Elliptic Curve Cryptography

Sai Manoj

02/02/2022

1 Weierstrass Equations

The *Weierstrass Equation* for an elliptic curve is of the form $y^2 = x^3 + Ax + B$ where A, B are constants. If K is a field such that the constants belong to K, then the elliptic curve E is said to defined over K.

$E(L) = (\infty) \cup ((x, y) \in L \times L | y^2 = x^3 + Ax + B)$

The point ∞ is always contained in this set.
For a cubic equation with roots $r1, r2, r3$, the discriminant is given by
$((r1 - r2)(r2 - r3)(r3 - r1)) + (4A^3 + 27B^2)$

For there to be no multiple roots, none of $r1 - r2, r2 - r3, r3 - r1$ should be zero. This implies that $4A^3 + 27B^2 \neq 0$.

1.1 Generalized Weierstrass Equation

The generalized Weierstrass equation is of the form $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$. There is also a more generalized form which is used when working with the fields of characteristic 2 and 3.

Note :- The characteristic of a field F is 0 if $Z \subset F$, or is a prime p. The *prime subfield* is the smallest subfield of F which is either Q or F_p.

Some definitions : -

— A ring is a set R which is closed under $+$ and $\times$.

— R is an Abelian group under $+$.

— Associativity of $\times$

— Distributive property is satisfied.

— A field is a ring in which all non-zero elements are invertible.

Consider the example equation : - $cy^2 = dx^3 + ax - b$
Multiplying with c^3d^2 on both sides, we get
$c^4d^2y^2 = c^3d^3x^3 + ac^3d^2x - bc^3d^2$
$=> (c^2dy)^2 = (cdx)^3 + ac^2d(cdx) - bc^3d^2$
Let $Y = c^2dy$ and $X = cdx$, then
$=> Y^2 = X^3 + AX + B$
It is still a Weierstrass equation.

Definition :- The point ∞ is a little strange, but we say that a line exactly passes through ∞ when it is vertical.
We also consider that the ends of the y-axis as wrapping around and meeting (perhaps somewhere in the back behind the page) in the point ∞. More related to this will come under Projective Coordinates (ends of Y-axis is not clear).

2 The Group Law

We have looked at the method where we get more points from two given points on an elliptic curve.
Consider two points, $P_1 = (x_1, y_1), P_2 = (x_2, y_2)$ on an elliptic curve E given by the equation $y^2 = x^3 + Ax + B$. The point $P_3^{'}$ is obtained from the intersection of line joining P_1 and P_2 and the elliptic curve. We also define the new point P_3, which is the image of $P_3^{'}$ with respect to the X-axis.
We define the operation $+_E$ on these points as follows,

$$P_1 +_E P_2 = P_3$$

Consider that the line joining P_1 and P_2 is not vertical. The equation of the line passing through y_1 can be written as $y = m(x-x_1)+y_1$. We can find the intersection with E by substituting this line into the equation of the curve.
$\Rightarrow (m(x - x_1) + y_1)^2 = x^3 + Ax + B$

For various cases of selecting the two points, we have the following law : -
(i) If $x_1 \neq x_2$, then

$x_3 = m_2 - x_1 - x_2$, $y3 = m(x1 - x3) - y1$, where $m = \dfrac{y_2 - y_1}{x_2 - x_1}$

(ii) If $x_1 = x_2$ but $y_1 \neq y_2$,then $P1 + P2 = \infty$.
(iii) If P$_1$ $=$ $P_2 and$y$_1$ $\neq$ 0,then $x_3 = m_2 - 2x_1$, $y_3 = m(x_1 - x_3) - y_1$, where $m = \dfrac{3x_1^2 + A}{2y_1}$.
(iv) If $P_1 = P_2$ and $y_1 = 0$, then $P_1 + P_2 = \infty$.

<u>*Note*</u> *:* $P + \infty = P$ for all points P on E.

E forms an additive **Abelian group** with ∞ as the identity element.