Elliptic Curve Cryptography

Chester Rebeiro

IIT Madras

Slides borrowed from Prof. D. Mukhopadhyay, IIT Kharagpur
Ref: NPTEL course by the same professor available on youtube

ECC vs RSA

NIST guidelines for public key sizes for AES

ECC KEY SIZE (Bits)	RSA KEY SIZE (Bits)	KEY SIZE RATIO	AES KEY SIZE (Bits)
163	1024	1 : 6	
256	3072	1 : 12	128
384	7680	1 : 20	192
512	15 360	1 : 30	256

Supplied by NIST to ANSI X9F1

Let's start with a puzzle

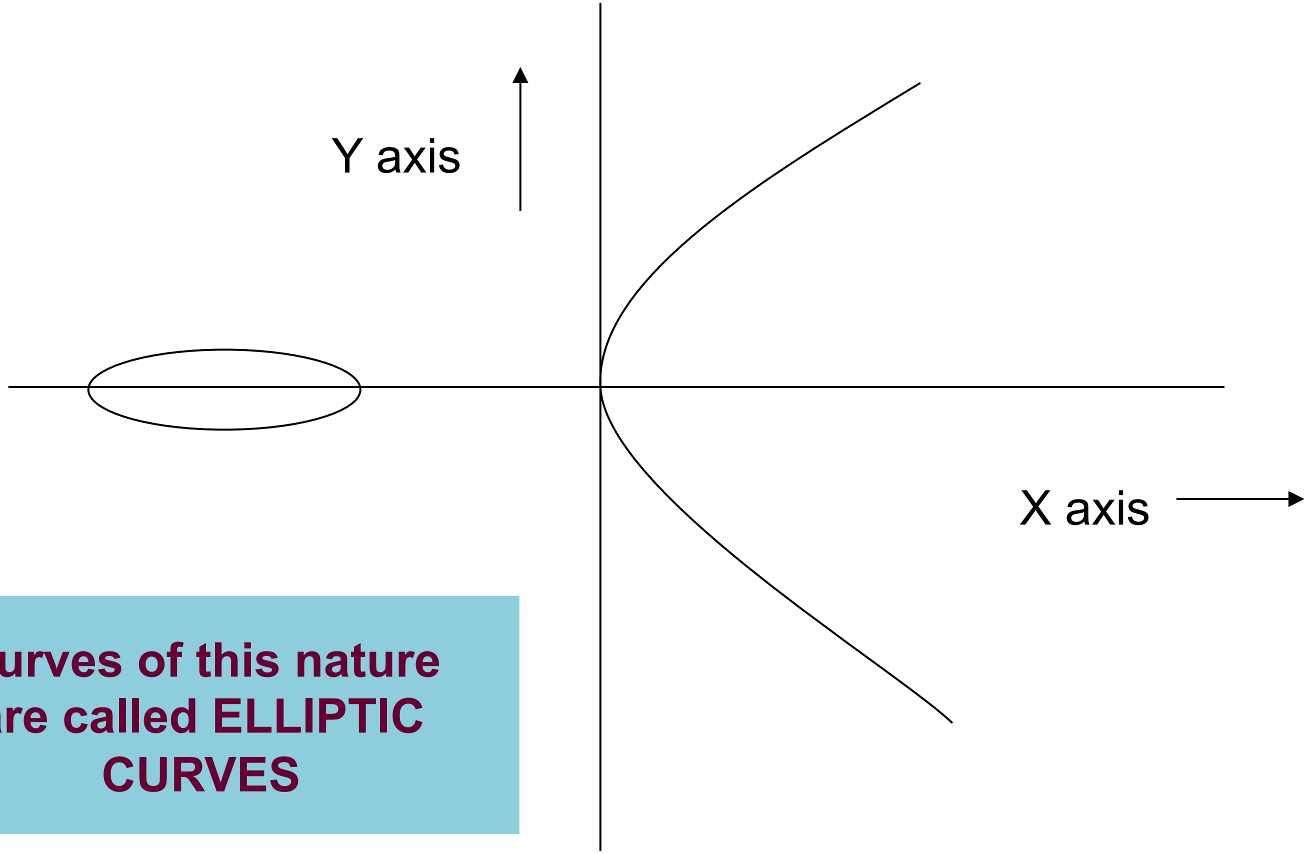
- What is the number of balls that may be piled as a square pyramid and also rearranged into a square array?

Solution: Let x be the height of the pyramid. We also want this to be a square:

$$\therefore 1^2 + 2^2 + 3^2 + \ldots + x^2 = \frac{x(x+1)(2x+1)}{6}$$

$$\boxed{y^2 = \frac{x(x+1)(2x+1)}{6}}$$

Graphical Representation



Curves of this nature are called ELLIPTIC CURVES

Method of Diophantus

- Uses a set of known points to produce new points
- (0,0) and (1,1) are two trivial solutions
- Equation of line through these points is y=x.
- Intersecting with the curve and rearranging terms:

$$x^3 - \frac{3}{2}x^2 + \frac{1}{2}x = 0$$

- We know that 1 + 0 + x = 3/2 =>

  x = ½ and y = ½
- Using symmetry of the curve we also have (1/2,-1/2) as another solution

Method of Diophantus

- Consider the line through (1/2,-1/2) and (1,1) => y=3x-2
- Intersecting with the curve we have:

$$x^3 - \frac{51}{2}x^2 + \ldots = 0$$

- Thus ½ + 1 + x = 51/2 or x = 24 and y=70
- Thus if we have 4900 balls we may arrange them in either way

Elliptic Curves in Cryptography

- 1985 independently by Neal Koblitz and Victor Miller.

- One Way Function: Discrete Log problem in Elliptic Curve Cryptography

Elliptic Curve on a finite set of Integers

- Consider $y^2 = x^3 + 2x + 3 \pmod 5$

  $x = 0 \Rightarrow y^2 = 3 \Rightarrow$ no solution $\pmod 5$

  $x = 1 \Rightarrow y^2 = 6 = 1 \Rightarrow y = 1,4 \pmod 5$

  $x = 2 \Rightarrow y^2 = 15 = 0 \Rightarrow y = 0 \pmod 5$

  $x = 3 \Rightarrow y^2 = 36 = 1 \Rightarrow y = 1,4 \pmod 5$

  $x = 4 \Rightarrow y^2 = 75 = 0 \Rightarrow y = 0 \pmod 5$

- Then points on the elliptic curve are
  $(1,1)$ $(1,4)$ $(2,0)$ $(3,1)$ $(3,4)$ $(4,0)$ and the point at infinity: ∞

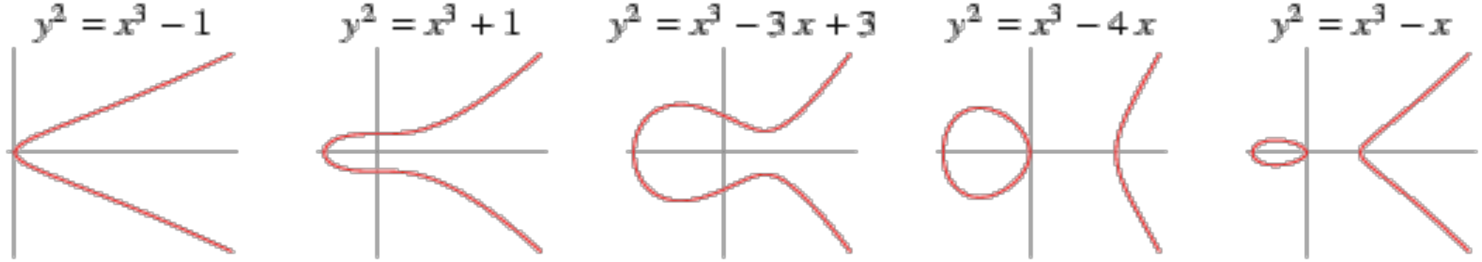
Using the finite fields we can form an Elliptic Curve Group where we have a Elliptic Curve DLP problem: ECDLP

General Form of an Elliptic Curve

- An *elliptic curve* is a plane curve defined by an equation of the form

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

Examples



Weierstrass Equation

- Generalized Weierstrass Equation of elliptic curves:

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

Here, x and y and constants all belong to a field of say rational
numbers, complex numbers, finite fields (F_p) or
Galois Fields ($GF(2^n)$).

Elliptic Curves in Cryptography

- An elliptic curve over a field K is a nonsingular cubic curve in two variables, $f(x,y) = 0$ with a rational point (which may be a point at infinity).

- Elliptic curves groups for cryptography are examined with the underlying fields of

  - F_p (*where $p>3$ is a prime*) and

  - F_{2^m} (*a binary representation with 2^m elements*).

Curve Equations Depend on the Field

- If Characteristic field is not 2:

$$(y+\frac{a_1x}{2}+\frac{a_3}{2})^2 = x^3+(a_2+\frac{a_1^2}{4})x^2+a_4x+(\frac{a_3^2}{4}+a_6)$$
$$\Rightarrow y_1^{\ 2} = x^3+a_2^{'}x^2+a_4^{'}x+a_6^{'}$$

- If Characteristics of field is neither 2 nor 3:

$$x_1 = x + a_2^{'}/3$$
$$\Rightarrow y_1^{\ 2} = x_1^{\ 3}+Ax_1+B$$

Points on the Elliptic Curve

- Elliptic Curve over field L

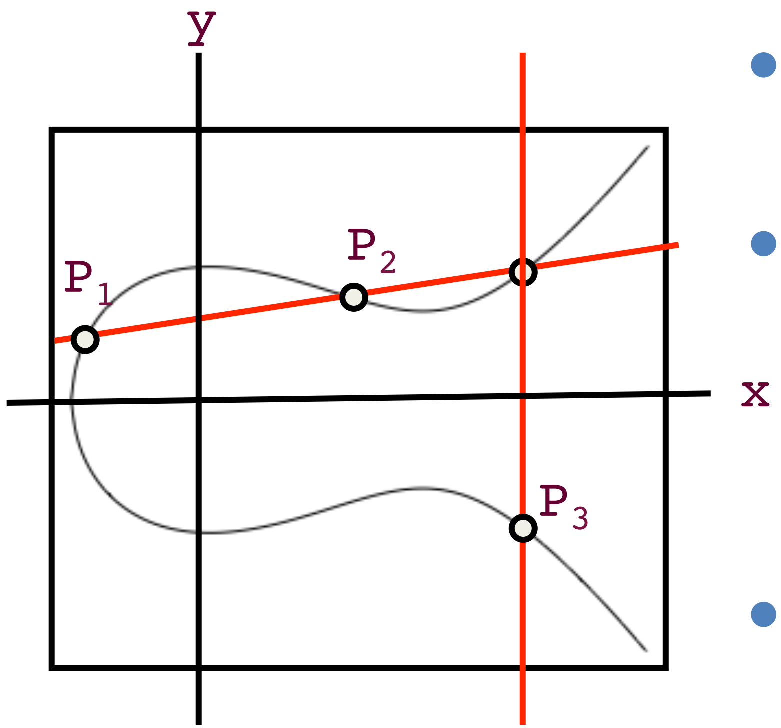
$$E(L) = \{\infty\} \cup \{(x, y) \in L \times L \mid y^2 + \ldots = x^3 + \ldots\}$$

- It is useful to add the point at infinity
  - The point is sitting at the top and bottom of the y-axis
  - Any line is said to pass through the point when it is vertical

Abelian Group

- Given two points P,Q in *E(Fp)*, there is a third point, denoted by $P+Q$ on *E(Fp)*, and the following relations hold for all P,Q,R in *E(Fp)*
  - $P + Q = Q + P$ (*commutativity*)
  - $(P + Q) + R = P + (Q + R)$ (*associativity*)
  - $P + O = O + P = P$ (*existence of an identity element*)
  - there exists $(-P)$ such that $-P + P = P + (-P) = O$ (*existence of inverses*)

The Big Picture



- Consider elliptic curve

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

- If P_1 and P_2 are on E, we can define

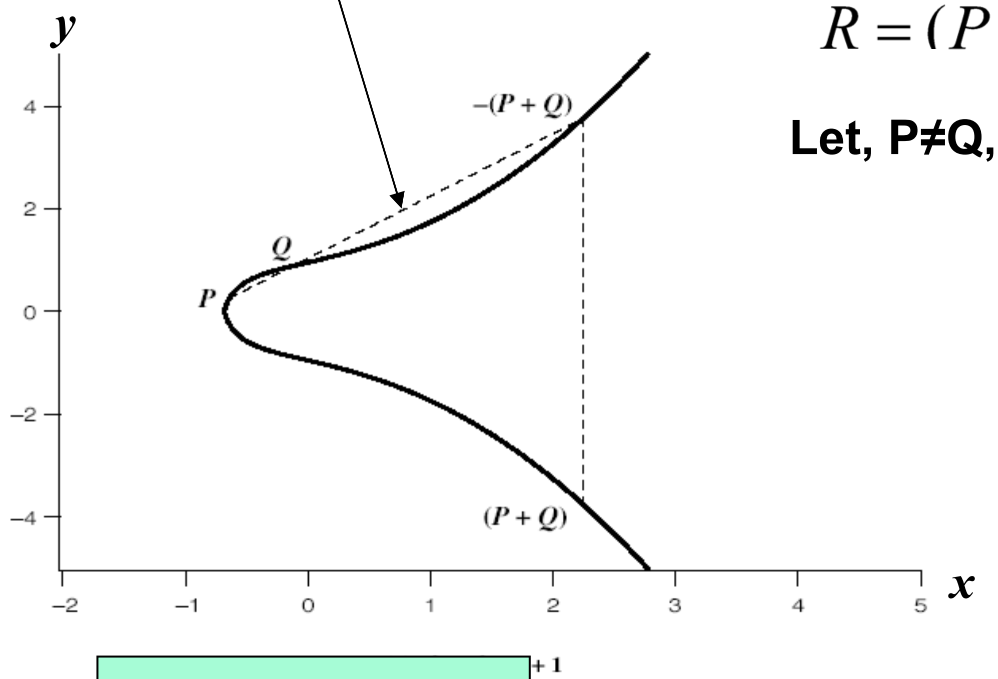
  $P_3 = P_1 + P_2$

  as shown in picture

- Addition is all we need

Addition in Affine Coordinates

$y=m(x-x_1)+y_1$



$y^2=x^3+Ax+B$

$$P=(x_1,y_1),Q=(x_2,y_2)$$
$$R=(P+Q)=(x_3,y_3)$$

Let, P≠Q,

Point Addition

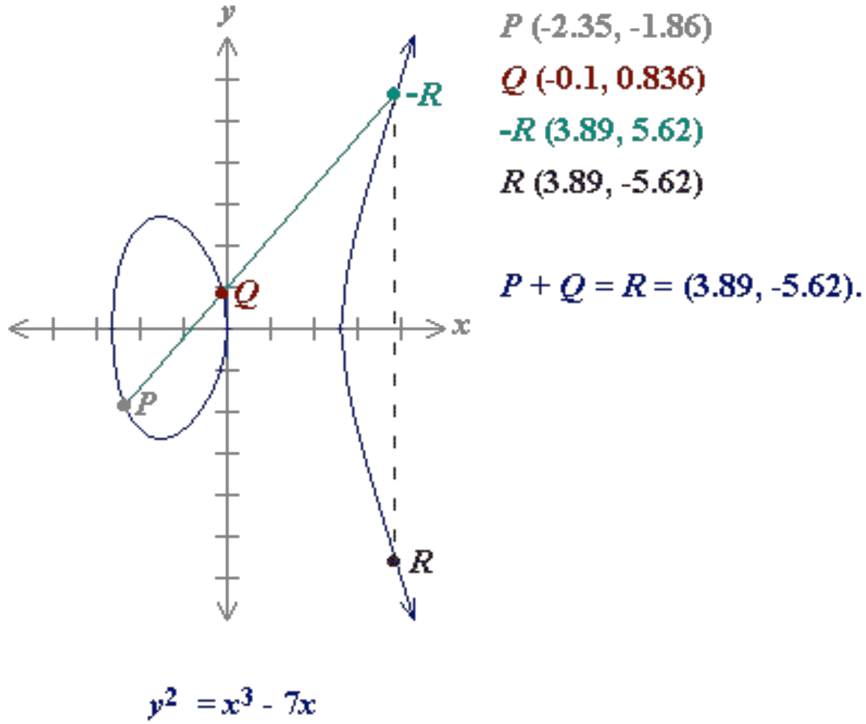
Define for two points ***P (x₁,y₁)*** and ***Q (x₂,y₂)*** in the Elliptic curve

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} \ for\ x_1 \neq x_2 \\ \dfrac{3x_1^{\ 2} + a}{2y_1} \ for\ x_1 = x_2 \end{cases}$$

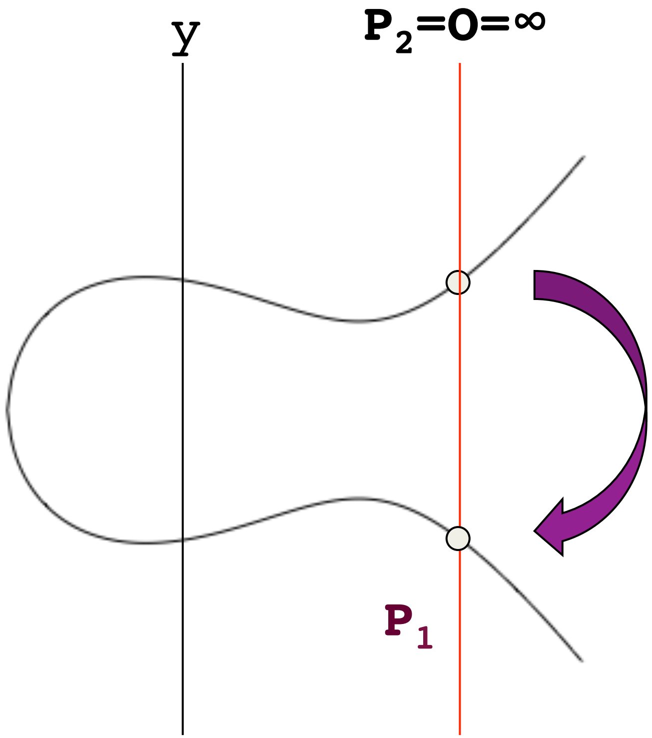
Then ***P+Q*** is given by ***R(x₃,y₃)*** :

$$x_3 = \lambda^2 - x_1 - x_2$$

$$y_3 = \lambda(x_3 - x_1) + y_1$$



Adding with Point O



$P_1 = P_1 + O = P_1$

Doubling a Point

P+P = 2P

- Let, P=Q

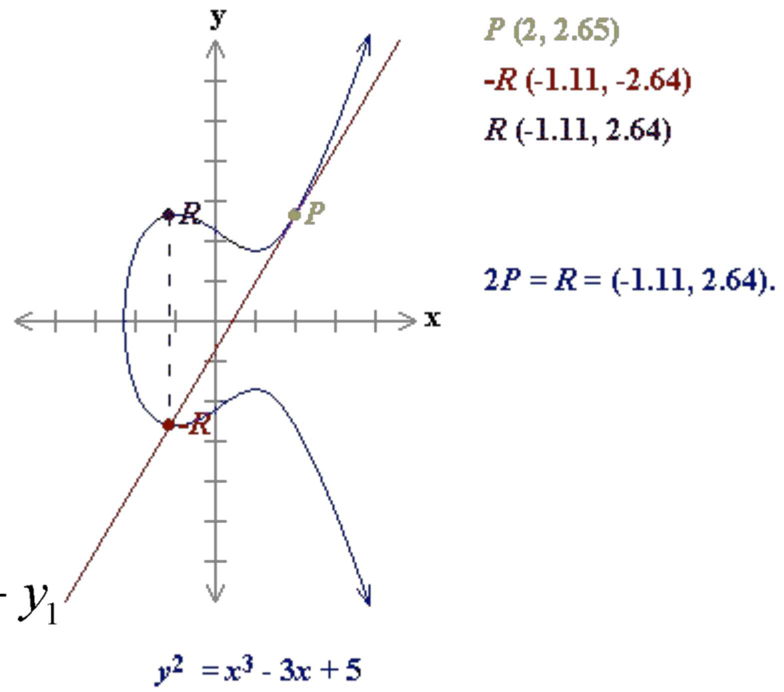
$$2y\frac{dy}{dx} = 3x^2 + A$$

$$\Rightarrow m = \frac{dy}{dx} = \frac{3x_1^2 + A}{2y_1}$$

$If, y_1 \neq 0$ (since then $P_1+P_2=\infty$):

$$\therefore 0 = x^3 - m^2x^2 + \ldots$$

$$\Rightarrow x_3 = m^2 - 2x_1, y_3 = m(x_1 - x_3) - y_1$$



- What is P + point at infinity

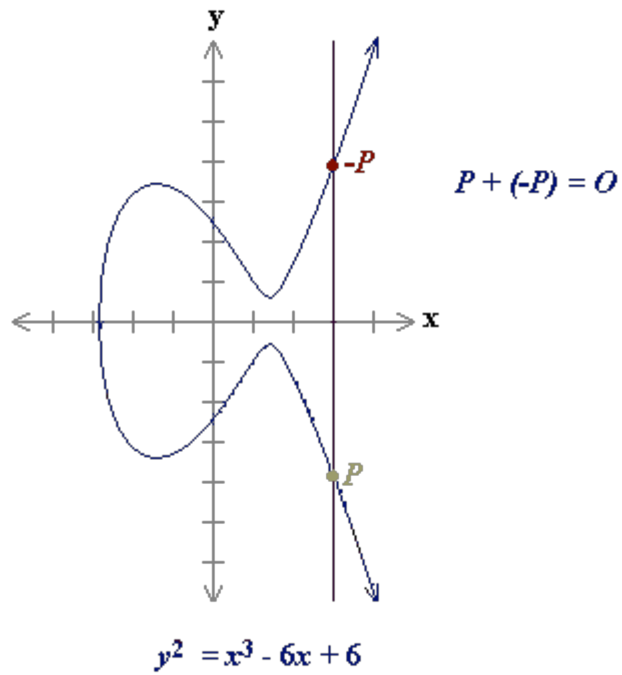
Point at Infinity

Point at infinity ***O***

As a result of the above case ***P=O+P***

O **is called the additive identity of the elliptic curve group.**

Hence all elliptic curves have an additive identity ***O***.



Elliptic Curve Scalar Multiplication

- Given a point P on the curve
- and a scalar k

computing Q = kP (can be easily done)

however, given points P and Q, obtaining the point k is difficult

Left-to-right Scalar Multiplication

Algorithm 3.27 Left-to-right binary method for point multiplication

INPUT: $k = (k_{t-1}, \ldots, k_1, k_0)_2$, $P \in E(\mathbb{F}_q)$.

OUTPUT: kP.

1. $Q \leftarrow \infty$.
2. For i from $t-1$ downto 0 do
   - 2.1 $Q \leftarrow 2Q$. Point Doubling
   - 2.2 If $k_i = 1$ then $Q \leftarrow Q + P$. Point Addition
3. Return(Q).

Point Operations over F(p)

Simplified Weierstrass Equation $y^2 = x^3 + ax + b$

Point addition. Let $P = (x_1, y_1) \in E(K)$ and $Q = (x_2, y_2) \in E(K)$, where $P \neq \pm Q$. Then $P + Q = (x_3, y_3)$, where

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2 \quad \text{and} \quad y_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3) - y_1.$$

Point doubling. Let $P = (x_1, y_1) \in E(K)$, where $P \neq -P$. Then $2P = (x_3, y_3)$, where

$$x_3 = \left(\frac{3x_1^2 + a}{2y_1}\right)^2 - 2x_1 \quad \text{and} \quad y_3 = \left(\frac{3x_1^2 + a}{2y_1}\right)(x_1 - x_3) - y_1.$$

Projective Coordinates

Maps (x, y) to projective coordinates (X, Y, Z), which reduces the number of inversions

2D projective space over the field is defined by the triplex (X, Y, Z), with X, Y, Z in the field

Projective Coordinates form an equivalence class $(X,Y,Z) \sim (\lambda X, \lambda Y, \lambda Z)$

Identify projective coordinates by their ratios : $(X:Y:Z)$

Suppose $Z \neq 0$ we take $\lambda = 1/Z$ then $(X/Z:Y/Z:1)$

Suppose $Z = 0$ we get the point at infinity

Transformation : (x, y) → (X, Y, 1)

Projective Coordinate Representation

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

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

Point Addition : 7M + 5S
Point Doubling : 12M + 2S