Elliptic Curve Cryptography

Sai Manoj

February 28, 2022

1 A Few Results

1.1 To Think About :

- An elliptic curve over the complex numbers C is isomorphic to a torus.
- Mordell-Weil theorem ;- If E is an elliptic curve define over Q, then $E(Q)$ is a finitely generated Abelian group.

1.2 Successive Doubling

Faster method for adding points on an elliptic curve is *successive doubling.*

$2P = P + P$
$4P = 2P + 2P$
$8P = 4P + 4P$
$16P = 8P + 8P$

Consider the point $20P$, the binary representation of 20 is 10100.
So, we can write the following,

$20P = 1 \times 2^4 P + 0 \times 2^3 P + 1 \times 2^2 P + 0 \times 2^1 P + 0 \times 2^0 P$
$20P = 16P + 4P$

If we have the points P and kP, it is very difficult to determine the value of k. This is the **discrete logarithm problem** for elliptic curves and an application of elliptic curves in cryptography.

Example : - Let E be an elliptic curve defined as follows :
$y^2 = x^3 + 9x + 17$ over F_{23},
The given points are $P = (16, 5)$ and $Q = (4, 5)$. We have to find the value of k such that $Q = kP$. (Can also be expressed this way -> What is the discrete logarithm k of $Q = (4, 5)$ to the base $P = (16, 5)$?)

(NAIVE) One method to find k is to compute multiples of P until Q is found.

$P = (16, 5)$
$2P = (20, 20)$
$3P = (14, 14)$
$4P = (19, 20)$
$5P = (13, 10)$
$6P = (7, 3)$
$7P = (8, 7)$
$8P = (12, 17)$
$9P = (4, 5)$

Since $9P = (4, 5) = Q$, the discrete logarithm of Q to the base P is $k = 9$.

In a real application, k would be large enough such that it would be infeasible to determine k in this manner.

2 Projective Space and the Point at Infinity

"Parallel lines meet at infinity"

Definition : - Let K be a field. The notation for a two-dimensional **projective space** is P_k^2. It is given by the equivalence classes of triples $(x : y : z)$ with $x, y, z \in K$ and at least one of x, y, z is non-zero.

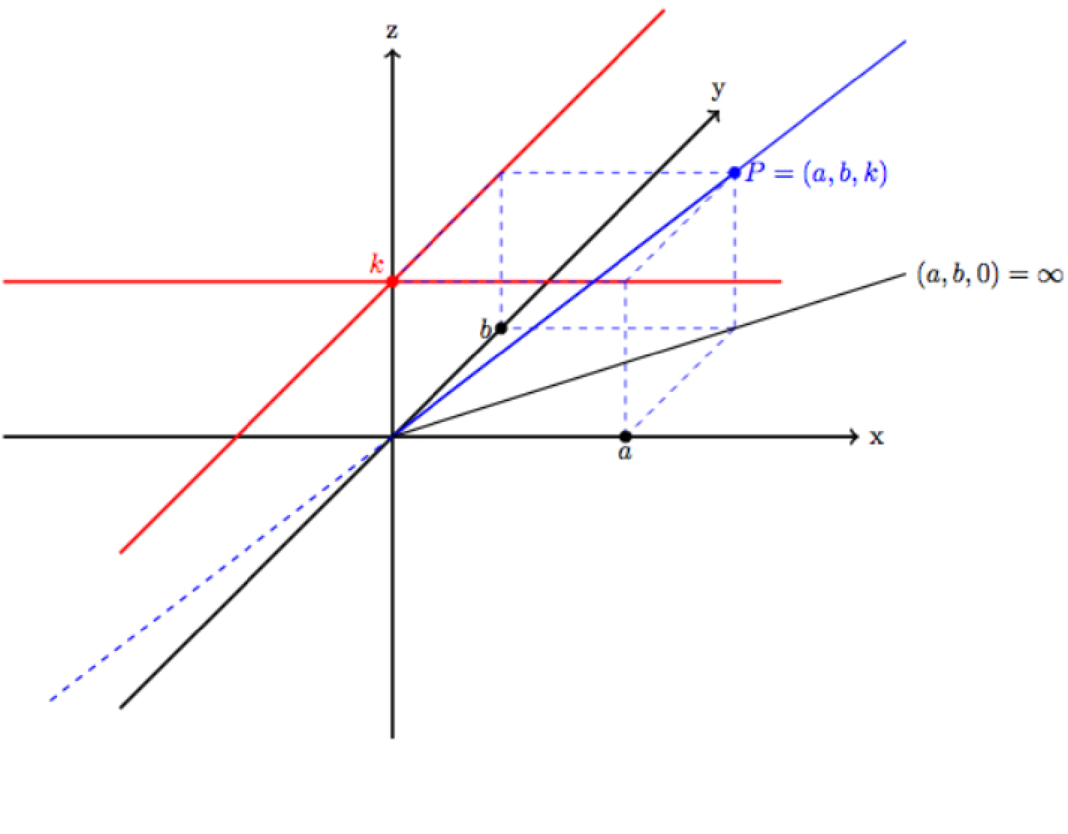
Note : - The equivalence class of a triple (x, y, z) is represented as (x : y : z).

Two triples $(x1, y1, z1), (x2, y2, z2)$ are said to be equivalent if
$(x1, y1, z1) \sim (\alpha \times x2, \alpha \times y2, \alpha \times z2)$ for some $\alpha \in K$.

Finite points from (x, y, z) can be generated as follows : $(x : y : z) = (x/z : y/z : 1)$ [Here, $z \neq 0$]. These are the **finite** points in P_K^2.

If $z = 0$, then the point is of the form $(x : y : 0)$.
Points of this form are called "points of infinity".

A representation of the projective plane P_K^2 in R^3



In the given diagram, $(a, b, k) = (a/k, b/k, 1)$ The projective space P_2 is the set of all rays from origin in R^3. For an example, $(1 : 2 : 3)$ and $(2, 4, 6)$ are the same point in P_K^2. The same ray passes through both the points, so they come under the same equivalence class.
So, $(0 : 0 : 0)$ is not a point in the projective space, because it does not correspond to any ray.

Definition : - The two-dimensional **affine plane** over K is denoted by
$A_K^2 = [(x, y) \in K \times K]$

Consider the following mapping $A_K^2 \mapsto P_K^2$
This is given by $(x, y) \mapsto (x : y : 1)$

This mapping gives us the relation between an affine plane and the projective space in the two-dimensional case. A projective space is an affine plane, with the addition of the line of infinity. When we take the complement of a line in the projective space, we get an affine plane associated with it (except when the line is the line of infinity).

We can consider the map backwards. i.e, $P_K^2 \mapsto A_K^2$ given by
$[x, y, z] \mapsto [x/z, y/z]$
Here we can clearly see that division is not defined when $z = 0$. So, the points on the line of infinity are not included in the affine plane.

Some more elementary definitions : -

A projective line (one - dimensional) is denoted by P_K^1. It can be represented by the equivalence class co-ordinates $[x_1, x_2]$.

The projective line may be identified with the line L extended by a point at infinity.

Cartesian coordinates label elements of the euclidean space R^n (which is an ordinary vector space), while homogeneous coordinates label elements of the projective space P_K^n.

Definition(Alternate) : -(An alternate definition from linear algebra) A projective space of dimension n is defined as the set of the **vector lines** (that is, vector subspaces of dimension one) in a vector space V of dimension $n + 1$.

2.1 COVERED

2.2 COVERED

2.3 How polynomials are related?

A polynomial is **homogeneous** of degree n if the sum of degrees of every variable in every algebraic term is the same. If a polynomial F is homogeneous of degree n, then $F(kx, ky, kz) = k^n F(x, y, z)$

A zero of F in P_K^2 does not depend on the choice of representative for the equivalence class, so the set of zeros of F in P_K^2 is well defined.

If $f(x, y)$ is a polynomial in x and y, then we can make it homogeneous by inserting appropriate powers of z. $F(x, y, z)$ is the homogenized version of $f(x, y)$.

Example : - Let $f(x, y) = y^2 - x^3 + Ax + B$, then $F(x, y, z)$ can be written as $F(x, y, z) = y^2z - x^3 + Axz^2 + Bz^3$. The degree of every term in this expression is 3.

$f(x, y) = F(x, y, 1)$

<u>**Parameterization**</u>
Consider two parallel lines, $y = mx + b1, y = mx + b2$
Then we can write the homogeneous forms of the two lines equations as follows
$y = mx + (b_1)z, \quad y = mx + (b_2)z$

Solving for the intersection of the given equations, we get
$y - mx = (b_1)z$
$y - mx = (b_2)z$
$(b_2 - b_1)z = 0$ ($b_1 \neq b_2$ because they are parallel and distinct lines)
This implies, $z = 0$ and $y = mx$. This is the solution of the homogenized equations.
The intersection of the lines would be $(x : mx : 0) = (1 : m : 0)$ for some slope m.

When slope of line is ∞ (the lines are parallel and vertical), the lines intersect at $(0 : 1 : 0)$ which is one of the points of infinity.

Consider the elliptic curve E given by the Weierstrass equation $y^2 = x^3 + Ax + B$. The homogeneous form of the elliptic curve can be written as $y^2z = x^3+Axz^2+Bz^3$. To find out the points of infinity on this elliptic curve, we set $z = 0$
This is because (x : y : 1) corresponds to the point (x : y), and the points of infinity are of the form (x : y : 0). We get $x^3 = 0$ which implies that $x = 0$.
Now, y is arbitrary, so the points of infinity are of the form (0 : y : 0). This can be expressed in equivalent form (0 : 1 : 0). This is the only point of infinity on E.

Observation : - (0 : 1 : 0) and (0 : -1 : 0) are the same, so the top and bottom of the Y-axis are the same.

2.4 Proof of Associativity

We prove that the operation of adding elliptic points is associative.

Outline of the proof : -

1. We start with an elliptic curve E and the points P, Q, R on it.
2. We try to compute the points $-((P + Q) + R)$ and $-(P + (Q + R))$.
3. We define the lines $l_1 = \overline{PQ}$, $l_2 = \overline{P + Q, \infty}$ and $l_3 = \overline{R, P + Q}$ to compute $-((P + Q) + R)$.
4. Similarly, we define lines $m_1 = \overline{QR}$, $m2 = \overline{Q + R, \infty}$ and $m_3 = \overline{P, Q + R}$
5. We are trying to prove that the points $P_{ij} = l_i \cap m_j$ all lie on the ellipse. Some are fairly easy to prove, but the one that we are interested in is P_{33}. An upcoming theorem lets us prove that P_{33} will lie on E given that all the other eight points lie on the curve.

Some things to keep in mind while continuing with the proof : -

1. Some of the points P_{ij} could be at infinity, so we need to use projective coordinates.
2. A line could be tangent to E, which means that two P_{ij} could be equal. Therefore, we need a careful definition of the order to which a line intersects a curve.
3. Two of the lines could be equal. Dealing with these technicalities takes up most of our attention during the proof.

PART - 1

Lemma : - Let $G(u,v)$ be a nonzero homogeneous polynomial and let $(u_0, v_0) \in P_K^1$. Then there exists an integer $k >= 0$ and a polynomial $H(u,v) \neq 0$ such that

$$G(u,v) = (v_0 u - u_0 v)^k H(u,v)$$

Proof Outline

1. From $G(u, v_0)$, factor out the largest power $u - u_0$, so we can write it as $g(u) = (u - u_0)^k h(u)$. $[g(u) = G(u, v_0)$
2. Here, k is an integer, and h is a polynomial of degree $m - k$
3. Let $H(u,v) = \dfrac{v^{m-k}}{v_0^m} h(uv_0/v)$, this is a homogeneous polynomial of degree $m - k$
4. Substituting this value into the equation containing $g(u)$, and writing that as $G(u, v_0$, we get $G(u,v) = (v_0 u - u_0 v)^k H(u,v)$

Let $f(x,y) = 0$ describe a curve C in the affine plane. The parametric forms of x, y can be written as
$x = a_1 t + b$, $y = a_2 t + b$ [Line L with parameter t]
So, $f(t) = f(a_1 t + b_1, a_2 t + b_2)$

Then L intersects C when $t = t_0$ if $(f(t_0) = 0$. We also say that L intersects the curve C to the order n if $(t - t_0)^n$ is the highest power of $(t - t_0)$ that divides $f(t)$.

The homogeneous version of the above statement can be expressed as follows : - Let $\tilde{F}(u,v) = F(a_1 u + b_1 v, a_2 u + b_2 v, a_3 u + b_3 v)$, then L intersects C to order n at the point $P = (x0 : y0 : z0)$ corresponding to $(u : v) = (u_0 : v_0)$ if $v_0 u - u_0 v)^n$ is the highest power of $(v_0 u - u_0 v)$ diving $F(u,v)$.
This is denoted by $ord_{L,P}(F) = n$.

If $\tilde{F}$ is identically 0, then it is defined that $ord_{L,P}(F) = \infty$.

The advantage of the homogeneous formulation is that it allows us to treat the points at infinity along with the finite points in a uniform manner

PART - 2

Lemma : - Let L_1, L_2 be lines intersecting in a point P, and let L_1 be the linear polynomial defining L_1 and $L_2(x, y, z)$ be the linear polynomial defining L_2. Then $ord_{L_1,P}(L_2) = 1$ unless $L_1(x, y, z) = \alpha L_2(x, y, z)$ for some constant α, in which case $ord_{L_1,P}(L_2) = \infty$

Proof Outline

1. We substitute the parameterization forL_1 into $L_2(x, y, z)$ to get $\tilde{L_2}$. This is a linear expression in (u, v)
2. Let the point P correspond to $(u_0 : v_0)$. Since L_1 and L_2 intersect at P, $\tilde{L_2}(u_0, v_0) = 0$
3. This implies that $\tilde{L_2}(u, v) = \beta(v_0 u - u_0 v)$ [because they are lines, order cannot be greater than 1]
4. If the constant β is not zero, the order is 1.
5. If $\beta = 0$, then all the points of L_1 lie on L_2. So, they are linearly dependent.
6. Doubt : - How is the order ∞ if the lines are coincident?

PART - 3

Definition : - A curve C in P_K^2 defined by $F(x, y, z) = 0$ is said to be **nonsingular** at a point P if at least one of the partial derivatives F_x, F_y, F_z is non-zero.

Definition : - If P is a nonsingular point of a curve $F(x, y, z) = 0$, then the tangent line at P is $F_x(P)x + F_y(P)y + F_z(P)z = 0$.

Consider the curve $F(x, y, z) = y^2 z - x^3$ Any line through the point $(0 : 0 : 1)$ can be written as $x = au, y = bu, z = v$ where $(u : v) = (0 : 1)$. The parameterized form of $F(x, y, z)$ is $\tilde{F}(u, v) = u^2(b^2 v - a^3 u)$. So every line through P intersects C to order at least 2. The line with b = 0, which is the best choice for the tangent at P, intersects C to order 3. The point (0, 0) is a singularity of the curve, which is why the intersections at P have higher orders than might be expected. This is a situation we usually want to avoid.

PART - 4

Lemma : - Let $F(x, y, z) = 0$ define a curve C. If P is a nonsingular point of C, then there is exactly one line in P_K^2 that intersects C to order at least 2,and it is the tangent to C at P.

Proof Outline : -

1. Let L be a line intersecting C to order $k >= 1$
2. Parameterize L and substitute into F. This yields F(u, v).
3. Let $(u_0 : v_0)$ correspond to P.
4. Then $\tilde{F} = (v_0 u - u_0 v)^k H(u, v)$
5. We compute partial derivatives with respect to u, v