathbb{Z}/7\mathbb{Z}$	5	Dujella & Kulesz (2001), Elkies (2006)
$\mathbb{Z}/8\mathbb{Z}$	6	Elkies (2006)
$\mathbb{Z}/9\mathbb{Z}$	4	Fisher (2009)
$\mathbb{Z}/10\mathbb{Z}$	4	Dujella (2005,2008), Elkies (2006)
$\mathbb{Z}/12\mathbb{Z}$	4	Fisher (2008)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	14	Elkies (2005), Eroshkin (2008), Dujella & Eroshkin (2008)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$	8	Elkies (2005)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$	6	Elkies (2006)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$	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)

Assume that E has a rational point of order 2. In that case the computation of the rank is usually much easier than in the general case. The method is called the "descent using 2-isogeny". We may assume that the point of order 2 is the point $(0,0)$. Then E has the equation of the form

$$y^2 = x^3 + ax^2 + bx.$$

The "2-isogenous curve" E' has the equation

$$y^2 = x^3 - 2ax^2 + (a^2 - 4b)x$$

In general, an isogeny is a homomorphism between two elliptic curves which is given by rational functions. In our case, the isogeny is $\varphi : E \to E'$, $\varphi(P) = (\frac{y^2}{x^2}, \frac{y(x^2-b)}{x^2})$ for $P = (x,y) \neq \mathcal{O}, (0,0)$, and $\varphi(P) = \mathcal{O}$ otherwise. Analogously we can define $\psi : E' \to E$. It holds that $\psi \circ \varphi(P) = 2P$, and these two isogenies appear in the first step of the proof of Mordell-Weil theorem.

Write x and y in the form $x = \frac{m}{e^2}$, $y = \frac{n}{e^3}$ and insert them in the equation for E. We obtain

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

Let $b_1 = \pm\gcd(m, b)$, $mb_1 > 0$. Then $m = b_1 m_1$, $b = b_1 b_2$, $n = b_1 n_1$ and

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

Since the factors on the right hand side are coprime, we conclude that there exist 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 finally we obtain the equation

$$N^2 = b_1 M^4 + aM^2 e^2 + b_2 e^4 \tag{3}$$

in unknowns M, e and N. We also have the following conditions $\gcd(M, e) = \gcd(N, e) = \gcd(M, N) = 1$.

The rank of E can be computed in the following way. For each factorization $b = b_1 b_2$, where b_1 is a square-free integer, we write down the equation (3). We need to decide whether or not each of these equations has a solution in integers (note that for such equations everywhere local solubility does not imply global global solubility). Each solutions (M, e, N) of the equation (3) induce a point on E with the 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 the corresponding equation (3) has a solution, and let r_2 be the number defined in the same way for the curve E'. Then there exist nonnegative integers e_1 and e_2 such that $r_1 = 2^{e_1}$, $r_2 = 2^{e_2}$ and it holds that

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

In the case when rank is equal to 0 (and we are able to prove this), using Lutz-Nagell theorem we can find all rational, and then also all integer points on that elliptic curve. This is not unrealistic assumption, since it is expected that a "random" elliptic curve has 50% chance to have rank 0.

Example 2.3. *Consider the set* $\{1, 2, 5\}$. *It has so called property* $D(-1)$ *since* $1 \cdot 2 - 1$, $1 \cdot 5 - 1$ *and* $2 \cdot 5 - 1$ *are perfect squares. We may ask is it possible to extended this triple to a quadruple with the same property, i.e. does it exist* $x \in \mathbb{Z}$ *such that*

$$1 \cdot x - 1, \quad 2 \cdot x - 1, \quad 5 \cdot x - 1$$

are perfect square. We will show that $x = 1$ *is the only solution, and since* $1 \in \{1, 2, 5\}$, *this means that* $\{1, 2, 5\}$ *cannot be extended to a* $D(-1)$*-quadruple. We will solve this problem by finding all integer points on the elliptic curve*

$$y^2 = (x - 1)(2x - 1)(5x - 1). \tag{4}$$

Solution: Multiplying the equation by 10^2 and with substitution $10y \mapsto y$, $10x \mapsto x$ we obtain the equation in the Weierstrass form:

$$y^2 = x^3 - 17x^2 + 80x - 100.$$

By translation $x \mapsto x + 5$, we get the equation in which the points $(0, 0)$ is a point of order 2:

$$E\,; \quad y^2 = x^3 - 2x^2 - 15x.$$

Its 2-isogenous curve is

$$E' : \quad y^2 = x^3 + 4x^2 + 64x.$$

For the curve E, possibilities for the number b_1 are ± 1, ± 3, ± 5, ± 15, with the corresponding Diophantine equations $N^2 = M^4 - 2M^2e^2 - 15e^4$, $N^2 = -M^4 - 2M^2e^2 + 15e^4$, $N^2 = 3M^4 - 2M^2e^2 - 5e^4$, $N^2 = -3M^4 - 2M^2e^2 + 5e^4$,

$N^2 = 5M^4 - 2M^2e^2 - 3e^4$, $N^2 = -5M^4 - 2M^2e^2 + 3e^4$, $N^2 = 15M^4 - 2M^2e^2 - e^4$, $N^2 = -15M^4 - 2M^2e^2 + e^4$. Because of the symmetry, it is enough to examine the first four equations. The first equation has a solution $M = 1$, $e = 0$, $N = 1$, and the fourth equation has a solution $M = 1$, $e = 1$, $N = 0$. The second equation leads to $N^2 = (3e^2 - M^2)(5e^2 + M^2)$. Since $\gcd(3e^2 - M^2, 5e^2 + M^2) \in \{1, 2\}$, we have two possibilities. However, $3e^2 - M^2 = s^2$ is impossible modulo 3 because $(\frac{-1}{3}) = -1$, while $5e^2 + M^2 = 2t^2$ is impossible modulo 5 because $(\frac{2}{5}) = -1$. The third equation leads to $N^2 = (M^2 + e^2)(3M^2 - 5e^2)$. Again we have two possibilities, but they both lead to a contradiction: $3M^2 - 5e^2 = t^2$ is impossible modulo 5 because $(\frac{3}{5}) = -1$, while $M^2 - 5e^2 = 2t^2$ is impossible modulo 8 because $3M^2 - 5e^2 \equiv 6 \pmod 8$ and $2t^2 \equiv 2 \pmod 8$. Hence, $e_1 = 2$.

For E' we have $b_1' \in \{\pm 1, \pm 2\}$ and the corresponding Diophantine equations are $N^2 = M^4 + 4M^2e^2 + 64e^4$, $N^2 = -M^4 + 4M^2e^2 - 64e^4$, $N^2 = 2M^4 + 4M^2e^2 + 32e^4$ and $N^2 = -2M^4 + 4M^2e^2 - 32e^4$. The first equation has a solution $M = 1$, $e = 0$, $N = 1$. The second and fourth equations lead to $N^2 = -(M^2 - 2e^2)^2 - 60e^4$, resp. $N^2 = -2(M^2 - e^2)^2 - 30N^2$, and obviously have no solutions. The third equation leads to $2 \cdot (N/2)^2 = (M^2 + e^2)^2 + 15e^4$, and it has no solutions modulo 5 because $(\frac{2}{5}) = 1$. Hence, $e_2 = 0$.

We conclude that $\operatorname{rank}(E) = 2 + 0 - 2 = 0$.

It remains to find torsion points on E. We have three points of order 2: $(0, 0)$, $(-3, 0)$, $(5, 0)$. All other torsion points (x, y) should satisfy $y^2 | 14400$, i.e. $y | 120$. We can check all possibilities and we find no integer solution. Alternatively, we can observe that $|E(\mathbb{F}_7)| = 4$ and $7 \nmid \Delta$, so $E(\mathbb{Q})_{\text{tors}}$ cannot have more than 4 points. Hence, all rational points on E are $\mathcal{O}$, $(0, 0)$, $(-3, 0)$, $(5, 0)$, which implies that all rational points on the curve (4) are $\mathcal{O}$, $(1, 0)$, $(\frac{1}{2}, 0)$, $(\frac{1}{5}, 0)$. Thus, the only integer x with the property that $1 \cdot x - 1$, $2 \cdot x - 1$ and $5 \cdot x - 1$ are perfect squares is $x = 1$. ♢

3 Some classical problems related to elliptic curves

3.1 Hardy-Ramanujan taxicab problem

The taxicab problem is related with a famous mathematical story. When Ramanujan was in the hospital in London, his colleague Hardy came to visit. Hardy remarked that he had come in taxicab number 1729, and surely that was a rather dull number. Ramanujan instantly replied that, to the contrary, 1729 is a very interesting number, since it is the smallest number expressible as the sum of two cubes in two different ways. Indeed, $1729 = 9^3 + 10^3 = 1^3 + 12^3$. We may consider the cubic equation

$$x^3 + y^3 = 1729. \tag{5}$$

We claim that all integer points on (5) are given by $(x, y) = (9, 10)$, $(10, 9)$, $(1, 12)$, $(12, 1)$. This is easy to prove because the cubic $x^3 + y^3$ factors. We

have

$$(x+y)(x^2-xy+y^2) = 1729 = 7 \cdot 13 \cdot 19.$$

So we consider all possible factorizations $1729 = AB$ and solve the system $x+y = A$, $x^2-xy+y^2 = B$. We find that we only get integer solutions for the two pairs $(A,B) = (3,133)$ and $(A,B) = (9,91)$, and these lead to the four solutions listed above.

We may ask whether there exist a positive integer m which can be represented as a sum of two cubes in three different ways, or more generally in M different ways. The answer is that for every positive integer M there exist a positive integer m such that the equation $x^3+y^3 = m$ has at least M integer solutions.

Consider the curve

$$C : \; x^3+y^3 = 9.$$

It has an obvious rational points $(1,2)$. By substitutions $s = 12/(x+y)$, $t = 12(x-y)/(x+y)$ we find that C is birationally equivalent to the elliptic curve

$$E : \; t^2 = s^3 - 48.$$

The point $(1,2)$ on C corresponds to the point $P = (4,4)$ on E. Since $3P = (73/9, 595/27)$, by Lutz-Nagell theorem, we conclude that P is a point of infinite order (in fact, P is the generator of $E(\mathbb{Q})$), and therefore the curves E and C have infinitely many rational points. For the given positive integer M we choose M rational points $Q_1, Q_2, \ldots, Q_M$ on the curve C. It is easy to see that the coordinates of these point are of the form $Q_i = (a_i/d_i, b_i/d_i)$. Let us define $m = 9(d_1 d_2 \cdots d_M)^3$. Now we have M integer points on the curve $x^3+y^3 = m$, with coordinates obtained by multiplying the coordinates of the points Q_i $(i = 1, \ldots M)$ by $d_1 d_2 \cdots d_M$.

The smallest number which can be represented as a sum of two cubes on three different ways is

$$87539319 = 167^3 + 436^3 = 228^3 + 423^3 = 255^3 + 414^3.$$

Remark 3.1. Similar construction can be used to show that for any positive integer N, there exist integers u and v such that the system of Pellian equations

$$x^2 - 2y^2 = u, \quad y^2 - 3z^2 = v$$

has more than N integer solutions.

3.2 Diophantine m-tuples

A set of m positive integers with the property that the product of any two of them increased by unity is a perfect square is called a *Diophantine m-tuple*. Set of m nonzero rationals with the same property is called a *rational Diophantine m-tuple*. The first rational Diophantine quadruple, the

set $\{1/16, 33/16, 17/4, 105/16\}$, was found already by Diophantus. The first Diophantine quadruple (in integers) was found by Fermat, and it was the set $\{1, 3, 8, 120\}$. Indeed, we have

$$1 \cdot 3 + 1 = 2^2, \;\; 1 \cdot 8 + 1 = 3^2, \;\; 1 \cdot 120 + 1 = 11^2,$$
$$3 \cdot 8 + 1 = 5^2, \;\; 3 \cdot 120 + 1 = 19^2, \;\; 8 \cdot 120 + 1 = 31^2.$$

Euler showed that Fermat's set can be extended with the fifth rational number 777480/8288641. The first rational Diophantine 6-tuple was found in 1999 by Gibbs. It was the set

$$\{11/192, 35/192, 155/27, 512/27, 1235/48, 180873/16\}.$$

Several such 6-tuples are known (with all possible combinations of signs), but it is not known whether there exist any rational Diophantine 7-tuple.

In 1969, Baker and Davenport, using Baker's theory on linear forms in logarithms of algebraic numbers and a reduction method based on continued fractions, proved that if d is a positive integer such that $\{1, 3, 8, d\}$ forms a Diophantine quadruple, then $d = 120$. It implies that the Fermat's set $\{1, 3, 8, 120\}$ cannot be extended to a Diophantine quintuple. It is known (Dujella, 2004) that there does not exist a Diophantine 6-tuple, and there are only finitely many Diophantine quintuples. On the other hand, no absolute upper bound for the size of rational Diophantine tuples is known.

Let $\{a, b, c\}$ be a (rational) Diophantine triple, i.e.

$$ab + 1 = r^2, \;\; ac + 1 = s^2, \;\; bc + 1 = t^2.$$

In order to extend this triple to a quadruple, we have to solve the system

$$ax + 1 = \square, \;\; bx + 1 = \square, \;\; cx + 1 = \square. \tag{6}$$

It is natural idea to assign to this system the elliptic curve

$$E : \; y^2 = (ax + 1)(bx + 1)(cx + 1).$$

There are three rational points on E of order 2: $A = (-1/a, 0)$, $B = (-1/b, 0)$, $C = (-1/c, 0)$, and also obvious rational points $P = (0, 1)$, $S = (1/abc, rst/abc)$. It is not so obvious, but it is easy to verify that $S = 2R$, where $R = ((rs + rt + st + 1)/abc, (r + s)(r + t)(s + t)/abc)$.

It is clear that every rational solution of the original system (6) induce a rational point on E. On the other hand, it can be shown that the x-coordinate of the point $T \in E(\mathbb{Q})$ satisfies (6) if and only if $T - P \in 2E(\mathbb{Q})$. Hence, the x-coordinates of the points $P + S$ and $P - S$ satisfy the system (6). These x-coordinates are

$$a + b + c + 2abc \pm 2rst,$$

which shows that every Diophantine triple can be extended to a Diophantine quadruple. The addition and subtraction of the point S has another interesting property. Namely, if x-coordinate of the point $T \in E(\mathbb{Q})$ satisfies (6), then for the points $T \pm S = (u, v)$ it holds that $xu + 1$ is a square. This result implies that every Diophantine quadruple $\{a, b, c, d\}$ can be extended to a rational Diophantine quintuple $\{a, b, c, d, e\}$. Note that the number e obtained by this construction satisfies $e < 1$, and therefore e is not a positive integer.

Exercise 3.1. *Extend Diophantus' set* $\{1/16, 33/16, 17/4, 105/16\}$ *to a rational Diophantine quintuple.*

Example 3.1. *The elliptic curve*

$$y^2 = (x + 1)(3x + 1)(8x + 1) \tag{7}$$

has rank equal to 1*, so it has infinitely many rational points and the Diophantine triple* $\{1, 3, 8\}$ *can be extended to infinitely many rational Diophantine quadruples (e.g. by* $x = \frac{777480}{8288641}$*). However, this curve only the following integer points*

$$(x, y) = (-1, 0),\ (0, \pm 1),\ (120, \pm 6479).$$

From (7) we have

$$\begin{aligned} x + 1 &= \mu_2\mu_3 x_1^2, \\ 3x + 1 &= \mu_1\mu_3 x_2^2, \\ 8x + 1 &= \mu_1\mu_2 x_3^2, \end{aligned}$$

where μ_1, μ_2, μ_3 are square-free integers such that $\mu_1|5$, $\mu_2|7$, $\mu_3|2$. Using elementary arguments, we can exclude all possibilities except $\mu_1 = \mu_2 = \mu_3$. Indeed, it is clear that only solution in negative integers is $x = -1$, so we may assume that $x \geq 0$ and that μ_1, μ_2, μ_3 are positive. But, the equations $8x + 1 = 5x_3^2$, $8x + 1 = 7x_3^2$ and $8x + 1 = 35x_3^2$ are all impossible modulo 8. Hence, $\mu_1 = \mu_2 = 1$. But, the system $x + 1 = 2x_1^2$, $3x + 1 = 2x_2^2$ is also impossible modulo 8, which shows that $\mu_3 = 1$.

As we already mentioned, the case $\mu_1 = \mu_2 = \mu_3$ has been solved by Baker and Davenport, by transforming the problem into an inequality for the linear form in logarithms

$$\Lambda = n \log(2 + \sqrt{3}) - m \log(3 + 2\sqrt{2}) + \log\left(\frac{2\sqrt{2}(1 + \sqrt{3})}{\sqrt{3}(2\sqrt{2} \pm 1)}\right).$$

An analogous result is known (Dujella, 2000) for the family of elliptic curves

$$E_k : \ y^2 = ((k - 1)x + 1)((k + 1)x + 1)(4kx + 1),$$

($k \geq 3$), under the assumption that rank $(E_k) = 1$ (it is expected that this assumption holds for 50% of curves in the family, since it has the "generic rank" equal to 1). It is proved that all integer points on E_k for $k \geq 3$ are

$$(x, y) = (0, \pm 1),\ (16k^3 - 4k, \pm(128k^6 - 112k^4 - 20k^2 - 1)).$$

Note that for $k = 2$ we have exactly the curve (7). Also, $\{k - 1, k + 1, 4k\}$ is a Diophantine triple for all $k \geq 2$. We conjecture that the result does not depend on the rank (some experimental supports to this conjecture are given by Dujella (2000) and Najman (2009)).

4 Elementary results on the equation $\mathbf{y^2 = x^3 + k}$

Mordell proved in 1922 that the number of integer points on an elliptic curve is finite. In 1929, Siegel generalized this result and proved that any curve, defined over the rationals, with genus at least 1, had only finitely many integer points. In 1966, Baker proved an explicit upper bound for the size of solutions (i.e. $\max(|x|, |y|)$). These are very deep results. But there are many elementary results on integer points on some concrete elliptic curves. We give here some results of such type for Mordell curve $y^2 = x^3 + k$. The results are mainly due to Mordell. Let us mentioned that these curves were systematically studied by Gebel, Pethő and Zimmer, who solved them for all integers k in the range $0 < |k| \leq 10000$.

Proposition 4.1. *Let $k = (4b - 1)^3 - 4a^2$, where a is an integer with no prime factors of the form $4l + 3$. Then the equation $y^2 = x^3 + k$ has no solutions in integers x and y.*

Proof: As $k \equiv -1 \pmod 4$, we have $y^2 \equiv x^3 - 1 \pmod 4$. Since $y^2 \equiv 0$ or $1 \pmod 4$, x cannot be even nor congruent to -1 modulo 4. Hence, $x \equiv 1 \pmod 4$. We can write the equation $y^2 = x^3 + (4b - 1)^3 - 4a^2$ in the form

$$y^2 + 4a^2 = x^3 + (4b - 1)^3 = (x + 4b - 1)(x^2 - x(4b - 1) + (4b - 1)^2).$$

The second factor $x^2 - x(4b - 1) + (4b - 1)^2$ is congruent to 3 modulo 4. Thus it has at least one prime factor p which is congruent to 3 modulo 4. But, p can divide a sum of two squares $y^2 + 4a^2$ only if y and a are both divisible by p, contradicting the assumption that a has no prime factors of the form $4l + 3$. □

Some integers k satisfying the conditions of Proposition 4.1: $k = -5$, 11, 23, -73.

The proof of the following result is completely analogous to the proof of Proposition 4.1.

Proposition 4.2. *Let $k = (4b + 2)^3 - (2a + 1)^2$, where all prime factors of $2a + 1$ are of the form $4l + 1$. Let the equation $y^2 = x^3 + k$ has no solutions in integers x and y.*

Proposition 4.3. *Let $k = 2b^2 - a^3$, where $a \equiv 2, 4 \pmod 8$, $b \equiv 1 \pmod 2$ and all prime factors of b are of the form $8l \pm 1$. Then the equation $y^2 = x^3 + k$ has no integer solutions.*

Proof: From $y^2 \equiv x^3 + 2 \pmod 4$, it follows that $x \not\equiv 0 \pmod 2$ and $x \not\equiv 1 \pmod 4$. Hence, $x \equiv 3 \pmod 4$, i.e. $x \equiv 3$ ili $7 \pmod 8$. We can write our equation in the form

$$y^2 - 2b^2 = x^3 - a^3 = (x - a)(x^2 + ax + a^2).$$

If $x \equiv 3 \pmod 8$, then $x^2 + ax + a^2 \equiv 1 + 3a + a^2 \equiv \pm 3 \pmod 8$, which implies that $x^2 + ax + a^2$ has at least one prime factor p of the form $8l \pm 3$. By the assumption, p does not divide b, and therefore

$$\left(\frac{2}{p}\right) = \left(\frac{2b^2}{p}\right) = \left(\frac{y^2}{p}\right) = 1,$$

contradicting the fact that $(\frac{2}{p}) = 1$ if and only if $p \equiv \pm 1 \pmod 8$.

If $x \equiv 7 \pmod 8$, then $x - a \equiv 7 - a \equiv \pm 3 \pmod 8$, so $x - a$ has at least one factor of the form $8l \pm 3$, and we obtain a contradict in the same way as before. □

Some values of k satisfying the the conditions of Proposition 4.3: $k = -6$, 34, 58, -62, 66, 90.

The proof of the following result is completely analogous to the proof of Proposition 4.3.

Proposition 4.4. *Let $k = -2b^2 - a^3$, where $a \equiv 4 \pmod 8$, $b \equiv 1 \pmod 2$ and all prime factors of b have the form $8l + 1$ or $8l + 3$. Then the equation $y^2 = x^3 + k$ has no integer solutions.*

Exercise 4.1. *Show that the equation $y^2 = x^3 + 45$ has no integers solutions.*

5 Elliptic curves and Thue equations

Consider the equations of the form

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

where the coefficients a, b, c are integers, and the cubic polinomial $f(x) = x^3 + ax^2 + bx + c$ has no multiple roots. We will describe Mordell's argumentation which shows that this equation has only finitely many integer solution. Since there are methods for efficient solving of Thue equation (Tzanakis and de Weger), this will also give one general method for finding integer points on an elliptic curve.

The idea is to factorize the polynomial

$$f(x) = x^3 + ax^2 + bx + c = (x - \vartheta_1)(x - \vartheta_2)(x - \vartheta_3). \tag{8}$$

Thus we get the fields $\mathbb{Q}(\vartheta_i)$ in which we consider the equation (8). There are three possiblities:

1) all three roots of f are rational (and integer);

2) one root of f is rational, while other two are quadratic irrationals;

3) f is irreducible over $\mathbb{Q}$, its roots are algebraic integers of degree 3.

We will give some details only for the third case. In $\mathbb{Z}$, the following simple fact holds: if $XY = Z^l$ and $\gcd(X, Y) = 1$, then there exist $U, V \in \mathbb{Z}$ such that $X = \pm U^l$, $Y = \pm V^l$. We need here the following generalization of this fact in an algebraic number field $\mathbb{K}$:

Lemma 5.1. *All solutions of the equation $XY = cZ^l$, where $(X, Y)|\delta$ for given ideal δ, have the shape*

$$X = \lambda\varepsilon_1 U^l, \quad Y = \mu\varepsilon_2 V^l, \quad Z = \nu\varepsilon_3 UV,$$

where U and V are arbitrary integers in $\mathbb{K}$, $\varepsilon_1, \varepsilon_2, \varepsilon_3$ are units, λ, μ, ν are elements $\mathbb{K}$. The six numbers $(\varepsilon_1, \varepsilon_2, \varepsilon_3, \lambda, \mu, \nu)$ are taken from a finite set and they satisfy $\lambda\mu\varepsilon_1\varepsilon_2 = c\nu^l\varepsilon_3^l$.

Let us consider the equation (8) in the field $\mathbb{K} = \mathbb{Q}(\vartheta_i)$. We will describe the transformation of an elliptic curve to Thue equations. Lemma 5.1 implies

$$x - \vartheta_i = m(r + s\vartheta_i + t\vartheta_i^2)^2, \tag{9}$$

where $r, s, t \in \mathbb{Z}$, and m is an element of a finite set in $\mathbb{Q}(\vartheta_i)$. Indeed, ϑ_i is an algebraic number of degree 3, so every element in $\mathbb{K}$ can be written in the form $\alpha + \beta\vartheta_i + \gamma\vartheta_i^2$, $\alpha, \beta, \gamma \in \mathbb{Q}$. Although $\{1, \vartheta_i, \vartheta_i^2\}$ need not be a basis for $O_{\mathbb{K}}$, it can be shown that if $\frac{1}{d}(r + s\vartheta_i + t\vartheta_i^2) \in O_{\mathbb{K}}$ and $\gcd(d, r, s, t) = 1$, then d^2 divides the discriminant $\Delta[1, \vartheta_i, \vartheta_i^2] = (\vartheta_1 - \vartheta_2)^2(\vartheta_1 - \vartheta_3)^2(\vartheta_2 - \vartheta_3)^2$. Thus we have only finitely many possibilities for d, which can be "transferred" to m.

The number m (each of finitely many of them) can also be written in the form $m = r_0 + s_0\vartheta_i + t_0\vartheta_i^2$, where $r_0, s_0, t_0 \in \mathbb{Q}$. If we insert this in (9), and express ϑ_i^3 and ϑ_i^4 in terms of $1, \vartheta_i, \vartheta_i^2$, the comparison of the coefficients of 1, ϑ_i and ϑ_i^2, gives three equations of the form

$$f_1(r, s, t) = 0, \quad f_2(r, s, t) = 1, \quad f_3(r, s, t) = x,$$

where f_1, f_2, f_3 are ternary quadratic forms with rational coefficients. The solvability of the equation $f_1(r, s, t) = 0$ can be determined efficiently. If it is solvable, then all solutions are given by

$$gr = q_1(u, v), \quad gs = q_2(u, v), \quad qt = q_3(u, v),$$

where q_1, q_2, q_3 are binary quadratic forms with integer coefficients, and g can assume only finitely many integer values. Inserting this in the equation $f_2(r,s,t) = 1$, we obtain finitely many equation of the form

$$h(u,v) = g^2, \tag{10}$$

where h is a homogeneous polynomial of degree 4 with integer coefficients. It can be checked that h is not a square of a polynomial of degree 2. Thue's theorem implies that (10) has only finitely many solutions, and therefore the original elliptic equation also has only finitely many integer solutions (which can be obtained from $f_3(r,s,t) = x$).

Example 5.1. *Find all triangular numbers which are equal to a product of three consecutive positive integers (problem was introduced by Mohanty in 1988, and solved by de Weger in 1989). Triangular numbers are numbers of the form* $T_n = \frac{n(n+1)}{2}$. *De Weger showed that there are exactly 6 solutions of this problem:*

$$T_3 = 1\cdot 2\cdot 3, \quad T_{15} = 4\cdot 5\cdot 6, \quad T_{20} = 5\cdot 6\cdot 7, \quad T_{44} = 9\cdot 10\cdot 11,$$
$$T_{608} = 56\cdot 57\cdot 58, \quad T_{22736} = 636\cdot 637\cdot 638.$$

The given condition can be written in the form $\frac{n(n+1)}{2} = m(m+1)(m+2)$. Under the substitution $x = 2m+2$, $y = 2n+1$, we obtain the elliptic equation

$$y^2 = x^3 - 4x + 1 \tag{11}$$

(we are interested in integer points on (11) such that $x \geq 4$ is even and $y \geq 3$ is odd). We claim that the elliptic curve (11) has exactly 22 integer points:

$$(x,y) = (-2,\pm 1), (-1,\pm 2), (0,\pm 1), (2,\pm 1), (3,\pm 4), (4,\pm 7), (10,\pm 31),$$
$$(12,\pm 41), (20,\pm 89), (114,\pm 1217), (1274,\pm 45473).$$

It is easy to check that exactly last 6 pairs satisfy the desired conditions.

The claim is easy to check for $x \leq 0$ (since then obviously $x \geq -2$), so we may assume that $x \geq 1$. We are working in the number field $\mathbb{K} = \mathbb{Q}(\vartheta)$, where $\vartheta^3 - 4\vartheta + 1 = 0$. Let $\vartheta = \vartheta_1 \approx 0.2541$, $\vartheta_2 \approx -2.1149$, $\vartheta_3 \approx 1.8608$. We need the following information on the field $\mathbb{K}$: $O_{\mathbb{K}} = \mathbb{Z}[\vartheta]$, $h(\mathbb{K}) = 1$ and fundamental units are ϑ and $2 - \vartheta$. From

$$y^2 = (x - \vartheta)(x^2 + \vartheta x + (\vartheta^2 - 4)). \tag{12}$$

we conclude that

$$x - \vartheta = \pm \vartheta^i (2 - \vartheta)^j U^2, \quad U \in \mathbb{Z}[\vartheta], \;\; i,j \in \{0,1\}.$$

The same relation holds for each of the conjugates ϑ_i. For ϑ_1 we obtain (since $x \geq 1$ and $U \in \mathbb{R}$) that in (12) we have to take the sign $+$, while for

ϑ_2 we obtain that $i = 0$. Thus it remains to consider to cases: $j = 0$ and $j = 1$.

$\boxed{j = 0}$

We are searching for solutions of the form

$$x - \vartheta = (r + s\vartheta + t\vartheta^2)^2. \tag{13}$$

By comparison of the coefficients of powers of ϑ in (13), we get

$$s^2 + 4t^2 + 2rt = 0, \quad t^2 - 2rs - 8st = 1, \quad r^2 - 2st = x.$$

It is clear that s is even and t is odd, so r is even. Putting $r = 2r_1$ and $s = 2s_1$, we obtain

$$(2s_1)^2 + (2t + r_1)^2 = r_1^2.$$

Thus there exit $u, v \in \mathbb{Z}$ such that

$$s_1 = uv, \quad 2t + r_1 = u^2 - v^2, \quad r_1 = \pm(u^2 + v^2).$$

For the sign $+$ we get $t = -v^2$, and for the sign $-$ we get $t = u^2$. Inserting these values in the second equation we obtain the equations

$$v(v^3 + 8uv^2 - 8u^2v) = 1,$$

and

$$u(u^3 + 8u^2v - 8uv^2) = 1.$$

Sinve both homogenous polynomials are reducible, these equations can be very easily solved. We get the solution $(u, v) = (0, 1), (1, 1), (0, -1), (-1, -1)$ in the first case, and $(u, v) = (1, 0), (1, 1), (-1, 0), (-1, -1)$ in the second case. This yields $(r, s, t) = (2, 0, -1), (4, 2, -1), (-2, 0, 1), (-4, 2, 1)$, and $x = 4, 20, 12$.

$\boxed{j = 1}$

We are searching for solutions of the form

$$x - \vartheta = (2 - \vartheta)(r + s\vartheta + t\vartheta^2)^2. \tag{14}$$

We obtain the equations

$$2s^2 + 9t^2 - 2rs + 4rt - 8st = 0, \quad r^2 + 4s^2 + 18t^2 - 4rs + 8rt - 18st = 1,$$
$$2r^2 + s^2 + 4t^2 + 2rt - 4st = x.$$

The first equation yield

$$0 = 2s^2 + 9t^2 - 2rs + 4rt - 8st = 2(s - 2t)^2 + t^2 - 2r(s - 2t).$$

The substitution $z = s - 2t$ gives $t^2 = 2z(r - z)$.

If z is odd, then there exist $u, v \in \mathbb{Z}$ such that $z = u^2$, $r - z = 2v^2$, so that

$$r = u^2 + 2v^2, \quad s = u^2 + 4uv, \quad t = 2uv,$$

and we obtain the Thue equation

$$u^4 - 4u^3v - 12u^2v^2 + 4v^4 = 1. \tag{15}$$

If z is even, then there exist $u, v \in \mathbb{Z}$ such that $z = 2u^2$, $r - z = v^2$, so that

$$r = 2u^2 + v^2, \quad s = 2u^2 + 4uv, \quad t = 4uv,$$

and we obtain the Thue equation

$$4u^4 - 8u^3v - 12u^2v^2 + v^4 = 1. \tag{16}$$

The equations (15) and (16) are indeed Thue equations, i.e. the corresponding homogeneous polynomials are irreducible. Thus solving these equations is not so simple task as in the previous case. However, using the algorithms for solving Thue equations, based on linear forms in logarithms and LLL-reduction, it is possible to solve them efficiently. The result is that all solutions of the equation (15) are $(u, v) = (\pm 1, 0)$, while all solutions of the equation (15) are $(u, v) = (0, \pm 1)$, $(1, -1)$, $(-1, 1)$, $(3, 1)$, $(-3, -1)$, $(1, -3)$, $(-1, 3)$.

6 Application of elliptic logarithms

We have already seen that we can efficiently find all integer points on an elliptic curve if its rank is equal to 0.

In the general case, using elliptic logarithms, it is possible to obtain the estimate $N \leq N_0$ for $N = \max\{|n_1|, \ldots, |n_r|\}$ in the expression of an integer point in the form $P = T + n_1P_1 + \cdots + n_rP_r$. This bound can be significantly decreased using LLL-algorithm. This method has been proposed in 1994 by Gebel, Pethő and Zimmer, and independently by Stroeker and Tzanakis. However, for the application of this method it is crucial to know the rank and the generators $P_1, \ldots, P_r$, which might be a hard problem.

Consider the elliptic curve in Weierstrass form

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

It is isomorphic to a curve with the equation

$$E' : \ y^2 = 4x^3 - g_2x - g_3,$$

and this is exactly the equation satisfied by the Weierstrass $\wp$-function and its derivative. Function $\wp$ is doubly periodic and we may assume that its

period satisfy $\omega_1 \in \mathbb{R}$ and $\Im(\omega_1/\omega_2) > 0$. Let L be a lattice defined by ω_1 and ω_2. We have an isomorphism $\phi : \mathbb{C}/L \to^{\phi} E$, given by

$$z \mapsto \begin{cases} (\wp(z) - \frac{b_2}{12}, (\wp'(z) - a_1 x - a_3)/2), & z \notin L, \\ \mathcal{O}, & z \in L, \end{cases}$$

where $b_2 = a_1^2 + 4a_2$. The inverse map ψ is called the *elliptic logarithm*. It can be computed as

$$\psi(P) = \int_{\infty}^{x+b_2/12} \frac{dt}{\sqrt{4t^3 - g_2 t - g_3}} \pmod{L} \tag{17}$$

(using the arithmetic-geometric mean). Its name comes from the following property

$$\psi(P+Q) = \psi(P) + \psi(Q) \pmod{L}.$$

Let P be an integer point on E. We write $P = T + n_1 P_1 + \cdots + n_r P_r$, where T is a torsion point and $P_1, \ldots, P_r$ are generators of $E(\mathbb{Q})/E(\mathbb{Q})_{\text{tors}}$. We want to obtain an upper bound for $N = \max\{|n_1|, \ldots, |n_r|\}$.

To simplify notation, we will assume that $E(\mathbb{R})$ has one component (otherwise one can use the fact that if P is in the "egg", then $2P$ is in the infinite component). The starting point is the following inequality

$$\frac{1}{x(P)} \leq c_1 e^{-c_2 N^2} \tag{18}$$

(The constants $c_1, c_2, \ldots$ is this section depends only on E, and possibly on the basis of its Mordell-Weil group.) In the proof of (18), the regulator matrix is used. It is defined as $R = (< P_i, P_j >)$, where

$$< P, Q >= \frac{1}{2}(\hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q))$$

and the Neron-Tate height $\hat{h}$ is defined by

$$\hat{T} = \lim_{n \to \infty} \frac{h(2^n P)}{4^n}.$$

By the work of Silverman and Siksek we know that there exist constants C_1 and C_2 (depending on E) such that

$$C_1 \leq \hat{h}(P) - h(P) \leq C_2.$$

On the other hand, by examining the integral appearing in (17), we can obtain the inequality

$$|\psi(P)| \leq \frac{c_3}{|x(P)|}. \tag{19}$$

Putting the inequalities (18) and (19) together we obtain

$$|\psi(P)| \leq c_4 e^{-c_5 N^2}. \tag{20}$$

We have

$$\psi(P) = n_1\psi(P_1) + \cdots + n_r\psi(P_r) + m\omega_1,$$

where $|m| \leq rN + 1$.

Now we can use deep and powerful result by David (1995), which implies the following inequality:

$$|\psi(P)| > e^{-c_6(\log N + c_7)(\log\log N + c_8)^{r+2}}. \tag{21}$$

Comparing (20) and (21) with obtain that $N \leq N_0$, where N_0 is a huge absolute constant (usually something like 10^{100}). However, using a version of LLL-reduction due to de Weger, this huge upper bound can be significantly reduced. Thus we obtain $N \leq N_1$, where N_1 is typically around 10. Hence, provided that r is not too large (say if $r \leq 8$), then we can test all $(2N_1+1)^r$ candidates and find all integers points on our elliptic curve.

References

[1] H. Cohen, *Number Theory. Volume I: Tools and Diophantine Equations*, Springer Verlag, Berlin, 2007.

[2] J. E. Cremona, *Algorithms for Modular Elliptic Curves*, Cambridge University Press, Cambridge, 1997.
`http://www.warwick.ac.uk/~masgaj/book/amec.html`

[3] L. J. Mordell, *Diophantine Equations*, Academic Press, London, 1969.

[4] S. Schmitt, H.G. Zimmer: *Elliptic Curves. A Computational Approach*, de Gruyter, Berlin, 2003.

[5] J.H. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, 1996, 2009.

[6] J. H. Silverman, J. Tate, *Rational Points on Elliptic Curves*, Springer-Verlag, Berlin, 1992.

[7] N. P. Smart, *The Algorithmic Resolution of Diophantine Equations*, Cambridge University Press, Cambridge, 1998.

[8] C. Washington, *Elliptic Curves: Number Theory and Cryptography*, CRC Press, Boca Raton, 2008.

[9] B. M. M. de Weger, *Algorithms for Diophantine Equations*, Centrum voor Wiskunde en Informatica, Amsterdam, 1989.