Elliptic Curve

By: Arun Mishra
DIAT, Pune

Acknowledgement

Much material in this course owe their ideas and existence to

- Lawrence C Washington, University of Maryland
- Behrouz A. Forouzan

Reference Material

- "Introduction to Cryptography with Coding Theory" by Wade Trappe & Lawrence C Washington, New Jersey, Pearson Education, 2006.
- Behrouz A. Forouzan, "Cryptography and Network Security", McGraw Hill

A Pyramid of Cannonballs

- $$1^2 + 2^2 + 3^2 + \cdots + x^2 = \frac{x(x+1)(2x+1)}{6}$$

- We want this to be perfect square,

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

- An equation of this type represents an **elliptic curve.**

- Let’s start with the points (0,0) and (1,1). The line through these two points is y = x.

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

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

- We already know two roots of this equation: $x = 0$ and $x = 1$. We could factor the polynomial to find the third root.

$$(x-a)(x-b)(x-c) = x^3 - (a+b+c)x^2 + (ab+ac+bc)x - abc$$

- We have roots 0, 1, and x, so

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

- Therefore, $x = \frac{1}{2}$. Since the line was $y = x$, we have $y = \frac{1}{2}$.
- We automatically have on more point, namely $\left(\frac{1}{2}, -\frac{1}{2}\right)$, because of the symmetry of the curve

Elliptic curve

- An **elliptic curve** E is the graph of the equation of the form

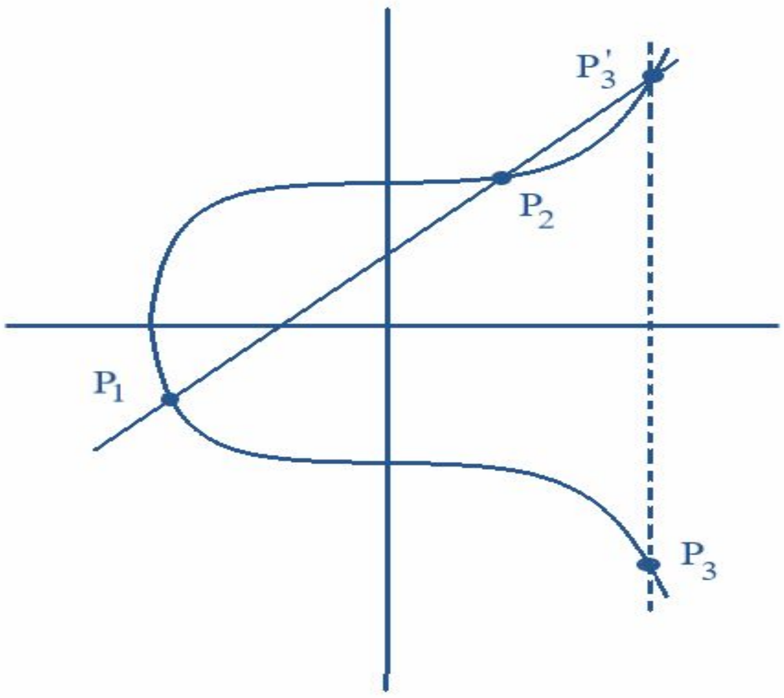
$$y^2 = x^2 + Ax + B$$

- It will be taken to be elements of the fields.

- It is not possible to draw meaningful pictures of elliptic curves over most fields. For institution, it is useful to think in terms of graphs over the real numbers.

$$4A^3 + 27B^2 \neq 0.$$

Adding Points on an Elliptic Curve



- Start with two points

$$P_1 = (x_1, y_1), \qquad P_2 = (x_2, y_2)$$

- To obtain P_3

$$P_1 + P_2 = P_3.$$

- Assume first that $P_1 \neq P_2$ and neither point is ∞. Draw the line L through P_1 and P_2. Its slope is

$$m = \frac{y_2 - y_1}{x_2 - x_1}$$

- Let's assume that $x_1 \neq x_2$.

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

- To find the intersection with E, substitute to get

$$(m\,(x - x_1) + y_1)^2 = x^3 + Ax + B.$$

- Rearranged to form

$$0 = x^3 - m^2x^2 + \cdots.$$

- If we have a cubic polynomial $x^3 + ax^2 + bx + c$ with roots *r*, *s*, *t*, then

$$x^3 + ax^2 + bx + c = (x - r)(x - s)(x - t) = x^3 - (r + s + t)x^2 + \cdots.$$

Therefore,

$$r + s + t = -a.$$

- We can recover the third as $t = -a - r - s$.

  We obtain

$$x = m^2 - x_1 - x_2$$

and

$$y = m\,(x - x_1) + y_1.$$

- Reflect across the $x\text{-}axis$ to obtain the point $P_3 = (x_3, y_3)$

$$x_3 = m^2 - x_1 - x_2, \qquad y_3 = m(x_1 - x_3) - y_1.$$

- In the case that $x_1 = x_2$ but $y_1 \neq y_2$, the line through P_1 and P_2 is a vertical line, which therefore intersects E in ∞. Therefore, in this case $P_1 + P_2 = \infty$.

- In the case where $P_1 = P_2 = (x_1, y_1)$. Two points on the curve are very close to each other, the line through them approximates a tangent line.

$$2y\frac{dy}{dx} = 3x^2 + A, \qquad so \qquad m = \frac{dy}{dx} = \frac{3x_1^2 + A}{2y_1}$$

- If $y_1 = 0$ then the line is vertical and we set $P_1 + P_2 = \infty$, as before. Therefore assume that $y_1 \neq 0$.

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

- We obtain the cubic equation

$$0 = x^3 - m^2x^2 + \cdots.$$

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

- Suppose $P_2 = \infty$. The line through P_1 and ∞ is a vertical line that intersect E in the point P_1' that is the reflection of P_1. P_1' across the x-axis to get $P_3 = P_1 + P_2$.

Therefore,

$$P_1 + \infty = P_1.$$

Thank You!