Elliptic Curves

Sarup Hussain
Roll No: 202123040

October 29, 2021

Contents

1 History of Elliptic Curves and its use in Cryptography

Elliptic curves occurred first time in the work of Diophantus in second century A.D. Since then the theory of elliptic curves were studied in number theory. Till 1920, elliptic curves were studied mainly by Cauchy, Lucas, Sylvester, Poincare.

In 1984, Lenstra used elliptic curves for factoring integers and that was the first use of elliptic curves in cryptography. Fermat's Last theorem and General Reciprocity Law was proved using elliptic curves and that is how elliptic curves became the centre of attraction for many mathematicians.

Elliptic curve cryptography is introduced by Victor Miller and Neal Koblitz in 1985 and now it is extensively used in security protocol.

2 Affine space , Projective space and Points at infinity

Affine n-space (over$K$) is the set of n-tuples
A^n={ $p = (x_1, x_2...., x_n) : x_i \varepsilon \overline{K}$ }

Projective n-space (over K), denoted by P^n, is the set of all n+1 tuples
$(x_0, x_1, ..., x_n) \varepsilon A^{n+1}$
such that at least one x_i is nonzero , modulo the equivalence relation
$(x_0, ..., x_n)$ ~ $(y_0, y_1, ..., y_n)$
if there exists a $\lambda \varepsilon \overline{K}$ such that $x_i = \lambda y_i$ for all i. An equivalence class $\{(\lambda x_0, ..., \lambda x_n) : \lambda \varepsilon \overline{K}\}$ is denoted by $[x_0, ..., x_n]$ and the individual $x_0, x_1, ..., x_n$ are called homogeneous coordinates for the corresponding point in P^n.

we can embed the affine space A^n in P^n by the map
$A^n \rightarrow P^n$, $(x_1, ..., x_n) \rightarrow [1, x_1, ..., x_n]$ whose image is the subset $U_0 := \{[x_0, ..., x_n] : x_0 \neq 0\}$ of P^n. We will often consider A^n as a subset of P^n in this way, i. e. by setting $x_0 = 1$. The other coordinates $x_1, ..., x_n$ are then called the inhomogeneous or affine coordinates on U_0. The remaining points of P^n are of the form $[0, x_1, .., x_n]$ which form a set that is naturally bijective to P^{n-1} ,corresponding to the 1-dimensional linear subspaces of K^n.
we can regard them as points at infinity; there is hence one such point for each direction in K^n.

Genus One: Intuitively, genus is the number of "holes" of a surface. By Riemann-Roch theorem,an irreducible plane curve of degree d has geometric genus $g = \frac{(d-1)(d-2)}{2} - s$ where s is the number of singularities.

3 Definition of Elliptic Curve

An elliptic curve is a pair (E, O), where E is a smooth projective curve of genus one and O is a point of E. The elliptic curve is said to be defined over the field K if the underlying curve is defined over K and the point O is defined over K.

Every elliptic curve can be embedding as a smooth cubic curve in projective 2-space P^2 given by an equation of the form

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

Such an equation is called a Weierstrass equation for E. The point O is the point $[0, 1, 0]$ at infinity. If E is defined over K, then the a_i's can be chosen in K.

If $char(\overline{K}) \neq 2, 3$, then E has a Weierstrass equation of the form
(1) E: $y^2 = x^3 + Ax + B$
A curve f is non-singular if its gradient doesn't vanish at any of its points.
gradient of E of (1) is $(3x^2 + A, 2y)$ which is non zero if $x^3 + Ax + B$ and $3x^2 + A$ share no roots in $\overline{K}$.
In general, two nonzero polynomials f and g over a field k share no roots in k when

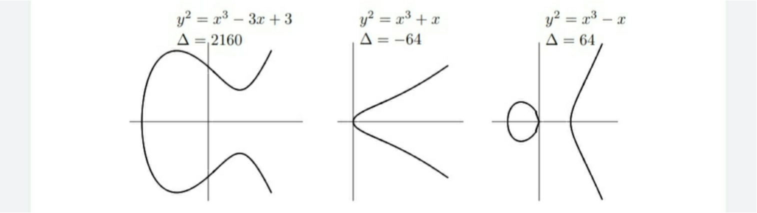
their resultant is nonzero. The resultant is a polynomial function of the coefficients of the two polynomials, the determinant of a matrix called the Sylvester matrix.

$$S = \begin{vmatrix} 1 & 0 & A & B & 0 \\ 0 & 1 & 0 & A & B \\ 3 & 0 & A & 0 & 0 \\ 0 & 3 & 0 & A & 0 \\ 0 & 0 & 3 & 0 & A \end{vmatrix} = 4A^3 + 27B^2 \neq 0$$

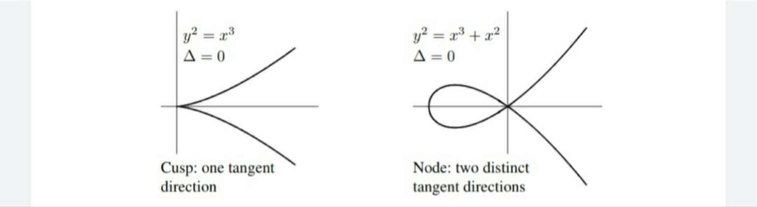
Thus the condition for non-singularity is $4A^3 + 27B^2 \neq 0$ in K
The resultant of a polynomial and its derivative is (up to sign) the discriminant of the polynomial.

We also define the j-invariant of E to be the quantity
$j(E) = 1728\frac{4A^3}{\Delta}$.

Examples



Non Elliptic Curves



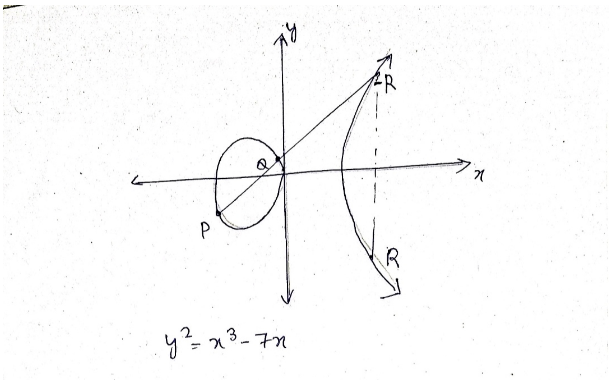
3.1 Elliptic Curve as a group

3.1.1 Geometry of elliptic Curves as a group

Elliptic curve groups are additive groups.The addition of two points in an elliptic curve is defined geometrically.

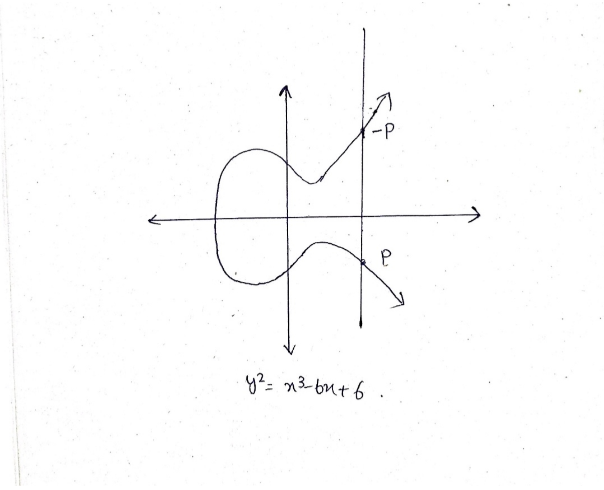
Adding distinct points P and Q

Suppose that P and Q are two distinct points on an elliptic curve, and the P is not $-Q$. To add the points P and Q, a line is drawn through the two points. This line will intersect the elliptic curve in exactly one more point, call $-R$. The point $-R$ is reflected in the x-axis to the point R. The law for addition in an elliptic curve group is $P + Q = R$.



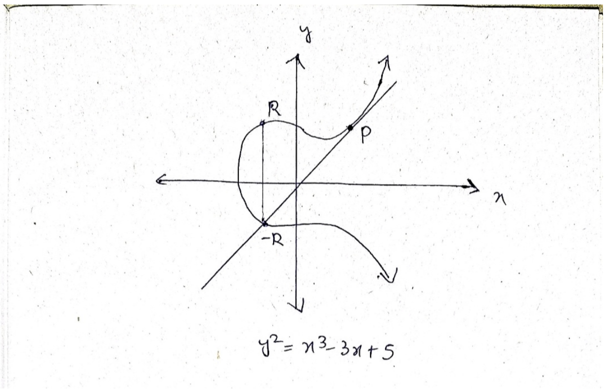
Adding P and $-P$

The line through P and $-P$ is a vertical line which does not intersect the elliptic curve at a third point; thus the points P and $-P$ cannot be added as previously. It is for this reason that the elliptic curve group includes the point at infinity O. By definition, $P + (-P) = O$. As a result of this equation, $P + O = P$ in the elliptic curve group .O is called the additive identity of the elliptic curve group; all elliptic curves have an additive identity.



Doubling the point if $y_p \neq 0$

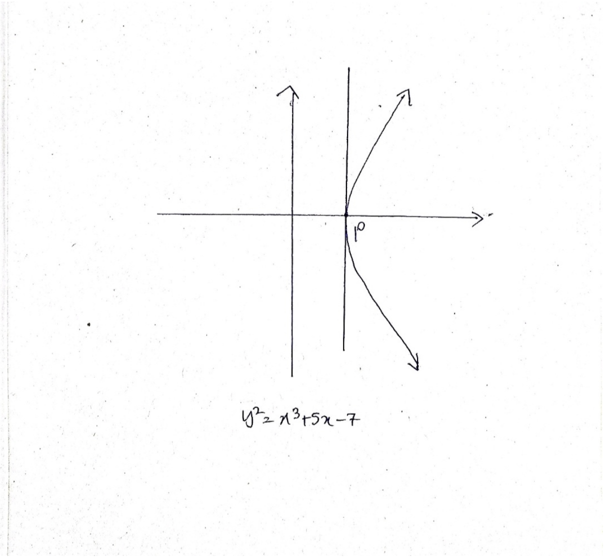
To add a point P to itself, a tangent line to the curve is drawn at the point P. If y_P is not 0, then the tangent line intersects the elliptic curve at exactly one other point, $-R$. $-R$ is reflected in the x-axis to R. This operation is called doubling the point P; the law for doubling a point on an elliptic curve group is defined by:
$P + P = 2P = R$



Doubling the point if $y_p = 0$

The tangent from P is always vertical if $y_P = 0$ If a point P is such that $y_P = 0$, then the tangent line to the elliptic curve at P is vertical and does not intersect the elliptic curve at any other point. By definition, $2P = O$ for such a point P. If one wanted to find $3P$ in this situation, one can add $2P + P$. This becomes $P + O = P$ Thus $3P = P$.

$3P = P, 4P = O, 5P = P, 6P = O, 7P = P$, etc.



3.1.2 Algebraic Definition of Elliptic Curve as a group

We define $+ : EXE \rightarrow E$, $(A, B) \rightarrow A + B$ as follows:
(a) We set $A + O = O + A = A$ for all A
(b) If $(x_A, y_A) = (x_B, -y_B)$ then $A + B := O$
(b) If $(x_A, y_A) \neq (x_B, -y_B)$ then we define $A + B := (x_{AB}, y_{AB})$ where
$x_{AB} := \alpha(A, B)^2 - x_A - x_B$
$y_{AB} := -y_A + \alpha(A, B)(x_A - x_{AB})$
with $\alpha(A, B) = \frac{y_A - y_B}{x_A - x_B}$ if $x_A \neq x_B$ and $\alpha(A, B) = \frac{3x_A^2 + a}{2y_B}$ if $x_A = x_B$

Example: Consider the ellptic curve E: $y^2 = x^3 - x$.
let $(x_A, y_A) = (3, \sqrt{24})$ and $(x_B, y_B) = (0, 0)$ are points in E. Applying the above formula we get $(x_{AB}, y_{AB}) = (-\frac{1}{3}, \frac{\sqrt{24}}{9})$ where the point $(x_{AB}, -y_{AB})$ is collinear to the point (x_A, y_A) and (x_B, y_B).

Composition Law: Let $P, Q \epsilon E$, let L be the line through P and Q (if $= Q$, let L be the tangent line to E at P), and let R be the third point of intersection of L with E. Let L be the line through R and O. Then L intersects E at R, O, and a third point. We denote that third point by $P \bigoplus Q$.

The composition law has the following properties: (a) If a line L intersects E at the (not necessarily distinct) points P, Q, R, then

$(P \bigoplus Q) \bigoplus R = O$.

(b) $P \bigoplus O = P$ for all $P \in E$.

(c) $P \bigoplus Q = Q \bigoplus P$ for all $P, Q \epsilon E$.

(d) Let $P \epsilon E$. There is a point of E, denoted by $\bigominus P$, satisfying

$P \bigoplus \bigominus P) = O$.

(e) Let $P, Q, R \in E$. Then

$(P \bigoplus Q) \bigoplus R = P \bigoplus (Q \bigoplus R)$.

Finite field Example

The formulas giving the group law on E are valid if the points have coordinates in any field, even if the geometric pictures don't make sense. For example, we can take points with coordinates in F_p. Example. The curve

$E : y^2 = x^3 - 5x + 8\ (mod 37)$

contains the points P = (6, 3) ϵ $E(F_{37})$ and Q = (9, 10) ϵ $E(F_{37})$.

Using the addition formulas, we can compute in E(F37):

2P=(35,11), 3P=(34,25),

4P=(8,6), 5P=(16,19),. . .
P+Q=(11,10),. . .

3P+4Q=(31,28),. . .

Substituting in each possible value $x = 0, 1, 2, ..., 36$ and checking if
$x^3 - 5x + 8$ is a square modulo 37, we find that $E(F_{37})$ consists of the following 45 points modulo 37.

Application Elliptic Curves are applicable for encryption, digital signatures, pseudo-random generators and other tasks. They are also used in several integer factorization algorithms that have applications in cryptography.

Example Discrete logarithm problem
Let E: represents elliptic curve over finite field. Let P, Q be points on elliptic curve. The problem is to find an integer k such that $Q = KP$.

Let Consider an elliptic curve given by the equation $y^2 = x^3 + 9x + 17(mod 23)$. Let $P = (4, 5)$ and $Q = (16, 5)$, Elliptic curve discrete logarithm problem is to find an integer k such that $kP = Q$.
The integer k can be found by repeated point doubling till we get Q.
Since $P = (16, 5)$, $2P = (20, 20)$, $3P = (14, 14)$, $4P = (19, 20)$, $6P = (7, 3)$, $7P = (8, 7)$, $9P = (4, 5) = Q$.
Thus $9P = Q$ and hence $k = 9$.

4 References

Joseph H.Silverman The Arithmetic of Elliptic Curves , Wikipedia