Appendix - A

1. Here are some graphs of curve developed using the MATLAB. The curve is defined over a finite field $F_q$ and of the form $y^2 = x^3 + ax + b$ and is represented as $E_q(a,b)$.

![The points in $E_{121}(1,1)$](image)

Fig.1  Number of points-144
From the below mentioned figures we can see that number of points of the curve is not only dependent on the size of the field but also on the parameters a and b. size of the field but also on the parameters a and b.

II. 1. Here is some of the sample MATLAB code for generation of curves and certain operations done using MAT Lab in this thesis

/* This is a MATLAB function for generation of curve along with points. The
 p is the field size, a and b are the parameters of the curve $y^2 = x^3 + ax + b$. The
 function generates the curve generates the points along with number of points
 on curve. It also plot the points on graph. */
function [points,n] = curvepoints (a, b, p)
points=zeros(1,1);
R1 = zeros(3,1);
L1 = zeros(3,1);
X = zeros(2,1);
Y = zeros(2,1);
for i=0:1:(p-1)
    R1(i+1) = (i)^3 + a*(i) + b;
    R1(i+1) = rem(R1(i+1),p);
    L1(i+1) = (i)^2;
    L1(i+1) = rem(L1(i+1),p);
end
ii=1;
for z=0:1:(p-1)
    I=find(R1==z);
    J=find(L1==z);
    e1 = isempty(I);
    e2 = isempty(J);
    if (e1) == 0
        if (e2) == 0
            n=length(I);
            m=length(J);
            for h=1:n
                for g=1:m
                    X(ii)=I(h)-1;
                    Y(ii)=J(g)-1;
                    P=[X(ii),Y(ii)];
                    points(ii)=P;
                    ii=ii+1;
                end
            end
        end
    end
end
n=length(X) + 1;
disp(n);
%Generation of curve as points on a graph%
M=plot(X,Y,'x');
z = [X,Y];
disp(' X Y');
disp(z);
set(h(1),'LineWidth',2);
xlabel('X','FontSize',14,'FontWeight','regular');
ylabel('Y','FontSize',14,'FontWeight','regular');

II.2 function [x3,y3,m] = ECADD(x1,y1,x2,y2,a,p)
% This function performs Elliptic Curve addition over an elliptic curve y^2 = x^3 + ax + b .Here we are adding two points P1(x1,y1) and P2(x2,y2) to get a third point P3(x3,y3) which is the sum of P1 and P2.
if x1 == Inf
    x3 = x2; y3 = y2;
    return
end

if x2 == Inf
    x3 = x1; y3 = y1;
    return
end

if x1 == x2
    if y1 == y2
        display('X3 is infinity')
        x3 = Inf; y3 = Inf;
        return
    end
    n = sym((3*(x1)^2 + a)/(2*(y1)))
    n = 3*(x1)^2 - a;
    d = 2*(y1);
    m = mod(n * inverse(d, p), p);%*Slope of the curve is generated *%
    x3 = mod(m^2 - x1 - x2, p);
    y3 = mod(m*(x1 - x3) - y1, p);
    return
end

display('P3 is infinity');

m = mod((n * inverse(d, p), p));

x3 = mod(m^2 - x1 - x2, p);

y3 = mod(m*(x1 - x3) - y1, p);
Appendix – B

I. Hasse’s Theorem

Hasse’s theorem states that Let \( t = q + 1 - \#E(F_q) \). Then

\[ \#E(F_q^k) = q^k + 1 - \alpha^k - \beta^k \]

where \( 1 - tx + qx^2 = (1 - \alpha x)(1 - \beta x) \).

II. Chinese remainder Theorem

Theorem 1: For \( a, m \in \mathbb{Z} \) such that \( ax = 1 \mod m \) if and only if \( \gcd(a, m) = 1 \).

Proof: There is \( a, x \in \mathbb{Z} \) such that \( ax \equiv 1 \mod m \) \( \Rightarrow \) there are \( x, y \in \mathbb{Z} \) such that \( ax - my = 1 \).

Suppose \( m_1, \ldots, m_r \in \mathbb{N} \) are relatively prime in pairs, i.e. \( \gcd(m_i, m_j) = 1 \) for \( i \neq j \). Let \( a_1, \ldots, a_r \in \mathbb{Z} \). Then, the system of \( r \) congruences is given by

\[ x \equiv a_i \pmod{m_i} \quad (1 \leq i \leq r) \]

has a unique solution modulo \( M = m_1 \times \ldots \times m_r \) given by

\[ x = \sum_{i=1}^{r} a_i M_i y_i \mod M \]

where \( M_i = M/m_i \) and \( M_i y_i \equiv 1 \mod m_i \).

Proof: Note that \( M_i \) is the product of all \( m_j \) where \( j \neq i \). So if \( j \neq i \) then \( M_i \equiv 0 \mod m_j \). Note also that \( \gcd(M_i, m_i) = 1 \), so by Theorem 1, \( M_i y_i \equiv 1 \mod m_i \) has a solution \( y_i \). Thus, \( x = \sum_{i=1}^{r} a_i M_i y_i \equiv a_i M_i y_i \equiv a_i \mod m_i \) for all \( i, 1 \leq i \leq r \). Therefore, \( x \) is a solution to the system of congruences.
III Euler’s function

Euler’s function $\varphi : \mathbb{N} \rightarrow \mathbb{N}$ is defined as

$$\varphi(m) = \# \{ k \in \mathbb{N} \mid 1 \leq k \leq m, \, \gcd(k, m) = 1 \}$$

IV Schoof’s Algorithm

In 1985, Schoof presented a deterministic algorithm that could compute $\#E(F_q)$ (its precise value; not a bound or an estimate) in $O(\log q)$ bit operations (where $F_q$ is a finite field of characteristic $= 2, 3$)

1. Let $l_1 = 3, l_2 = 5, l_3 = 7, \ldots , l_k$ be the $k$ consecutive primes starting at 3, where $k$ is the largest integer such that

$$\prod_{i=1}^{k} l_i \leq 4 \sqrt[q]{q} \quad \text{set} \quad L = l_k$$

2. Compute $\tau_i \pmod{l_i}$ for all $i (1 \leq i \leq k)$.

3. Use the Chinese Remainder Theorem to compute

$$T = \sum_{i=1}^{k} \tau_i M_i y_i \pmod{M} \quad \text{where} \quad M = \prod_{i=1}^{k} l_i, \quad M_i = M/l_i \quad \text{and} \quad M_i y_i \equiv 1 \pmod{l_i}.$$  

Find a $t$ that satisfies $|t| \leq 2$ (Hasses theorem) i.e if $t > 2\sqrt[q]{q}$ set $t = t - M$.

4. Compute $\#E(F_q) = q + 1 - t$.

V Koblitz’s random Selection method

1. Randomly select three elements from $F_q$; Let them be $x, y, a$.

2. Set the value for $b$ by computing $b = y^2 - (x^3 + ax)$ since curve equation (1.5) is $y^2 = x^3 + ax + b$. 

3. Check that cubic on the right side of equation 1.2, so that it should not have multiple roots, i.e. check that \(4a^3 + 27b^2 \neq 0\).

If condition in step 3 is not met, return to step 1.

Else set \(P = (x, y)\) and let \(y^2 = x^3 + ax + b\) be our elliptic curve.

**VI. Koblitz's construction algorithm**

1. Randomly choose a large prime \(q\).
2. Use Koblitz's random selection method to find an elliptic curve \(E(F_q)\) of the type defined in (2.4).
3. Use Schoof algorithm to compute \(#E(F_q)\).
4. Verify that \(#E(F_q)\) is a (large) prime.
5. If step 4 is not satisfied return to step 2.

If Koblitz's algorithm is performed, then any point in \(E\) other than \(O\) would be the generator of \(E\) and the ECDLP over \(E\) will be intractable.