Elliptic Curve Arithmetic

Why ECC?

- ✓ Good security even with far smallest key than RSA
- ✓ Reduce the processing overhead

Basics for ECC:

Abelian Groups:

- ✓ {G, •} is a set of elements with a binary operations
- ✓ It should satisfy the following properties
  - Closure : if a and b belongs to G, than a • b also in G.
  - Associative : a • (b •c) = (a • b) • c for all a,b,c in G.
  - Identity elements: a • e = e • a = a for all a in G.
  - Inverse element : a • a’ = a’ • a = e.
  - Commutative: a • b = b • a for all a, b in G.
- ✓ In Diffie-Hellman, keys are generated by exponentiation defined by repeated multiplication
  - a^k mod q = (aXaXaX … .Xa) mod q
- ✓ In ECC, operations are in addition. Multiplication is defined by repeated addition.
  - aXk = (a+a+a+ ….. +a)

ECC definition

- Elliptic curve is represented as $E_p(a,b)$. P is a prime number and a,b are restricted to mod p
- The curve is represented by $y^2 = x^3 + ax + b$.
- Elliptic curves are not ellipse but the equation of ecc is described by calculation of circumference of ellipse (i.e. cubic equation with highest degree of 3)
- For determining the security of various elliptic curve ciphers, the number of points in a finite abelian group defined over an elliptic curve.
- In case of the finite group $E_p(a,b)$, the number of points N is bounded by:

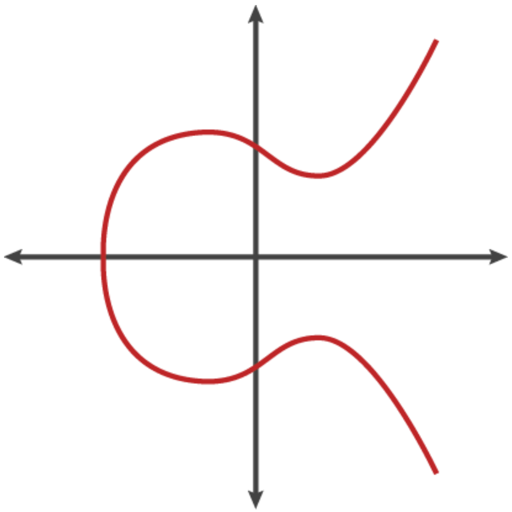
$$p+1-\sqrt{p} \leq N \leq p+1+2\sqrt{p}$$

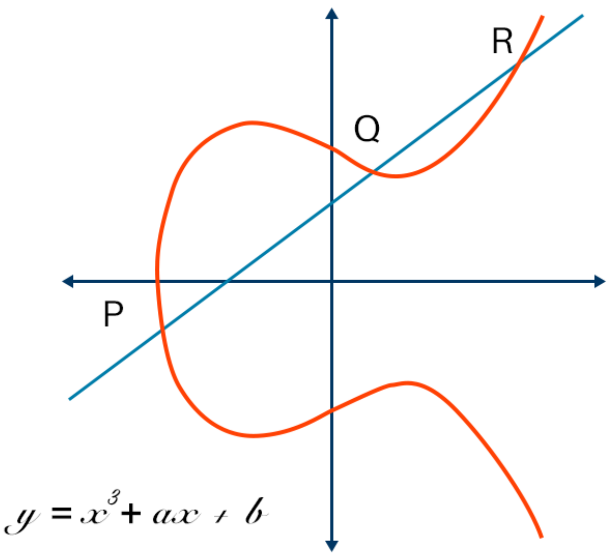
- No. of points in $E_p(a,b)$ is approximately equal to the number of elements in Z_p, namely p elements.

How the elliptic curve is Symmetric?

$$y = \sqrt{x^3 + ax + b}$$

This gives a value of x as $\pm$ x. So, each curve is symmetric curve about y=0.





Affine points: The points present in Elliptic curve

O points: There is a point called 0 point in which P + (-P) becomes infinity.

ECC can be defined as EC over Z_p (prime curve) and EC over $GF(2^m)$ (binary curve).

ECC can be used for key exchange and Encryption.

Elliptic curves over Z_p:

- ✓ The curve of this type is prime curve
- ✓ The variables and coefficients are restricted to elements of a finite field
- ✓ The values are restricted from 0 through p-1, If the values exceeds the range perform modulo p.
- ✓ The curveis represented by y^2 mod p = (x^3+ax+b) mod p
- ✓ The curve is to be focused in only one of the quadrant from (0,0)through (p-1,p-1) containing non negative integers
- ✓ The number of points N is bounded by

$$p+1-\sqrt{p} \leq N \leq p+1+2\sqrt{p}$$

Addition

- Adding 2 points $P(x_p, y_p)$ and $Q(x_q, y_q)$ gives $R(x_r, y_r)$.
- Steps:
  - Find the slope λ:
  - $\lambda = (y_q - y_p) / (x_q - x_p)$ if $P \neq Q$
  - $\lambda = (3x_p^2 + a) / 2y_p$ if $P = Q$ where a is obtained from $E_p(a,b)$
  - Find the sum: R (i.e. (x_r, y_r)) = P + Q
  - $x_r = \lambda^2 - x_p - x_q$
  - $y_r = \lambda(x_p - x_r) - y_p$

Negating a point:

- ✓ if $Q = (x_q,y_q)$
- ✓ then $–Q = -(x_q,y_q) = (x_q,-y_q)$

Subtraction:

- ✓ $P – Q = (x_p,y_p) – (x_q, y_q) = (x_p,y_p)+(x_q,-y_q \bmod p)$. Now perform addition.

Multiplication:

- ✓ Only Scalar multiplication is possible. Multiplication between two points are not possible. Repeated addition is performed.
- ✓ 2P = P+P, 3P = P+P+P and so on. Note for slope (λ) calculation use the formula P=Q.
- ✓ Division: Only Scalar division is possible. $[1/a(x_p,y_p)] = a^{-1} (x_p,y_p)$. Multiplication steps can be followed.