Elliptic curves

Andrej Dujella

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

Elliptic curves are important objects in many areas of mathematics, such as number theory, algebraic geometry, complex analysis and public key cryptography.

In this talk, we will give an introduction to elliptic curves over the rationals and describe basic algorithms for obtaining information on their Mordell-Weil group.

We will briefly mention cryptographic applications of elliptic curves over finite fields.

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 (affine) 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 $a, b, c, \dots, j \in \mathbb{K}$, 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 char($\mathbb{K}$) $\neq 2, 3$, then the equation (1) can be transformed to the form

$$y^2 = x^3 + ax + b, \qquad (2)$$

which is called the *short Weierstrass form*. Here 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* $\Delta = -4a^3 - 27b^2$ is nonzero.

Thus, if 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

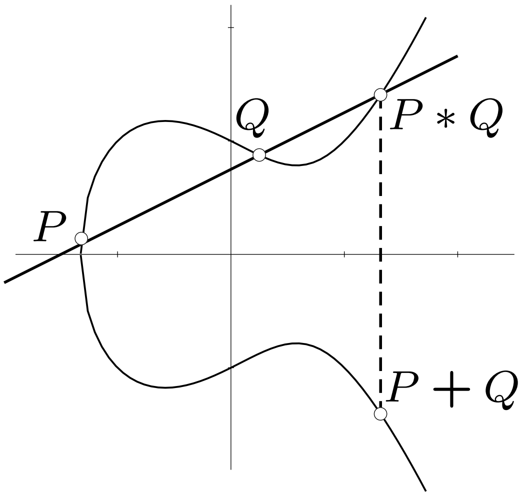
$$Y^2Z = X^3 + aXZ^2 + bZ^3.$$

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 $\mathcal{O}$.

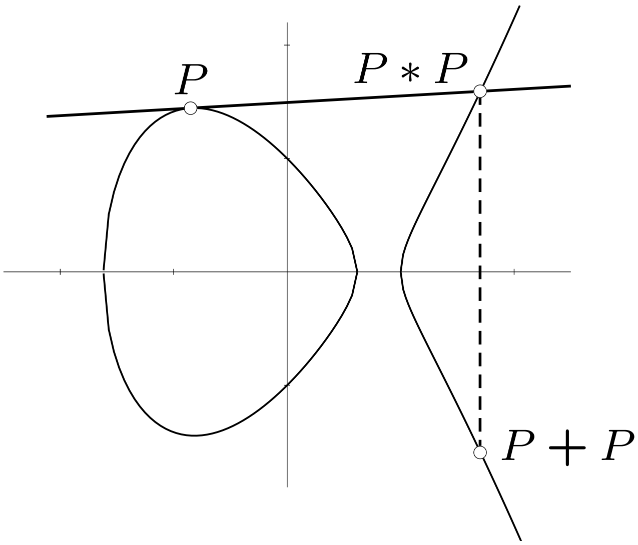
One of the most important facts about elliptic curves is that the set of points on an elliptic curve forms an abelian group (Poincaré, 1908).

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 $f(x) = x^3 + ax + b$.

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 $P \in E(\mathbb{R})$.



1 root - component
secant line



3 roots - 2 components
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 $P + Q = (x_3, y_3)$,
$x_3 = \lambda^2 - x_1 - x_2$,
$y_3 = -y_1 + \lambda(x_1 - x_3)$,

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

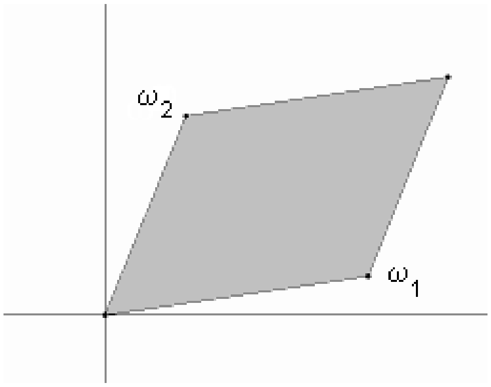
It can be shown that these formulas give an abelian group law on an elliptic curve over any field $\mathbb{K}$. All properties of an abelian group are evident, except the associative law.

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

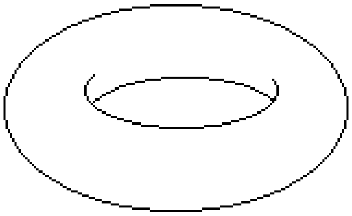
$$\left(\frac{\wp'}{2}\right)^2 = \wp^3 + a\wp + b.$$

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 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

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

Solution: We have $\Delta = -1728$. If $y = 0$, then $x = -2$ and we have the point $(-2, 0)$ 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, $E(\mathbb{Q})_{\text{tors}} = \{\mathcal{O}, (-2, 0)\} \cong \mathbb{Z}/2\mathbb{Z}$.

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 multiples 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.

$y^2+xy+y=x^3-x^2-$
$2006776241557552658503320820933854275093023031217895650 2x+$
$34481611795030556467032985690390720374855944359319180361266008296291939448732243429$

Independent points of infinite order:

P_{1}=[−2124150091254381073292137463,259854492051899599030515511070780628911531]
P_{2}=[2334509866034701756884754537,188720041954944691808683165528036279 31531]
P_{3}=[−1671736054062369063879038663,2517093772611442878085069472413191260 49131]
P_{4}=[2139130260139156666492982137,366395091714397292024214596929412975 27531]
P_{5}=[1534706764467120723885477337,854295853460176942890210328627810727 99531]
P_{6}=[−2731079487875677033341575063,262521815484332191641284072623902143387531]
P_{7}=[2775726266844571649705458537,128457554740140602488694876990826403 69931]
P_{8}=[1494385729327188957541833817,884866055277334059861164945140492334 11451]
P_{9}=[1868438228620887358509065257,592374032144377087127251403930593585 89131]
P_{10}=[2008945108825743774866542537,476906778801255528821517507815414247 11531]
P_{11}=[2348360540918025169651632937,174929300062005578573403324764488043 63531]
P_{12}=[−1472084007090481174470008663,246643450653503714199947441549759798469131]
P_{13}=[2924128607708061213363288937,283502644314888785014883564747673758 99531]
P_{14}=[5374993891066061893293934537,2861889084272633864511750319164798937 31531]
P_{15}=[1709690768233354523334008557,718988349746860894661597005292159809 21631]
P_{16}=[2450954011353593144072595187,444522817353263435704926255061071473 6531]
P_{17}=[2969254709273559167464674937,327668930753662708013336825431604696 87531]
P_{18}=[2711914934941692601332882937,206843661277838169865041398150659061 3531]
P_{19}=[2007858607799685452877832893 7,2779608541137806604656051725624624030091531]
P_{20}=[2158082450240734774317810697,349943734019640268099696622418009012 54731]
P_{21}=[2004645458247059022403224937,480493297807046455224398669998884754 67531]
P_{22}=[2975749450947996264947091337,333989898260753223202089344101048578 69131]
P_{23}=[−2102490467686285150147347863,259576391459875789571677393171687203227531]
P_{24}=[311583179915063034902194537,1681043852299806035401094729156601534 73931]
P_{25}=[2773931008341865231443771817,126321628346499210024141162737692758 13451]
P_{26}=[2156581188143768409363461387,351250929640229088970041505163751780 87331]
P_{27}=[3866330499872412508815659137,1211977556559442262930369267150258473 22531]
P_{28}=[2230868289773576023778678737,285587600305974856633870206007686400 28531]

History of elliptic curves rank records:

rank $\geq$	year	Author(s)
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

http://web.math.hr/~duje/tors/rankhist.html

Mestre's polynomial method (1991):

Lemma: Let $p(x) \in \mathbb{Q}[x]$ be a monic polynomial and $\deg p = 2n$. Then there exist 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 obtained from the asymptotic expansion of $\sqrt{p}$.

Assume now that $p(x) = \prod_{i=1}^{2n}(x - a_i)$, where $a_1, \ldots, a_{2n}$ are distinct rationals. The curve

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

contains the points $(a_i, \pm q(a_i))$, $i = 1, \ldots, 2n$. If $\deg r = 3$ or 4, and $r(x)$ has only simple roots, then C is an elliptic curve. This statement is clear for $\deg r = 3$. If $\deg r = 4$, we choose one rational point on C (e.g. $(a_1, q(a_1))$) for the points in infinity and transform C into an elliptic curve.

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 by the mentioned transformation we may expect to obtain an elliptic curve with rank ≥ 9. Mestre constructed a family of elliptic curves (i.e. a curve over $\mathbb{Q}(t)$) with rank ≥ 11, by taking $n = 6$ and $a_i = b_i + t$, $i = 1, \ldots, 6$; $a_i = b_{i-6} - t$, $i = 7, \ldots, 12$, and by choosing numbers $b_1, \ldots, b_6$ in such a way that the coefficient with x^5 in $r(x)$ be equal to 0 (e.g. $b_1 = -17$, $b_2 = -16$, $b_3 = 10$, $b_4 = 11$, $b_5 = 14$, $b_6 = 17$).

- extended by Mestre, Nagao and Kihara up to rank 14 over $\mathbb{Q}(t)$

- generalized by Fermigier, Kulesz and Lecacheux to curves with nontrivial torsion group

- Elkies (2006): rank 18 over $\mathbb{Q}(t)$ (methods from algebraic geometry)

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 $b_1 = \pm\,\mathrm{gcd}(m, b)$, $mb_1 > 0$. 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 $\mathrm{gcd}(M, e) = \mathrm{gcd}(N, e) = \mathrm{gcd}(M, N) = 1$.

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

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

Applications of elliptic curves

It is well-known that elliptic curves have applications in factorization of large integers and primality proving. The main idea is to replace the group $\mathbb{F}_p^*$ with (fixed) order $p-1$, by a group $E(\mathbb{F}_p)$ with more flexible order. Namely, by Hasse theorem we have

$$p+1-2\sqrt{p} < |E(\mathbb{F}_p)| < p+1+2\sqrt{p}.$$

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 $\mathbb{F}_p^*$:
find a such that $\alpha^a \equiv \beta$ (mod p)
Index Calculus Method:
$\mathbb{F}_p^* \to \mathbb{Z}$;
factor base $\mathcal{F} =$ small primes
$\alpha^k \bmod p = \prod p_i^{c_i}$ for many k's, gives $\log_\alpha p_i$
$\beta\alpha^k \bmod p = \prod p_i^{d_i}$ for some k, gives $\log_\alpha \beta$

ECDLP:
find m such that $P + \cdots + P = mP = Q$
$E(\mathbb{F}_p) \to E(\mathbb{Q})$;
factor base $\mathcal{F} =$ generators of $E(\mathbb{Q})$

One of the reasons why Index Calculus Method cannot be applied on elliptic curves is that it is difficult to find elliptic curves with large rank and generated by points of small height (generators of $E(\mathbb{Q})$ should play the role of small primes).

Silverman and Suzuki (1998) estimated that for $p \approx 2^{160}$, which is the size of standard values is use today, in order to apply the Index Calculus Method to $E(\mathbb{F}_p)$ we need rank $r \approx 180$.

In that way, cryptosystems based on DLP for $E(\mathbb{F}_p)$ with 160 bits long p provide the same level of security as cryptosystems based on DLP for F_p^* with 1024 bits long p.