Elliptic curves

Mathematical Cryptography, Lectures 15 - 16

Contents

Elliptic curves over $\mathbb{R}$

Groups of points on elliptic curves play an important role in modern cryptography. Let us first show elliptic curves over reals and only in a simplified form as follows:

Definition

An elliptic curve over $\mathbb{R}$ is the set of all points $(x, y) \in \mathbb{R}^2$ satisfying

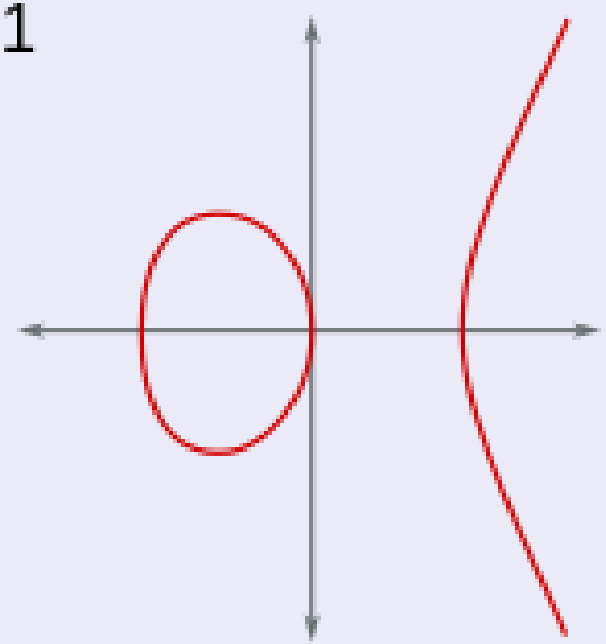
$$y^2 = x^3 + ax + b$$

where the cubic polynomial $x^3 + ax + b$ has only simple roots in $\mathbb{C}$, which happens just if the discriminant $D = 4a^3 + 27b^2 \neq 0$.

Elliptic curves over $\mathbb{R}$

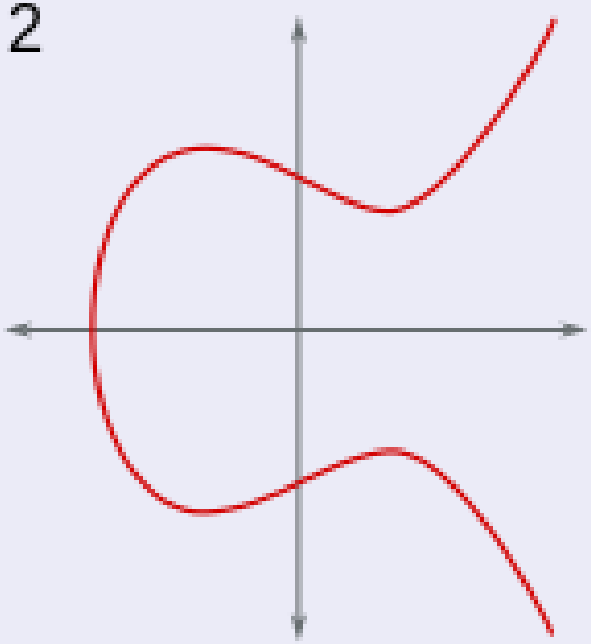
Example

1



$y^2 = x^3 - x$

2



$y^2 = x^3 - x + 1$

Elliptic curves over $\mathbb{R}$

Addition of points - geometrically

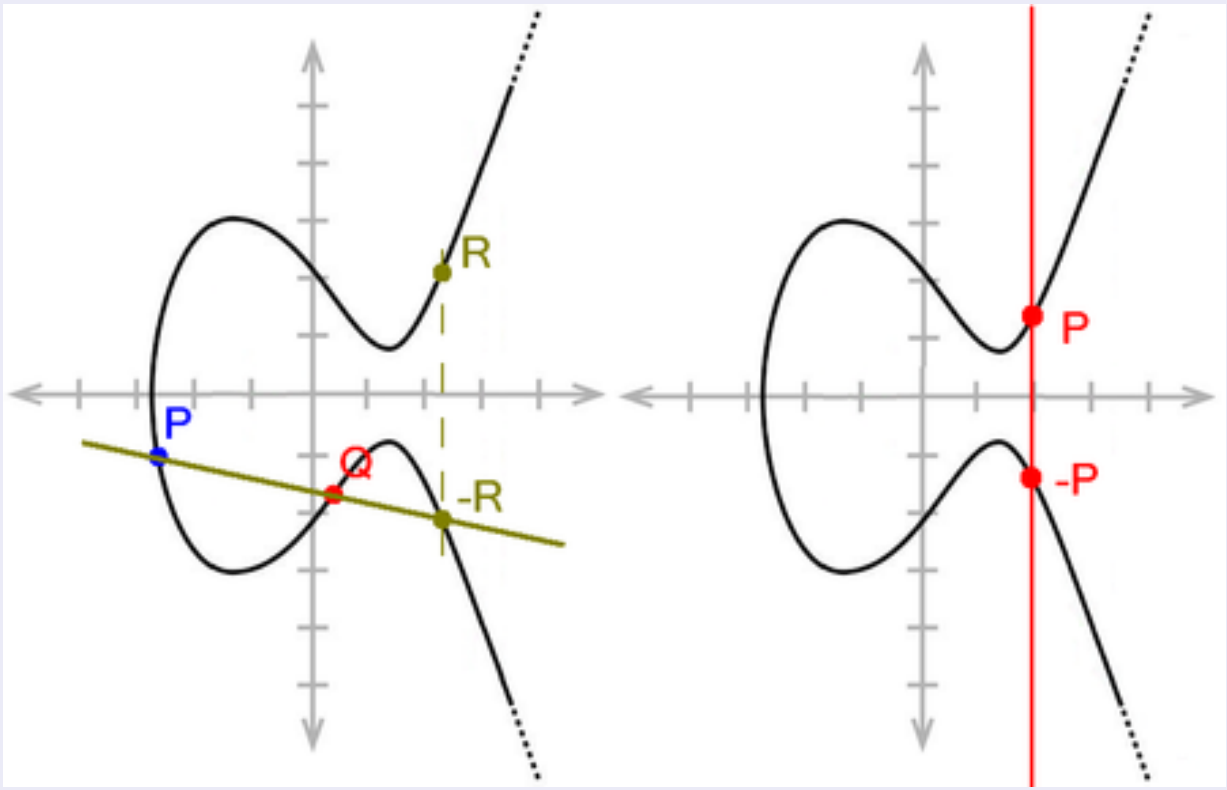
We can define addition of points on an elliptic curve.
The definition uses symmetry of the curve along the x-axis.

- If $P \neq Q$, then points P and Q determine one line. In most cases, this line intersects the curve at just one more point. The sum $P + Q$ is defined to be the point R, which is the mirror image of this intersection (with respect to the x-axis).
- If the line PQ is a tangent to the elliptic curve at a point P (or Q), then the sum $P + Q$ is defined as the point R which is the mirror image of the point P (or Q).
- If the line PQ is parallel to the y-axis, the sum $P + Q$ is defined as a point at infinity (denoted O).

Elliptic curves over R

Addition of points - geometrically

For $P = (p_1, p_2)$ we denote by $-P = (p_1, -p_2)$ the point symmetrical with P with respect to the x-axis.



$P + Q = R$ $\qquad$ $P + (-P) = O$

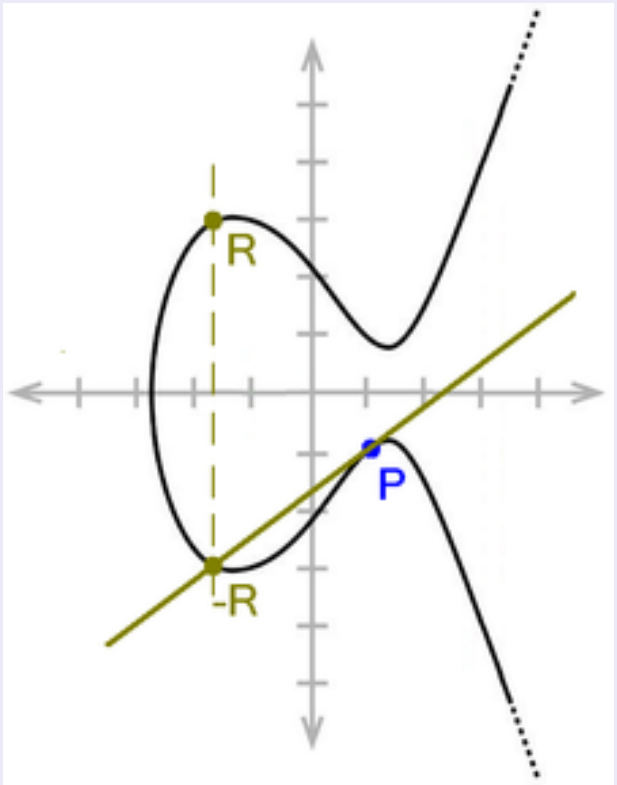
Elliptic curves over $\mathbb{R}$

Addition of points - geometrically

- If $P = Q$, then we make a tangent to the elliptic curve at the point P. This tangent usually intersects the curve at just one more point. The sum $P + P$ is defined to be the point R, which is the mirror image of this intersection (with respect to the x-axis).
- If the tangent at P is parallel to the y-axis, the sum $P + P$ is defined as a point at infinity (denoted by O).
- Finally, let's define $O + P = P$, $P + O = P$, $O + O = O$.

Elliptic curves over $\mathbb{R}$

Addition of points - geometrically

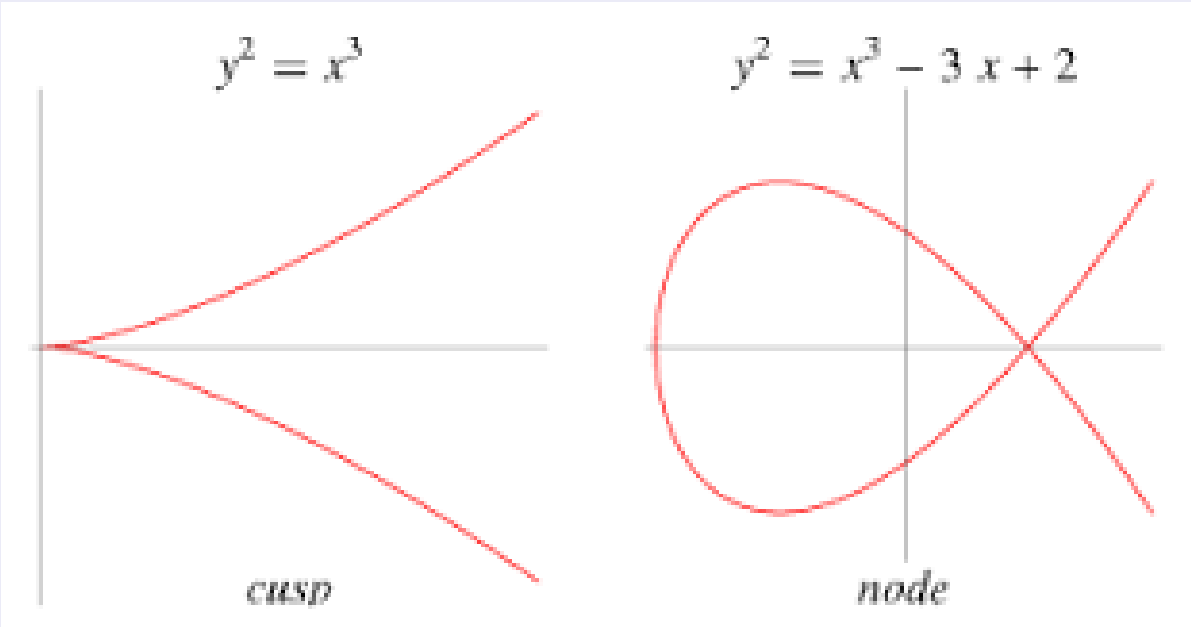


$$2P = P + P = R$$

Elliptic curves over $\mathbb{R}$

Note

The non-zero discriminant guarantees that the elliptic curve does not intersect itself and that it does not have a sharp break. In this case, the sum of two points is uniquely defined for all pairs on the curve by geometrical constructions.



Elliptic curves over $\mathbb{R}$

Proposition

Let $E(\mathbb{R})$ be a set of all points at the elliptic curve $y^2 = x^3 + ax + b$, where $D = 4a^3 + 27b^2 \neq 0$, along with the point at infinity O. The set $E(\mathbb{R})$ together with the addition defined geometrically forms an abelian group. $(E(\mathbb{R}), +)$ is called the *group of points on an elliptic curve*.

Proof: Commutativity is obvious, associativity is more difficult to verify. The identity element is the point at infinity O, the opposite element to a point P is the point $-P$ symmetrical with respect to the x-axis.

Elliptic curves over $\mathbb{R}$

Addition of points - arithmetically

Let $P = (p_1, p_2)$, $Q = (q_1, q_2)$ be points on the elliptic curve

$$y^2 = x^3 + ax + b, \text{ where } D = 4a^3 + 27b^2 \neq 0.$$

We want to derive the coordinates of the point $R = P + Q$ from the coordinates of the points P and Q. Let us denote the coordinations of the point $R = (r_1, r_2)$.

Elliptic curves over $\mathbb{R}$

Addition of points - arithmetically

1) Let first $P \neq Q$ (nor $-P \neq Q$).
The line determined by points P, Q has the equation $y = \lambda x + \kappa$, where $\lambda = \frac{q_2 - p_2}{q_1 - p_1}$ (for $p_1 \neq q_1$), $\kappa = p_2 - \lambda p_1$.

We find the $x-$coordinate of the intersection of the line and the given curve (which is r_1): $(\lambda x + \kappa)^2 = y = x^3 + ax + b$,
$0 = x^3 - (\lambda x + \kappa)^2 + ax + b$,
where the coefficient by x^2 equals to $-\lambda^2 = -(p_1 + q_1 + r_1)$ (Viet's formulas for roots). Hence $r_1 = \lambda^2 - p_1 - q_1$.

The $y-$coordinate of the intersection of the line and the curve (which is $-r_2$) is $-r_2 = \lambda r_1 + \kappa$. Hence $r_2 = \lambda(p_1 - r_1) - p_2$.

If the line PQ was a tangent to the curve at the point P, then we get $R = -P$.

Elliptic curves over $\mathbb{R}$

Addition of points - arithmetically

2) Let $P = Q$ (but $p_2 \neq 0$).
By the equation $F(x, y) = y^2 - x^3 - ax - b = 0$, a function $y(x)$ is implicitly defined around the point P (assuming the partial derivation of F by y is nonzero at the point P). This allows us to compute the tangent directive to the elliptic curve at the point P as $y'(x) = \frac{3x^2+a}{2y}$ (the derivation calculated in the point P).

The tangent to the elliptic curve at point P has the equation $y = \lambda x + \kappa$, where $\lambda = \frac{3p_1^2+a}{2p_2}$ (for $p_2 \neq 0$), $\kappa = p_2 - \lambda p_1$.

By substituting into the equation of the elliptic curve, we find the $x-$coordinate of the intersection of the tangent and the given curve, $r_1 = \lambda^2 - 2p_1$. Then the $y-$coordinate of the mirror image of the intersection is $r_2 = \lambda(p_1 - r_1) - p_2$.

Elliptic curves over $\mathbb{R}$

Addition of points - arithmetically

Let $P = (p_1, p_2)$, $Q = (q_1, q_2)$ be points on the elliptic curve $E: y^2 = x^3 + ax + b$, where $D = 4a^3 + 27b^2 \neq 0$.
The sum $R = P + Q$ is defined as follows:

- If $p_1 = q_1$, $p_2 = -q_2$, then $P + Q = O$, where O is a point at infinity.
- $P + O = P$, $O + P = P$, $O + O = O$.
- In other cases, $P + Q = R = (r_1, r_2)$,
  where $r_1 = \lambda^2 - p_1 - q_1$, $r_2 = \lambda(p_1 - r_1) - p_2$,
  $$\lambda = \frac{q_2 - p_2}{q_1 - p_1} \text{ if } P \neq Q,$$
  $$\lambda = \frac{3p_1^2 + a}{2p_2} \text{ if } P = Q.$$

Elliptic curves over $\mathbb{Z}_p$

Arithmetically, to add points on an elliptic curve, we need addition and subtraction, multiplication and division by non-zero numbers in $\mathbb{R}$. But we can do all this in any field!

Deriving the coordinates of the intersection of the line $y = \lambda x + \kappa$ and the curve $y^2 = x^3 + ax + b$ can be done over any field (including the formal derivation of polynomials). In doing so, the $x-$coordinate of the intersection r_1 was the third root of a certain cubic polynomial, but a cubic polynomial has at most three roots in any field and Viet's formulas are valid there.

Finally, we can analogously introduce a group of points on an elliptic curve over a finite field, where addition will be defined by the same relations as over $\mathbb{R}$ (we will multiply by inverse elements instead of division).

Elliptic curves over $\mathbb{Z}_p$

Every finite field is isomorphic to a Galois field and has p^k elements, where p is a prime. We will denote it by $GF(p^k)$. The number p is called the characteristic of such a field.

In practice, there are mostly used $\mathbb{Z}_p$ or $GF(2^k)$.

We will be concerned with groups of points on an elliptic curve over $\mathbb{Z}_p$, but everything can be defined analogously for any field $GF(p^k)$.

Elliptic curves over $\mathbb{Z}_p$

Definition

An elliptic curve over a field $\mathbb{Z}_p$, where $p > 3$ is prime, is the set of all points $(x, y) \in \mathbb{Z}_p^2$ satisfying the equation:

$$y^2 = x^3 + ax + b,$$

where $a, b \in \mathbb{Z}_p$ and $D = 4a^3 + 27b^2 \neq 0$ in $\mathbb{Z}_p$.

Let $E(\mathbb{Z}_p)$ denote the set of all these points together with the added point O.

Proposition

The set $E(\mathbb{Z}_p)$ together with the addition introduced arithmetically by the same way as in $E(\mathbb{R})$ forms an abelian group.

Elliptic curves over $\mathbb{Z}_p$

Example

The elliptic curve over $\mathbb{Z}_{17}$ is given by $y^2 = x^3 + 7x + 13$.
Determine the points on this curve.

For $x = 0$ we get $y^2 = 13$, where $13^{\frac{p-1}{2}} = 13^8 = 1$ in $\mathbb{Z}_{17}$,
so 13 is a square and we count $y = \pm 8$ by brute force.
The points $(0, 8)$, $(0, 9)$ are on the curve.

For $x = 3$ we get $y^2 = 10$, and $10^{\frac{p-1}{2}} = 10^8 = -1$ in Z_{17},
so 10 is not a square. There is no point $(3, y)$ on the curve.

The group $E(\mathbb{Z}_{17}) = \{(0, 8), (0, 9), (1, 2), (1, 15), (2, 1), (2, 16),$
$(6, 4), (6, 13), (14, 4), (14, 13), (15, 5), (15, 12), O\}$ has 13 elements.

$P + Q = (1, 2) + (6, 4) = ((-3)^2 - 1 - 6, -3(1 - r_1) - 2) = (2, 1)$,
since $\lambda = 2 \cdot 5^{-1} = -3$ in $\mathbb{Z}_{17}$.

Elliptic curves over $\mathbb{Z}_p$

An estimate of the order of the group $E(\mathbb{Z}_p)$

- $|E(\mathbb{Z}_p)| \leq 2p + 1$, since for every $x \in \mathbb{Z}_p$, $x^3 + ax + b$ has at most two square roots.
- $|E(\mathbb{Z}_p)| \doteq p$, since only half of the elements in $\mathbb{Z}_p$ are squares and the results of $x^3 + ax + b$ are roughly uniformly distributed in $\mathbb{Z}_p$.
- Hasse's theorem: For every elliptic curve over $\mathbb{Z}_p$, the following holds:
  $p + 1 - 2\sqrt{p} \leq |E(\mathbb{Z}_p)| \leq p + 1 + 2\sqrt{p}$
- Hasse's theorem also holds for elliptic curves over $GF(p^k)$ when p is replaced by p^k in the estimate.

Elliptic curves over $\mathbb{Z}_p$

Structure of the group $E(\mathbb{Z}_p)$

- $E(\mathbb{Z}_p) \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$, where $n_2 \mid \gcd(n_1, p-1)$.
  Or, the group is the internal direct sum of two cyclic subgroups of orders n_1 and n_2, so $|E(\mathbb{Z}_p)| = n_1 \cdot n_2$.
- If $n_2 = 1$, then $E(\mathbb{Z}_p)$ is cyclic.
- If n_2 is small (like $2, 3, 4$), then we say $E(\mathbb{Z}_p)$ is almost cyclic.
- The groups of points of elliptic curves over $GF(p^k)$ have the same structure, except that here $n_2 \mid \gcd(n_1, p^k - 1)$.

Elliptic curves over $\mathbb{Z}_p$

General definition

The general form of the equation for an elliptic curve over a field :

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

If the characteristic of the field $\neq 2$, the equation can be transformed to the form $y^2 = x^3 + ax^2 + bx + c$.
If the characteristic of $\neq 2, 3$ can be obtained as $y^2 = x^3 + ax + b$.

For the field $GF(2^k)$, the equation can be modified to $y^2 + xy = x^3 + ax^2 + b$, or to $y^2 + cy = x^3 + ax + b$.

Each equation has a different discriminant and different formulas for adding the points of the elliptic curve.

Elliptic curves in cryptography

Diffie-Hellman key establishment

Alice chooses a group of points on an elliptic curve $E(\mathbb{Z}_p)$ and a point A of order n. So, $G = \langle A \rangle$ is a cyclic subgroup of order n.

Then she chooses $x \in \mathbb{Z}_n$ and computes $B = xA$ in $E(\mathbb{Z}_p)$.
Alice sends to Bob the element B and informations about the group $(E(\mathbb{Z}_p), n, A)$.

Bob chooses $y \in \mathbb{Z}_n$ and computes $C = yA$ in $E(\mathbb{Z}_p)$.
Bob sends to Alice the element C.

Alice computes $S_A = xC$ and Bob computes $S_B = yB$ in $E(\mathbb{Z}_p)$.
Both of them have the same secret key $S = S_A = S_B = xyA$.

Analogously, we can use the subgroup $G = \langle A \rangle$ of $E(\mathbb{Z}_p)$ for ElGamal encryption.

Elliptic curves in cryptography

Diffie-Hellman key establishment

Computation time:

- We compute the integer multiple xP of a point P on the elliptic curve $E(\mathbb{Z}_p)$ by the repeated doubling algorithm. This requires $O(len(n))$ additions for $x \in \mathbb{Z}_n$.
  The repeat doubling algorithm is an additive analogue to the repeat squaring algorithm.
- The sum of two points $P + Q$ requires 6 additions, 3 multiplications, and 1 computing inverse in $\mathbb{Z}_p$. Doubling a point $2P = P + P$ requires one more multiplication. This means that one addition in $E(\mathbb{Z}_p)$ is about five times slower than one multiplication in $\mathbb{Z}_p$.

Elliptic curves over $\mathbb{Z}_p$

Example

The elliptic curve over $\mathbb{Z}_{17}$ is given by $y^2 = x^3 + 7x + 13$.

The group $E(\mathbb{Z}_{17}) = \{(0,8),(0,9),(1,2),(1,15),(2,1),(2,16),(6,4),(6,13),(14,4),(14,13),(15,5),(15,12),O\}$ has 13 elements, therefore it is cyclic and any element except O is a generator.

Alice and Bob use $E(\mathbb{Z}_{17}) = \langle A = (1,2) \rangle$ of order $n = 13$.

Alice chooses $x = 5$ and computes $B = 5 \cdot (1,2) = (2,16)$.
Bob chooses $y = 2$ and calculates $C = 2 \cdot (1,2) = (0,9)$.
The exchanged secret key is $S = 2 \cdot B = (14,13)$.

Elliptic curves in cryptography

Discrete logarithm problem

Let $G = \langle A \rangle$ of order n be a subgroup of the group $E(\mathbb{Z}_p)$.
For $B \in G$ we search for $x \in \mathbb{Z}_n$ such that $B = xA$ in $E(\mathbb{Z}_p)$.

- In most groups $E(\mathbb{Z}_p)$, the discrete logarithm problem is an exponential problem with complexity $O(\sqrt{n})$ or $O(\sqrt{q})$, where q is the largest prime in the factorization of n.
- The baby step/giant step algorithm and the Pohling-Hellman algorithm work in groups $E(\mathbb{Z}_p)$, for computing the discrete logarithm (so does Pollard's $\rho-$ method).
  The subexponential index calculus algorithm (SEDL) does not work here.

Elliptic curves in cryptography

Discrete logarithm problem

- A different subexponential algorithm is known for groups of so-called supersingular curves, which are curves:
  $y^2 = x^3 + ax$ over a field $GF(p^k)$, where $p \equiv -1 \,(mod\, 4)$,
  $y^2 = x^3 + b$ over a field $GF(p^k)$, where $p \equiv -1 \,(mod\, 3)$.

Note

We also need to solve the problem of how to convert messages to points on an elliptic curve (message encoding).

Elliptic curves

Literature

- Hankerson, Menezes, Vanstone: Guide to Elliptic Curve Cryptography. Chapters 1. and 3.1 and 4.1.
- Koblitz: A Course in Number Theory and Cryptography. Chapter 6.1-2.