Applications of elliptic curves in public key cryptography

Andrej Dujella

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

Abstract:

The most popular public key cryptosystems are based on the problem of factorization of large integers and discrete logarithm problem in finite groups, in particular in the multiplicative group of finite field and the group of points on elliptic curve over finite field. Elliptic curves are of special interest since they at present alow much shorter keys, for the same level of security, compared with cryptosystems based on factorization or discrete logarithm problem in finite fields.

In this course we will briefly mentioned basic properties of elliptic curves over the rationals, and then concentrate on important algorithms for elliptic curves over finite fields. We will discuss efficient implementation of point addition and multiplication (in different coordinates). Algorithms for point counting and elliptic curve discrete logarithm problem will be described.

Factorization and primality testing and proving are very important topics for security of public key cryptosystems. Namely, the starting point in the construction of almost all public key cryptosystems is the choice of one or more large (secret or public) prime numbers. We will describe algorithms for factorization and primality proving which use elliptic curves.

Program:

1. Public Key Cryptography
2. Elliptic curves over the rationals
3. Elliptic curves over finite fields
4. Implementation of operations
5. Algorithms for determining the group order
6. Elliptic Curve Cryptosystems
7. Comparing elliptic curve with other types of cryptography
8. Elliptic curve discrete logarithm problem
9. Lenstra's elliptic curve factoring method
10. Elliptic curve primality proving algorithm

Bibliography:

[1] I. Blake, G. Seroussi, N. Smart: *Elliptic Curves in Cryptography*, Cambridge University Press, Cambridge, 1999.

[2] I. Blake, G. Seroussi, N. Smart (Eds), *Advances in Elliptic Curve Cryptography*, Cambridge University Press, 2005.

[3] H. Cohen, G. Frey (Eds), *Handbook of Elliptic and Hyperelliptic Curve Cryptography*, CRC Press, Boca Raton, 2005.

[4] R. Crandall, C. Pomerance: *Prime Numbers. A Computational Perspective*, Springer-Verlag, New York, 2001.

[5] D. Hankerson, A. Menezes, S. Vanstone, *Guide to Elliptic Curve Cryptography*, Springer-Verlag, New York, 2004.

[6] N. Koblitz, *A Course in Number Theory and Cryptography*, Springer-Verlag, New York, 1994.

[7] M. Rosing, *Implementing Elliptic Curve Cryptography*, Manning, Greenwich, 1999.

[8] J. H. Silverman, Elliptic curves and cryptography, in: P. Garrett, D. Lieman (Eds.), *Public-Key Cryptography*, American Mathematical Society, Providence, 2005, pp.91–112.

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

[10] N. Smart, *Cryptography. An Introduction*, McGraw-Hill, New York, 2002.

[11] D.R. Stinson: *Cryptography. Theory and Practice*, CRC Press, Boca Raton, 2005.

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

`http://web.math.hr/~duje/bilbao.html`

1. Public Key Cryptography

The classical situation in cryptography is that two persons - ALICE and BOB - wish to perform some form of communication while an eavesdropper - EVE - wishes to spy the communication between Alice and Bob. Of course, there is no assumption that Alice and Bob (or Eve) are actually human. They may be computers on some network.

In classical model of cryptography, Alice and Bob secretly choose the key K, which then gives an encryption rule e_K and a decryption rule d_K, and d_K is either the same as e_K, or easily derived from it. Cryptosystems of this type are called *private-key* systems or *symmetric* systems. One drawback of this system is that it requires prior communication of the key K between Alice and Bob, using a secure channel. This may be very difficult to achieve.

The idea of a *public-key* cryptography is that it might be possible to find a cryptosystem where it is computationally infeasible to determine d_K from e_K. If so, then the encryption rule e_K could be made public by publishing it in a directory. Now Alice (or anyone else) can send an encrypted message to Bob (without prior communication of a secret key) by using public encryption rule e_K. But Bob will be the only person that can decrypt the ciphertext, using his secret decryption rule d_K.

The idea of a public-key system was introduced in 1976 by Diffie and Hellman. The first realization of a public-key system was proposed in 1977 by Rivest, Shamir and Adleman (RSA Cryptosytem), and its security is based on the problem of factorization of large integers.

Modern cryptography, as applied in commercial world, is concern with a number of (new) problems. The most important of these are:

1. Confidentiality: A message sent form Alice to Bob cannot be read by anyone else.

2. Authenticity: Bob knows that only Alice could have sent the message he has just received.

3. Integrity: Bob knows that the message from Alice has not been tampered with in transit.

4. Non-repudiation: It is impossible for Alice to deny later that she sent the message.

The typical situation is that Alice wishes to buy some item over the Internet from Bob.

It should be said that the public key systems are much slower than best symmetric systems (e.g. Advanced Encryption Standard - AES). Therefore, their use in confidentiality is usually limited to the transmission of key for symmetric ciphers. On the other hand, *digital signatures*, which give the users the authenticity, integrity and non-repudiation properties required in electronic commerce, require the use of public-key cryptography.

Idea of digital signatures: Alice signs the message x by sending to Bob the ciphertext $z = d_A(y) = d_A(e_B(x))$. Bob decrypts the cipher using Alice's public key e_A and his secret key d_B:

$$d_B(e_A(z)) = d_B(e_A(d_A(e_B(x)))) = x.$$

Bob now knows that only Alice could have sent the message he has just received because only Alice knows d_A. If Alice later denies that she sent the message, Bob can present the messages x and z and confirm that $e_B(x) = e_A(z)$.

Diffie-Hellman key exchange protocol:

1. Alice and Bob agree on a group G and an element g of G of order n. The group G and the element g are assumed to be public knowledge, and in particular to be known to Eve.

2. Alice chooses secret integer $a \in \{1, 2, ..., n-1\}$, computes $A = g^a$ and sends A to Bob.

3. Bob chooses secret integer $b \in \{1, 2, ..., n-1\}$, computes $B = g^b$ and sends B to Alice.

4. Alice computes $B^a = g^{ab}$.

5. Bob computes $A^b = g^{ab}$.

Bob and Alice both know the value $A^b = g^{ab} = B^a$.

Eve knows G, g, A and B. She has to compute g^{ab} (*Diffie-Hellman problem* (DHP)). If she can solve *discrete logarithm problem* (DLP), i.e. determine a from g and $A = g^a$, then she can use a and B to compute g^{ab}.

DLP is easy in some groups. E.g. $\mathbb{Z}/n\mathbb{Z}$ under addition, the Euclidean algorithm solves the DLP.

But for some groups, DLP is quite difficult, and can be used in Diffie-Hellman protocol, or serve as a base for building a public key cryptosystem. Such group is e.g. the multiplicative group $\mathbb{F}_p^*$ of a finite field under multiplication. Indeed, when someone refers to the DLP with no further adjectives, it generally indicates this case. Best known algorithm (Index Calculus Method) for solving DLP in $\mathbb{F}_p^*$ is sub-exponential.

However, there are groups where it takes fully exponential time to solve the DLP. The most important examples are groups of elliptic curves over finite fields.

2. Elliptic curves over the rationals

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 $a, b, c, \ldots, j \in \mathbb{K}$, 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 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*. 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 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".

If char($\mathbb{K}$) $= 2$, then we have two types of equations:

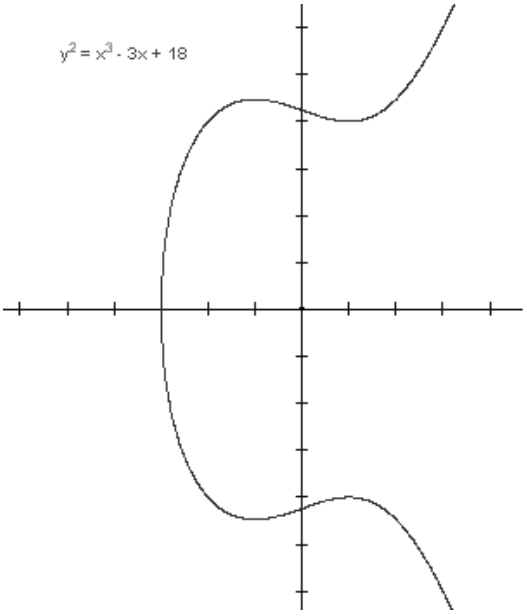
$y^2 + cy = x^3 + ax + b$ or $y^2 + xy = x^3 + ax^2 + b$.

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

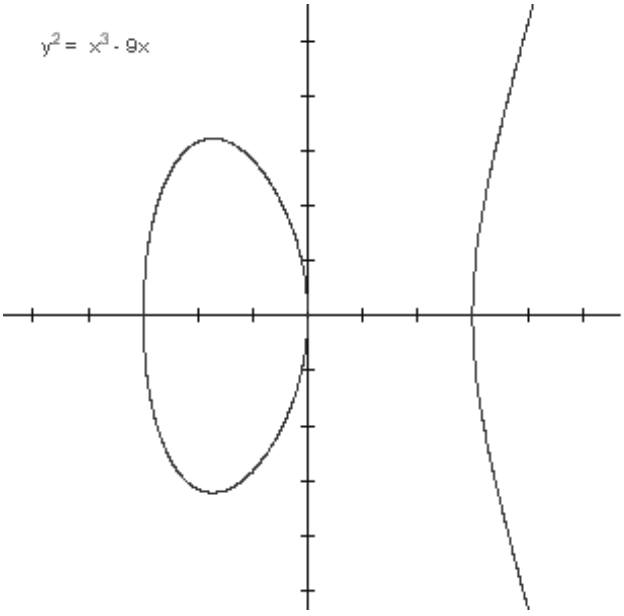
$$Y^2Z = X^3 + aXZ^2 + bZ^3.$$

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

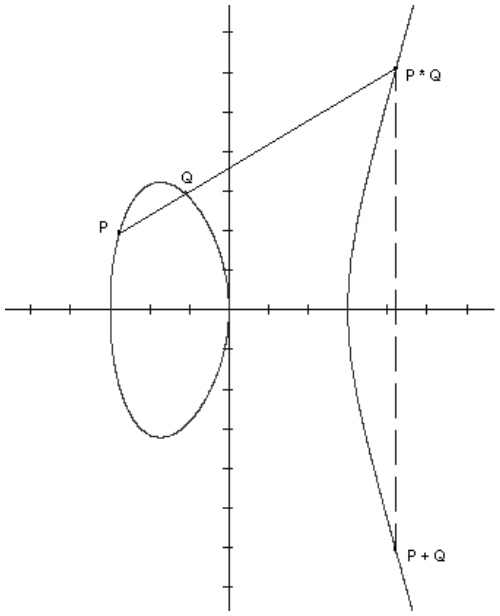


1 root – 1 component

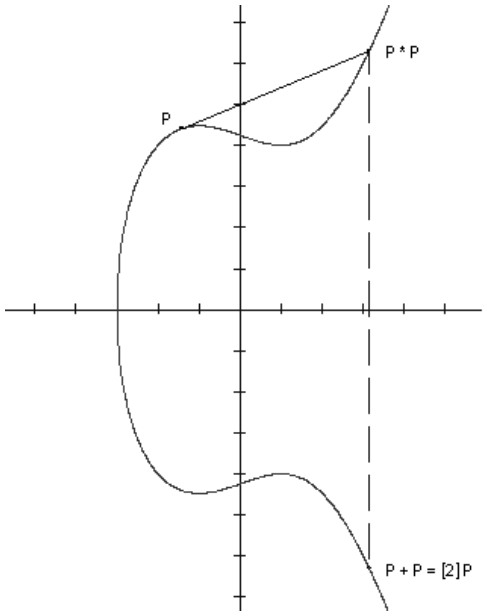


3 roots – 2 components

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 $P \in E(\mathbb{R})$, where $\mathcal{O}$ is the point in infinity.



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), and give an abelian group law on the points of an elliptic curve.

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

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

Let E be an elliptic curve over $\mathbb{Q}$.

By Mordell's theorem, the group $E(\mathbb{Q})$ of rationals points on E is a finitely generated abelian group. Hence, it is the product of the torsion group and $r \geq 0$ copies of infinite cyclic group:

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

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.

By Mazur's theorem, we know that $E(\mathbb{Q})_{\text{tors}}$ is one of the following 15 groups:

$\mathbb{Z}/n\mathbb{Z}$, with $1 \leq n \leq 10$ or $n = 12$,
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z}$, with $1 \leq m \leq 4$.

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 Lutz-Nagell theorem:

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.)

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

On the other hand, it is not know what values of rank r are possible for elliptic curves over $\mathbb{Q}$. The "folklore" conjecture is that a rank can be arbitrary large, but it seems to be very hard to find examples with large rank. The current record is an example of elliptic curve over $\mathbb{Q}$ with rank ≥ 28, found by Elkies in May 2006.

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`

There is even a stronger conjecture that for any of 15 possible torsion groups T we have $B(T) = \infty$, where

$B(T) = \sup\{\text{rank}\,(E(\mathbb{Q})) : \text{torsion group of } E \text{ over } \mathbb{Q} \text{ is } T\}$.

Montgomery (1987): Proposed the use of elliptic curves with large torsion group and positive rank in factorization.

It follows from results of Montgomery, Suyama, Atkin & Morain (*Finding suitable curves for the elliptic curve method of factorization*, 1993), that $B(T) \geq 1$ for all torsion groups T.

Womack (2000): $B(T) \geq 2$ for all T

Dujella (2003): $B(T) \geq 3$ for all T

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

The best known lower bounds for $B(T)$:

T	$B(T) \geq$	Author(s)
0	28	Elkies (06)
$\mathbb{Z}/2\mathbb{Z}$	19	Elkies (09)
$\mathbb{Z}/3\mathbb{Z}$	13	Eroshkin (07,08,09)
$\mathbb{Z}/4\mathbb{Z}$	12	Elkies (06)
$\mathbb{Z}/5\mathbb{Z}$	8	Dujella & Lecacheux (09), Eroshkin (09)
$\mathbb{Z}/6\mathbb{Z}$	8	Eroshkin (08), Dujella & Eroshkin (08), Elkies (08), Dujella (08)
$\mathbb{Z}/7\mathbb{Z}$	5	Dujella & Kulesz (01), Elkies (06), Eroshkin (09), Dujella & Lecacheux (09), Dujella & Eroshkin (09)
$\mathbb{Z}/8\mathbb{Z}$	6	Elkies (06)
$\mathbb{Z}/9\mathbb{Z}$	4	Fisher (09)
$\mathbb{Z}/10\mathbb{Z}$	4	Dujella (05,08), Elkies (06)
$\mathbb{Z}/12\mathbb{Z}$	4	Fisher (08)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	15	Elkies (09)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$	8	Elkies (05), Eroshkin (08), Dujella & Eroshkin (08)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$	6	Elkies (06)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$	3	Connell (00), Dujella (00,01,06,08), Campbell & Goins (03), Rathbun (03,06), Flores, Jones, Rollick & Weigandt (07), Fisher (09)

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

Construction of high-rank curves

1. Find a parametric family of elliptic curves over $\mathbb{Q}$ which contains curves with relatively high rank (i.e. an elliptic curve over $\mathbb{Q}(t)$ with large generic rank); e.g. by Mestre's polynomial method.

2. Choose in given family best candidates for higher rank. General idea: a curve is more likely to have large rank if $\#E(\mathbb{F}_p)$ is relatively large for many primes p. Precise statement: Birch and Swinnerton-Dyer conjecture. More suitable for computation: Mestre's conditional upper bound (assuming BSD and GRH), Mestre-Nagao sums, e.g. the sum:

$$s(N) = \sum_{p \leq N,\ p \text{ prime}} \frac{\#E(\mathbb{F}_p) + 1 - p}{\#E(\mathbb{F}_p)} \log(p)$$

3. Try to compute the rank (Cremona's program MWRANK - very good for curves with rational points of order 2), or at least good lower and upper bounds for the rank.

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 point 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)

3. Elliptic curves over finite fields

For the applications in cryptography, the most important case is when $\mathbb{K}$ is a finite field.

Let $\mathbb{F}_q$ denotes a field which has q elements. Let p be a characteristic of $\mathbb{F}_q$. Then $\mathbb{F}_q$ contains the prime field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, and so it is a vector space over $\mathbb{F}_p$. Let k denotes dimension of $\mathbb{F}_q$ as an $\mathbb{F}_p$ - vector space. Then $\mathbb{F}_q$ has p^k elements, i.e. $q = p^k$.

Moreover, for every prime power $q = p^k$ there is a field of q elements, and it is unique (up to isomorphism). It can be represented as $\mathbb{F}_p[x]/(f(x))$, where $f(x)$ is an irreducible polynomial od degree k over $\mathbb{F}_p$ (we have p^k polynomials in $\mathbb{F}_p[x]$ of degree at most $k-1$, and addition and multiplication is as in $\mathbb{Z}_p[x]$, followed by a reduction modulo $f(x)$).

The number of irreducible polynomials in $\mathbb{F}_p[x]$ of degree k is approximately p^k/k.

Testing irreducibility uses the fact that $f(x)$ is irreducible if and only if

$$\gcd(f(x), x^{p^j} - x) = 1, \text{ for } j = 1, \ldots, \lfloor k/2 \rfloor.$$

For better efficiency, it is advisable to use polynomials $f(x)$ with small weight W (number of nonzero coefficients). In the case $q = 2^k$, it seems that it is always possible to choose $W = 3$ or $W = 5$. E.g. in the case $q = 2^8$ (which is used in AES), we may take $f(x) = x^8 + x^4 + x^3 + x + 1$.

Let $\mathbb{F}_q^*$ denotes the multiplicative group of the field $\mathbb{F}_q$. The group $\mathbb{F}_q^*$ is cyclic, i.e. there exist an element $g \in \mathbb{F}_q^*$ such that the powers of g run through all of the elements of $\mathbb{F}_q^*$.

Example: Let us consider the elliptic curve

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

over $\mathbb{F}_7$. We want to find all elements and the structure of the group $E(\mathbb{F}_7)$.

Note that squares in $\mathbb{F}_7$ are 0, 1, 2 and 4. Inserting $x = 0, 1, 2, 3, 4, 5, 6$ in $y^2 = x^3+x+3$ we get equations $y^2 = 3, 5, 6, 5, 1, 0, 1$ in $\mathbb{F}_7$. We conclude that exactly for $x = 4, 5$ and 6 corresponding equations are solvable, and we find that

$$E(\mathbb{F}_7) = \{\mathcal{O}, (4,1), (4,6), (5,0), (6,1), (6,6)\}.$$

Let us determine the structure of the group $E(\mathbb{F}_7)$. Take $P = (4,1)$ are compute its multiples:

$$[2]P = (6,6),\ [3]P = (5,0),\ [4]P = (6,1),$$
$$[5]P = (4,6),\ [6]P = \mathcal{O}.$$

Hence, $E(\mathbb{F}_7)$ is a cyclic group of order 6.

Let E be an elliptic curve over finite field $\mathbb{F}_q$ with $q = p^k$ elements. It is easy to see that $\#E(\mathbb{F}_q) \leq 2q + 1$, since we have the point at infinity and for every x at most two y's. But since only half of elements of $\mathbb{F}_q^*$ have square roots (those of the form g^{2n}, where g is a generator of the multiplicative cyclic group $\mathbb{F}_q^*$), we may expect that $\#E(\mathbb{F}_q)$ will only about a half of that number. The precise version of this observation is given by Hasse's theorem:

$$|q + 1 - \#E(\mathbb{F}_q)| \leq 2\sqrt{q}.$$

The quantity t defined by $\#E(\mathbb{F}_q) = q + 1 - t$ is called the *trace of Frobenius*. We have $|t| \leq 2\sqrt{q}$.

For curves over $\mathbb{F}_p$, where p is a prime, there is an elliptic curve with group of rational points of any given order in the interval $\langle p+1-2\sqrt{p}, p+1+2\sqrt{p}\rangle$ (Deuring). In subinterval

$$\langle p + 1 - \sqrt{p}, p + 1 + \sqrt{p}\rangle$$

each order occurs with an almost uniform distribution (Lenstra).

In general case, $q = p^k$, there exist an elliptic curve E over $\mathbb{F}_q$ such that $\#E(\mathbb{F}_q) = q + 1 - t$ if and only if $|t| \leq 2\sqrt{q}$ and t satisfies one of the following conditions:
1) $\gcd(t, p) = 1$;
2) k is even and $t = \pm 2\sqrt{q}$ or ($t = \pm\sqrt{q}$ and $p \not\equiv 1 \pmod 3$) or ($t = 0$ and $p \not\equiv 1 \pmod 4$);
3) k is odd and $t = 0$ or ($t = \pm\sqrt{2q}$ and $p = 2$) or ($t = \pm\sqrt{3q}$ and $p = 3$).

Contrary to the case of elliptic curves over $\mathbb{Q}$ where the characterization of possible ranks of groups $E(\mathbb{Q})$ is an open problem, in the case of elliptic curves of finite fields we know that

$$E(\mathbb{F}_q) \cong (\mathbb{Z}/n_1\mathbb{Z}) \times (\mathbb{Z}/n_2\mathbb{Z}),$$

where n_1, n_2 are positive integers satisfying $n_1 | n_2$ and $n_1 | q-1$ (including the possibility that $n_1 = 1$). Thus, $E(\mathbb{F}_q)$ is "almost cyclic".

4. Implementation of operations

If we want to use some group G as a basis for a public-key cryptosystem, it is important that we can make multiplication and exponentiation efficiently. Since the group law on elliptic curves is written additively, we will talk on *points addition* and *point multiplication*:

$$[m]P = \underbrace{P + P + \cdots + P}_{m \text{ summands}}.$$

From the formulas for point addition we see that when $P \neq Q$ the computation of $P + Q$ requires one field inversion and three multiplications (1I + 3M) (we neglect the cost of field additions and multiplications by small constants). When $P = Q$, the cost of the point doubling is 1I + 4M.

These results are for fields of characteristic > 3. In characteristic 2, the situation is similar, except that is this case the cost of squaring operation is much smaller than that of a general multiplication (so we have 1I + 2M).

The inverse the be compute by extended Euclidean algorith (ordinary integer version in the case $q = p$, and polynomial version in the case $q = 2^k$). Although the complexity of the Euclidean algorithm is theoretically comparable with the complexity of the field multiplications, in practise the multiplication is much faster than inversion.

The field inversion can be avoided by using weighted projective representation, where the projective point (X, Y, Z) corresponds to $(X/Z^2, Y/Z^3)$ (first coordinate has weight 2, a second has weight 3). In these coordinates we need 16M for computing $P + Q$ and 10M for $P + P$ (and no inversion). The equation in this new coordinates is

$$Y^2 = X^3 + aXZ^4 + bZ^6.$$

Let $P = (X_1, Y_1, Z_1)$. Then the coordinates of $P + P = (X_2, Y_2, Z_2)$ can be computed by

$$\lambda_1 = 3X_1^2 + aZ_1^4, \;\; \lambda_2 = 4X_1Y_1^2, \;\; \lambda_3 = 8Y_1^4,$$
$$X_2 = \lambda_1^2 - 2\lambda_2, \;\; Y_2 = \lambda_1(\lambda_2 - x_2) - \lambda_3,$$
$$Z_2 = 2Y_1Z_1.$$

There are other type of (projective) coordinates which avoid computing the inverse. Recently, the Edwards coordinates were introduced which unify formulas for $P+Q$ and $P+P$.

The point multiplication on elliptic curves is a special case of the general problem of the exponentiation in abelian groups. As such, it benefits from all techniques available for the general problem.

The simplest (and oldest) efficient method for points multiplication relies on the binary expansion of m. It is called *binary method*, *binary ladder* or *repeated squaring method*.

E.g. assume that we want to compute $[13]P$. The binary expansion of 13 is $(1\,1\,0\,1)_2$. Now, we can compute $[13]P$ as

$$[13]P = P + [2]([2]P) + [2]([2][2]P)).$$

Here we read the expansion from right to left. By reading it from left to right, we can compute $[13]P$ as

$$[13]P = [2]([2](P + [2]P)) + P.$$

Thus, we have the following two algorithms for computing $Q = [m]P$, where $m = (m_d, \ldots, m_0)_2$.

Binary method (from right to left):

$Q = \mathcal{O}$; $R = P$
for $i = 0$ to $d - 1$
    if $(m_i = 1)$ then $Q = Q + R$
    $R = [2]R$
$Q = Q + R$

Binary method (from left to right):

$Q = P$
for $i = d - 1$ to 0 by -1
    $Q = [2]Q$
    if $(m_i = 1)$ then $Q = Q + P$

Both variants have the same number of operations: d duplications and number of additions is equal to number of nonzero digits in binary expansion for m (which is $\leq d+1$, and $d/2$ in average). The variant "from left to right" has an advantage that in the step $Q = Q + P$, always the same point P is added, and this might be used for more efficient implementation. The number of bit operations for computing $[m]P$ is $O(\log m \log^2 q)$.

There are several general improvements of the binary method, but we will mention one method which is specific for elliptic curves. Namely, in elliptic curve group the *subtraction* has virtually the same cost as the addition ($-(x, y) = (x, -y)$; and in characteristic 2, $-(x, y) = (x, x+y)$), while usually division in a group is more computationally expensive then multiplication.

This lead us to consider the *signed digit* (SD) representation of the form $m = \sum_{i_0}^{d} s_i 2^i$, where $s_i \in \{-1, 0, 1\}$. Such representation is clearly not unique. E.g.

$$3 = (0\ 1\ 1) = (1\ 0\ \text{-}1).$$

Thus we may choose the representation which leads to more efficient multiplication algorithm. We say that a SD representation is *sparse* or *non-adjacent form* (NAF) if it has no adjacent nonzero digits, i.e. $s_i s_{i+1} = 0$ for all $i \geq 0$. It can be proved that every integer m has a unique NAF, and NAF has the lowest weight (number of nonzero digits) among all SD representations of m. Expected weight of NAF of lenght d is $d/3$ (compared with $d/2$ in binary method).

The following algorithm computes NAF representation $(s_d, \ldots, s_0)$ of number n, starting from its binary representation $(n_{d-1}, \ldots, n_0)_2$.

Algorithm for NAF representation

$c_0 = 0$
for $i = 0$ to d
$\quad c_{i+1} = \lfloor (n_i + n_{i+1} + c_i)/2 \rfloor$
$\quad s_i = n_i + c_i - 2c_{i+1}$

Alternatively, we can use the following table, which for all possible inputs (n_i, c_i, n_{i+1}) give the corresponding outputs (c_{i+1}, s_i).

n_i	0	0	0	0	1	1	1	1
c_i	0	0	1	1	0	0	1	1
n_{i+1}	0	1	0	1	0	1	0	1
c_{i+1}	0	0	0	1	0	1	1	1
s_i	0	0	1	-1	1	-1	0	0

It is straightforward to adapt binary method to NAF.

Signed binary method (from left to right):

$Q = P$
for $i = d - 1$ to 0 by -1
    $Q = [2]Q$
    if $(m_i = 1)$ then $Q = Q + P$
    if $(m_i = -1)$ then $Q = Q - P$

For applications in cryptography, the most important finite fields are prime fields $\mathbb{F}_p$ and fields of characteristic two $\mathbb{F}_{2^k}$. With p and 2^k of the same size they offer the same level of security. The choice of $\mathbb{F}_{2^k}$ is better for hardware applications. But if a crypto coprocessor (accelerate modular arithmetic) is already available, then $\mathbb{F}_p$ may offer performance advantages over $\mathbb{F}_{2^k}$.

To minimize time to perform modular multiplication, it is recomended that p has the form $2^m \pm c$ for some small c (e.g. Mersenne primes $2^m - 1$, $2^{160} + 7$, $2^{255} + 95$, ...).

For $\mathbb{F}_{2^k}$, some popular choices are $q = 2^{155}$, 2^{163}, 2^{191}, 2^{239}, 2^{431}. In the case of a field $\mathbb{F}_{2^k}$, we should also select a representation for the elements of $\mathbb{F}_{2^k}$. Namely, there are many different bases of $\mathbb{F}_{2^k}$ over $\mathbb{F}_2$. We will mention two types: trinomial and normal bases.

If $f(x)$ is an irreducible polynomial of degree k over $\mathbb{F}_2$, the the field $\mathbb{F}_{2^k}$ can be represented as the set of polynomials of degree less then k over $\mathbb{F}_2$. Such a representation is called *polynomial basis representation*.

A *trinomial basis representation* is a polynomial basis representation in which the polynomial $f(x)$ has the form $f(x) = x^k + x^m + 1$. Such representations have the advantage that reduction modulo $f(x)$ can be performed efficiently, both in software and hardware. Irreducible trinomials exist over half of values k in the range $k \leq 1000$, but they do not exist e.g. if $k \equiv 0 \pmod 8$.

A *normal basis* for $\mathbb{F}_{2^k}$ over $\mathbb{F}_2$ is a basis of the form

$$\{b, b^2, b^{2^2}, \ldots, b^{2^{k-1}}\},$$

where $b \in \mathbb{F}_{2^k}$. Such a basis always exists. The field squaring is trivial in normal basis representation: if $a = (a_0, a_1, \ldots, a_{k-1})$, then

$$a^2 = (a_{k-1}, a_0, a_1, \ldots, a_{k-2}),$$

i.e. squaring is just a cyclic shift. However, the multiplication in a general normal basis is more complicated. The normal basis in which the cost of multiplication in minimal are called *optimal normal basis* (ONB). One of necessary conditions for the existence of a ONB is that $k + 1$ or $2k + 1$ is a prime.

5. Algorithms for determining the group order

To decide whether an elliptic curve E over $\mathbb{F}_q$ is "good" for applications in cryptography, we should know the order of the group $E(\mathbb{F}_q)$. There are several types of curves with should be avoided.

- Pohlig-Hellman reduction implies that $\#E(\mathbb{F}_q)$ should be divisible by a sufficiently large prime p' to resist the BSGS or Pollard ρ attack (e.g. $p' > 2^{160}$.

- E should not be "anomalous". *Anomalous* curves are those with trace of Frobenius $t = 1$, i.e. $\#E(\mathbb{F}_q) = q$. For such curves there exist a polynomial-time algorithm for ECDLP (Smart, Satoh, Araki, Semaev).

- E should not be "supersingular". The curve over $\mathbb{F}_{p^k}$ is *supersingular* if $p|t$. For curves over $\mathbb{F}_p$ with $p \geq 5$ this means that $t = 0$ and $\#E(\mathbb{F}_p) = p + 1$. For such curves there is the MOV attack (Menezes, Okamoto, Vanstone) which in polynomial time reduces ECDLP in $E(\mathbb{F}_q)$ to DLP in $\mathbb{F}_{q^2}$. More generally, one should avoid curves such that

$$q^l \equiv 1 \pmod{\#E(\mathbb{F}_q)}$$

for small l (say $l \leq 20$), because then MOV attack reduces the problem to DLP in $\mathbb{F}_{q^l}$.

A straightforward method for computing $\#E(\mathbb{F}_p)$ is by using Legendre's symbol:

$$\#E(\mathbb{F}_p) = p + 1 + \sum_{x \in \mathbb{F}_p} \left(\frac{x^3 + ax + b}{p} \right).$$

It has complexity $O(p \ln^2 p)$, thus it is applicable only for small p's, say $p < 10000$.

We will know describe the *Shanks-Mestre method*, which has complexity $O(p^{1/4+\varepsilon})$ and works in practise for $p < 10^{30}$.

By the Hasse theorem we know that $\#E(\mathbb{F}_p) = p+1-t$, $|t| \leq 2\sqrt{p}$. Choose random $P \in E(\mathbb{F}_p)$. We want for find a number $N \in \langle p+1-2\sqrt{p}, p+1+2\sqrt{p} \rangle$ such that $[N]P = \mathcal{O}$. Such number N certainly exists since order of P divides $\#E(\mathbb{F}_p)$. If the order P is greater than $4\sqrt{p}$ (by a result of Mestre, the point P with this property exists on E or its twist E' if $p > 457$), then such N is unique and equal to $\#E(\mathbb{F}_p)$.

The search for N is based of Shanks' "baby step - giant step" (BSGS) method. Let $Q = [p+1+\lfloor 2\sqrt{p}\rfloor]P$. Then $n = p+1+\lfloor 2\sqrt{p}\rfloor - N$ satisfies $0 \leq n \leq 4\sqrt{p}$ and

$$[n]P = [p+1+\lfloor 2\sqrt{p}\rfloor - N]P = Q.$$

Actually this is a discrete logarithm problem. We do not have very efficient algorithm for this problem, but at least we can do better than just testing all possibilities for n.

Shanks-Mestre's method:

$m = \lceil 2p^{1/4} \rceil$
$P \in E(\mathbb{F}_p)$, $|P| > 4\sqrt{p}$
$Q = [p+1+\lfloor 2\sqrt{p}\rfloor]P$
for $(0 \leq j \leq m-1)$
    compute and save $[j]P$
for $(0 \leq i \leq m-1)$ {
    if $(Q - [i]([m]P) = [j]P$ for some
        $0 \leq j \leq m-1)$ then
        $t = im + j - \lfloor 2\sqrt{p}\rfloor$ }
return t

Example: Given is the curve

$$E : y^2 = x^3 + 3x + 5$$

over $\mathbb{F}_{163}$. Compute the order of the group $E(\mathbb{F}_{163})$.

We have $m = 8$. Take $P = (1, 3)$. Then $Q = [163 + 1 + 25]P = (106, 61)$. In the next table "baby steps" are given:

j	0	1	2	3
$[j]P$	$\mathcal{O}$	$(1, 3)$	$(162, 162)$	$(4, 154)$
j	4	5	6	7
$[j]P$	$(11, 37)$	$(143, 101)$	$(77, 80)$	$\mathbf{(118, 5)}$

We compute $R = [8]P = (97, 150)$.
"Giant steps" are given in the next table:

i	0	1	2	3
$Q - [i]R$	$(106, 61)$	$(79, 83)$	$(145, 65)$	$\mathbf{(118, 5)}$
i	4	5	6	7
$Q - [i]R$	$(1, 160)$	$(142, 61)$	$(7, 83)$	$(124, 8)$

Hence, $n = 3 \cdot 8 + 7 = 31$, $t = 31 - 25 = 6$ and finally $\#E(\mathbb{F}_{163}) = 163 + 1 - 6 = 158$.

The first polynomial-time algorithm for computing $\#E(\mathbb{F}_q)$ was proposed in 1985 by Schoof. Its complexity is $O(\log^8 q)$, and it is not efficient enough for all q's of practical interest. There are some improvements of this algorithm by Atkin and Elkies which works satisfactory for q's of 160 bits.

Let us say just few words about Schoof's algorithm. By Hasse's theorem, $\#E(\mathbb{F}_q) = q+1-t$, $|t| \leq 2\sqrt{q}$. The idea of Schoof's algorithm is the determination of t modulo primes l, for $l \leq l_{max}$, where l_{max} is the smallest prime such that

$$\prod_{\substack{l \text{ prime} \\ l \leq l_{max}}} l > 4\sqrt{q}.$$

Then from $t \bmod l$ for $2 \leq l \leq l_{max}$, by CRT we can determine uniquely the value of t. By Prime Nubmer Theorem we have $l_{max} = O(\log q)$, so the number of congruences is $O(\frac{\ln q}{\ln \ln q})$.

In determining $t \mod l$, the *Frobenious endomorphism* is used. This is the map $\varphi : E(\mathbb{F}_q) \to E(\mathbb{F}_q)$ given by $\varphi(x, y) = (x^q, y^q)$, $\varphi(\mathcal{O}) = \mathcal{O}$. Frobenius endomorphism φ and Frobenius trace t are related by

$$\varphi^2 - [t]\varphi + [q] = [0],$$

i.e. for each $P = (x, y) \in E(\mathbb{F}_q)$ it holds

$$(x^{q^2}, y^{q^2}) - [t](x^q, y^q) + [q](x, y) = \mathcal{O}.$$

Let $P \in E(\mathbb{F}_q)$ be such that $[l]P = \mathcal{O}$, and let $q_l = q \mod l$. If $\tau \in 0, 1, \ldots, l-1$ satisfies $\varphi^2(P) + [q_l]P = [\tau]\varphi(P)$, then $t \mod l = \tau$.

6. Elliptic Curve Cryptosystems

Definition: A *cryptosystem* is a five-tuple $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$, where the following conditions are satisfied:
$\mathcal{P}$ is a finite set of possible *plaintexts*;
$\mathcal{C}$ is a finite set of possible *ciphertexst*;
$\mathcal{K}$ is a finite set of possible *keys*;
For each $K \in \mathcal{K}$, there is an *encryption rule* $e_K \in \mathcal{E}$ and a corresponding *decryption rule* $d_K \in \mathcal{D}$. Each $e_K : \mathcal{P} \to \mathcal{C}$ and $d_K : \mathcal{C} \to \mathcal{P}$ are functions such that $d_K(e_K(x)) = x$ for every $x \in \mathcal{P}$.

ElGamal cryptosystem from 1985, is a public key cryptosystem bases on the discrete logarithm problem in $\mathbb{F}_p^*$. Actually, it can be easily transformed in finite abelian group G. For being suitable for such applications, the group G should be present in such a way that multiplication and exponentiation are easy, while computing discrete logarithm is hard. It should also be possible to generate random elements from the group with an almost uniform distribution.

ElGamalov kriptosustav: Let p be a prime and $\alpha \in \mathbb{Z}_p^*$ a primitive root modulo p. Let $\mathcal{P} = \mathbb{Z}_p^*$, $\mathcal{C} = \mathbb{Z}_p^* \times \mathbb{Z}_p^*$ i

$$\mathcal{K} = \{(p, \alpha, a, \beta) \,:\, \beta \equiv \alpha^a \pmod{p}\}.$$

The values p, α, β are public, and the value a is secret.

For $K \in \mathcal{K}$ and secret random number $k \in \{0, 1, \ldots, p-1\}$ we define

$$e_K(x, k) = (\alpha^k \bmod p,\, x\beta^k \bmod p).$$

For $y_1, y_2 \in \mathbb{Z}_p^*$ we define

$$d_K(y_1, y_2) = y_2 (y_1^a)^{-1} \bmod p.$$

We can say that the plaintext x is "masked" by multiplying it by β^k. Those how knows the secret exponent a, using α^k, can compute β^k and "remove the mask".

ElGamal cryptosystem can be easily modified to work with the group $E(\mathbb{F}_p)$. But direct translation might have some disadvantages. The first problem is that it is not so straightforward to code elements of plaintext into points on an elliptic curve. There is no deterministic algorithm for that purpose, but only a probabilistic algorithm which uses that fact the one half of elements of a fine field are squares. This means that in k attempt with probability $1-\frac{1}{2^k}$ we may expect to find an x such that x^3+ax+b is a square $\mathbb{F}_p$. For practical purposes we may take $k = 30$.

The second problem is that the ciphertext in this variant of ElGamal cryptosytem consists of a pair of points on an elliptic curve. Thus it is four times longer than the plaintext (but only two times longer in the original ElGamal cryptosytem).

There is a modification of ElGamal cryptosytem due to Menezes and Vanstone, which solves both of these problems. It uses elliptic curves only for "masking", while plaintexts and ciphertexts are arbitrary pair of elements in the field (and not necessarily pairs which correspond to coordinates of points on the elliptic curve). Thus the ciphertext is only two times longer than the plaintext.

Menezes-Vanstone cryptosystem:
Let E be an elliptic curve over $\mathbb{F}_p$, and H cyclic subgroup of E generated by α. Let $\mathcal{P} = \mathbb{F}_p^* \times \mathbb{F}_p^*$, $\mathcal{C} = E \times \mathbb{F}_p^* \times \mathbb{F}_p^*$ and

$$\mathcal{K} = \{(E, \alpha, a, \beta) : \beta = [a]\alpha\},$$

where $[a]\alpha$ denotes $\alpha + \alpha + \cdots + \alpha$ (a times), and $+$ is addition on the elliptic curve E.

The values E, α, β are public, and the value a is secret.

For $K \in \mathcal{K}$ and secret random number $k \in \{0, 1, \ldots, |H| - 1\}$, and for $x = (x_1, x_2) \in \mathbb{Z}_p^* \times \mathbb{F}_p^*$ we define

$$e_K(x, k) = (y_0, y_1, y_2),$$

where $y_0 = [k]\alpha$, $(c_1, c_2) = [k]\beta$, $y_1 = c_1 x_1 \bmod p$, $y_2 = c_2 x_2 \bmod p$.

For a ciphertext $y = (y_0, y_1, y_2)$ we define

$$d_K(y) = (y_1 (c_1)^{-1} \bmod p,\ y_2 (c_2)^{-1} \bmod p),$$

where $[a]y_0 = (c_1, c_2)$.

7. Comparing elliptic curve with other types of cryptography

RSA Cryptosystem was invented in 1977 by Rivest, Shamir and Adleman. Its security is based on the difficulty of factoring large integers.

Description of RSA:
Each user chooses two primes p and q, and sets $n = p \cdot q$.
Knowing factorization of n, it is easy to compute

$$\varphi(n) = (p-1)(q-1) = n + 1 - p - q.$$

Next, the user chooses an integer e between 1 and $\varphi(n)$ such that $\gcd(e, \varphi(n)) = 1$.
He computes the multiplicative inverse of e modulo $\varphi(n)$ by Euclidean algorithm:

$$d \cdot e \equiv 1 \pmod{\varphi(n)}.$$

The values n and e are public, while the values p, q and d are secret.
Enciphering transformation is $x \mapsto x^e \bmod n$.
Deciphering transformation is $y \mapsto y^d \bmod n$.

If the RSA Cryptosystem is to be secure, it is necessary that $n = pq$ must be large enough that factoring it will be computationally infeasible. Hence, it is recommended that one should choose p and q to each be primes having at least 100 digits.

There are basically two types of factoring algorithms: special-purpose (use special features of the number n) and general-purpose (depend only on the size of n). The special-purpose algorithms suggest which kind of numbers n (i.e. p and q) should be avoided. E.g. if p and q are very close to each other, then they can be discovered by testing numbers near $\sqrt{n}$ (Fermat's factorization). Also, if $p-1$ or $q-1$ have only small prime factors (they are "smooth"), then Pollard's $p-1$ can be efficient.

However, in the case of RSA modulus n, such special-purpose algorithms are easy to avoid, so for the serious attacks on RSA, the general-purpose algorithms are more relevant. The best such algorithms today are quadratic sieve (QS) and number field sieve (NFS). They are based on idea of using a factor base of primes in order to find numbers s and t satisfying $t^2 \equiv s^2 \pmod{n}$, and then to find a nontrivial factor of n by $\gcd(t \pm s, n)$.

The running time for both algorithms is subexponential. More precisely, let

$$L_n[u, v] = e^{v(\log n)^u (\log\log n)^{1-u}}$$

(for $u = 0$ we have $L_n[0, v] = (\log n)^v$ - polynomial time; for $u = 1$ we have $L_n[1, v] = n^v$ - exponential time). Then running times are:
for QS: $L_n[\frac{1}{2}, 1 + \varepsilon]$,
for NFS: $L_n[\frac{1}{3}, (\frac{32}{9})^{1/3} + \varepsilon)]$.

It should be mentioned that the best know algorithms of DPL in $\mathbb{F}_q$ (Index Calculus Method) have very similar complexity.

There also other attack on RSA besides factorization. It is known that RSA is insecure if encryption exponent is very small. So $e = 3$ is not recommended, but $e = 2^{16} + 1$ can be safely used. There are attacks also on RSA with small decryption exponent d.

If $d < \sqrt[4]{n}$, the d can be recovered from continued fraction expansion of (publicly known) e/n (Wiener's attack). There are also extensions of Wiener's attack to slightly larger value of d which use tools from Diophantine approximations and LLL-algorithm (Verheul & van Tilborg, Dujella, Boneh & Durfee, Blömer & May).

In 2001, Lenstra and Verheul gave the recommendations for key sizes needed for reasonable security. They compared symmetric cryptosystems (DES, AES), public key cryptosystems based on factorization or DLP in $\mathbb{F}_q^*$ (RSA, ElGamal) and cryptosystems based on elliptic curves (ECC). Compared are key size needed for equivalent strength security (MIPS years needed to recover one key). The term MIPS year denotes the computational power of a MIPS (million-instructions-per-second) computer utilized for one year.

Year	DES key size	RSA key size	ECC key size
1990	63	622	117
2000	70	952	132
2010	78	1369	146
2020	86	1881	161
2030	93	2493	176
2040	101	3214	191

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 sub-exponential 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 $\alpha^a \equiv \beta \pmod{p}$
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 $P + \cdots + P = [m]P = Q$
$E(\mathbb{F}_p) \to E(\mathbb{Q})$;
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.

We may conclude that ECC offers the higher strength-per-key-bit of any known public key system (7 times smaller key compared with RSA and ElGamal; standard values are 1024 for RSA and 160 for ECC). The smaller key size results is smaller system parameters, smaller public-key certificates, faster implementation and smaller hardware processors. In particular, this is important in applications (like smart-cards) with limited space for storing keys.

8. Elliptic curve discrete logarithm problem

The basis for the security of elliptic curve cryptosystems is the apparent intractability of the *Elliptic Curve Discrete Logarithm Problem* (ECDLP):

Given an elliptic curve defined over $\mathbb{F}_q$, a point $P \in E(\mathbb{F}_q)$ of order n, and a point $Q \in E(\mathbb{F}_q)$, determine the integer m, $0 \leq m \leq n-1$, such that $Q = [m]P$, provided that such an integer exists.

Let us describe the *Pohlig-Hellman algorithm* which reduces the determination of m to the determination of m modulo each of the prime factors of n. An obvious consequence of this algorithm is that to maintain security of a system based on ECDLP, n should have a large prime divisor.

The algorithm works in any finite abelian group G. Let G has the order n divisible by a prime p and suppose that we wish to solve the following DLP: $Q = mP$. Then the problem can be reduced to a subgroup of order p by solving

$$Q' = n'Q = m_0(n'P) = m_0P',$$

where $n' = n/p$, $m \equiv m_0 \pmod{p}$. Thus P' is a point of order p. Solving this problem will determine the value m_0.

The values of m modulo $p^2, p^3, \ldots, p^c$ (where p^c is the largest power of p dividing n) can be computed in the following way. Suppose $m \equiv m' \pmod{p^i}$ is known and $m = m_i + \lambda p^i$ for some integer λ. Then

$$R = Q - m_i P = \lambda(p^i P) = \lambda S,$$

where R and S are known and S has order $s = n/p^i$. The value of $\lambda \bmod p$ can be determined just as $m \bmod p$ was found above.

Continuing in this manner, by solving DLPs in subgroups of order p, we eventually determine $m \bmod p^c$. After computing m modulo p^α for all prime divisor p of n, the true solution, number m, to the original DLP can be obtained using the Chinese Remainder Theorem (CRT).

Example: Given is the curve

$$E : \ y^2 = x^3 + 71x + 602$$

over $\mathbb{F}_{1009}$. The order of $E(\mathbb{F}_{1009})$ is $1060 = 2^2 \cdot 5 \cdot 53$. Given are points $P = (1, 237)$, $Q = (190, 271)$ on $E(\mathbb{F}_{1009})$. Solve ECDLP $Q = [m]P$.

The point P has the order $530 = 2 \cdot 5 \cdot 53$ in the group $E(\mathbb{F}_{1009})$. Thus, we have $n = 530$ and by the Pohlig-Hellman algorithm we have to compute m modulo 2, 5 and 53.

Modulo 2: Multiplying the points P and Q by $530/2 = 265$, we obtain the points $P_2 = [265]P = (50, 0)$ and $Q_2 = [265]Q = (50, 0)$. We get ECDLP

$$Q_2 = (m \bmod 2)P_2,$$

which clearly gives $m \equiv 1 \pmod 2$.

Modulo 5: Multiplying the points P and Q by $530/5 = 106$, we obtain the points
$P_5 = [106]P = (639, 160)$ and
$Q_5 = [106]Q = (639, 849)$. Clearly, $Q_5 = -P_5$, which implies $m \equiv -1 \equiv 4 \pmod 5$.

Modulo 53: Now we multiply the points by $530/53 = 10$. We obtain the points $P_{53} = [10]P = (32, 737)$ and $Q_{53} = [10]Q = (592, 97)$. Thus, we get EDLP in a group of order 53. We will solve it later as an illustration of BSGS method. The result is $m \equiv 48 \pmod{53}$.

The solution of the original problem $Q = [m]P$, za $P = (1, 237)$, $Q = (190, 271)$, is obtained by solving the system of congruences

$$m \equiv 1 \pmod 2,\ m \equiv 4 \pmod 5,\ m \equiv 48 \pmod{53}.$$

By the Chinese Remainder Theorem, we get $m = 419$.

There are several known methods for solving ECDLP which have complexity $O(\sqrt{n})$. Such methods are the *Pollard ρ-method* and the *baby step - giant step* (BSGS) method due to Shanks. We will explain the BSGS method. This is a method for a general finite abelian group G. It has complexity $O(\sqrt{n})$, where $\#G = n$. But it requires also the storage of $O(\sqrt{n})$ group elements.

Let $P, Q \in G$ with $Q = mP$. By simple Euclidean division we know m can be written as

$$m = \lceil\sqrt{n}\rceil a + b, \quad \text{where } 0 \leq a, b < \sqrt{n}.$$

The only problem is that the values of a and b are not known. The equation $Q = mP$ is rewritten in the form

$$(Q - bP) = a(\lceil\sqrt{n}\rceil P).$$

It may seem like just an added complication, but it allows us to perform space/time trade off.

A table of "baby steps" is first computed. This is a table of all values of

$$R_b = Q - bP, \quad \text{for } b = 0, 1, \ldots, \lceil\sqrt{n}\rceil - 1.$$

This table shoud be sorted and stored in memory so that it can be efficiently searched.

After having computed "baby steps", the "giant steps" are computed:

$$S_a = a(\lceil\sqrt{n}\rceil P), \quad \text{za } a = 0, 1, \ldots, \lceil\sqrt{n}\rceil - 1.$$

On each computation of a giant step it is checked whether S_a occurs in the table. If it does, the values of a and b are recovered. This procedure must terminate before a reaches the value $\lceil\sqrt{n}\rceil$

Example: Let us consider again the curve

$$E : \ y^2 = x^3 + 71x + 602$$

over $\mathbb{F}_{1009}$. After the application of the Pohlig-Hellman algorithm, we arrived to ECDLP $Q' = [m_0]P'$, where $Q' = (592, 97), P' = (32, 737)$.

We know that the order of P' is 53. Since $\lceil\sqrt{53}\rceil = 8$, eight baby steps are required. So we compute:

b	$R_b = Q' - [b]P'$
0	$(592, 97)$
1	$(728, 450)$
2	$(537, 344)$
3	$(996, 154)$
4	$(817, 136)$
5	$(365, 715)$
6	$(627, 606)$
7	$(150, 413)$

The giant steps $a([8]P')$ are computed:

a	$S_a = [a]([8]P')$
1	$(996, 855)$
2	$(200, 652)$
3	$(378, 304)$
4	$(609, 357)$
5	$(304, 583)$
6	$(592, 97)$

We see that a match is obtained with $a = 6$ and $b = 0$, which implies that $m_0 = 8a + b = 48$. (Note that already from $a = 1$ we might conclude that $S_1 = -R_3$ and $[8]P' = -Q + [3]P'$, which again gives $m \equiv -5 \equiv 48 \pmod{53}$.)

9. Lenstra's elliptic curve factoring method

Pollard's $p-1$ factorization method, proposed in 1974, is a special-purpose factorization algorithm. Its starting point is Fermat's little theorem. Let n be a composite number and p its unknown prime factor. Then $a^{p-1} \equiv 1 \pmod{p}$ for $\gcd(a,p) = 1$.

Moreover, $a^m \equiv 1 \pmod{p}$ for any multiple of $p-1$. If we can find such multiple m, then $\gcd(a^m - 1, n)$ will give us a factor (hopefully nontrivial) of n. But, how we can find a multiple of $p-1$ if we don't know p? This can be done if we somehow know that $p-1$ has only small prime factors (this is why the method is "special-purpose"). We say that $p-1$ is *smooth*. Assume that all prime powers dividing $p-1$ are $\leq B$. Then we may take $m = \mathrm{lcm}(1, 2, \ldots, B)$. In the worst case, when $\frac{p-1}{2}$ is a prime, this method is not better than simple trial division.

The success of $p-1$ method depends on smoothness of the number $p-1$. There are variants of this method which use smoothness of numbers $p+1$, p^2+p+1, p^2+1 or p^2-p+1. But the most important modification of $p-1$ method is Lenstra's elliptic curve factorization method (ECM), proposed in 1987. It replaces the group $\mathbb{F}_p^*$ of order $p-1$ with the group $E(\mathbb{F}_p)$, which order varies inside Hasse's interval $[p+1-2\sqrt{p}, p+1+2\sqrt{p}]$, and thus we may expect to find an elliptic curve over $\mathbb{F}_p$ with sufficiently smooth order.

We will work with elliptic curves over the ring $\mathbb{Z}/n\mathbb{Z}$. We may assume that $\gcd(n,6)=1$, so we consider elliptic curves of the form

$$E_{a,b}: \quad y^2 = x^3 + ax + b,$$

where $\gcd(4a^3+27b^2, n) = 1$. When n is a prime, then there is exactly one point at infinity on the curve. For composite n, we may have more such points.

Let us describe the basic steps in ECM.

- The choice of the elliptic curve:

We can randomly choose elements $a, x, y \in \mathbb{Z}/n\mathbb{Z}$ and then compute $b = (y^2 - x^3 - ax) \bmod n$. Let $g = \gcd(4a^3 + 27b^2, n)$. If $1 < g < n$, then we are done, since we have found a nontrivial factor of n. If $g = n$, then we have to choose new a, x, y. If $g = 1$, then we have found an elliptic curve over $E_{a,b}$ over $\mathbb{Z}/n\mathbb{Z}$ and a point $P = (x, y)$ on it.

- Let $k = \mathrm{lcm}(1, 2, \ldots, B)$, for suitably chosen bound B. We may start with $B = 10000$, and increase it latter if necessary.

- We compute $[k]P \in E_{a,b}(\mathbb{Z}_n)$ according to formula for the addition:

$$(x_3, y_3) = (\lambda^2 - x_1 - x_2 \bmod n,\ \lambda(x_1 - x_3) - y_1 \bmod n),$$

where $\lambda = (3x_1^2 + a) \cdot (2y_1)^{-1} \bmod n$ if the points are equal, and
$\lambda = (y_1 - y_2)(x_1 - x_2)^{-1} \bmod n$, otherwise.

- If in the computation of $[k]P$ we cannot compute the sum of certain points because we cannot compute d^{-1} since d has no inverse modulo n, then we compute $g = \gcd(d, n)$. If $g \neq n$, then we have found a nontrivial factor of n.

- If the algorithm fails (i.e. we are able to compute $[k]P$), then we can increase the bound B or choose new elliptic curve.

Example: Factorize $n = 209$.

Let $B = 3$, so that $k = 6$. Let us choose the elliptic curve

$$y^2 = x^3 + 4x + 9$$

and an obvious point on it $P = (0, 3)$. We compute $[6]P = [2](P + [2]P)$. First we compute $[2]P$. Corresponding λ is $4 \cdot 6^{-1} = 140 \bmod 209$, and we get $[2]P = (163, 169)$. Then we compute $[3]P = P + [2]P$. Corresponding λ is $166 \cdot 163^{-1} = 60 \bmod 209$, and we have $[3]P = (148, 143)$. Finally, we compute $[6]P = [2]([3]P)$. Corresponding λ is $90 \cdot 77^{-1}$. In an attempt to compute the inverse of 77 modulo 209, we get that the inverse does not exist because $\gcd(77, 209) = 11$. Thus, we conclude that the number 11 is a factor of 209. Indeed, $209 = 11 \cdot 19$.

This algorithm we be successful if k is a multiple of $\#E(\mathbb{Z}_p)$, where p is a prime factor of n. Indeed, in that case while computing the point $[k]P$, the corresponding denominator will be divisible by p, so it will not have an inverse modulo n. Namely, in $E(\mathbb{Z}_p)$ it will hold that $[k]P = \mathcal{O}$.

We can use elliptic curves E with large torsion group over $\mathbb{Q}$ (and known point of infinite order), as the torsion group will inject into $E(\mathbb{F}_p)$ for all primes p of good reduction, and thus we will have that $\#E(\mathbb{Q})_{\text{tors}} \mid \#E(\mathbb{F}_p)$. This in turn makes the order of $E(\mathbb{F}_p)$ more likely to be smooth (Montgomery, Atkin & Morain). Recently, the analogous applications of elliptic curves with large torsion and positive rank over number fields of small degree are studied (Brier & Clavier, Dujella & Najman).

In estimating the complexity of ECM algorithm, the crucial question is how to choose optimally the bound B. Using the fact that the orders $\#E(\mathbb{Z}_p)$ are almost uniformly distributed in Hasse's interval, it can be proved that the optimal value is approximately

$$B = e^{(\sqrt{2}/2+\varepsilon)\sqrt{\ln p \ln\ln p}},$$

which lead to complexity

$$e^{(\sqrt{2}+\varepsilon)\sqrt{\ln p \ln\ln p}}.$$

In the worst case (when $p = O(\sqrt{n})$), the complexity is $e^{O(\sqrt{\ln n \ln\ln n})}$. Hence, this is a subexponential algorithm. Complexity is of the same order as in QS, and it is worse then in NFS. However, an important property of ECM is that its complexity depends on the smallest prime factor of n. This is not an advantage in factorizing RSA modulus, i.e. number of the form $n = pq$, where p and q are primes of the same size.

But in factorization of "random numbers" , ECM often has the best performances, since such numbers usually have some prime factor which is significantly smaller than $\sqrt{n}$.

There are some famous factorizations obtained by ECM, like finding 33-digits factor of Fermat number $2^{2^{15}} + 1$ (Crandall, van Halewyn, 1997), and 49-digit factor of Mersenne number $2^{2071} - 1$ (Zimmermann, 1998).

10. Elliptic curve primality proving algorithm

In the construction of almost all public key cryptosystems one of the starting points is choosing one or more large prime numbers. Thus it is very important fact that there exist very efficient primality tests which can be used for that purpose. In particular, these test are much more efficient than best known factorization methods. All these tests start with Fermat's little theorem, which gives important property of primes, but do not characterize them. Thus some modifications are needed in order to conclude (with reasonable probability) that the number which passes the test is indeed a prime.

Very efficient primality test is the *Miller-Rabin* test. It combines two simple properties of primes:

$a^{p-1} \equiv 1 \pmod{p}$ if $\gcd(a, p) = 1$;

$x^2 \equiv 1 \pmod{p}$ implies $x \equiv \pm 1 \pmod{p}$.

Definition: Let n be an odd composite positive integer and $n - 1 = 2^s \cdot t$, with t odd. If for an integer b it holds

$$b^t \equiv 1 \pmod{n}$$

or there exists r, $0 \leq r < s$ such that

$$b^{2^r t} \equiv -1 \pmod{n},$$

then we say that n is a *stong pseudoprime in base* b (n is spsp(b)).

Fact: An odd composite positive integer n is spsp(b) for at most $(n-1)/4$ basis b, $0 < b < n$.

Thus, if n passes Miller-Rabin primality tests in k different basis, the probability that n is composite is less than $1/4^k$.

If an integer n passes several good primality tests (like Miller-Rabin test for several different bases), then we can be reasonable sure that n is prime. For the most of applications in cryptography (e.g. for choosing primes p and q in RSA) this is fine. However, these tests do not proved a *proof* that n is prime. We will now discuss some methods for primality proving.

Theorem (Pocklington): Let s be a divisor of $n-1$ which is greater than $\sqrt{n}$. Assume that there exists a positive integer a with the following property

$$a^{n-1} \equiv 1 \pmod{n},$$

$$\gcd(a^{(n-1)/q} - 1, n) = 1$$

for all prime divisors q of s. Then n is a prime.

Proof: If n is composite, then it has a prime factor $p \leq \sqrt{n}$. Let $b = a^{(n-1)/s}$. Then

$$b^s \equiv a^{n-1} \equiv 1 \pmod{n},$$

and so $b^s \equiv 1 \pmod{p}$. We claim that s is the order of b modulo p. Indeed, if a divisor q of s satisfies $b^{s/q} \equiv 1 \pmod{p}$, then p divides n and $b^{s/q} - 1$, i.e. $a^{(n-1)/q} - 1$, contrary to our assumption that n and $a^{(n-1)/q} - 1$ are coprime. From Fermat's little theorem we have $b^{p-1} \equiv 1 \pmod{p}$, and thus we conclude that s divided $p - 1$. But this is impossible since $s > \sqrt{n}$, and $p \leq \sqrt{n}$.

A problem with the application of Pocklington's theorem is that it requires partial factorization of the number $n-1$. This number $n-1$ can be viewed as the order of the group $(\mathbb{Z}/n\mathbb{Z})^*$ (if n is prime). One idea (introduced by Goldwasser and Killian in 1986) how to overcome this problem is to replace (again) the group $(\mathbb{Z}/n\mathbb{Z})^*$ by the group $E(\mathbb{Z}/n\mathbb{Z})$, where E is certain elliptic curve. Namely, with orders of $E(\mathbb{Z}/n\mathbb{Z})$ we have much larger flexibility, so we may expect to find some curve with order which will be easy to factorize.

Theorem: Let E be an elliptic curve over $\mathbb{Z}/n\mathbb{Z}$, where $\gcd(6,n)=1$ and $n>1$, given by the equation $y^2=x^3+ax+b$. Let m be a positive integer with a prime factor $q>(n^{1/4}+1)^2$. If there exists a point $P\in E(\mathbb{Z}/n\mathbb{Z})$ such that

$$[m]P=\mathcal{O} \quad \text{and} \quad [m/q]P\neq\mathcal{O},$$

then n is a prime.

Proof: If n is composite, then it has a prime factor $p \leq \sqrt{n}$. Consider the elliptic curve E' over $\mathbb{F}_p$ given by the same equation as E. Let m' be the order of the group $E'(\mathbb{F}_p)$. By Hasse's theorem

$$m' \leq p + 1 + \sqrt{p} = (\sqrt{p} + 1)^2 \leq (n^{1/4} + 1)^2 < q.$$

Hence, $\gcd(m', q) = 1$, and there exists $u \in \mathbb{Z}$ such that $uq \equiv 1 \pmod{m'}$. Let $P' \in E'(\mathbb{F}_p)$ be the point obtained from P by reducing the coordinates modulo p. By the assumption of the theorem, $[m/q]P$ is well defined and $\neq \mathcal{O}$, so we conclude that $[m/q]P' \neq \mathcal{O}$. But, on the other hand we have

$$[m/q]P' = [uq \cdot \frac{m}{q}]P' = [um]P' = [u]([m]P') = \mathcal{O}.$$

Example: Let us prove that $n = 907$ is prime.

Let E be the elliptic curve given by the equation $y^2 = x^3 + 10x - 2$ over $\mathbb{Z}/n\mathbb{Z}$. The order of $E(\mathbb{Z}/n\mathbb{Z})$ is $m = 923 = 71 \cdot 13$. Let us take $P = (56, 62)$ and $q = 71$. Then $[13]P = (338, 305) \neq \mathcal{O}$ and $[923]P = [71]([13]P) = \mathcal{O}$ (using algorithms for point multiplications explained before; note that NAF representation are $13 = (1, 0, 1, 0, -1)$ and $71 = (1, 0, 0, 1, 0, 0, -1)$). Since $71 > (907^{1/4} + 1)^2$, we conclude that 907 is prime (assuming that we already know that 71 is prime; otherwise we apply the same method for $n = 71$).

In 1993, Atkin and Morain proposed a variant of this method which uses elliptic curves with complex multiplication with corresponding imaginary quadratic field $\mathbb{Q}(\sqrt{-d})$. For such curves E it is known that if $4p = x^2 + dy^2$, then the order of $E(\mathbb{F}_p)$ is $p + 1 \pm x$. This method is efficient for numbers with up to 1000-digits.