

Introduction to Elliptic Curve Cryptosystem

The cubic equation

$y^2 = f(x) = x^3 + ax^2 + bx + c$, assuming complex roots of $f(x)$ are distinct, we have the elliptic curve. If we take the co-efficient of a , b , c to be rational, in practice it turns out that the polynomial $f(x)$ of degree three has at least one real root. In real numbers it can be written in terms of factors as $f(x) = (x - \text{Alpha})(x^2 + \text{Beta} * x + \text{gamma})$ where Alpha, Beta, and gamma are real. If it has one real root, the curve looks as shown below.

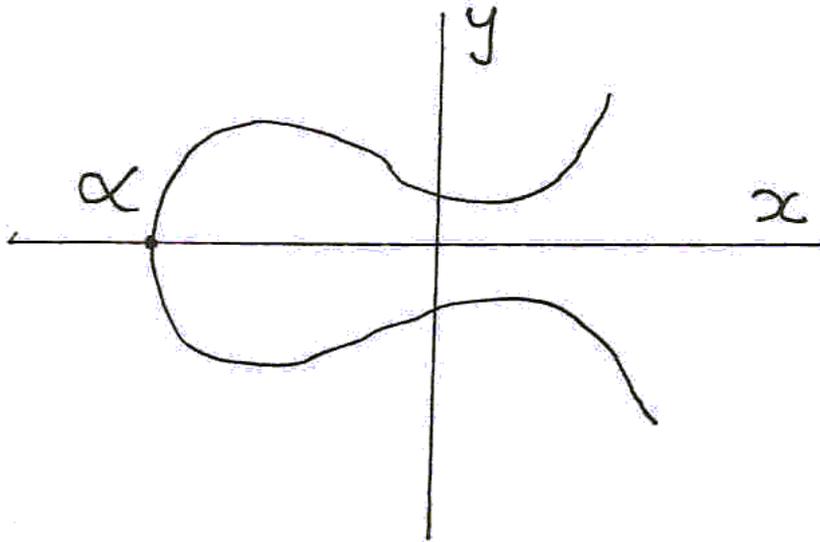


Fig 5. One real component

If $f(x)$ has 3 real roots, then the curve looks as below. (All roots are distinct)

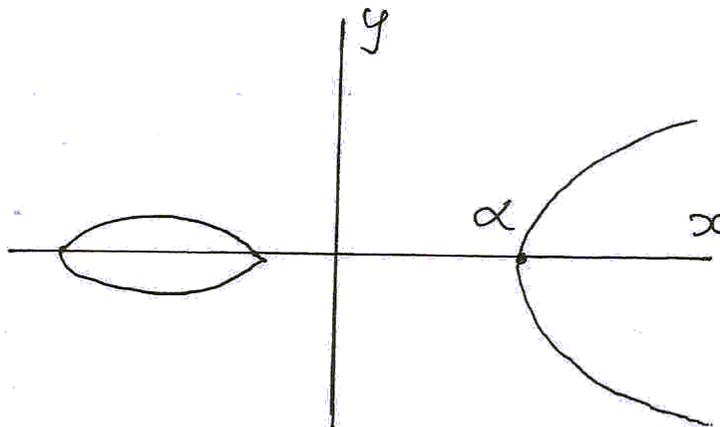


Fig 6. Two real components

If we take $F(x, y) = y^2 - f(x) = 0 \rightarrow (1)$ and their partial derivatives

$$dF/dx = -f'(x);$$

$$dF/dy = 2y,$$

if there is no point on the curve at which both the partial derivatives yields zero simultaneously, then the curve is non-super singular.

If dF/dx and dF/dy were to be equal to zero simultaneously at a point $P(x_1, y_1)$, then $y_1=0$, which implies $f(x)=0$ due to equation (1).

Hence $f(x)$ and $f'(x)$ have a common root x_1 . So x_1 is a double root of $f(x)$.

If $p > 3$ be an odd prime and $q = p$, in the finite field F_p , the elliptic curve in Weierstrass form is $y^2 = x^3 + ax + b$, where $((4a^3 + 27b^2) \bmod p) \neq 0 \rightarrow (\text{Condition 1})$

For the curve,

$$y^2 = f(x) = x^3 + ax^2 + bx + c \rightarrow (1), \text{ the discriminant of } f(x) \text{ is}$$

$$D = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2$$

$$\text{If } a=0, y^2 = f(x) = x^3 + bx + c \text{ and } D = -4b^3 - 27c^2$$

If $D = 0$, the roots are real and equal, which is undesirable. Even if the elliptic curve chosen is non super-singular, this need not hold true for the points generated by the elliptic curve modulo a prime. So if $D = 0$, we discard the curve parameters and try out a new set of parameters, when used in Elliptic Curve Cryptography.

If $D > 0$, the roots are real and distinct, which are points on a non-super singular curve, as desired.

If $D < 0$, there is exactly one real root.

Elliptic curve parameters and their validation over F_p

- Verify that n is an odd prime and P be a point on the non-super singular elliptic curve, then, $nP = O$, n being the order of the point P .
- The co-factor $h = \#E(F_q)/n$, n is a large prime close to the field size.
- If $n > 4 \cdot \sqrt{p}$, then compute $h = \text{floor}(((\sqrt{p}+1)^2)/n)$ and verify $h = h'$
- Verify Condition 1.

If any of the tests fail, reject the curve parameters and test for another set of parameters.

If $n < 4 \cdot \sqrt{p}$, there are other efficient methods to verify correctness of h . However usually n (is close to) p and $n > 4 \cdot \sqrt{p}$ is satisfied.