Elliptic Curve Criptography

Paolo Bettelini

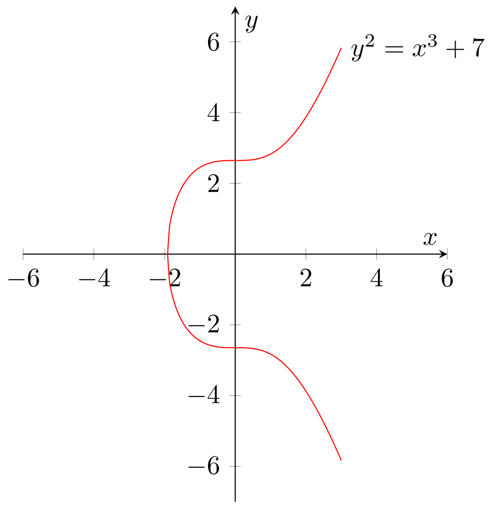
Contents

1 Elliptic Curves

1.1 Definition

An elliptic curve E is a set of points such that

$$E = \{(x, y) \,|\, y^2 = x^3 + ax + b\} \cup \{O\}, \quad 4a^3 + 27b^2 \neq 0$$



Where O is a point at infinity.

The elliptic curve is symmetrical about the x-axis.
The opposite of a point P is its reflection $-P$.

The coefficients a, b be part of

- $\mathbb{R}$ Real numbers
- $\mathbb{Q}$ Rational numbers
- $\mathbb{C}$ Complex numbers
- $\mathbb{Z}/p\mathbb{Z}$ Finite field

1.2 Addition

Given two points $P, Q \in E$ we can describe a unique third point.
We take the line that intersects P and Q, the opposite of the third intersection with the curve is out point.

$$P + Q = -R$$

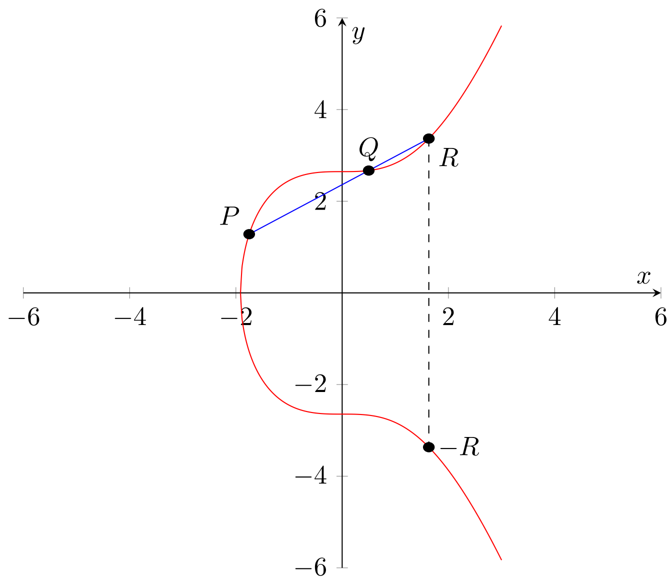
If $P = Q$, the intersection line will be given by the tangent at that point.
If $P = -Q$, $P + Q = O$.
If $P = -P$ (inflection point, the concavity of the curve changes) $R = P$, $P + P = -P = P$.
We consider $-O$ to be O.

The intersection line $mx + q$ is given by

$$m = \frac{P_y - Q_y}{P_y - Q_x}$$

and

$$q = P_y - mP_x$$



1.3 Scalar Multiplication

Given a point $P \in E$, multiplying kP where $k \in \mathbb{Z}$ is equivalent to adding P to itself k times. Computing $2P$ is the equivalent of $P + P$ which can be calculated as $P + Q = -R$.

2 Diffie Hellman

Diffie–Hellman key exchange is a method of securely exchanging cryptographic keys over a public channel.

Scenario: a *client* and a *server* want to establish a shared secret.

- The *client* generates a random private key k_c
- The *server* generates a random private key k_s
- The two parts publicly establish a common G (generator)

We define a function

$$y = f(G, k)$$

such that given y and G it is very hard to get k.
The function must also satisfy the following identity

$$f(f(G, k_1), k_2) = f(f(G, k_2), k_1)$$

For instance the function G^k would satisfy this identity since $\left(G^{k_1}\right)^{k_2} = \left(G^{k_2}\right)^{k_1}$, but not the first property.

Given the function $f(G, k)$

- The *client* computes $y_c = f(G, k_c)$
- The *server* computes $y_s = f(G, k_s)$
- The two parts publicly exchange y_c and y_s
- The *client* computes $y = f(y_s, k_c)$
- The *server* computes $y = f(y_c, k_s)$

Now the *client* and *server* share the same value of y since $f(y_s, k_c) = f(y_c, k_s)$.
The value of y is unknown to anyone who has traced the communication between the *client* and the server.