Elliptic Curve Cryptography

Nancy Mathur

A dissertation submitted for the partial fulfilment of
BS-MS dual degree in Science

Indian Institute of Science Education and Research Mohali
April 2014

Certificate of Examination

This is to certify that the dissertation titled ” Elliptic Curve Cryptography” submitted by Miss Nancy Mathur (Reg. No. MS09086) for the partial fulfillment of BS-MS dual degree programme of the Institute, has been examined by the thesis committee duly appointed by the Institute. The committee finds the work done by the candidate satisfactory and recommends that the report be accepted.

Dr. Amit Kulshrestha	Dr. Chandrakant S Aribam	Prof. Kapil H. Paranjape
		(Supervisor)

Dated: April 25th 2014

Declaration

The work presented in this dissertation has been carried out by me under the guidance of Prof. Kapil H. Paranjape at the Indian Institute of Science Education and Research Mohali.

This work has not been submitted in part or in full for a degree, a diploma, or a fellowship to any other university or institute. Whenever contributions of others are involved, every effort is made to indicate this clearly, with due acknowledgement of collaborative research and discussions. This thesis is a bonafide record of original work done by me and all sources listed within have been detailed in the bibliography.

Acknowledgment

I would like to thank my supervisor Prof. Kapil Hari Paranjape for guiding me, encouraging me and allowing me to explore the subject with out any restriction. I would also like to thank my committee members, Dr. Amit Kulshrestha, Dr. Chandrakant Aribam for giving me valuable suggestions.

Nancy Mathur
MS09086

Contents

Chapter 1

An Introduction to Elliptic Curve

1.1 Definition of an Elliptic Curve

An elliptic curve is a non-singular cubic curve of genus one in two variables over a field K with points having coordinates in field K together with a special point, point at infinity $\mathcal{O}$.

Definition 1.1 *An Elliptic curve E defined over a field K is the set of points $(x, y) \in \bar{K} \times \bar{K}$ satisfying a Tate Weierstrass equation of the form;*

$$E : y^2 + a_1xy + a_3y = x_3 + a_2x^2 + a_4x + a_6 \tag{1.1}$$

along with a point at infinity $\mathcal{O}$ and where a_1, a_2, a_3, a_4, $a_6 \in K$.

If k is a subfield of K, then

$$E(k) = \mathcal{O} \cup \left\{(x, y) \in k \times k \mid y^2 + a_1xy + a_3y = x_3 + a_2x^2 + a_4x + a_6\right\}$$

If the characteristic of field is different than 2 or 3, then by the change of variables we can simplify the equation (1.1) of an Elliptic curve.

1. when char$(K) \neq 2$, then we can divide by 2 and complete the square on the left hand side of the equation (1.1),

   $$\left(y + \frac{a_1x}{2} + \frac{a_3}{2}\right)^2 = x^3 + \left(a_2 + \frac{a_1^2}{4}\right)x^2 + \left(a_4 + \frac{a_1a_3}{2}\right)x + \left(a_6 + \frac{a_3^2}{4}\right)$$

   Then after putting $Y = \left(y + \frac{a_1x}{2} + \frac{a_3}{2}\right)^2$, $A = \left(a_2 + \frac{a_1^2}{4}\right)$, $B = \left(a_4 + \frac{a_1a_3}{2}\right)$ and $C = \left(a_6 + \frac{a_3^2}{4}\right)$. The equation (1.1) can be written as;

   $$E : Y^2 = X^3 + AX^2 + BX + C \qquad char(K) \neq 2 \tag{1.2}$$

where A, B, C are constants and lie in K.

2. If char$(K) \neq 2, 3$. Then by putting $X = x_1 - \frac{A}{3}$ in equation (1.2), we get

$$\begin{aligned} Y^2 &= \left(x_1 - \frac{A}{3}\right)^3 + A\left(x_1 - \frac{A}{3}\right)^2 + B\left(x_1 - \frac{A}{3}\right) + C \\ &= x_1^3 - \frac{A^3}{27} - x_1^2 A + \frac{x_1 A^2}{3} + x_1^2 A - \frac{A^3}{9} - \frac{2A^2 x_1}{3} + Bx_1 - \frac{AB}{3} + C \\ &= x_1^3 + x_1\left(\frac{A^2}{3} - \frac{2A^2}{3} + B\right) + \left(C - \frac{A^3}{27} - \frac{AB}{3} - \frac{A^3}{9}\right) \end{aligned}$$

For some constants A_1 and B_1 we can write the equation as

$$E : Y^2 = x_1^3 + A_1 x_1 + B_1 \qquad char(K) \neq 2, 3 \tag{1.3}$$

where $A_1, B_1 \in K$ and are constants.

Definition 1.2 *An elliptic curve $E : y^2 = x^3 + Ax + C$ is non-singular if and only if the polynomial in x has distinct roots i.e. it's discriminant $\Delta = -16(4a^3 + 27b^2)$ is non-zero, otherwise we call it a singular curve.*

The rational points on singular cubic curves and on non-singular cubic curves behave differently. The set of rational points on a non-singular cubic curve is finitely generated but the group of rational points on singular curve is not finitely generated.

1.2 Weierstrass Normal Form

A cubic curve is said to be in Weierstrass form if it has the form

$$y^2 = 4x^3 - g_2 x - g_3$$

or more generally,

$$y^2 = x^3 + Ax^2 + Bx + C$$

Now, we will show that every cubic with a rational point can be transformed into a Weierstrass normal form and the rational points on the original curve corresponds to rational points on the transformed curve.

Let C be any cubic curve

$$C : ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0$$

Here, we want to choose the axis in the projective plane such that the equation of the curve will have simple form. For this, let $\mathcal{O}$ be a given rational point on the curve C, and take $Z = 0$ to be the tangent line at the point $\mathcal{O}$. Then the tangent line intersects the curve at another point and take $X = 0$ be the tangent at that point. After that choose $Y = 0$ be any line passing through the point $\mathcal{O}$ where $\mathcal{O}$ is not an inflection point, In the case of an inflection point, we take $X = 0$ to be any line not containing $\mathcal{O}$. After choosing the axis let $x = \dfrac{X}{Z}$ and $y = \dfrac{Y}{Z}$. This transformation is called projective transformation.

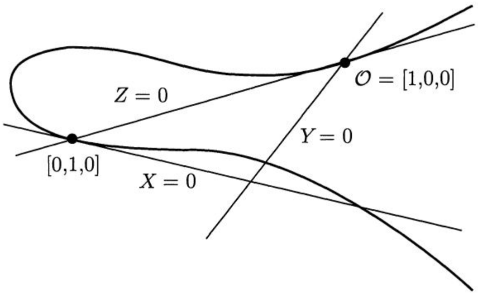

Figure 1.1: Projective transformation

After transforming the cubic by projective transformation we get the curve,

$$C : AX^3+BX^2Y+CXY^2+DY^3+EX^2Z+FXYZ+GY^2Z+HXZ^2+IYZ^2+JZ^3 = 0 = f(X,Y,Z)$$

As $\mathcal{O} = [1,0,0]$ is a point on the curve C so $A = 0$ and the point $[0,1,0] \in C$ so $D = 0$. Then,

$$\frac{df}{dX}[1,0,0] = 0$$
$$\frac{df}{dY}[1,0,0] = B$$
$$\frac{df}{dZ}[1,0,0] = E$$

Therefore, the equation of the tangent at the point $[1,0,0]$ is given by

$$(X-1)\frac{df}{dX}[1,0,0] + Y\frac{df}{dY}[1,0,0] + Z\frac{df}{dZ}[1,0,0] = 0$$

Since, we know that $Z = 0$ is also the equation of tangent. By comparing the coefficients of the equation we get $B = 0$. Thus, the equation for C becomes;

$$x_1 y_1^2 + (ax_1 + b)y_1 = cx_1^2 + dx_1 + e.$$

Now, multiply by x_1

$$(x_1 y_1)^2 + (ax_1 + b)x_1 y_1 = cx_1^3 + dx_1^2 + ex_1.$$

Let $x_1 y_1 = y_2$ to obtain,

$$y_2^2 + (ax_1 + b)y_2 = cx_1^3 + dx_1^2 + ex_1.$$

After putting $y_2 = y_3 - \frac{1}{2}(ax_1 + b)$ we get;

$$y_3^2 - \frac{1}{4}(ax_1 + b)^2 = cx_1^3 + dx_1^2 + ex_1.$$

Now, let $x_1 = \lambda X$ and $y_3 = \lambda^2 Y$ to get

$$\lambda^4 Y^2 - \frac{(a\lambda X + b)^2}{4} = \lambda^4 X^3 - d\lambda^2 X^2 + E\lambda X$$

After cancelling λ^4 and rearranging the above equation, the equation becomes;

$$Y^2 = X^3 + AX^2 + BX + C$$

Example 1.3 : Consider the cubic curve

$$u^3 + v^3 = \alpha$$

where α is a rational number.

Let $u = \frac{U}{W}$ and $v = \frac{V}{W}$. Then homogeneous form of the curve is $U^3 + V^3 = \alpha W^3$ and it contains the rational point $[1, -1, 0]$. The point $[1, -1, 0]$ is an inflection point as $\alpha W^3 = 0$. For F: $U^3 + V^3 - \alpha W^3 = 0$,

$$\frac{dF}{du} = 3 \quad ; \quad \frac{dF}{dV} = 3; \qquad \frac{dF}{dW} = 0;$$

Then the equation of tangent at this rational point is $3(U - 1) + 3(V + 1) = 0 \Rightarrow U + V = 0$. By substituting $U + V = Z$ in the equation $U^3 + V^3 - \alpha W^3 = 0$, we get $Z^3 - 3VZ^2 + 3V^2 Z - \alpha W^3 = 0$. Put $Z = 1$, to get $1 - 3V + 3V^2 = \alpha W^3$. After multiplying α^2 on both sides of the equation and then multiplying by $(12)^3$ on both sides, we get;

$$(36\alpha(2V-1))^2 + 432\alpha^2 = (12\alpha W)^3$$

Now, let $X = 12\alpha W$ and $Y = (36\alpha(2V-1))$. Then the equation becomes;

$$Y^2 = X^3 - 432\alpha^2$$

where $X = \dfrac{12\alpha}{u+v}$ and $Y = 36\alpha\dfrac{u-v}{u+v}$.

1.3 Why Elliptic Curves are called Elliptic

In this section, we will show why Elliptic curves are called Elliptic and how the problem of parametrising the arc-length of an ellipse leads to elliptic curves.
Let E be an Elliptic curve, then by definition it is the set of solutions (x, y) to an equation of the form:

$$y^2 = x^3 + Ax^2 + Bx + C\ .$$

The equation of an Ellipse is;

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$$

where $a > b$. Then, to calculate the arc-length of the ellipse, first express the ellipse equation in terms of x, and then calculate it's derivative. $\dfrac{dy}{dx} = -\dfrac{b}{a^2}\dfrac{x}{\sqrt{1-\dfrac{x^2}{a^2}}}$.

Let L be the arc-length of an ellipse then,

$$\begin{aligned}
L &= \int \sqrt{1 + \left(\frac{dy}{dx}\right)^2}\ dx \\
&= \int \sqrt{1 + \left(\frac{b^2x^2}{a^2(a^2-x^2)}\right)}\ dx \\
&= \int \sqrt{\frac{a^4 - (a^2-b^2)x^2}{a^2 - x^2}}\ dx \\
&= \int \sqrt{\frac{1 - (1 - b^2/a^2)(x/a)^2}{1 - (x/a)^2}}\ dx \quad \textit{(dividing by } a^2\textit{)}
\end{aligned}$$

Now put $t = x/a$ and $k = 1 - (b^2/a^2)$, then $dt = dx/a$

$$\begin{aligned} L &= \int \sqrt{\frac{1-k^2t^2}{1-t^2}}\, dt \\ &= \int \frac{1-k^2}{\sqrt{(1-t^2)(1-k^2t^2)}}\, dt \end{aligned}$$

Indefinite integrals of the type $\int R(x;y)dx$, where $R(x;y)$ is a rational function of x and y and y^2 is a polynomial of degree three or four in x without multiple roots, are called *elliptic integrals.* The elliptic integrals are multiple- valued functions, their inverse function is a single-valued meromorphic function on the whole complex plane. The elliptic functions are doubly periodic with two periods ω_1 and ω_2, where $\frac{\omega_1}{\omega_2} \neq real.$

1.4 Group Law on Elliptic Curve

Elliptic Curves have the property that given any two points or even one point, we can define one another point. The basic idea behind the addition on elliptic curve is that a line will intersect the curve three times by Bezout's theorem. Moreover, all three points of intersection of the line and an elliptic curve need not to be distinct. So, for given two points say P and Q we can draw a line passing through P and Q and can find the third point, which is the intersection point of the line with a curve. In the case of a given single point say P we can draw a tangent line at P, here tangent line meet the curve with multiplicity two at the point P and the third point is the intersection point of the elliptic curve with the tangent line at the point P. But we can see that the set of points obtained by the intersection of the line and a curve is not a group as it does not have identity element. Therefore, the first thing we need to do to make it into a group is to find the identity element. For that we define $\mathcal{O}$ (the point of infinity) to act as the zero or the identity element of the group and group law by $+$.

Definition 1.4 **Group Law:** *Let P and $Q \in E$, and l be the line passing through P and Q (If $P = Q$, then l be the tangent line to E at P), and $P * Q$ be the third point of intersection of l with the curve E. Let $\acute{l}$ be the line through $P * Q$ and $\mathcal{O}$. Then $\acute{l}$ intersects E at $P * Q$, $\mathcal{O}$ and a third intersection point $R = P + Q$. Thus $P + Q = \mathcal{O} * (P * Q)$.*

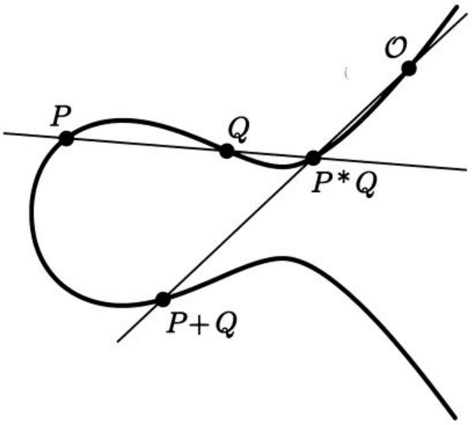

Figure 1.2: The Group Law on an Elliptic Curve

Theorem 1.5 *The points on elliptic curve E form an additive abelian group as it satisfies the following properties with $\mathcal{O}$ acting as the identity element;*

1. ***Commutativity*** *: $P+Q=Q+P$, $\forall P,Q \in E$.*

2. ***Existence of identity****: $P+\mathcal{O}=P$, $\forall P \in E$.*

3. ***Existence of inverse****: Given $Q \in E$, $\exists -Q \in E$ such that $Q+(-Q)=\mathcal{O}$.*

4. ***Associativity****: $(P+Q)+R=P+(Q+R)$, $\forall P,Q,R \in E$.*

Proof

1. The commutativity for elliptic curve is trivial as line passing through the point P and Q is same as the line passing through the points Q and P. Therefore, $P+Q=Q+P$, $\forall P,Q \in E$.

2. For verifying $\mathcal{O}$ as the identity element, first draw a line passing through P and $\mathcal{O}$. Then from the intersection of the line and curve we get a third intersection point $P*\mathcal{O}$. Now join that intersection point with $\mathcal{O}$ and we get $(P*\mathcal{O})*\mathcal{O}$ and $(P*\mathcal{O})*\mathcal{O}=P$ as a third intersection point. Hence proved.

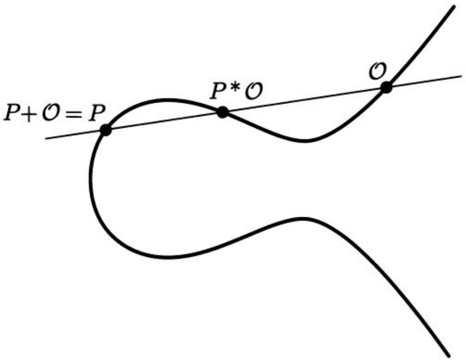

Figure 1.3: $\mathcal{O}$ is the Identity element

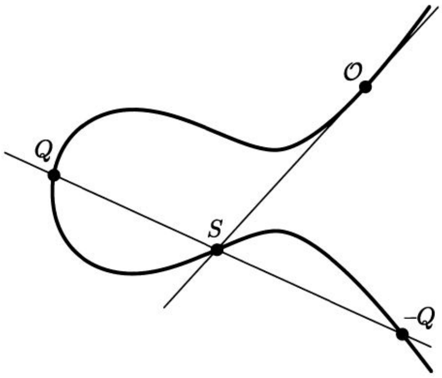

Figure 1.4: Inverse of a point

3. To prove existence of inverse, we draw a tangent line to the cubic at $\mathcal{O}$ and let S be the point where the tangent line meet the curve. Then for a given point Q, draw a line passing through Q and S. Then the third intersection point $Q * S$, which we get is equal to $-Q$. To prove that draw a line through Q and $-Q$, then the third intersection point of the line and the curve is S. After that join S and $\mathcal{O}$ and then the third intersection point is $S * \mathcal{O}$ and here $S * \mathcal{O} = \mathcal{O}$. The reason is that the line passing through S and $\mathcal{O}$ is tangent to the cubic at $\mathcal{O}$, so it will meet the cubic curve twice at $\mathcal{O}$ and once at S. Therefore, $Q + (-Q) = \mathcal{O}$.

4. To prove that associativity holds, we will show that $(P+Q)*R = P*(Q+R)$ where $P, Q, R \in E$. To get $(P+Q)*R$, start with two points P and Q, draw a line passing through P and Q and get the third intersection point $P*Q$. After

that draw a line passing through $P * Q$ and $\mathcal{O}$, the third intersection point which we get is $(P * Q) * \mathcal{O} = P + Q$. Now, to add $P + Q$ and R. We draw a line passing from $P + Q$ and R and the line meets the curve at $(P + Q) * R$. Then join a line passing through $(P+Q)*R$ and $\mathcal{O}$ to get a third intersection point $(P+Q)+R$. Now, for $P*(Q+R)$, first take two points Q and R, draw a line through them and take the third intersection point $Q * R$, now to get $Q+R$, draw a line passing through $Q*R$ and $\mathcal{O}$ and this line will intersect the curve at third point $(Q * R) * \mathcal{O}$ which is $Q + R$. Now join $Q + R$ to P, to get third intersection point $P * (Q + R)$. $P, Q, R, P * Q, Q * R, Q + R, \mathcal{O}$ all these points lie on the curve. The intersection of the line through P and $Q+R$, and the line through $P+Q$ and R lie on the curve. Thus,$(P+Q)*R = P*(Q+R)$. Hence, we have proved that $(P + Q) + R = P + (Q + R)$, $\forall P, Q, R \in E$.

□

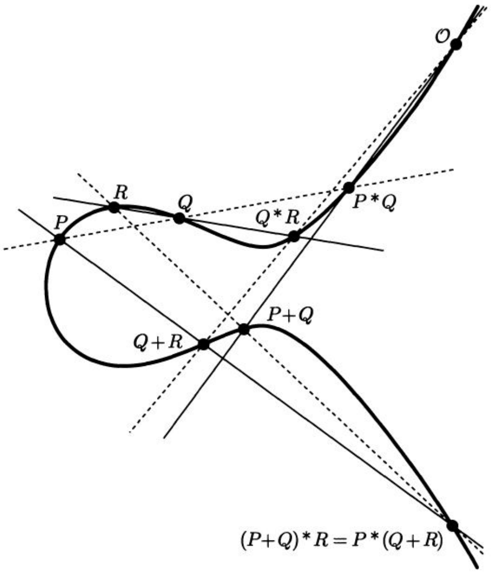

Figure 1.5: Associative Law

Theorem 1.6 *Let $E : y^2 = x^3+Ax^2+Bx+C$ be an elliptic curve. Let $P = (x_1, y_1)$and $Q = (x_2, y_2)$ be two points on the curve with $P, Q \neq \mathcal{O}$. Then $P+Q = R = (x_3, -y_3)$ as follows;*

1. *If $x_1 \neq x_2$, then $x_3 = m^2 - x_1 - x_2$, $\quad -y_3 = m(x_1 - x_3) - y_1$, $\quad$ where $m = \dfrac{y_2 - y_1}{x_2 - x_1}$.*

2. *If* $x_1 = x_2$ *but* $y_1 \neq y_2$*, then* $P + Q = \mathcal{O}$*.*

3. *If* $P = Q$ *and* $y_1 \neq 0$*, then*
   $$x_3 = m^2 - 2x_1, \quad -y_3 = m(x_1 - x_3) - y_1, \quad \textit{where } m = \frac{3x_1^2 + Ax_1 + B}{2y_1}.$$

4. *If* $P = Q$ *and* $y_1 = 0$*, then* $P + Q = \mathcal{O}$*.*

Proof Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be two points on elliptic curve E in the Weierstrass form. An elliptic curve in Weierstrass form is symmetric about the $x-$axis. So to find $P + Q$,

1. Draw a line l passing through P and Q.
2. Line l will intersect the curve at the third point $P * Q = (x_3, y_3)$.
3. Then reflect the point $P * Q$ about the $x-$axis.
4. So, $P + Q = R = (x_3, -y_3)$

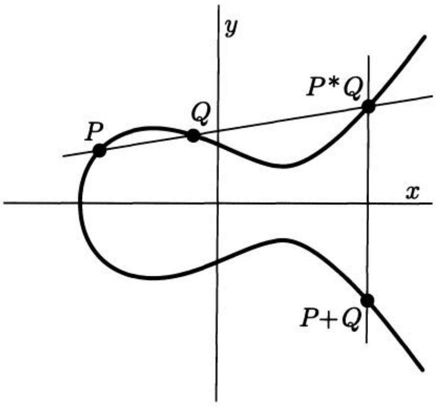

Figure 1.6: Addition of points on an Elliptic curve in the Weierstrass form

Moreover, the negative of a point can be obtained by reflecting the point about the $x-$axis. So, if we have a point $P = (x_1, y_1)$, then $-P = (x_1, -y_1)$. It is due to the fact that the line through P and $-P$ is a vertical line, so the third point of intersection is the point at infinity. And the line passing through $\mathcal{O}$ and $\mathcal{O}$ again meets the curve at $\mathcal{O}$, that's because the line at infinity meets the curve with a multiplicity of three at $\mathcal{O}$. Therefore, $P + (-P) = \mathcal{O}$.

Let $P = (x_1, y_1)$, $Q = (x_2, y_2)$ and $P * Q = (x_3, y_3)$. Let $l : y = \lambda x + \upsilon$ be the equation of the line joining the points $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ and λ be the slope of the line l.

1. Assume $x_1 \neq x_2$, then $\lambda = \dfrac{y_2 - y_1}{x_2 - x_1}$. As P and Q lies on the line l so $\upsilon = y_1 - \lambda x_1 = y_2 - \lambda x_2$. The line l intersects the curve at three points and we know that two of them are P and Q as they lie on both the curve E and the line l, so to find the third point of intersection, put the equation of the line l in the curve E. From which we get

$$y^2 = (\lambda x + \upsilon)^2 = x^3 + Ax^2 + Bx + C.$$

This equation can be arranged into;

$$x^3 + (A - \lambda^2)x^2 + (B - 2\lambda\upsilon)x + (C - \upsilon^2) = 0.$$

The three roots of this cubic equation in x are x_1, x_2, x_3, which are the $x-$coordinates of the three points of intersection. Thus, we can write the cubic in this form

$$\begin{aligned} x^3 + (A - \lambda^2)x^2 + (B - 2\lambda\upsilon)x + (C - \upsilon^2) &= (x - x_1)(x - x_2)(x - x_3) \\ &= x^3 - (x_1 + x_2 + x_3)x^3 + \dots. \end{aligned}$$

Now, to get x_3 equate the coefficients of x^2 on both sides,

$$x_1 + x_2 + x_3 = -(A - \lambda^2) \Longrightarrow x_3 = \lambda^2 - A - x_1 - x_2.$$

Then, by plugging the value of x_3 into the equation of line l, we get

$$\begin{aligned} y_3 = \lambda x_3 + \upsilon = \lambda(x_3) + (y_1 - \lambda x_1) &= \lambda(x_3) + (y_2 - \lambda x_2) \\ = \lambda(x_3 - x_1) + y_1 &= \lambda(x_3 - x_2) + y_2. \end{aligned}$$

To get the $y-$coordinate of $P + Q = R$, reflect (x_3, y_3) about the $x-$axis. So,

$$R = (x_3, -y_3) = (\lambda^2 - A - x_1 - x_2,\ \lambda(x_1 - x_3) - y_1).$$

2. If $x_1 = x_2$ but $y_1 \neq y_2$ then l is a vertical line and third intersection of a vertical line with curve is point at infinity. The reflection of $\mathcal{O}$ across the axis gives $\mathcal{O}$ again. Hence, $P + Q = \mathcal{O}$.

3. If on the curve $y^2 = x^3 + Ax^2 + Bx + C = f(x)$, $P = Q = (x_1, y_1)$ and $y_1 \neq 0$ then the line l is a tangent line at point P with slope

$$\lambda = \frac{dy}{dx} = \frac{f'(x)}{2y} = \left(\frac{3x_1^2 + 2Ax_1 + B}{2y_1}\right)^2$$

Then, substitute the value of λ into $R = (x_3, -y_3) = (\lambda^2 - A - x_1 - x_2,\ \lambda(x_1 - x_3) - y_1)$ to get $P + P = 2P = (x_3, -y_3)$, i.e.,

$$\begin{aligned} x\ coordinate\ of\ 2P = 2(x_1, y_1) &= \lambda^2 - 2x_1 \\ &= \frac{f'(x_1)}{2y_1} \\ &= \left(\frac{3x_1^2 + 2Ax_1 + B}{2y_1}\right)^2 \\ &= \left(\frac{x^4 - 2Bx - 8Cx + B^2 - 4Ac}{4x^3 + 4Ax^2 + 4Bx + 4C}\right) \end{aligned}$$

$\because y_1^2 = x_1^3 + 2Ax_1^2 + Bx_1 + C.$
Here, y coordinate of $2P = \lambda(x_1 - x_3) - y_1$.

Moreover, formula for $x(2P)$ is called the *duplication formula.*

4. If $P = Q$ and $y_1 = 0$, then the line l is the vertical line. Hence, $P + Q = \mathcal{O}$.

□

1.5 Divisors

Divisors can be consider as a device for keeping track of zeroes and poles of a function.

Definition 1.7 *A divisor group denoted by $Div(E)$ is a free abelian group generated by the points of the elliptic curve E. The divisor $D \in Div(E)$ is defined as*

$$D = \sum_{P \in E} n_P[P],$$

where $n_P \in \mathbb{Z}$ and $n_P = 0$ for all but finitely many $P \in E$. (The brackets [ ] denotes the elements of $Div(E)$)

- The degree of a divisor D is given by

$$\text{degD} = \sum_{P \in E} n_P.$$

- The sum of a divisor D is given by

$$\text{Sum(D)} = \sum_{P \in E} n_P P.$$

The divisor of degree 0 forms a subgroup of $Div(E)$ and it's denoted by $Div^0(E)$.

$$Div^0(E) = \{D \in Div(E) : degD = 0\}.$$

Polynomial and Rational Functions

Definition 1.8 *The polynomials on elliptic curve $E : y^2 = x^3 + ax + b$ are the elements of the quotient ring and is given by*

$$K[E] = K[x, y]/(y^2 - x^3 - ax - b)$$

where $(y^2 - x^3 - ax - b)$ is an ideal generated by the polynomial $y^2 - x^3 - ax - b \in K[x, y]$. Thus we can say that polynomials on E are the elements of $K[x, y]$, the ring of polynomials in x and y.

Whenever we have a polynomial $f \in K[E]$ with power of y greater then one, then a power of y greater than one that appears in f can be replaced by the term $x^3 + ax + b$ without changing the equivalence class of f. So f can be written in canonical form, $f(x, y) = v(x) + yw(x)$ with $v, w \in K[x]$ i.e. polynomials in one variable.

Definition 1.9 *Let $f \in K[E]$ be the polynomial in canonical form $f(x, y) = v(x) + yw(x)$. Then conjugate of f is defined as $f(x, y) := v(x) - yw(x)$ and is denoted by $\bar{f}$. The norm of f is defined by $N_f := f\overline{f}$. So,*

$$\begin{aligned} N_f &= (v(x) + yw(x))(v(x) - yw(x)) \\ &= v^2(x) - y^2 w^2(x) \end{aligned}$$

As, $y^2 = x^3 + ax + b$ so f can be written as $N_f = v^2(x) - s(x)w^2(x)$, so $N_f \in K[x]$ i.e. a polynomial in only one variable.

Definition 1.10 *:*
A rational function on an elliptic curve E over a field K is an element of the quotient ring denoted by $K(E)$ of the integral domain

$$K[x, y]/(y^2 - x^3 - ax - b).$$

The rational function $r \in K(E)$ is of the form $\dfrac{f(P)}{g(P)}$ at a finite point $P \in E$ where f and $g \in K[E]$ and $g(P) \neq 0$. In the case when $g(P) = 0$ at a point P then we denote $r(P) = \mathcal{O}$.

Theorem 1.11 *For each $P \in E$, $\exists$ a rational function u, zero at P and with the property that if r is any rational function not identically zero then $r = u^d s$ for some integer d and some rational function s that is finite and non-zero at P. Furthermore, the number d does not depend on the choice of the function u.*

Proof There are three cases:

1. Assume P is not a point of order 2 and that P is not $\mathcal{O}$. For $P = (a, b)$, we will show that there exist a rational function $u(x, y) = x - a$. Suppose r has a zero at P then $r = \frac{f}{g}$ with $f(P) = 0$ and $g(P) \neq 0$. If we can decompose $f = u^d s$ in the above equation, then we can simply divide by g and get the corresponding result for r.
   Let $f(x, y) = v(x) + yw(x)$.If $\overline{f}(P) = 0$, then since the characteristic is not two and $y(P) = b \neq 0$, we can solve the linear equations

   $$v(a) + bw(a) = 0$$
   $$v(a) - bw(a) = 0,$$

   to conclude that $v(a) = 0$,$w(a) = 0$. Since v and w are polynomials in one variable, we get

   $$f(x, y) = (x - a)s_1(x, y)$$

   for some polynomial s_1. If $\overline{f}(P) \neq 0$ then we can multiply f by $(\overline{f})/(\overline{f})$ to get

   $$f(x, y) = \frac{v^2(x) - s(x)w^2(x)}{\overline{f}(x, y)},$$

where $s(x) = x^3 + Ax + B$ Now $f(P) = 0$ *and* $\overline{f} \neq 0$ implies

$$v^2(x) - s(x)w^2(x) = 0 \; for \; x = a,$$

and the polynomial on the left is a polynomial in one variable. Again we conclude that

$$f(x) = (x - a).s_1(x, y),$$

where this time s_1 is some rational functional that is finite at P. In either case, if $s_1(P) = 0$, we can continue the process. If $f(x, y) = (x - a)^d s_1(x, y)$, then $N(f)(x) = (x - a)^{2d} N(s_1)(x)$. We know that $N(s_1)(x)$ does not have a pole at P so $2d$ must be less than the degree of $N(f)$ as a function of x alone. Thus if r has a zero at $P = (a, b)$, then we can take $u(x, y) = x - a$. If r has a pole at P, then $1/r$ has a zero at P, and u is same with negative d. If r has neither a zero nor a pole at P, then we can take $d = 0$ and $s = r$ and in the generic case we take $u(x, y) = x - a$.

2. Assume that P is a point of order two say $P = (w_1, 0)$. We will show that we can take $u(x, y) = y$ in this case. As above if r has a zero at P, we can assume $r = f/g$ and $f(P) = 0$. Now $f(w_1, 0)$ implies $v(w_1) = 0$ where $f(x, y) = v(x) + yw(x)$. Hence we can write $v(x) = (x - w_1)v_1(x)$ for some polynomial v_1. Since the roots of $s(x)$ are distinct, $(x - w_2)$ and $(x - w_3)$ do not vanish at P, so we get

$$\begin{aligned} f(x, y) &= (x - w_1)v_1(x) + yw(x) \\ &= \frac{(x - w_1)(x - w_2)(x - w_3)v_1(x) + yw_1(x)}{(x - w_2)(x - w_3)} \\ &= \frac{y^2 v_1(x) + yw_1(x)}{(x - w_2)(x - w_3)} \\ &= y\left[\frac{yv_1(x) + w_1(x)}{(x - w_2)(x - w_3)}\right] \end{aligned}$$

where $w_1(x) = (x - w_2)(x - w_3)w(x)$. Now if the function in brackets still vanishes at P, we can do the process over again to the polynomial $w_1(x) + yv_1(x)$. This process also terminate since in every step we factor $x - w_1(x)$ from v, which we can contain only finitely many such factors. Hence in the case of order two, we can take $u(x, y) = y$.

3. When $P = O$, we show that $u(x, y) = x/y$ works. Suppose $r = f/g$ and $r(O) = 0$. This means that $deg(f) - deg(g) = d < 0$. Since $deg(y) - deg(x) = 1$, $deg(y^d f) = deg(x^d g)$, and $(y/x)^d$ will be finite and non-zero at identity. Since

$$r = (x/y)^d \left[(y/x)^d r\right]$$

we see that we can take $u(x, y) = x/y$ at identity.

4. uniqueness of number d:
Suppose that u and $\bar{u}$ are both rational functions satisfying the condition of the theorem. This mean we can write $u = (\bar{u})^e s$ and $\bar{u} = u^f t$, so $u = u^{ef}(t^e s)$. If $ef \neq 1$, then dividing this equation by u and plugging in P, we get $1 = 0$. We therefore must have $e = f = 1$. Thus if r is any rational function not identically zero that vanishes at P, we can write $r = u^d s = (\bar{u})^d t$.

□

Definition 1.12 **Uniformizing Variable or Uniformizer**: *A function u that satisfies the above theorem at point P is called the uniformizing variable or uniformizer at P.*

Definition 1.13 **Order of the function** : *If r is a rational function and $r = u^d s$ and u is a uniformizing variable at P, then order of r at P is d and we write*

$$ord_P(r) = d$$

Definition 1.14 *For a non-zero rational function $r \in \bar{K}(E)$, we define divisor by*

$$div(r) = \sum_{P \in E} ord_P(r)[P].$$

Definition 1.15 *1. The multiplicity of a zero =order of the function*

2. The multiplicity of a pole= $-$(order of the function).

Theorem 1.16 *Let r be a rational function on E. Then*

$$\sum_{P \in E} ord_P(r) = 0.$$

Definition 1.17 *A divisor $D \in Div(E)$ is said to be a* **principal divisor** *denoted by* prin(E) *if there exist a rational function $f \in \bar{K}(E)^*$ such that $D = div(f)$.*

Definition 1.18 *Two divisors D_1, $D_2 \in Div(E)$ are said to be* **linearly equivalent** *($D_1 \sim D_2$) if $D_1 - D_2 = div(f)$ for some $f \in K(E)$.*

Definition 1.19 *The* **Divisor class group** *or* **Picard group** *of E is given by*

$$cl(E) = Div(E)/\mathrm{prin(E)}$$

Proposition 1.20 *Let E be an elliptic curve and f be a rational function $\in \bar{K}(E)^*$. Then*

1. *if $div(f) = 0$ then f is a constant.*
2. *$deg(div(f)) = 0$.*

Theorem 1.21 *Let E be an elliptic curve over a field K and the divisor $D = \sum_{P \in E} n_P[P] \in Div(E)$. Then there exist a rational function $f \in E$ such that $div(f) = D$ if and only if $deg(D) = 0$ and $sum(D) = \mathcal{O}$.*

Chapter 2

Elliptic Curve over Complex Numbers

2.1 Introduction

An Elliptic Curve over complex numbers $\mathbb{C}$ is isomorphic to a torus $\mathbb{C}/\mathbf{L}$, where $\mathbf{L}$ is a lattice in $\mathbb{C}$ and addition of complex numbers (modulo the lattice $\mathbf{L}$)corresponds to addition of points on the elliptic curve. To prove this, first we will show that every lattice $\mathbf{L}$ gives rise to an elliptic curve E over $\mathbb{C}$ and then we show that every elliptic curve E over $\mathbb{C}$ arises from a lattice $\mathbf{L}$. In order to prove that map $\phi : \mathbb{C}/\mathbf{L} \longrightarrow E(\mathbb{C})$ is isomorphic to an elliptic curve, we will define doubly periodic functions(elliptic functions) on $\mathbb{C}$,i.e. Weierstrass $\wp$ - function and general properties of elliptic functions.

2.2 Elliptic Functions

Definition 2.1 *A lattice $\boldsymbol{L}$ in $\mathbb{C}$ is a discrete subgroup of the form $\boldsymbol{L} = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ generated by ω_1 and ω_2 which are linearly independent over $\mathbb{R}$.*

Definition 2.2 **Eisenstein series**
Let $\boldsymbol{L}$ be a lattice, then the weight$-k$ Eisenstein series for $\boldsymbol{L}$ is the sum

$$G_k(L) = \sum_{\omega \in \boldsymbol{L}-0} \frac{1}{\omega^k} \tag{2.1}$$

where $k > 2$ is an integer.

Theorem 2.3 *For any lattice $\boldsymbol{L}$, the sum $G_k(L) = \sum_{\omega \in \boldsymbol{L}-0} \dfrac{1}{\omega^k}$ converges absolutely for all $k > 2$.*

2.3 The Weierstrass $\wp$ - function

Definition 2.4 *The Weierstrass $\wp$ function of a lattice $\boldsymbol{L}$ is given by the infinite sum*

$$\wp(z) = \wp(z;\boldsymbol{L}) = \frac{1}{z^2} + \sum_{\omega \in \boldsymbol{L}-0} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right) \tag{2.2}$$

Properties of Weierstrass $\wp$ -function :
For any lattice $\mathbf{L}$,

1. The $\wp(z)$ converges absolutely and uniformly on compact sets, where $z \notin \mathbf{L}$.
2. The function $\wp(z;\mathbf{L})$ is a meromorphic even function whose only poles are double poles at points in $\mathbf{L}$.
3. $\wp\prime(z;\mathbf{L}) = -2\sum_{\omega \in \mathbf{L}} \dfrac{1}{(z-\omega)^3}$ is a meromorphic odd function whose only poles are triple poles at each $\omega \in \mathbf{L}$.
4. $\wp(z+\omega) = \wp(z)$ for all $\omega \in \mathbf{L}$.

Theorem 2.5 *The Laurent series expansion for $\wp(z;\boldsymbol{L})$ at $z = 0$ is given by*

$$\wp(z;\boldsymbol{L}) = \frac{1}{z^2} + \sum_{j=1}^{\infty} (2j+1) G_{2j+2}\, z^{2j} \tag{2.3}$$

where $G_k(L)$ denotes the Eisenstein series of weight k.

Proof For $|z| < |\omega|$

$$\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} = \frac{1}{\omega^2} \left(\frac{1}{\left(\dfrac{z-\omega}{\omega}\right)^2} - 1 \right) = \frac{1}{\omega^2} \left(\frac{1}{\left(1 - \dfrac{z}{\omega}\right)^2} - 1 \right) \tag{2.4}$$

As for all $|x| < 1$, the power series expansion

$$\frac{1}{(1-x)^2} = 1 + 2x + 3x^2 + 4x^3 \ldots = \textstyle\sum_{n=0}^{\infty} (n+1)x^n$$

So, we can write equation 2.4 as

$$\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} = \frac{1}{\omega^2}\sum_{n=1}^{\infty}(n+1)\left(\frac{z}{\omega}\right)^n = \sum_{n=1}^{\infty}\frac{(n+1)z^n}{\omega^{n+2}} \tag{2.5}$$

Therefore,

$$\begin{aligned}
\wp(z) &= \frac{1}{z^2} + \sum_{\omega\in\mathbf{L}-0}\left(\frac{1}{(z-\omega^k)^2} - \frac{1}{\omega^2}\right)\\
&= \frac{1}{z^2}\sum_{\omega\in\mathbf{L}-0}\sum_{n=1}^{\infty}\frac{(n+1)z^n}{\omega^{n+2}}\\
&= \frac{1}{z^2} + \sum_{n=1}^{\infty}(n+1)z^n\sum_{\omega\in\mathbf{L}-0}\frac{1}{\omega^{n+2}}\\
&= \frac{1}{z^2} + \sum_{n=1}^{\infty}G_{n+2}(L)z^n\\
&= \frac{1}{z^2} + \sum_{n=1}^{\infty}G_{2n+2}(L)z^2n.
\end{aligned}$$

In the last step sum is taken over the even integers $2n$ as $\wp$ is an even function, therefore coefficients of the odd terms are zero. □

2.4 Lattice defines Elliptic curve

Theorem 2.6 *For a lattice $\boldsymbol{L}$ and for all $z \notin \boldsymbol{L}$, the differential equation for Weierstrass $\wp$ function is given by*

$$\wp\prime(z)^2 = 4\wp(z;\boldsymbol{L})^3 - g_2(\boldsymbol{L})\wp(z) - g_3(\boldsymbol{L}) \tag{2.6}$$

where $g_2(\boldsymbol{L}) = 60G_4(\boldsymbol{L})$ and $g_3(\boldsymbol{L}) = 140G_6(\boldsymbol{L})$.

Proof We have proved earlier that;

$$\begin{aligned}
\wp(z) &= \frac{1}{z^2} + \sum_{n=1}^{\infty}(2n+1)G_{2n+2}(\mathbf{L})z^{2n}.\\
\wp\prime(z) &= \frac{-2}{z^3} + \sum_{n=1}^{\infty}(2n+1)G_{2n+2}(\mathbf{L})z^{2n-1}.
\end{aligned}$$

So, We can write the first few terms of the laurent series for $\wp(z)$ and $\wp\prime(z)$;

$$\begin{aligned}\wp(z) &= \frac{1}{z^2} + 3G_4(\mathbf{L})z^2 + 5G_6(\mathbf{L})z^4 + \dots\\ \wp(z)^3 &= \frac{1}{z^6} + G_4(\mathbf{L})\frac{1}{z^2} + 15G_6(\mathbf{L}) + \dots\\ \wp\prime(z) &= \frac{-2}{z^3} + 6G_4(\mathbf{L})z + 20G_6(\mathbf{L})z^3 + \dots\\ \wp\prime(z)^2 &= \frac{4}{z^6} - 24G_4(\mathbf{L})z^{-2} - 80G_6(\mathbf{L}) + \dots\end{aligned}$$

Now, let $f(z) = \wp\prime(z)^2 - 4\wp(z;\mathbf{L})^3 + 60G_4(\mathbf{L})\wp(z) + 140G_6(\mathbf{L})$. The function f is holomorphic at $z = 0$ and $f(0) = 0$. The function f is holomorphic because $\wp(z)$ and $\wp\prime(z)$ have poles only at points of $\mathbf{L}$. Moreover, f is a compact set as all values attained by f are attained on the closure of a fundamental parallelogram. So, f is a bounded set. Then by Liouville's Theorem we can conclude that f is a constant function and the fact that $f(0) = 0$ implies that f is identically zero i.e $f(z) = 0$. Hence, we have proved that for a lattice $\mathbf{L}$, $\wp(z)$ and it's derivative satisfy the equation;

$$\wp\prime(z)^2 = 4\wp(z;\mathbf{L})^3 - 60G_4(\mathbf{L})\wp(z) - 140G_6(\mathbf{L}) \tag{2.7}$$

With $y = \wp(z)$ and $x = \wp\prime(z)$, the equation(2.11) corresponds to the curve

$$y^2 = 4x^3 - g_2(\mathbf{L})x - g_3(\mathbf{L}). \tag{2.8}$$

This equation can be transformed into Weierstrass equation by putting $g_2(\mathbf{L}) = -4A$ and $g_3(\mathbf{L}) = -4B$.

Now in order to prove that the above curve is an elliptic curve, we need to show that it's discriminant is non zero. For that we can show that the projective curve defined by equation is not singular i.e. it's discriminant is non-zero.

The projective curve of the above curve is given by the equation;

$$zy^2 = 4x^3 - g_2(\mathbf{L})xz^2 - g_3(\mathbf{L})z^3. \tag{2.9}$$

Suppose if all the partial derivatives of the above equation vanish simultaneously at some point, $12x^2 - g_2(\mathbf{L})z^2 = 0$, $2zy = 0$, $y^2 = 2xzg_2(\mathbf{L}) - 3g_3(\mathbf{L})z^2$ So, $z = o \Rightarrow x = 0 \Rightarrow y = 0$. $(0, 0, 0)$ is not allowed in the projective space, so we can assume that $z = 1$. Plugging $z = 1$ in the equation $2zy = 0$ gives $y = 0$. As $y = 0$ and

$z = 1$, the equation become $2xg_2(\mathbf{L}) - 3g_3(\mathbf{L}) = 0$ and we get $x = \dfrac{-3g_3(\mathbf{L})}{2g_2(\mathbf{L})}$. As a result, the equation $12x^2 - g_2(\mathbf{L})z^2 = 0$ gives $g_2^3 - 27g_3^2 = 0$.

Thus, we can say that every lattice $\mathbf{L}$ gives us an equation which defines an elliptic curve over $\mathbb{C}$ provided $\Delta = g_2^3 - 27g_3^2 \neq 0$. □

Proposition 2.7 *For every lattice* $\boldsymbol{L}$, $\Delta(\boldsymbol{L}) = (g_2^3 - 27g_3^2) \neq 0$.

2.5 The isomorphism from a torus to its corresponding elliptic curve

Thus, $E : y^2 = 4x^3 - g_2(\mathbf{L})x - g_3(\mathbf{L})$ is the equation of the elliptic curve and we have a map from $z \in \mathbb{C}/\mathbf{L}$ to the points with complex coordinates $(\wp(z), \wp\prime(z))$ on an elliptic curve.

Theorem 2.8 *Let* $\boldsymbol{L}$ *be a lattice and* $E : y^2 = 4x^3 - g_2(\boldsymbol{L})x - g_3(\boldsymbol{L})$ *be an elliptic curve. Then the map*

$$\begin{aligned} \phi : \mathbb{C}/\boldsymbol{L} &\longrightarrow E(\mathbb{C}) \\ z &\longmapsto (\wp(z), \wp\prime(z)) \\ 0 &\longmapsto \mathcal{O} \end{aligned}$$

is an isomorphism between the additive groups $\mathbb{C}/\boldsymbol{L}$ *and* $E(\mathbb{C})$.

Definition 2.9 *For a lattice* $\mathbf{L}$, $j-$*invariant is defined by*

$$j(\boldsymbol{L}) = 1728\frac{g_2(\boldsymbol{L})^3}{\delta\boldsymbol{L}} = 1728\frac{g_2(\boldsymbol{L})^3}{g_2^3 - 27g_3^2}$$

where $\delta\mathbf{L}$ *is always non-zero.*

The elliptic curve $E : y^2 = 4x^3 - g_2(\mathbf{L})x - g_3(\mathbf{L})$ corresponding to lattice $\mathbf{L}$ is isomorphic to the elliptic curve $y^2 = x^3 + Ax + B$ where $g_2(\mathbf{L}) = -4A$ and $g_3(\mathbf{L}) = -4B$. So,

$$j(\mathbf{L}) = 1728\frac{g_2(\mathbf{L})^3}{g_2^3 - 27g_3^2} = 1728\frac{(-4A)^3}{(-4A)^3 - 27(-4B)^3}$$

This shows that the $j-$invariant of a lattice is the same as that of the corresponding elliptic curve.

Definition 2.10 *If there exist $\lambda \in \mathbb{C}^*$ with $\lambda \boldsymbol{L} = \boldsymbol{L}^{'}$ then two lattices $\boldsymbol{L}$ and $\boldsymbol{L}^{'}$ in $\mathbb{C}$ are said to be homothetic. Moreover, multiplication by λ induces an isomorphism $\lambda : \dfrac{\mathbb{C}}{\boldsymbol{L}} \longrightarrow \dfrac{\mathbb{C}}{\boldsymbol{L}^{'}}$.*

Chapter 3

Riemann Roch Theorem

Riemann-Rock theorem is important for computing the dimension of the space of the meromorphic functions with prescribed zeros and allowed poles. Riemann-Roch theorem can be used to study the elliptic curves and to show that every elliptic curve has a Weierstrass equation. Here, we will discuss canonical divisor in order to state Riemann Roch theorem.

Let f be a non-zero meromorphic function on C with finitely many zeros and poles. Let S be the finite set of poles and zeros of the function f. Then, we define

$$\text{div(f)} = \sum_{s \in C} ord_s(f)[s]$$

$$\text{deg(div(f))} = \sum_{s \in C} ord_s(f) = 0$$

Let $\tau(D)$ be the space of meromorphic functions with poles bounded by D then

$$\tau(D) = \{f \in \mathbb{C}(C)\ /div(f) + D \geqslant 0\}$$

Theorem 3.1 ***Riemann Inequality:***
Let M be a Riemann surface of genus g. Then for any divisor D, the Riemann Inequality is given by the equation

$$dim(\tau(D)) \geqslant deg(D) + 1 - g$$

where $\tau(D)$ is the space of meromorphic functions with poles bounded by D.

Definition 3.2 *The divisor class group of a Riemann surface denoted by $Cl(M)$ is defined as*

$$Cl(M) = Div(M)/div(\mathbb{C}^*(M)).$$

Canonical Divisor

Let Ω_M be the space of meromorphic differential form on M and for every $\omega \in \Omega(M)$ there exists a unique function $f \in \mathbb{C}(M)$ such that $\omega = fdz$ and the divisor associated with ω is given by

$$div(\omega) = \sum_{s \in M} ord_s(\omega)[s] \in Div(M).$$

If $\omega_1, \omega_2 \in \Omega_M$ are nonzero differentials, then $\omega_1 = f\omega_2$ for some function $f \in \mathbb{C}(M)$ and

$$div(\omega_1) = div(f) + div(\omega_2)$$

Definition 3.3 **Canonical divisor** *is the divisor class of meromorphic* $1-$*form on* M.
Let K *be a canonical divisor on* M *and* $K = div(\omega)$*, then* $div(f) \geqslant -div(\omega)$ *for each function* $f \in \tau(K)$.

Now, Let $f_0 \in \mathbb{C}^*(M)$ then

$$\tau(D + div(f_0)) = \{g \in \mathbb{C}(\mathbb{M}) : div(g) + D + div(f_0) \geqslant 0\}$$

Theorem 3.4 ***Riemann Roch Theorem**:*
Let M *be a Riemann surface of genus* g*. Then for any divisor* D *and any canonical divisor* K*,*

$$dim(\tau(D)) - dim(\tau(K - D)) = deg(D) + 1 - g.$$

Proposition 3.5 *Let* $D \in Div(C)$*, If* $deg(D) < 0$*, then* $\tau(D) = \{0\}$ *and* $dim(\tau(D)) = 0$.

Proof Let $f \in \tau(D)$ and $f \neq 0$ then $div(f) \geq -D \implies deg(div(f)) \geq deg(-D) = -deg(D)$ but $deg(div(f)) = 0$. Therefore, $deg(D)$ must be greater than or equal to zero. □

Corollary 3.6 *Let M be a Riemann surface of genus g. Let D be a divisor and K be a canonical divisor then,*

1. $dim(\tau(K)) = g$.

2. $deg(K) = 2g - 2$.

3. *If* $deg(D) > 2g - 2$, *then*

$$dim(\tau(D)) = deg(D) - g + 1.$$

Proof

1. Let $D = 0$, then by the Riemann-Roch theorem, we get, $dim(\tau(0)) - dim(\tau(K)) = 1 - g$. But $dim(\tau(0)) = 1$ so $dim(\tau(K)) = g$.

2. After putting $D = K$ in the Riemann-Roch theorem, we get $dim(\tau(K)) - dim(\tau(0)) = deg(K) + 1 - g$. Since $dim(\tau(K)) = g$ and $dim(\tau(0)) = 1$, we get $deg(K) = 2g - 2$.

3. If $deg(D) > 2g - 2$, then $deg(K - D) < 0$. Therefore, $dim(\tau(K - D)) = 0$, hence $dim(\tau(D)) = degD - g + 1$.

. □

Now, Consider an elliptic curve $E : y^2 = x^3 + ax + b$ then $4a^3 - 27b^2 \neq 0$. Any rational function on E is an element of $\mathbb{C}(E)$. So, every $f \in \mathbb{C}(E)$ can be written in the form

$$f = \frac{a(x) + b(x)y}{c(x)}$$

for suitable polynomials $a(x), b(x, c(x) \in \mathbb{C}(E)$. As, $y^2 = x^3 + ax + b$, so every even power of y can be replaced by a polynomial in x and any odd power of y can be replaced by a polynomial in x times a power of y not higher than one by the above relation.

Divisor of a line:

Let l be a line on an elliptic curve and the points $P, Q, R \in l \cap E$ are distinct then divisor of line l is given by

$$Div(l) = [P] + [Q] + [R] - 3[\mathcal{O}]$$

Now, let $D = [P] + [Q] + D^1$ and assume that D and D_1 are equivalent. Thus, we can write $D - D_1 = Div(l)$ as $deg(div(l)) = 0$. After plugging D into the equivalence relation we get,

$$D_1 = D^1 + 3[\mathcal{O}] - [R]$$

As, $D \sim D_1$, So without loss of generality we can write $D \sim -[s] + n[\mathcal{O}]$ where n denotes the number of poles with multiplicity and $s \in l \cap E$. Now, consider a line $x - a = 0$ passing through $s = (a, b)$ and $-s = (a, -b)$. Then, $div(x - a) = [s] + [-s] - 2[\mathcal{O}]$. Thus, we can write $D \sim -[s] + (degD + 1)[\mathcal{O}]$.

$$\begin{aligned} dim\ \tau(D) &= dim\ \tau\left((degD + 1)[\mathcal{O}] - [s]\right) \\ &= deg(D) + 1 - 1 \\ &= degD \end{aligned}$$

Let ω is the invariant differential associated to the elliptic curve E and $\omega = \dfrac{dy}{x}$. As ω doesn't have zeros and poles anywhere so $div(\omega) = 0$. So $K = 0$, from this we get $deg(\tau(0 - D)) < 0$. Hence, $dim(\tau(0 - D) = 0$. As, we know that an elliptic curve is a curve of genus 1. Hence, the Riemann-Roch theorem holds for elliptic curve. □

Remark

- Let P be a point on an elliptic curve then $dim(\tau(P)) = 1$, therefore $\tau(P)$ contains the constant functions, which have no zeroes and poles.
- Consider the point at infinity $\mathcal{O}$ on the elliptic curve E. Then, $dim(\tau(2(\mathcal{O})) = 2$. Thus, the basis for $\tau(2(\mathcal{O}))$ are $1, x$.
- Thus, the basis for $\tau(3(\mathcal{O}))$ are $1, x, y$.
- $1, x, y, x^2, xy, x^3, y^2$ are the basis for $\tau(6(\mathcal{O}))$ but $dim(\tau(6(\mathcal{O})) = 6$ as y^2 can be written in terms of x.

Chapter 4

Elliptic Curve over Finite Fields

In this chapter we will discuss that E has only finitely many points with coordinates in $\mathbb{F}$ and those finitely many points form an abelian group where $\mathbb{F}$ be a finite field and E be an elliptic curve defined over $\mathbb{F}$. After that, we will discuss the problem of estimating the number of points on elliptic curve over finite field and then Hasse theorem which provides a lower and upper bound on the number of points of the elliptic curve over $\mathbb{F}$. And later on, about the endomorphisms of the Elliptic curve over finite field.

4.1 Rational Points over Finite field

Consider the curve $C : y^2 = f(x)$, where $f(x)$ is a polynomial with coefficients in $\mathbb{F}_p$ and suppose $p \neq 2$. Then we can find the rational points of the curve C, as x and y are in $\mathbb{F}_p$ therefore we can take each of the non-zero values from 1 to $p-1$ of the field $\mathbb{F}_p$ as the possibility for the value of x and then plug into the polynomial $f(x)$. If $f(x) = 0$, then $y = 0$ is the only solution. If $f(x) \neq 0$ then for half of the values of x there exist a solution as $f(x)$ is a square in $\mathbb{F}_p^*$(the quadratic residue) and for half of the values of x solution does not exist as $f(x)$ is non-square(the quadratic nonresidue). So, we get approximately p solutions from the p possible values of x and one solution is at point at infinity. Thus, the group $E(\mathbb{F}_p)$ is a finite group and $\#E(\mathbb{F}_p) \approx p + 1$. And Hasse theorem gives us the precise number of points of Elliptic curve over finite field.

Theorem 4.1 *Let E be an elliptic curve over the finite field $\mathbb{F}_p$. Then the group of points $E(\mathbb{F}_p)$ is always either a cyclic group or a product of two cyclic groups. i.e.,*

$$E(\mathbb{F}_p) \simeq \mathbb{Z}_n \text{ or } E(\mathbb{F}_p) \simeq \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$$

where n, n_1, $n_2 \geqslant 1$ and n_1 divides n_2.

Example 4.2 Let $E : y^2 = x^3 + x + 1$ be the elliptic curve over $\mathbb{F}_5$. For counting the number of points on $E(\mathbb{F}_5)$, we take each of the five possible of values of x and calculate x^3+x+1 and then check for the square roots y of $x^3+x+1 \mod 5$. Doing this, we get 9 points on the curve including the point at infinity, i.e, $E(\mathbb{F}_5) = 9$

x	$x^3 + x + 1$	y	*points*
0	1	± 1	$(0,1),(0,4)$
1	3	$-$	$-$
2	1	± 1	$(2,1),(2,4)$
2	1	± 1	$(3,1),(3,4)$
4	4	± 2	$(4,2),(4,3)$
$\mathcal{O}$		$\mathcal{O}$	$\mathcal{O}$

Therefore, by the above theorem, $E(\mathbb{F}_5)$ is either a cyclic group of order nine or a product of two cyclic groups of order three. To find out, let's start with the point $P = (0,1)$ on E. By using the formula's given in theorem 1.5 we get

$$\begin{aligned} &2P = (4,2), \quad 3P = (2,1), && 4P = (3,4), \quad 5P = (3,1), \\ &6P = (2,4), \quad 7P = (4,3), && 8P = (0,4), \quad 9P = \mathcal{O}, \end{aligned}$$

Thus, $E(\mathbb{F}_5)$ is a cyclic group of order 9 and $P = (0,1)$ is the generator of the cyclic group. The points $Q = (2,1)$ *and* $R = (2,4)$ are of order 3 and all other non-zero points of $E(\mathbb{F}_5)$ except Q and R have order 9.

Theorem 4.3 **Hasse Theorem***:*

Let E be an elliptic curve over finite field $\mathbb{F}_p$. Then the number of points on elliptic curve satisfies

$$|\, p + 1 - \#E(\mathbb{F}_p)\, | \quad \leqslant 2\sqrt{p}.$$

4.2 Endomorphism

In this section, we will discuss maps between the elliptic curves.

Definition 4.4 **Isogenies** *Let E_1 and E_2 be two elliptic curves over a finite field K. Then an isogeny of elliptic curves E_1 and E_2 is a morphism ϕ which maps the identity point of E_1 to the identity point of E_2. i.e.,*

$$\phi : \quad E_1 \longrightarrow E_2 \quad \textit{such that} \;\; \phi(\mathcal{O}) = \mathcal{O}.$$

Moreover, An isogeny is surjective and it's kernel is a finite subgroup of E_1.

Two elliptic curves are said to be **isogenous** if $\exists$ an isogeny from E_1 to E_2 and $\phi(E_1) \neq \mathcal{O}$.

Definition 4.5 **Degree of Isogeny** ϕ *Let E_1 and E_2 are elliptic curves defined over finite field K. Then the degree of $\phi : E_1 \longrightarrow E_2$, denoted by deg($\phi$) is the degree of the extension field $\bar{K}(E_1)/\phi^*\bar{K}(E_2)$, where $\phi^* : \bar{K}(E_2) \longrightarrow \bar{K}(E_1)$ and deg$[0] = 0$.*

The maps between Elliptic curves forms a group as Elliptic curves forms an abelian group. The set of isogenies from E_1 to E_2 are given by

$$Hom(E_1, E_2) = \{isogenies \;\; E_1 \longrightarrow E_2\}.$$

Let ϕ and ψ are two isogenies from E_1 to E_2 and P be any point on E_1. Then sum of two isogenies is defined as

$$(\phi + \psi)(P) = \phi(P) + \psi(P),$$

Therefore, $(\phi + \psi)$ is a morphism, so it's also an isogeny . Thus, we can say that $Hom(E_1, E_2)$ is a group.

If $E_1 = E_2$ then we can also compose isogenies. So, $Hom(E, E) = End(E)$ where $End(E)$ is called the endomorphism ring of E such that $(\phi\psi)(P) = (\psi\phi)(P)$ and $(\phi + \psi)(P) = \phi(P) + \psi(P)$.

Definition 4.6 **Endomorphism** *An endomorphism of an elliptic curve E over a field K is a morphism $\phi : E(\bar{K}) \longrightarrow E(\bar{K})$ given by rational functions $R_1(x, y), R_2(x, y)$ with coefficients in $\bar{K}$ such that*

$$\phi(x, y) = (R_1(x, y), R_2(x, y))$$

and $\phi(\mathcal{O}) = \mathcal{O}$.

Let $E : y^2 = x^3 + ax + b$ be an elliptic curve over a field K. Then for all $(x, y) \in E(\bar{K})$, any higher power of y greater than one can be replaced by a polynomial in x times a power of y not higher than one. Therefore, any rational function $R(x, y)$ on points in $E(\bar{K})$ can be written as

$$R(x, y) = \frac{p_1(x) + p_2(x)y}{p_3x + p_4(x)y}.$$

Now, after multiplying the numerator and denominator by $p_3(x) - p_4(x)y$, we get

$$\begin{aligned} R(x, y) &= \frac{p_1(x) + p_2(x)y}{p_3x + p_4(x)y} \frac{p_3(x) - p_4(x)y}{p_3(x) - p_4(x)y} \\ &= \frac{p_1(x)p_3(x) + (p_2(x)p_3(x) - p_1(x)p_4(x))y - p_1(x)p_4(x)y^2}{p_3^2(x) - p_4^2(x)y^2} \end{aligned}$$

After replacing y^2 term by $x^3 + ax + b$ we get,

$$R(x, y) = \frac{q_1(x) + q_2(x)y}{q_3(x)}$$

Let ϕ be an endomorphism given by

$$\phi(x, y) = (R_1(x, y), R_2(x, y)),$$

As ϕ is a homomorphism by definition, so

$$\phi(x, -y) = \phi(-(x, y)) = -\phi(x, y).$$

Therefore, $R_1(x, -y) = R_1(x, y)$ and $R_2(x, -y) = -R_2(x, y)$. As, we have discussed earlier that $R(x, y) = \dfrac{q_1(x) + q_2(x)y}{q_3(x)}$ and $R_1(x, -y) = R_1(x, y)$. So $q_2(x) = 0$ for $R_1(x, y)$. Now, as $R_2(x, -y) = -R_2(x, y)$, so $q_1(x)$ must be equal to zero in order to satisfy the above condition for $R_2(x, y)$. Thus, we can write

$$\phi(x, y) = (r_1(x), r_2(x)y),$$

where $r_1(x)$ and $r_2(x)$ are rational functions. Since, $r_1(x)$ and $r_2(x)$ are quotients of two polynomial functions. So, what happens if one of the rational function is not defined at a point. Let $r_1(x, y) = \frac{p(x)}{q(x)}$, where p(x) and q(x) are polynomials in x such that p(x)and q(x) have no common root. In case of $q(x) = 0$, we define $\phi(x, y) = \mathcal{O}$.

Definition 4.7 **Degree of Endomorphism**:
The degree of an endomorphism map $\phi : E(\bar{K}) \longrightarrow E(\bar{K})$ *given by* $\phi(x, y) = \left(\frac{p(x)}{q(x)}, y\frac{p_2(x)}{q_2(x)}\right)$ *is given as*

$$deg(\phi) = Max\left\{degp(x), degq(x)\right\}$$

For $\phi = 0$ *we define* $deg(0) = 0$.

Definition 4.8 **Separable Endomorphism**:
An Endomorphism is said to be separable if the derivative $r_1'(x)$ *is not identically zero i.e, at least one of the* $p'(x)$ *and* $q'(x)$ *is not zero.*

Theorem 4.9 *: Let* $\phi \neq 0$ *be an endomorphism of an Elliptic curve over a field K where,* $\phi : E(\bar{K}) \longrightarrow E(\bar{K})$. *Let Kernel of* ϕ *is denoted by* $Ker(\phi)$ *and* $deg(\phi)$ *is degree of the endomorphism map.*

1. *If* ϕ *is a separable endomorphism, then* $deg\phi = \#Ker(\phi)$.
2. *If* ϕ *is not a separable endomorphism, then* $deg\phi > \#Ker(\phi)$.

Proof As ϕ is an endomorphism, so $\phi(x, y) = (r_1(x), r_2(x)y)$ where $r_1(x) = \frac{p(x)}{q(x)}$. If ϕ is separable then $r_1'(x) \neq 0$, hence $p'q - pq'$ is not the zero polynomial. Let M be the set of $x \in \bar{K}$ such that $(pq' - p'q)(x)q(x) = 0$. Let $(a, b) \in E(\bar{K})$ such that it satisfies these four properties:

1. $a \neq =, b \neq 0$, so $(a, b) \neq \mathcal{O}$, since $\phi(\mathcal{O}) = \mathcal{O}$.
2. $deg(p(x) - aq(x)) = Max\left\{deg(p), deg(q)\right\} = deg(\phi)$
3. $a \notin r_1(M)$, otherwise ϕ becomes not separable
4. $(a, b) \in \phi(E(\bar{K}))$.

We can observe that M is a finite set as $pq'-p'q$ is not a zero polynomial so there exist only finite number of $x \in \bar{K}$ such that $(pq'-p'q)(x)q(x)$ becomes zero. Moreover, $\phi(x \in M)$ is also a finite set. If we look at $r_1(x)$ function then we can easily conclude that $r_1(x)$ takes infinitely many distinct values. Moreover, $\phi(E(\bar{K})$ is an infinite set as for each x we can find a point $(x,y) \in E(\bar{K})$. So, $\exists$ an $(a,b) \in E(\bar{K})$. Now, we want to prove that for a separable endomorphism $deg\phi = \#Ker(\phi)$. So, we will show that there are exactly $deg(\phi)$ points $(x_1,y_1) \in E(\bar{K})$ such that $\phi(x_1,y_1) = (a,b)$. So, $r_1(x) = \dfrac{p(x)}{q(x)} = a$ and $y_1r_2(x_1) = b$. We have assumed that $(a,b) \neq \mathcal{O}$, therefore, $q_(x_1) \neq 0$ and also assumed that $b =\neq 0$ so, $y_1 = \dfrac{b}{r_2(x_1)}$. This shows that value of y_1 depends on the value of x_1, so it's sufficient to count the values of x_1 in order to calculate the number of elements in the kernel of ϕ. Since, we have also assumed that $deg(p(x)-aq(x)) = deg(\phi)$ i.e, the polynomial $p(x)-aq(x) = 0$ has deg(ϕ) roots including multiplicities. Now, we need to show that all roots of the polynomial are distinct. We will show this by contradiction. So, suppose that $p-aq$ has multiple roots and let x_0 is a multiple root. So, $p(x_0 - aq(x_0) = 0$ and $p'(x_0) - aq'(x_0) = 0$. After multiplying these two equations, we get $ap(x_0)q'(x_0) = ap'(x_0)q(x_0)$. As, we have assumed that $a \neq 0$ so x_0 must be a root of $pq'-p'q$. But $x_0 \in M$, thus $a = r_1(x-0) \in r_1(M)$, it's a contradiction to what we have assumed. Hence, $p-aq$ has no multiple roots and it has $deg(\phi)$ distinct roots. That implies that there are $deg(\phi)$ points (x_1,y_1) such that $\phi(x_1,y_1) = (a,b)$. Hence, $deg\phi = \#Ker(\phi)$.

When ϕ is not a separable endomorphism, $r_1(x) = 0 \Longrightarrow p' - aq'$ is always a zero polynomial, thus $p(x)-aq(x) = 0$ has multiple roots. Since, it has multiple roots, $deg\phi > \#Ker(\phi)$. □

Definition 4.10 *: Let E be an elliptic curve over $\bar{K}$, then for every integer m, the multiplication-by-m map $[m]$ is an endomorphism of E;*

$$[m] : E \longrightarrow E$$

Where if $m > 0$, then for a point $P \in \bar{K}$, $[m](P) = \underbrace{P+P+...+P}_{m\ terms}$ and if $m < 0$, then $[-m](-P) = \underbrace{-P+-P+...+-P}_{-m\ terms}$. and $[0](P) = \mathcal{O}$. Addition here is the group law on the elliptic curve.

Corollary 4.11 *Let E be an elliptic curve and m be a non-zero integer then $deg([m]) = m^2$.*

Definition 4.12 **Dual Isogeny***: Let $\phi : E_1 \longrightarrow E_2$ be an isogeny. Then the dual isogeny to ϕ is the isogeny*

$$\hat{\phi} : E_2 \longrightarrow E_1$$

such that $\hat{\phi} \circ \phi = [m]$.

Definition 4.13 **Torsion m-subgroup** *Let E be an elliptic curve defined over a field K and n be a positive integer then m-torsion subgroup of E is the collection of all points of finite order m and is defined as*

$$E[m] = \left\{P \in E(\bar{K}) : mP = \mathcal{O}\right\}.$$

Definition 4.14 **Torsion subgroup** *The torsion subgroup of E is the set of all points of finite order*

$$E_{tors} = \cup_{m=1}^{\infty} E[m].$$

Theorem 4.15 *Let E be an Elliptic curve over a field K and let $m \geqslant 2$ be an integer, then*

1. *If either $char(K) = 0$ or $char(K) = p > 0$ and p does not divide m, then*

$$E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$$

2. *If $char(K) = p > 0$ and p/m, where $m = p^r n$ with p does not divide n. Then either $E[m] \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ or $E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.*

Definition 4.16 **Distortion map** *Let E be an elliptic curve over a finite field $\mathbb{F}_q$, m is relatively prime to the characteristic of the finite field $\mathbb{F}_q$ and the points $P, Q \in E(\mathbb{F}_q)$ generate the group $E[m]$. Then distortion map on E is an endomorphism ϕ of E such that $\phi(P) \notin < P >$.*

4.3 Frobenius Endomorphism

Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$ where $q = p^r$, p is a prime. Then we define Frobenius map ϕ_q as;

$$\begin{aligned} \phi_q :& E \longrightarrow E \\ & (x, y) \longrightarrow (x^q, y^q) \end{aligned}$$

where $\phi_q(\mathcal{O}) = \mathcal{O}$. The map ϕ_q basically acts on the coordinates of points in E($\bar{\mathbb{F}}_q$).

Lemma 4.17 *Let $E/\bar{\mathbb{F}}_q$ and $(x, y) \in E(\bar{\mathbb{F}}_q)$ then $\phi_q(x, y) \in E(\bar{\mathbb{F}}_q)$.*

Proof Let p is the characteristic of the field then for elements $a, b \in \mathbb{F}_q$, $(a + b)^q = a^q + b^q$. Let E be given by $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ and if $(x, y) \in E(\mathbb{F}_q)$ and $a_i \in \mathbb{F}_q$ then

$$(y^q)^2 + a_1(x^q y^q) + a_3(y^q) = (x^q)^3 + a_2(x^q)^2 + a_4(x^q) + a_6$$

as (x^q, y^q) satisfies the equation of E, so it lies on E. Hence, proved. □

Lemma 4.18 *Let E be an elliptic curve defined over $\mathbb{F}_q$. Then the Frobenius map ϕ_q is an endomorphism map of degree q and the map ϕ_q is not separable.*

Proof By the definition of the Frobenius map, we have $\phi_q(x, y) = (x^q, y^q)$, and the map is given by the rational functions (quotients of two polynomials) and $deg(\phi_q) = max(degreeoftwoquotientpolynomials) = q$. We will prove for Weierstrass normal form $E : y^2 = x^3 + ax + b$ that ϕ_q is an endomorphism. For this, let $P = (x_1, y_1)$, $Q = (x_2, y_2)$ be two points on $E(\mathbb{F}_q)$ and $P + Q = (x_3, y_3)$.

1. When $x_1 \neq x_2$. Then, by addition law, formula we get $x_3 = \lambda^2 - x_1 - x_2$ and $y_3 = \lambda(x_1 - x_3) - y_1$ where $\lambda = \dfrac{y_2 - y_1}{x_2 - x_3}$. As, $\phi_q(x, y) \longrightarrow (x^q, y^q)$ so, after raising everything to the q^{th} power we get, $x_3^q = \lambda'^2 - x_1^q - x_2^q$ and $y_3^q = \lambda'(x_1^q - x_3^q) - y_1^q$, where $\lambda' = \dfrac{y_2^q - y_1^q}{x_2^q - x_1^q}$. Since, $x_1, y_1 \in \mathbb{F}_q$, $x_1^q = x_1$ and $y_1^q = y_1$. Therefore $\phi_q(x_3, y_3) = (x_3^q, y_3^q) = (x_3, y_3)$. And,

$$\begin{aligned}\phi_q(x_1, y_1) + \phi_q(x_2, y_2) &= (x_1^q, y_1^q) + (x_2^q, y_2^q)\\ &= (x_1, y_1) + (x_2, y_2)\\ &= (x_3, y_3)\end{aligned}$$

   Therefore, $\phi_q(x_3, y_3) = \phi_q(x_1, y_1) + \phi_q(x_2, y_2)$. Hence, ϕ_q is an endomorphism.

2. when $x_1 = x_2$ but $y_1 \neq y_2$ then $P + Q = (x_3, y_3) = \mathcal{O}$. So, $\phi_q(x_3, y_3) = \mathcal{O}$ and $\phi_q(x_1, y_1) + \phi_q(x_2, y_2) = (x_1^q, y_1^q) + (x_2^q, y_2^q) = (x_1, y_1) + (x_2, y_2) = \mathcal{O}$. Thus, we get $\phi_q(x_3, y_3) = \phi_q(x_1, y_1) + \phi_q(x_2, y_2) = \mathcal{O}$. Hence, ϕ_q is an endomorphism.

3. When $P = \mathcal{O}$ then $P + Q = \mathcal{O}$. Thus, in this case too ϕ_q is an endomorphism.

4. If $P = Q$, then $2P = (x_3, y_3)$. By doubling formula, we get $x_3 = \lambda^2 - 2x_1$ and $y_3 = \lambda(x_1 - y_3) - y_1$, where $\lambda = \dfrac{3x_1^2 + a}{2y_1}$. Now, by raising to the q^{th} power, we get $x_3^q = \lambda'^2 - 2x_1^q$ and $y_3^q = \lambda'(x_1^q - y_3^q) - y_1^q$, where $\lambda' = \dfrac{3^q(x_1^q)^2 + a^q)}{2^q y_1^q}$. Since, $2, 3,\ a \in \mathbb{F}_q$, therefore $2^q = 2,\ 3^q = 3,\ a^q = a$. Therefore, $\phi_q(x_3, y_3) = (x_3^q, y_3^q) = (x_3, y_3)$. And,

$$\begin{aligned}\phi_q 2(x_1, y_1) &= 2(x_1^q, y_1^q)\\ &= 2(x_1, y_1)\\ &= (x_3, y_3)\end{aligned}$$

Therefore, $\phi_q(x_3, y_3) = \phi_q(x_1, y_1) + \phi_q(x_1, y_1)$. Hence, ϕ_q is an endomorphism.

Now, for separability we need to show that $\phi_q' \neq 0$ i.e, derivative of x^q should be non-zero. However as $q = 0$ in $\mathbb{F}_q$, thus derivative of x^q is identically zero. Hence, ϕ_q is not separable. □

Proposition 4.19 *Let E be an elliptic curve defined over $\mathbb{F}_q$ and ϕ_q be a Frobenius endomorphism*

$$\begin{aligned}\phi_q :& E \longrightarrow E\\ &(x, y) \longrightarrow (x^q, y^q)\end{aligned}$$

. Let m, n be non-zero integer and $char(K) = p$ does not divide m then the map

$$m + n\phi_q : E \longrightarrow E$$

is separable. Moreover, the map $1 - \phi_q$ is also separable.

Theorem 4.20 *Let E be an elliptic curve defined over $\mathbb{F}_q$ and ϕ_q be a Frobenius endomorphism*

$$\begin{aligned}\phi_q :& E \longrightarrow E\\ &(x, y) \longrightarrow (x^q, y^q)\end{aligned}$$

Since, $\phi_q^2 = \phi_q \circ \phi_q$ lies in the ring of endomorphism and endomorphism ring is a ring of characteristic zero. Then,

$$\phi_q^2 - t\phi_q + q = 0$$

is an endomorphism of E, where t is called the trace of the Frobenius endomorphism and is given by the relation $t = q + 1 - \#E(\mathbb{F}_q)$. That is, if $(x, y) \in E(\mathbb{F}_q)$, then

$$\left(x^{q^2}, y^{q^2}\right) - t(x^q, y^q) + q(x, y) = \mathcal{O}$$

Example 4.21 : Let $E : y^2 + xy = x^3 + 1$ be an elliptic curve over $\mathbb{F}_2$. Then we can count the number of points as

$$\begin{aligned} x = 0 &\Longrightarrow y^2 = 1 \Longrightarrow y = 1 \\ x = 1 &\Longrightarrow y^2 + y = 0 \Longrightarrow y = 0, 1. \end{aligned}$$

Therefore, $E(\mathbb{F}_2)$ is a cyclic group of order 4 as

$$E(\mathbb{F}_2) = \{\mathcal{O}, (0,1), (1,0), (1,1)\}.$$

Thus, we can calculate trace by the equation $t = q+1-\#E(\mathbb{F}_q)$. So, $t = -1$. Thus, satisfies the equation $X^2 + (X) + 2 = 0$.

Chapter 5

Weil Pairing

The Weil Pairing on the n-torsion subgroup of an elliptic curve plays a significant role in the theory of the elliptic curve. It can be applied to the problem of calculating the group structure of an elliptic curve over finite fields, For example to prove the Hasse theorem. Apart from this, Weil pairing has application in cryptography. The MOV attack uses the Weil pairing to reduce the discrete logarithm elliptic curve problem to the discrete logarithm problem in the multiplicative group of a finite field. Other application of Weil pairing are in Decision Diffie- Hellman problem on elliptic curve, ID-based public cryptosystems and in a digital signature scheme which gives signatures that are half the size of those produced by Digital Signature Algorithm.

5.1 Construction of the Weil Pairing

Let E be an elliptic curve over a field K and n be a positive integer. Assume that $char(K) = p$ does not divide n. Then by the theorem $E[n] \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. As, $E[n]$ is a free $\mathbb{Z}/n\mathbb{Z}$ module of rank two. Thus, we can construct a pairing given by:

$$e_n : E[n] \times E[n] \longrightarrow \mu_n$$

Where $\mu_n = \{x \in \bar{K}/x^n = 1\}$ is the group of n^{th} root of unity in $\bar{K}$. As, we have assume that $char(K)$ does not divide n, so the equation $x^n = 1$ has no multiple roots and has n roots in $\bar{K}$. Therefore, μ_n is a cyclic group of order n.

For this, Let $T \in E[n]$, then by the theorem (1.20) there exist a rational function $f \in \bar{K}(E)$ such that $div(f) = n[T] - n[\mathcal{O}]$. Here $deg(div(f)) = 0$ and as $t \in E[n]$ so $nT = \mathcal{O}$. Therefore, $sum(div(f)) = \mathcal{O}$.

Now, Let $T' \in E$ such that $nT' = T$, then there exist a function $g \in \bar{K}(E)$ such that

$$div(g) = \sum_{R \in E[n]} \left([T' + R] - [R]\right).$$

As we know that $\#E[n] = n^2$ so there are n^2 points R in $E[n]$. Moreover, the total number of points R in $\sum[T' + R]$ is equal to total number of points R in $\sum[R]$ and $n^2T' = nT = \mathcal{O}$. This result in $sum(div(g)) = 0$.

With out loss of generality, we can write

$$div(g) = \sum_{nT''=T} [T''] - \sum_{nR=\mathcal{O}} [R].$$

as g does not depend on the choice of T' and Moreover, any two choices of T' only differs by an element $R \in E[n]$.
To get the function $f \circ n$ start with a point on E, multiply it with n and then apply the function f.
Now, take the point $P = T' + R$ where $R \in E[n]$ and $nP = T$.
We get divisor of the function $f \circ n$ as:

$$div(f \circ n) = n \left(\sum_{R \in E[n]} [T' + R] \right) - \left(\sum_{R} [R] \right) = div(g^n)$$

as $div(g^n) = n\ div(g)$.
Therefore, $f \circ n$ is a constant multiple of g^n and by multiplying f by an appropriate constant from $\bar{K}$, we can assume that $f \circ n = g^n$.
Now, let $S \in E[n]$. Then, for any point $P \in E(\bar{K})$, we have

$$g(P + S)^n = f(nP + nS) = f(nP) = g(P)^n$$

as S $\in E[n]$ so, $nS = \mathcal{O}$.

Therefore, the function $g(P + S)/g(P) \in \mu_n$. The function $g(P + S)/g(P)$ is a continuous function of P and the map $S \longrightarrow \dfrac{g(P + S)}{g(P)}$ is not surjective so, the map to the finite discrete set μ_n is constant.

Thus, we can define a pairing

$$e_n : E[n] \times E[n] \longrightarrow \mu_n$$

by setting

$$e_n(S,T) = \frac{g(P+S)}{g(P)}$$

for every point $P \in E$ such that $g(P+S)$ and $g(P)$ are defined and both non-zero. Where $S, T \in E[n]$ and the value of e_n is independent of the choice of g.

5.2 Properties of Weil Pairing

Proposition 5.1 *Let E be an elliptic curve defined over field K and n be a positive integer. Assume that char(K) does not divide n. Then the Weil e_n pairing satisfies the following properties:*

1. *Bilinearity:*
   If $S, T, S_1, S_2, T_1, T_2 \in E[n]$, then
   $$e_n(S_1 + S_2, T) = e_n(S_1, T)e_n(S_2, T),$$
   $$e_n(S, T_1 + T_2) = e_n(S, T_1)e_n(S, T_2).$$
2. *Alternating:*
   $$If\ T\ \in E[n]\ then\ e_n(T,T) = 1.$$
   So, this along with linearity implies that if $S, T \in E[n]$ then $e_n(S,T) = e_n(T,S)^{-1}$.
3. *Non-degeneracy:*
   $$If\ e_n(S,T) = 1\ \forall\ S \in E[n],\ then\ T = \mathcal{O}.$$
4. *Galois invariant:*
   If $S,\ T \in E[n]$ then,
   $$e_n(S,T)^\sigma = e_n(S^\sigma, T^\sigma)\ \ \forall\ \ \sigma \in G_{\bar{K}/K}.$$
5. *Compatiblity:*
   If $S \in E[nm]$ and $T \in E[n]$ then,
   $$e_{nm}(S,T) = e_n(mS,T).$$

Proof

1. For any point $P \in E$, we have $e_n(S,T) = \dfrac{g(P+S)}{g(P)}$. So,

$$\begin{aligned} e_n(S_1+S_2,T) &= \frac{g(P+S_1+S_2)}{g(P)} \\ &= \frac{g(P+S_1+S_2)}{g(P+S_1)}\frac{g(P+S_1)}{g(P)} \\ &= e_n(S_2,T)e_n(S_1,T) \end{aligned}$$

As, we can write $e_n(S_2,T) = \dfrac{g(X+S_2)}{g(X)}$ for $X = P+S_1$.

Hence, linearity in first variable is proved.

Now, In order to prove linearity in second variable. Let $T_1, T_2, T_3, S \in E[n]$ where, $T_3 = T_1 + T_2$. Let f_i and g_i be the functions for the points T_i where $1 \leqslant i \leqslant 3$. Then, there exist a function $h \in \bar{K}(E)$ such that

$$div(h) = [T_1+T_2] - [T_1] - [T_2] + [\mathcal{O}].$$

This is because $deg(div(h)) = 0$ and $Sum(div(h)) = 0$ as $nT_1 = \mathcal{O}$, $nT_2 = \mathcal{O}$, $nT_3 = \mathcal{O}$. Since, $div(f_i) = n[T_i] - n[\mathcal{O}]$. So,

$$\begin{aligned} div\left(\frac{f_3}{f_1f_2}\right) &= n[T_3] - n[\mathcal{O}] - n[T_1] + n[\mathcal{O}] - n[T_2] + n[\mathcal{O}] \\ &= n[T_3] - n[T_1] - n[T_2] + n[\mathcal{O}] \\ &= ndiv(h) = div(h^n). \end{aligned}$$

Therefore, f_3/f_1f_2 is a constant multiple of h^n. Hence, there exist a constant $c \in \bar{K}^*$ such that

$$f_3 = cf_1f_2h^n.$$

As, we know that $f_i \circ n = g_i^n$. So, we can write

$$f_3 \circ n = c'.(f_1 \circ n).(f_2 \circ n).(h \circ n) \qquad\qquad where\ c' \in \bar{K}^*.$$

That is,

$$g_3 = c'g_1.g_2.(h \circ n) \qquad for\ some\ c' \in \bar{K}^*.$$

Therefore, by the definition of e_n and for some point $P \in E$. we get,

$$\begin{aligned} e_n(S, T_1 + T2) &= \frac{g_3(P+S)}{g_3(P)} \\ &= \frac{c' g_1(P+S)}{c' g_1(P)} \frac{g_2(P+S)}{g_2(P)} \frac{h\left(n(P+S)\right)}{h\left(n(P)\right)} \end{aligned}$$

Since S $\in E[n]$, nS $= \mathcal{O}$. So, $h\left(n(P+S)\right) = h\left(n(P)\right)$. Thus, $e_n(S, T_1 + T_2) = e_n(S, T_1) e_n(S, T_2)$. Hence proved.

2. First we will prove that for any point $T \in E[n]$, $e_n(T, T) = 1$. For that, we define a translation map τ_{jT} such that;

$$\begin{aligned} \tau_{jT} : E &\longrightarrow E, \\ P &\longrightarrow P + jT \end{aligned}$$

So, $f \circ \tau_{jT}$ denotes the function $P \longrightarrow f(P + jT)$. Thus, $div(f \circ \tau_{jT}) = n[T - jT] - n[-jT]$. Therefore, we can compute

$$div\left(\prod_{j=0}^{n-1} f \circ \tau_{jT}\right) = \sum_{j=0}^{n-1} \left(n[(1-j)T] - n[-jT]\right) = 0$$

Since, $div\left(\prod_{j=0}^{n-1} f \circ \tau_{jT}\right) = 0$ so, $\prod_{j=0}^{n-1} f \circ \tau_{jT}$ is constant. For some $T' \in E$ satisfying $nT' = T$ and as we know that $f \circ n = g^n$. So,

$$\begin{aligned} \left(\prod_{j=0}^{n-1} g \circ \tau_{jT'}\right)^n &= \prod_{j=0}^{n-1} f \circ \tau_{jT'} \\ &= \prod_{j=0}^{n-1} f \circ \tau_{jT} \circ n. \end{aligned}$$

This proves that $\prod_{j=0}^{n-1} g \circ \tau_{jT'}$ is also constant. Therefore, it takes the same value at P and $P + T'$, so

$$\prod_{j=0}^{n-1} g(P + T' + jT') = \prod_{j=0}^{n-1} g(P + jT').$$

After cancelling terms on the both sides, we get $g(P + nT') = g(P)$. As, $nT' = T$, so we get

$$e_n(T, T) = \frac{g(P+T)}{g(P)} = 1$$

From bilinearity property,

$$e_n(S+T, S+T) = e_n(S,S)e_n(S,T)e_n(T,S)e_n(T,T)$$

Since, $e_n(T,T) = 1$, $e_n(S,S) = 1$ and $e_n(S+T, S+T) = 1$. So, $e_n(S,T)e_n(T,S) = 1$. Therefore, $e_n(T,S) = e_n(S,T)^{-1}$. Hence, proved.

3. Let $T \in E[n]$ be such that $e_n(S,T) = 1$ for all $S \in E[n]$. Then, $g(P+S) = g(P)$ for all $S \in E[n]$. So, there exist a function $h \in \bar{K}(E)$ such that $g = h \circ n$. Then
$$(h \circ n)^n = g^n = f \circ n$$
Since, we know that multiplication by n is surjective on $E(\bar{K})$ which implies that $f = h^n$. Therefore,
$$n\ div(h) = div(f) = n[T] - n[\mathcal{O}]$$
Thus, $div(h) = [T] - [\mathcal{O}]$. By theorem, we get $T = \mathcal{O}$. Hence, proved.

4. Let $\sigma \in G_{\bar{K}/K}$. If f and g are the functions for T. Then, $div(f^\sigma) = n[T^\sigma] - n[\mathcal{O}]$ and similarly $(g^\sigma)^n = f^\sigma \circ n$, where f^σ and g^σ are the functions which are obtained by applying σ to the coefficients of the rational functions f and g. Therefore,
$$e_n(S^\sigma, T^\sigma) = \frac{g^\sigma(P^\sigma + S^\sigma)}{g^\sigma(P^\sigma)} = \left(\frac{g(P+S)}{g(P)}\right)^\sigma = e_n(S,T)^\sigma$$
Hence, proved.

5. Let f and g are two rational functions such that
$$div(f^m) = mdiv(f) = nm[T] - nm[\mathcal{O}]$$
and
$$(g \circ m)^{nm} = (f \circ mn)^m \qquad as\ f \circ n = g^n.$$
Therefore, by the definition of the Weil pairing
$$e_{nm}(S,T) = \frac{g \circ m(P+S)}{g \circ m(P)} = \frac{g(Y+mS)}{g(Y)} = e_n(mS,T).$$
where $mP = Y$. Hence, proved.

□

Corollary 5.2 *Let T_1, T_2 be a basis of $E[n]$. Then, $e_n(T_1, T_2)$ is primitive n-th root of unity. In particular, if $E[n] \subseteq E(K)$ then, $\mu_n \subseteq K^*$.*

Proof Suppose $e_n(T_1, T_2) = \zeta$ such that $\zeta^d = 1$. Then $e_n(T_1, T_2)^d = 1$. By bilinearity property $e_n(T_1, T_2)^d = e_n(dT_1, T_2) = e_n(T_1, dT_2)$. So, $e_n(dT_1, T_2) = 1$ and $e_n(T_1, dT_2) = 1$. Let S $\in E[n]$. Then, $S = aT_1 + bT_2$, where a,b $\in \mathbb{Z}$. Thus, for all $S \in E[n]$

$$e_n(S, dT_2) = e_n(T_1, dT_2)^a e_n(T_2, dT_2)^b = 1$$

Then, by non-degeneracy property $dT_2 = \mathcal{O}$. And, $dT_2 = \mathcal{O}$ if and only if n divides d. Thus, ζ is a primitive n-th root of unity.

If $E[n] \subseteq E(K)$ then the points in $E[n]$ are allowed to have coordinates in $\bar{K}$. So, we need to show that these points have all coordinates in K in order to prove that $\mu_n \subseteq K^*$. As, T_1, T_2 be the basis of $E[n]$ so T_1 and T_2 are assumed to have coordinates in K. Let $\sigma \in G_{\bar{K}/K}$. Then, by Galois invariance property of Weil pairing we have ,

$$\zeta = e_n(T_1, T_2) = e_n(T_1^\sigma, T_2^\sigma) = (e_n(T_1, T_2))^\sigma = \zeta^\sigma$$

The fundamental theorem of Galois theory implies that ζ lies in purely inseparable extension of K, but when $char(K)$ does not divide n then $n-$th root of unity generates a separable extension of K. Hence, $\zeta \in K$. Thus, $\mu_n \subseteq K^*$. □

Proposition 5.3 *Let E be an elliptic curve and $\alpha : E \longrightarrow E$. Then $e_n(\alpha S, \alpha T) = e_n(S, T)^{deg(\alpha)}$ for all separable endomorphisms α of E. This statement is also true in the case of a frobenius endomorphism α if the coefficients of E lie in the finite field $\mathbb{F}_q$.*

5.3 Modified Weil Pairing

For cryptographic applications we need to modify the definition of Weil Pairing to evaluate the pairing at points aP and bP for some integers a, b. As $e_n(aP, bP) = e_n(P, P)^{ab} = 1$ because of the alternating property of the Weil pairing .

Definition 5.4 *Let E be an elliptic curve over a finite field $\mathbb{F}_q$, $P \in E[n]$ and let ϕ be an n-distortion map for P. Then the* **modified Weil pairing** *denoted by*

$\tilde{e}_n$ is defined by $\tilde{e}_n(P_1, P_2) = e_n(P_1, \phi(P_2))$.

where e_n *is the usual Weil-Pairing and* $P_1, P_2 \in E[n]$*.*

Lemma 5.5 *Let* $3 \nmid n$ *and* $P \in E(\mathbb{F}_q)$ *is a point of order* n *then* $\tilde{e}_n(P, P)$ *is a primitive* n*-th root of unity.*

Proof Let $aP = b\phi(P)$ for some integers a and b. Then by the property of endomorphism we get

$$\phi(bP) = b\phi(P) = aP \in E(\mathbb{F}_q).$$

If $bP = \mathcal{O}$, then $aP = \mathcal{O}$, thus $a \equiv 0 (mod\, n)$. If $bP \neq \mathcal{O}$ then let $bP = (x, y)$ where $x, y \in \mathbb{F}_q$. Then

$$(\omega x, y) = \phi(bP) \in \mathbb{F}_q$$

Since the primitive third root of unity $\omega \notin \mathbb{F}_q$, then $x = 0$. Therefore, the two possibilities for bP are $(0, 1)$ and $(0, -1)$. But the order of these two points is 3 and we have already assumed that $3 \nmid$ n. So, if $aP = b\phi(P)$ then $a, b \equiv 0(mod\, n)$. Thus P and $\phi(P)$ are the basis of $E[n]$. Then by the corollary 5.2 $\tilde{e}_n(P, P) = e_n(P, \phi(P))$ is a primitive root of unity. □

Chapter 6

Cryptography

6.1 Introduction

Cryptography is the study of mathematical methods required for secure communication between parties over an insecure channel(in presence of adversary or eavesdropper who tries to get any piece of information being exchanged between the sender and the receiver). Suppose Alice wants to send a message, which is called as plaintext to Bob and in order to prevent the Eve (Eavesdropper) from reading the message, she converts it or encrypts it into unreadable form called as ciphertext. When Bob receives the message, he converts the ciphertext or decrypt the message to read it. Here Alice uses the encryption key to encrypt the message and Bob uses the decryption key for decrypting the ciphertext. So, in order to keep the Eve from reading the message we need to keep the decryption key secret from Eve.

Definition 6.1 *A cryptosystem is basically a five tuple* $(\mathcal{M}, \mathcal{C}, \mathcal{K}, E_k, D_d)$ *where it satisfies following conditions*

- $\mathcal{M}$ *denotes the message space and an element of* $\mathcal{M}$ *is called a plaintext.*
- $\mathcal{C}$ *denotes the ciphertext space and an element of* $\mathcal{C}$ *is called a ciphertext.*
- $\mathcal{K}$ *denotes the key space and an element of* $\mathcal{K}$ *is called a key.*
- *For each* $k \in \mathcal{K}$ *there exist a bijection map* E_k *called as an encryption function where* $E_k : \mathcal{M} \longrightarrow \mathcal{C}$
- *For each* $d \in \mathcal{K}$ *there exist a bijection map called as a decryption function* D_d *where* $D_d : \mathcal{C} \longrightarrow \mathcal{M}$.

- *The process of transforming the message $m \in \mathcal{M}$ to ciphertext by applying E_k is called encryption of m and the process of applying the transformation D_d to a ciphertext c is called decryption(inverse of encryption) of c.*

- *An encryption scheme consists of a set $E_k : k \in \mathcal{K}$ of encryption functions and a corresponding set $D_d : d \in \mathcal{K}$ of decryption functions such that for every plaintext element $m \in \mathcal{M}$ we get $D_d(E_k(m)) = m$. That is for each $k \in \mathcal{K}$ there exist a unique key $d \in \mathcal{K}$ such that $D_d = E_k^{-1}$.*

- *The pair of keys (k, d) is called key pair.*

The encryption scheme in which both the encryption and decryption key are same or one can be easily deduced from the other is called as **symmetric encryption**.

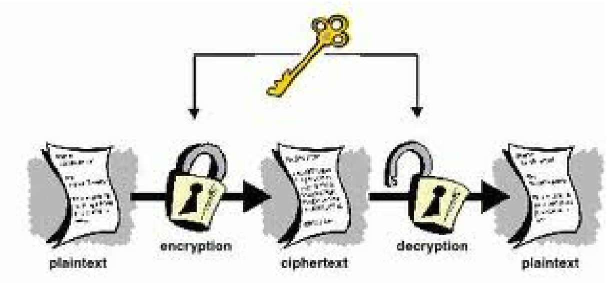

Figure 6.1: Symmetric encryption

When both the encryption and decryption key are different then the encryption scheme is known as **Public key encryption**. In this the encryption key can be made public so it is called as public key and decryption key is called as secret key or private key because it is kept secret.

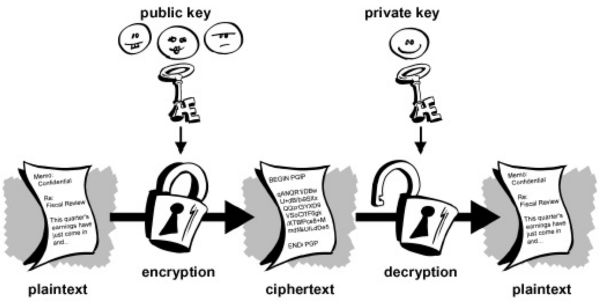

Figure 6.2: Asymmetric encryption

Main goals of cryptography are to provide Confidentiality, Data Integrity, Authentication and Non-repudiation from both the theoretical and practical aspects.

Definition 6.2 **Confidentiality** *means keeping the information content secret from all except the ones who are authorized to have it.*

Definition 6.3 **Data Integrity** *aims to prevent unauthorized alteration such as insertion, deletion and substitution of data.*

Definition 6.4 **Authentication** *deals with the identification of the entities participating in the communication and the information delivered over a channel.*

Definition 6.5 **Non- repudiation** *guarantees that an entity cannot later deny the previous commitments or actions .*

6.2 Classes of attacks and security models

An adversary can attack a cryptosystem in two ways:

1. In **Passive attack**, an adversary only monitors the communication channel and is capable of threatening the confidentiality of data only.
2. In **Active attack**, an adversary attempts to threatens the data integrity, authentication and confidentiality of data.

A passive attack on encryption scheme can be subdivided into following categories :

1. In **Ciphertext-only attack** aim of the adversary is to deduce the decryption key or plaintext from the corresponding ciphertext by only observing the ciphertext.
2. In **known plaintext attack** the adversary posses a quantity of plaintext and corresponding ciphertext when he mounts the attack.
3. In **Chosen plaintext attack(CPA)**, adversary chooses plaintext messages and gets encryption assistance to obtain the corresponding ciphertext messages. The adversary targets to weaken cryptosystem(to recover plaintext corrsponding to the previous unseen ciphertext) using the obtained plaintext-ciphertext pairs.

4. An **Adaptive chosen plaintext attack** is a chosen plaintext attack but in this attack the choice of plaintext may depend on the previously received ciphertext.

5. In **Chosen ciphertext attack(CCA)**, adversary chooses ciphertext and gets decryption assistance to obtain the corresponding plaintext messages. The adversary is successful if he gets some secret plaintext information from a target ciphertext(unseen) which is given to the adversary after the decryption assistance is stopped.

6. An **Adaptive chosen ciphertext attack** is a CCA but in this attack the choice of ciphertext may depend on the previously received plaintext.

The bijection function plays an important role in cryptography. They are used for encrypting the messages and the inverse transformation is used for decryption. Mostly functions which are used in cryptography are one way function and trapdoor function.

Definition 6.6 **One-way function** *A function $E_k : \mathcal{M} \longrightarrow \mathcal{C}$ is said to be a one way function if for all messages $m \in \mathcal{M}$ it is easy to calculate $E_k(m)$ but for all ciphertexts $c \in \mathcal{C}$ it is computationally infeasible to find any $m \in \mathcal{M}$ such that $E_k(m) = c$. That is, given k it is infeasible to find out the corresponding decryption key d.*

Definition 6.7 **Trapdoor one-way function** *A trapdoor one way function is a one way function but for any given $c \in \mathcal{C}$ it is computationally feasible to find an $m \in \mathcal{M}$ such that $E_k(m) = c$.*

The security of most of the cryptosystems are based on the hardness of the mathematical problem which are fast to compute but hard to inverse and the hardness of the problem is determined by the time taken by the algorithm to solve the problem. The problems which are believed to be secure and practical till date are Integer factorization problem, Finite field discrete logarithm problem and Elliptic curve discrete logarithm problem. The problems which are secure today doesn't mean they are unbreakable in future.

Definition 6.8 *The* **Integer factorization problem** *is that given a positive integer n, we need to find its prime factorization. That is, to write $n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$ where p_i are pairwise distinct primes and each $e_i \geq 1$.*

Example 6.9 Suppose we have two prime numbers, 3 and 7, then it takes no time to calculate the product, which is 21. But what if we have a number, 21, and we want to know which pair of primes are multiplied together to obtain this number. Calculating the product takes milliseconds, whereas factoring will take longer. The problem becomes much harder if we start with primes that have 400 digits or so, because the product will have 800 digits.

Definition 6.10 **Generalized discrete logarithm problem(GDLP):** *Given a generator α of the cyclic group G of order n, find the integer x, where $0 \leq x \leq n-1$, such that $\alpha^x = \beta$. Integer x can be written as $log_\alpha \beta$ and it is called as the discrete logarithm of β.*

Example 6.11 Suppose we want to take the number 3 to the $6th$ power; it is easy to calculate 36 = 729, but if we have the number 729 and we want to find out the two integers which we have used, x and y so that $log_x 729 = y$, it will take longer to find all possible solutions and select the used pair. The problem become much harder with the large values of x and y. The groups which are of most interest in cryptography are the multiplicative group $\mathbb{F}_q^*$ of the finite field including the multiplicative group $\mathbb{Z}_p^*$ of the integers modulo a prime p.

Definition 6.12 **Discrete logarithm problem(DLP):** *Given a prime p, a generator $\alpha \in \mathbb{Z}_p^*$ and an element $\beta \in \mathbb{Z}_p^*$, we need to find the integer x, where $0 \leq x \leq p-2$, such that $\alpha^x = \beta(modp)$.*

Definition 6.13 **Computational Diffie-Hellman problem (CDH):**
Given a cyclic group G, a generator $\alpha \in G$ and the group elements α^a and α^b we need to find α^{ab}, where $a, b \in [1, |G|]$.

The CDH problem is based on the assumption that discrete logarithm problem is hard problem and it is computationally intractable to compute the value of α^{ab} .

If cyclic group G is multiplicative group of integers then the CDH problem is : Given a prime p, a generator $\alpha \in \mathbb{Z}_p^*$ and elements α^a mod p and $alpha^b$ mod p, we need to find α^{ab} mod p , where $a, b \in [1, |G|]$.

Definition 6.14 **Decision Diffie-Hellman problem (DDH)** *Given a cyclic group G, a generator $\alpha \in G$ and elements α^a, α^b and α^c we need to determine whether $\alpha^c = \alpha^{ab}$.*

DDH is a computationally hard problem based on the intractability of DLP and it assumes that the values α^c and α^{ab} are computationally indistinguishable. It is used to prove the security of many cryptosystems such as ElGamal public encryption scheme.

6.3 Security of the cryptosystems

The objective of the adversary which is trying to break a cryptosystem is to deduce the secret key or private key. If he doesn't get successful in finding the secret key then his aim is to gain more information than the communicating parties wants. The adversaries goals are following:

- **Total break** :If an adversary is able to deduce the decryption key then the encryption scheme is said to be completely broken as the adversary now can decrypt any ciphertext that has been encrypted using that key.

- **Partial break**: If an adversary is able to decrypt the previous unseen ciphertext without finding the decryption key with some non-negligible probability or to deduce some specific information about the plaintext of the given ciphertext then the cryptosystem is said to be partial broken.

- **Distinguishability of ciphertexts** In this the adversary is able to distinguish between encryptions of two given plaintexts or between an encryption of a given plaintext and a random string with some probability exceeding 1/2.

In a secure cryptosystem no partial information regarding the plaintext should get revealed in polynomial time by observing the given ciphertext and ciphertext distinguishability should be computationally infeasible. Thus a cryptosystem should satisfy one of these strong notions of security:

Definition 6.15 **Polynomially secure**: *A cryptosystem is said to be polynomial secure if in polynomial time an adversary selects two messages m_1 and m_2 and is not able to distinguish between encryption of m_1 and m_2 with probability significantly greater than* 1/2.

A scheme that is polynomially secure is often said to have Indistinguishability of encryptions (IND).

Definition 6.16 **Semantically secure** *A cryptosystem is said to be semantically secure if the ciphertext does not reveal any partial information about the plaintext in expected polynomial time.*

In perfect secrecy, an adversary is not able to gain any information about the plaintext from the ciphertext even in the presence of infinite computational resources but may learn the length of the plaintext. Thus we can observe that semantic security is the polynomial bounded version of the perfect secrecy.

6.4 RSA

RSA is the best known public-key cryptosystem, named after its inventors Rivest, Shamir and Adleman. Its security is based on the intractability of the integer factorization problem and for that it is necessary to take the value of $n = pq$ to be large enough such that factoring will be computationally infeasible.

Both Alice and Bob have to create an RSA public key and a corresponding private key by using RSA paramater generation algorithm for setting up the RSA cryptosystem.

RSA Key Generation Algorithm:

- Generate two large random distinct prime numbers p and q .
- Compute $n = pq$ and $\phi(n) = (p-1)(q-1)$. Where ϕ is an euler function.
- Choose a random integer e where $1 < e < \phi(n)$ such that gcd $(e, \phi(n)) = 1$.
- Compute d where $1 < d < \phi(n)$ such that $de \equiv 1 \pmod{\phi(n)}$.
- The Public keys is (n, e) and private key is d.

Suppose both Alice and Bob have their own private key and public key and let Bob's public key is (n, e) and private key is d. For encrypting the message m (less than n) Alice should follow these steps:

- Alice first obtain the Bob's authentic public key (n, e).
- message m is encrypted by calculating $c = m^e \mod n$

- Alice sends the ciphertext c to Bob.

For decrypting the ciphertext Bob uses his private key d to recover message m by computing $m = c^d \mod n$.

6.5 Elliptic Curve cryptography

Elliptic Curve Cryptography (ECC) is an approach to public-key cryptography based on elliptic curve theory and the Elliptic curves are used in cryptosystems because of the reason that they provide security equivalent to classical cryptosystems. The security of such cryptosystems relies on the difficulty of the elliptic curve logarithm which is the DLP in a group defined by rational points lying on an elliptic curve over a finite field. This results in dramatic decrease in key size needed to achieve the same level of security in conventional Public key cryptography scheme. For example:A 160 bit elliptic curve cryptosystem key has about the same level of security as 1024 bit RSA key. Moreover, ECC is the best known algorithm that solves the ECDLP in exponential time where other conventional cryptosystems takes sub-exponential time. ECC keys takes much more effort to break compared to RSA and DSA keys. ECC device require less storage, less power, less memory, less bandwidth than other cryptosystems which allows to implement cryptography in platforms that are constraint such as wireless devices, smart cards, thin- clients.

6.5.1 Elliptic Curve Discrete Logarithm Problem

Given E an elliptic curve defined over a finite field $\mathbb{F}_p$ and points P and $Q \in E(\mathbb{F}_p)$, we need to find an integer m such that $Q = mP$.

Example 6.17 Let $E : y^2 = x^3 + x + 1$ be an elliptic curve over the field $\mathbb{F}_p$, where $p = 5$ and the points $P = (0, 1)$ and $Q = (2, 1) \in E(\mathbb{F}_5)$, then it is easy to calculate the multiple of P. That is, $2P = (4, 2)$, $3P = (2, 1)$, $4P = (3, 4)$, $5P = (3, 1)$, $6P = (2, 4)$, $7P = (4, 3)$, $8P = (0, 4)$, $9P = \mathcal{O}$, and find out the value of m such that $Q = mP$. But the problem become much harder for large values of p.

6.5.2 Diffie- Hellman Key Exchange(DHK)

In the case of public key encryption, every user has a public key known to everybody and a private key known only to the user itself to decrypt the ciphertexts. Thus private and authenticated communication is possible without having to meet to agree on a shared secret key. But in the case of symmetric-key cryptography, Alice and Bob have to meet before and agreed on a secret key for producing authentication information and verifying the validity of the authentication information. So, without prior contact the only communication channel which is available for exchanging the secret key is public. Thus, Diffie and Hellman key exchange provides a solution to the problem of establishing the secret key between two parties over a channel controlled by adversary.

Suppose Alice and Bob agree on an elliptic curve E over a finite field $\mathbb{F}_q$

1. Setup: Alice and Bob chooses an elliptic curve E over a finite field $\mathbb{F}_q$ such that DLP is hard in $E(\mathbb{F}_q)$ and a point $P \in E(\mathbb{F}_q)$ whose order is a large prime.

2. Alice chooses a random secret integer a and computes the value of $P_a = aP$ and sends it to Bob.

3. Bob chooses a random secret integer b and computes the value of $P_b = bP$ and sends it to Alice.

4. Alice receives bP and computes the secret key $aP_b = abP$.

5. Bob receives aP and computes the secret key $bP_a = abP$.

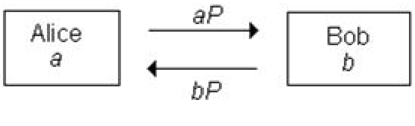

Figure 6.3: Diffee Hellman Key Exchange

6. Instead of taking abP as the secret key, Alice and Bob can also use some publically agreed method to extract the key from abP for example they could take the last 156 bits of the $x-$coordinate of the point abP or could obtain the value of secret key by applying a hash function on $x-$coordinate.

Diffie-Hellman Key Exchange(Generalized)		
Setup: A prime p and a generator $\alpha \in \mathbb{Z}_p^*$ where $2 \leq \alpha \leq p-2$ are selected and published.		
Alice	Adversary	Bob
chooses a random secret number x		chooses a random secret y.
Calculate $X_A = \alpha^x modp$		Calculate $X_B = \alpha^y modp$
Alice receives X_B	Can see X_A and X_B	Bob receives X_A
shared key $K = X_B^x \mod p$		shared key $K = X_A^y$ mod p.

The security of DHK is based on the intractability of the Diffie-Hellman problem as the information which is available to adversary is the $E(\mathbb{F}_q)$, the points P, aP and bP. So, adversary have to solve the DHP in order to break the cryptosystem .

Definition 6.18 **Diffie-Hellman problem**: *Given an elliptic curve E over a finite field $\mathbb{F}_q$ and the points P, aP, bP in $E(\mathbb{F}_q$, we need to compute abP.*

Definition 6.19 **Decision Diffie-Hellman problem** *Given an elliptic curve E over a finite field $\mathbb{F}_q$ and the points P, aP, bP, Q in $E(\mathbb{F}_q)$, we need to determine whether or not $Q = abP$.*

6.5.3 Tripartite Diffie-Hellman Key Exchange:

Suppose Alice, Bob and chris wants to establish a secret key or common key. For establishing the common key we can use the standard Diffie-Hellman key exchange protocol but it requires two rounds of communication and in some cases these two rounds can be very complicated so single round would be preferable.

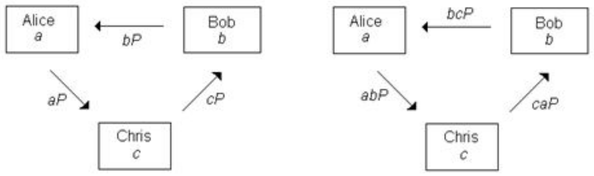

Figure 6.4: Two rounds of standard Diffee Hellman Key Exchange protocol

The Tripartite Diffie-Hellman key exchange protocol provides an efficient algorithm for establishing the secret key between more than two parties and it requires only one round of communication.

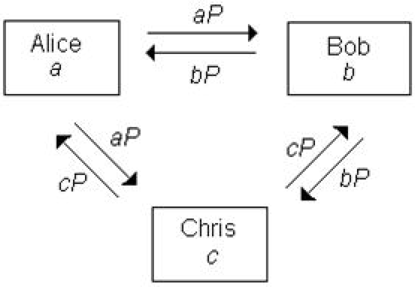

Figure 6.5: Tripartite Diffee Hellman Key Exchange

This algorithm is based on the application of Weil pairing on the elliptic curves. In this, an elliptic curve $E(\mathbb{F}_q)$ and a point P $\in E(\mathbb{F}_q)$ of order n where n is a large prime are public paramters.

Tripartite Diffie-Hellman Key Exchange		
Alice	Bob	Chris
Chooses secret integer $a \mod n$	Chooses secret integer $b \mod n$	Chooses secret integer $c \mod n$
Calculate aP	Calculate bP	Calculate cP
Receives bP, cP	Receives aP, cP	Bob Receives aP, bP
Computes $\tilde{e}_n(bP, cP)^a$	Computes $\tilde{e}_n(aP, cP)^b$	Computes $\tilde{e}_n(aP, bP)^c$
Secret key $= \tilde{e}_n(bP, cP)^a = \tilde{e}_n(aP, cP)^b = \tilde{e}_n(aP, bP)^c$		

6.5.4 Identity Based Encryption(IBE)

In this section we will discuss about the method by Boneh and Franklin which uses the Weil Pairing on the elliptic curves to obtain a cryptosystem. In this cryptosystem each user has a public key which is based on the public identity such as an email address and a corresponding private key which is assigned by a central trusted authority(TA) to each user. IBE cryptosystem is semantically secure assuming that Bilinear Diffie Hellman Problem(BDH) is problem is hard.

Definition 6.20 **BDH**: *Let G_1 and G_2 are two groups of prime order q, $\tilde{e}$ be the modified Weil pairing such that $\tilde{e} : G_1 \times G_1 \longrightarrow G_2$ and P be a generator of G_1. Then for given $\langle P, aP, bP, cP\rangle$ where $a, b, c \in \mathbb{Z}_q$ we need to compute $W = \tilde{e}(P, P)^{ab} \in \mathcal{G}_2$.*

An algorithm A has advantage ϵ in solving BDH in $< G_1, G_2, \tilde{e} >$ if

$$Pr\left[A(P, aP, bP, cP) = \tilde{e}(P, P)^{abc}\right] \geq \epsilon$$

where the probability is over the random choice of a, b, c in $\mathbb{Z}_q^*$, the random choice of $P \in G_1^*$.

BDH Parameter Generator We say that a randomized algorithm G is a BDH parameter generator if

1. G takes a security parameter $k \in \mathbb{Z}^+$,
2. G runs in polynomial time in k, and
3. G outputs a prime number q, two groups G_1, G_2 of order q, and a modified Weil pairing map $\tilde{e} : G_1 \times G_1 \to G_2$. $< q, G_1, G_2, \tilde{e} >$ is the output of G.

BDH Assumption Let G be a BDH parameter generator. We say that an algorithm A has advantage $\epsilon(k)$ in solving the BDH problem for G if for sufficiently large k:

$$Adv_{G,A(k)} = Pr\left[A(q, G_1, G_2, \tilde{e}, P, aP, bP, cP) = \tilde{e}(P, P)^{abc}\right] \geq \epsilon(k)$$

The BDH is said to be hard in groups generated by the BDH parameter generator if it satisfies the BDH assumption.

An IBE scheme is described by four randomized algorithms: **Setup**, **Extract**, **Encrypt**, **Decrypt**.

1. **Setup**: Given a security parameter $k \in \mathbb{Z}^*$, the setup algorithm does the following
   1: Run G the BDH parameter generator on input k to generate a prime q, two groups G_1, G_2 of order q, and the modified Weil pairing map $\tilde{e} : G_1 \times G_1 \to G_2$. Choose a random point $P \in G_1$.
   2: Chooses a random $s \in \mathbb{Z}_q^*$ and set $P_{pub} = sP$.
   3: Chooses cryptographic hash function H_1 and H_2 such that $H_1 : \{0,1\} * \to G_1^*$ and $H_2 : G_2 \to \{0,1\}^n$ for some n. Here n is the length of the messages that will be sent and the ciphertext space is $\mathbf{C} = G_1^* \times \{0,1\}^n$. The system parameters are publicly available, that is **params** $= \langle q, G_1, G_2, \tilde{e}, n, P, P_{pub}, H_1, H_2 \rangle$. The **master-key** is $s \in \mathbb{Z}_q^*$ is kept secret.
2. **Extract:**TA takes as input params, master key, a given string $ID \in \{0,1\}^*$ and returns a private key to the user with identity ID by doing the following:

(1) computes $Q_{ID} = H_1(ID)$. This is a point in the group G_1.
(2) computes the **private key** d_{ID} to be $d_{ID} = sQ_{ID}$ where s is the master key and sends d_ID to the user ID.

3. **Encrypt:** To encrypt $m \in M$ under the public key ID, we need to do the following:
(1) compute $Q_{ID} = H_1(ID) \in G_1^*$,
(2) choose a random $r \in \mathbb{Z}_q^*$,
3) compute $g_{ID} = \tilde{e}(Q_{ID}, P_{pub}) \in G_2^*$. (3) Set the ciphertext to be $C = \langle rP, m \oplus H_2(g_{ID}^r) \rangle$, where $\oplus$ denotes bitwise addition $\mod 2$.

4. **Decrypt:** To decrypt the ciphertext, let $C = \langle U, V \rangle \in \mathbf{C}$ using the public key do the following:
1) use the private key $d_{ID} \in G_1^*$ and compute $V \oplus H_2(\tilde{e}(d_{ID}, U))$

The decryption here works because

$$\begin{aligned}\tilde{e}(d_{ID}, U) &= \tilde{e}(sQ_{ID}, rP)\\ &= \tilde{e}(Q_{ID}, P)^{sr}\\ &= \tilde{e}(Q_{ID}, P_{pub})^r)\\ &= g_{ID}^r.\end{aligned}$$

Thus, applying decryption after encryption procedure gives us the original message m. That is,

$$\begin{aligned}&= V \oplus H_2(\tilde{e}(d_{ID}, U))\\ &= (m \oplus H_2(g_{ID}^r)) \oplus H_2(g_{ID}^r)\\ &= m\end{aligned}$$

Security The IBE scheme is a semantically secure assuming that BDH is hard in groups generated by G. and it can be proved by the following theorem.

Theorem 6.21 *Let H_1, H_2 are two hash functions. Then IBE is a semantically secure assuming BDH is hard in groups generated by G. Concretely, suppose there is an IND-ID-CPA adversary A that has advantage $\epsilon(k)$ against the IBE scheme. Suppose A makes at most $q_E > 0$ private key extraction queries and $q_{H_2} > 0$ hash queries to*

H_2. Then there is an algorithm B that solves BDH in groups generated by G with advantage at least:

$$Adv_{G,B}(k) = \frac{2\epsilon(k)}{e(1+q_E)q_{H_2}}$$

Here $e \sim 2.71$ is the base of the natural logarithm. The running time of B is $O(time(A))$.

Bibliography

[1] Joseph H. Silverman, *The Arithmetic of Elliptic Curve*, second ed, Springer, 1986.

[2] Lawrence C. Washington , *Elliptic curves: Number theory and Cryptography*, second ed, Chapman & Hall CRC.

[3] A. Menezes, Scott Vanstone, Paul Van Oorschot *Handbook of Applied Cryptology*, CRC Press 1996.

[4] Dan Boneh and Matthew Franklin *Identity-Based Encryption from the Weil Pairing.*, Springer-verlag 2001.

[5] Douglas R. Stinson , *Cryptography Theory and Practice*, third ed, Chapman & Hall CRC.

[6] J. Silverman and J. Tate, *Rational points on Elliptic Curves*, Springer UTM, 1992.

[7] Leonard S.Charlap and David P. Robbins, *An Elementary Introduction to Elliptic Curves*, CRD Expository Report 31, Dec 1998.

[8] Paulo S. L. M. Barreto, Hae Y. Kim, Ben Lynn, and Michael Scott, *Efficient Algorithms for Pairing-Based Cryptosystems.*