Elliptic curves over the rationals

Andrej Dujella

Department of Mathematics
University of Zagreb, Croatia
e-mail: duje@math.hr
URL: http://web.math.hr/~duje/

Let $\mathbb{K}$ be a field. An *elliptic curve* over $\mathbb{K}$ is a nonsingular projective cubic curve over $\mathbb{K}$ with at least one $\mathbb{K}$-rational point. 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

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad (1)$$

which is called the *Weierstrass form*.

Program packages which deal with elliptic curves (PARI/GP, KANT, SAGE, MAGMA, APECS) usually initialize an elliptic curve as the vector $[a_1, a_2, a_3, a_4, a_6]$.

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

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

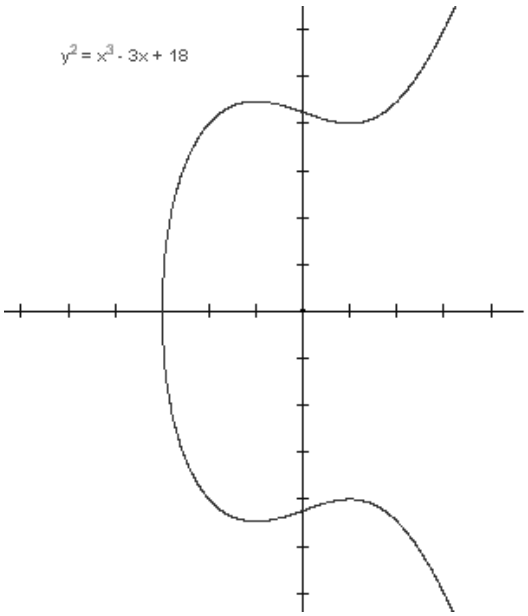
where $a, b \in \mathbb{K}$ and $4a^3 + 27b^2 \neq 0$, together with a single element denoted by $\mathcal{O}$ and called the "point in infinity".

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

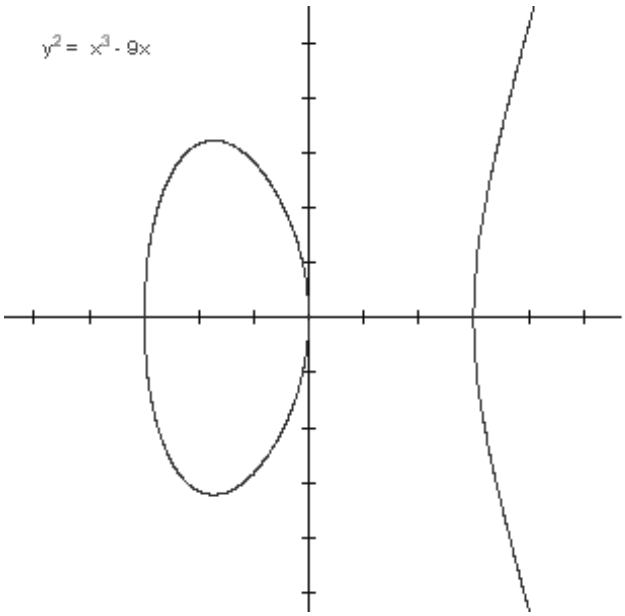
$$Y^2Z = X^3 + aXZ^2 + bZ^3.$$

If $Z \neq 0$, then (X, Y, Z) has representative of the form $(x, y, 1)$ and it may be identified with the affine point (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 $f(x) = x^3 + ax + b$.

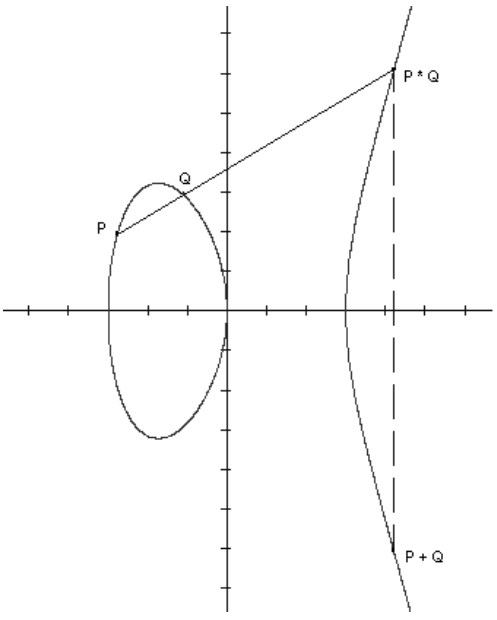


1 root – 1 component

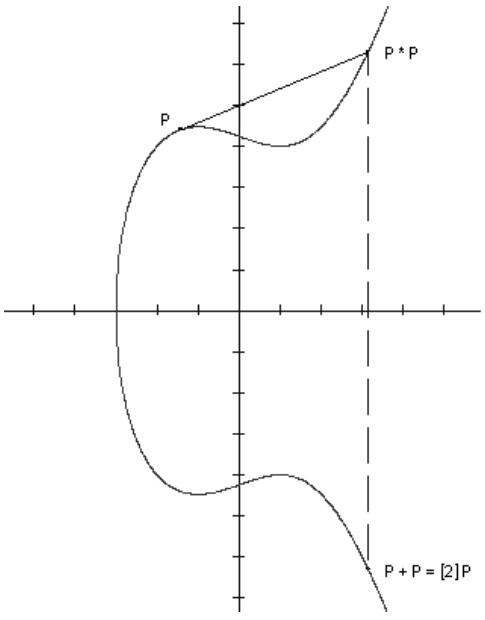


3 roots – 2 components

Let E be an elliptic curve over $\mathbb{R}$, and let P and Q be 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 $P + Q = (x_3, y_3)$,
$x_3 = \lambda^2 - x_1 - x_2$,
$y_3 = -y_1 + \lambda(x_1 - x_3)$,

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

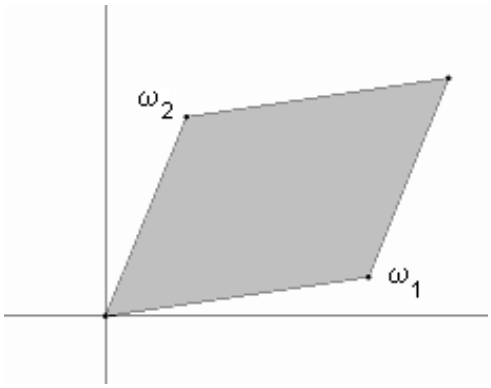
It can be shown that these formulas give an abelian group law on an elliptic curve over any field $\mathbb{K}$. All properties of an abelian group are evident, except the associative law.

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

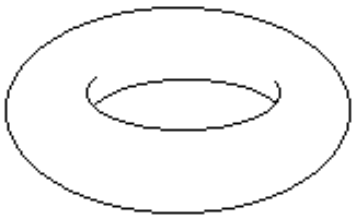
$$\left(\frac{\wp'}{2}\right)^2 = \wp^3 + a\wp + b.$$

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

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

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

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 $h(P) = \log H(x)$, 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

Corollary:

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

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 rank(E). Thus, 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 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 (Mazur): If E is an elliptic over over $\mathbb{Q}$, then $E(\mathbb{Q})_{\text{tors}}$ 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 points of finite order can be found by the following theorem.

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

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

Example: 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, $E(\mathbb{Q})_{\text{tors}} = \{\mathcal{O}, (0, -2)\} \cong \mathbb{Z}/2\mathbb{Z}$.

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 integer. 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: Find the torsion group for the elliptic curve

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

Solution: We have

$$4a^2+27b^3 = -372386507784192 = -2^{18}\cdot 3^{17}\cdot 11.$$

We take $p = 5$, 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 $\omega_1 = 0.198602\ldots$, $\omega_2 = 0.156713\ldots i$ and we compute

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

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

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

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. for any positive integer M there exist a curve E over $\mathbb{Q}$ such that rank$(E) \geq M$. However, the current record is the curve with rank ≥ 28 found by Elkies in 2006.

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

$$N^2 = b_1 M^4 + aM^2 e^2 + b_2 e^4 \qquad (3)$$

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

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

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: 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

$$y^2 = (x - 1)(2x - 1)(5x - 1). \qquad (4)$$

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 $\mathrm{rank}\,(E) = 2+0-2 = 0$.

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 $x = 1$.

The question how large can be the rank of an elliptic curve over $\mathbb{Q}$ has some relevance for cryptography. Namely, the discrete logarithm problem for multiplicative group $\mathbb{F}_q^*$ of a finite field can be solved in subexponential time using the Index Calculus method. For this reason, it was proposed by Miller and Koblitz in 1985 that for cryptographic purposes, one should replace F_q^* by the group of rational points $E(\mathbb{F}_q)$ on an elliptic curve over finite field.

DLP in $\mathbb{F}_p^*$:
$\mathbb{F}_p^* \to \mathbb{Z}$;
factor base $\mathcal{F}$ = small primes

ECDLP:
$E(\mathbb{F}_p) \to E(\mathbb{Q})$;
factor base $\mathcal{F}$ = generators of $E(\mathbb{Q})$

The main reasons why Index Calculus method cannot be applied on elliptic curves are that it is difficult:

- to find elliptic curves with large rank,

- to find elliptic curves generated by points of small height,

- to lift a point of $E(\mathbb{F}_p)$ to a point of $E(\mathbb{Q})$.

Silverman & Suzuki (1998):
For $p \approx 2^{160}$, we need rank $r \approx 180$.