ELLIPTIC CURVES & ELLIPTIC CURVE DISCRETE LOGARITHM PROBLEM

Dissertation submitted in partial fulfilment of the requirement for the

MASTER'S DEGREE IN MATHEMATICS

By

HIMA MANOJ K

Reg No. 200011014781

Under the Guidance of

Dr. PAUL ISSAC

Department of Mathematics

BHARATA MATA COLLEGE, THRIKKAKARA

(Affiliated to Mahatma Gandhi University, Kottayam)

2020-2022

DECLARATION

I Hima Manoj K hereby declare that this project entitled **‘ELLIPTIC CURVES & ELLIPTIC CURVE DISCRETE LOGARITHM PROBLEM’** is a bonafide record of work done by me under the guidance of Dr. Paul Issac, Associate Professor, Department of Mathematics, Bharata Mata College, Thrikkakara and this work has not previously formed by the basis for the award of any academic qualification, fellowship or other similar title of any other University or Board.

Hima Manoj K
Msc Mathematics
Bharata Mata College,Thrikkakara

Place: Thrikkakara
Date:

CERTIFICATE

This is to certify that the project entitled **'ELLIPTIC CURVES & ELLIPTIC CURVE DISCRETE LOGARITHM PROBLEM'** submitted for the partial fulfilment requirement of Master's Degree in Mathematics is the original work done by Hima Manoj K during the period of the study in the Department of Mathematics, Bharata Mata College, Thrikkakara under my guidance and has not been included in any other project submitted previously for the award of any degree.

Dr. Paul Issac
Supervisor

Place: Thrikkakara
Date:

ACKNOWLEDGEMENT

First and foremost I express my sincere gratitude towards the abiding presence and grace of God Almighty.

I sincerely express my gratitude to Dr. Paul Issac, Associate professor, Department of Bharata Mata College, Thrikkakara for guiding and helping me to complete this work.

I also express my profound gratitude to Dr. Seethu Varghese, Head of the Department of Mathematics for her wholehearted cooperation and valuable advices.

Finally, I am obliged to all our teachers of the Mathematics Department, Bharata Mata College for the encouragement for completing this work.

Hima Manoj K

CONTENTS

Introduction

Preliminary

Chapter 1: Introduction to Elliptic Curves

1.1 Elliptic Curves

1.2 Geometry of Elliptic Curves

1.3 Isogenies

1.4 Weierstass Equation for Elliptic Curves

Chapter 2: Elliptic curve over finite fields

2.1 No of Rational Points

2.2 Supersingular Elliptic Curves

Chapter 3: Elliptic Curves over C

3.1 Lattices and Fundamental Parallelogram

3.2 Analytic Maps

3.3 Weirstrass $\wp$ function

3.4 Uniformization

Chapter 4: Elliptic Curve Cryptosystems

4.1 Elliptic curve Cryptography

4.2 History of ECC

4.3 Example of ECC

Chapter 5: Elliptic Curve Discrete Logarithm Problem

5.1 Introduction to ECDLP

5.2 Solving ECDLP

5.2.1 Exhaustive Search method

5.2.2 Collision Search Method

5.2.3 Pollard's ρ Method

5.2.4 Parallelized Pollard's ρ Method

Chapter 6: Other Applications of Elliptic Curves

6.1 Factorizing using Elliptic Curve

6.2 Primality Testing

Conclusion

References

ABSTRACT

Elliptic Curves are the curves that's also naturally a group. From an elliptic curve, we can construct an algebra by adding, doubling and multiplying points. Its group structure helps to describe the various notion of mathematics. Those features of Elliptic curve are discussed in chapter 1. Elliptic curves hold different structures in various field. In chapter 2 and 3, we focus on the behavior of Elliptic curves in finite and complex field respectively. In a finite field, we can compute the points on the elliptic curve. A point is simply a pair (x, y) that satisfies the equation of the curve. Since there is a finite number of units in the field, there must be a finite number of unique points on the curve. This number is known as the order of the curve. For various cryptographic reasons, we desire that the order be a large prime, or have a large prime as one of its factors. For Complex field, we can reduce from the Weirstrass equation of elliptic curves that, complex tori are isomorphic to complex elliptic curves.

In Chapter 4 and 5 we discussed about Elliptic curve cryptography and Elliptic curve discrete logarithm problem. Elliptic curves started being used in cryptography and elliptic curve techniques were developed for factorization and primality testing. Elliptic curve cryptography (ECC) is one of the strongest algorithms in cryptography. ECC provides higher security in small keys in faster mode than other cryptographic algorithms. Elliptic curve discrete logarithm problem (ECDLP) is the hard problem supports ECC. The well-known attack to ECDLP is Pollard's rho algorithm. Other than Cryptography we have seen that elliptic curves are used for factorization and Primality testing. Chapter 7 gives these applications of elliptic curves. For any composite number n elliptic curve factorization method gives the factors of n. And there exist theorems using elliptic curves that provide the characteristic of a prime number.

INTRODUCTION

An elliptic curve over a field K is a non-singular complete curve of genus 1 with a distinguished point. Elliptic curves have been objects of intense study in Number Theory for the last 90 years. To quote “It is possible to write endlessly on Elliptic Curves (This is not a threat).” (Miller in Crypto 85). An important feature of an elliptic curve is their points have the structure of an abelian group. This feature makes theory of elliptic curves more interesting with links to various notions of mathematics. Elliptic curves appear in many diverse areas of mathematics, ranging from number theory to complex analysis, and from cryptography to mathematical physic Although the problem to find the points of an elliptic curve with rational numbers as coordinates fascinated many mathematicians since the time of the ancient Greeks, it was not until 1922 that it was proved that it is possible to construct all the points of an elliptic curve.

Cryptography is one of the main fields where research is done. Researchers spent quite a lot of time trying to explore cryptographic systems based on more reliable trapdoor functions and in 1985 succeeded by discovering a new method, namely the one based on elliptic curves which were proposed to be the basis of the group for the discrete logarithm problem. Researchers believe that elliptic curves guarantee more security and provide with much smaller key sizes than other groups.

Elliptic curve discrete logarithm problem (ECDLP) was brought into spot light along with the introduction of elliptic curve cryptography independently by Koblitz and Miller in 1985. If the elliptic curve groups is described using multiplicative notation, then the elliptic curve discrete logarithm problem is: given points P and Q in the group, find a number that Pk = Q; k is called the discrete logarithm of Q to the base P. When the elliptic curve group is described using additive notation, the elliptic curve discrete logarithm problem is: given points P and Q in the group, find a number k such that Pk = Q. The main goal of this project is to learn about elliptic curves over finite field and C , elliptic curve cryptography and elliptic curve discrete logarithm problem.

PRELIMINARIES

Projective plane curve

A (projective plane algebraic) curve (over K) is a non-constant homogeneous polynomial $F \in K[x, y, z]$. We call $V(F) = \{(x,y) \in P^2 : F(x,y) = 0\}$ its set of points.

Genus

Broadly, the genus of a curve is the number of handles added to a sphere. A sphere has genus g = 0. A torus has genus g = 1.

Non singular

Let $P=(a,b) \in E(K)$. If at least one of the partial derivatives $\frac{\partial f}{\partial X}, \frac{\partial f}{\partial Y}$ is nonzero at P, then P is said to be nonsingular

Point of inflection

A point of inflection is a point at which the graph of y = f (x) has a tangent line and where the concavity changes. So, if f is twice–differentiable, then f has a Point of Inflection where y changes sign. A point of inflection on an elliptic curve is, similarly, a point (x, y) on the curve where y is defined and changes sign.

Homomorphism

A homomorphism is a structure-preserving map between two algebraic structures of the same type such as two groups, two rings, or two vector spaces.

Automorphism

An automorphism is a structure preserving map from an algebraic structure to itself.

Frobenius endomorphism

Let *R* be a commutative ring with prime characteristic *p*. The Frobenius morphism *F* is defined by

$F(r) = r^p$ for all *r* in *R*.

Galois group

Suppose that E is an extension of the field F (written as E / F and read "E over F "). An automorphism of E / F is defined to be an automorphism of E that fixes F pointwise. In other words, an automorphism of E / F is an isomorphism $\alpha : E \to E$ such that $\alpha (x) = x$ for each $x \in F$. The set of all automorphisms of E / F forms a group with the operation of function composition. This group is sometimes denoted by Aut(E / F) . If E / F is a Galois extension, then Aut(E / F) is called the Galois group of E / F . A Galois extension is an algebraic field extension E/F that is normal and separable; or equivalently, E/F is algebraic, and the field fixed by the automorphism group Aut(E/F) is precisely the base field F.

Inseperable Extension

In algebra, a purely inseparable extension of fields is an extension $k \subseteq K$ of fields of characteristic $p > 0$ such that every element of K is a root of an equation of the form $x^q = a$, with q a power of p and a in k.

Height of Formal group

Let f be a formal group law over a commutative ring R, and fix a prime number p. We let v_n denote the coefficient of t^{p^n} p-series [p]. We will say that f has height $\geq n$ if $v_i = 0$ for $i < n$. We will say that f has height exactly n if it has height $\geq n$ and $v_n \in R$ is invertible.

Homothetic Lattices

Lattices L and M in C are homothetic if there is a complex number λ such that $M = \lambda L$.

1. INTRODUCTION TO ELLIPTIC CURVES

1.1 Elliptic Curves

Definition: Let K be a perfect field. An Elliptic Curve over K can be defined as,

(a) a nonsingular projective plane curve E over K of degree 3 together with a point O ∈ E(K)

(b) same as (a) except that O is required to be a point of inflection.

(c) A non-singular projective plane curve of the form

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

(d) a nonsingular projective curve E of genus 1 together with a point O ∈ E(K).

Let (E, O) be as in (b); we can show that a linear change of variables will carry E into the form (c) and O into the point (0:1:0) as, let $(a: b: c) \in P^2(K)$ and assume $b \neq 0$. The regular map

$(x : y: z) \mapsto (bx\text{-}ay :by :bz\text{-}cy) : P^2 \mapsto P^2$

sends $(a: b: c)$ to $(0 :b^2 :0) = (0 :1 :0)$ and is an isomorphism (it has an inverse of a similar form). If $b = 0$, but $c \neq 0$, we first interchange the y and z coordinates. Thus, we may suppose (0 :1 :0). Conversely, let E be as in (c); then O = (0:1:0) ∈ E(K) and is a point of inflection.

For the curve in (c), if Z=0, then we get $X^3=0$, thus X=0 is a solution. Thus we get (0:Y:0)=(0:1:0) ,an intersecting point of the curve with the line of infinity Z=0. Thus, The point O(0:1:0) is known as Point at Infinity.

Proposition 1.1

Let E be an elliptic curve defined over K.

(a) There exist functions x,y ∈ K(E) such that the map $\varphi : E \rightarrow P^2$, $\varphi = [x,y, 1]$, gives an isomorphism of E/K onto a curve given by a Weierstrass equation

$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$ with coefficients $a_1,\ldots,a_6 \in$ K and satisfying $\varphi(O) = [0, 1, 0]$. The functions x and y are called Weierstrass coordinates for the elliptic curve E.

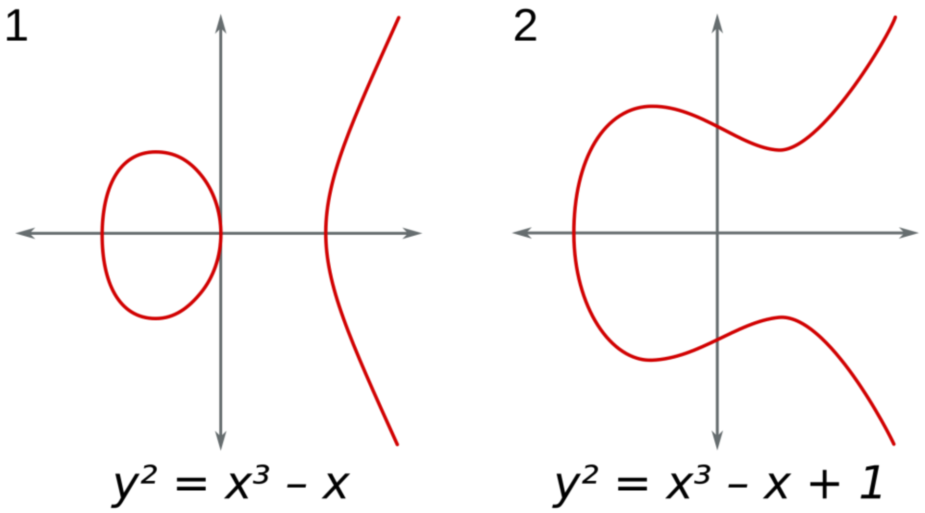
(It is explained in section 1.3)

(b) Any two Weierstrass equations for E as in (a) are related by a linear change of variables of the form

$X = u^2X' + r, \qquad Y = u^3Y' + su^2X' + t,$, with $u \in$ K* and $r,s,t \in$ K.

(c) Conversely, every smooth cubic curve C given by a Weierstrass equation as in (a) is an elliptic curve defined over K with base point O = [0, 1, 0].

Examples:



Every point in an elliptic curve E is either of finite order or of infinite order. Let P be a point in E, if there exist a *m* in Z such that *m*P=0, then P is said to have finite order. If there doesn't exist such an *m* in Z, then P has infinite order. By infinite order we mean that, we never get point of infinity after any *n* summands of P.

1.2 Geometry of elliptic curves

Let E be an Elliptic curve in K. Then E consist of a point P(*x*,*y*) satisfies the cubic equation together with the point at infinity. Let L be a line in K. Since the equation is third degree L intersects E at exactly 3 points.

Composition Law

Let P,Q ∈ E, let L be the line through P and Q (if P = Q, let L be the tangent line to E at P), and let R be the third point of intersection of L with E. Let L' be the line through R and O. Then L' intersects E at R, O, and a third point. We denote that third point by P ⊕Q

Proposition 1.2

The composition law has the following properties:

(a) If a line L intersects E at the (not necessarily distinct) points P,Q,R,
then (P ⊕Q) ⊕R = O.

(b) P ⊕O = P for all P ∈ E.

(c) P ⊕Q = Q ⊕P for all P,Q ∈ E.

(d) Let P ∈ E. There is a point of E, denoted by -P, satisfying P ⊕(-P) = O.

(e) Let P,Q,R ∈ E. Then (P ⊕Q) ⊕R = P ⊕(Q ⊕R).

In other words, the composition law makes E into an abelian group with identity element O.
Further:

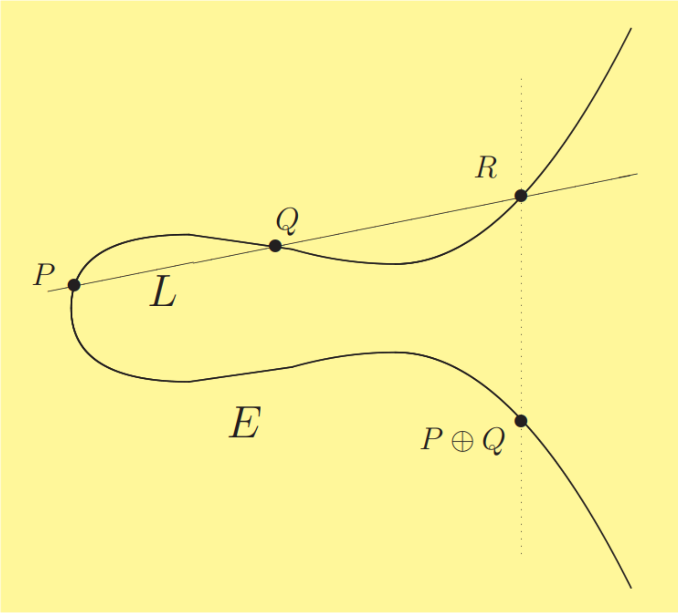
(f) Suppose that E is defined over K.

Then E(K) = $\{ (x,y) \in K^2 : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \} \cup \{O\}$ is a subgroup of E.

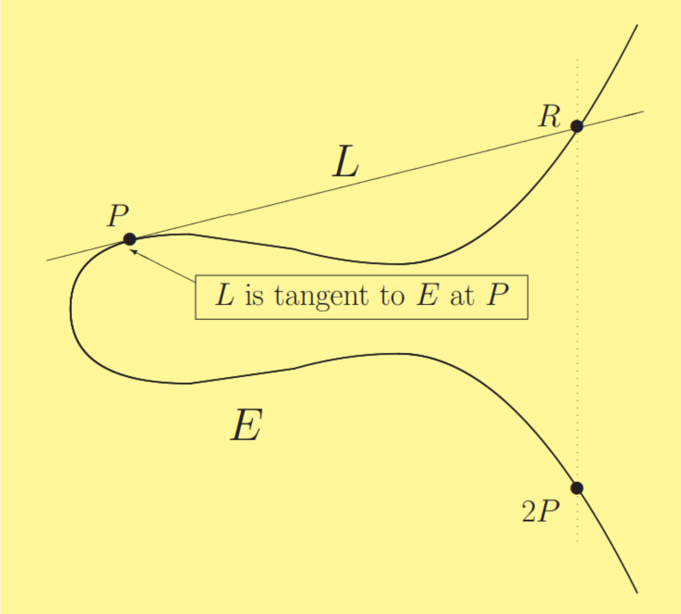
Illustration:

Consider the elliptic curve E. Let P and Q be two points on E. Let L be the line through P and Q. L meets E at a third point say R. The vertical line through R hits E at another point.

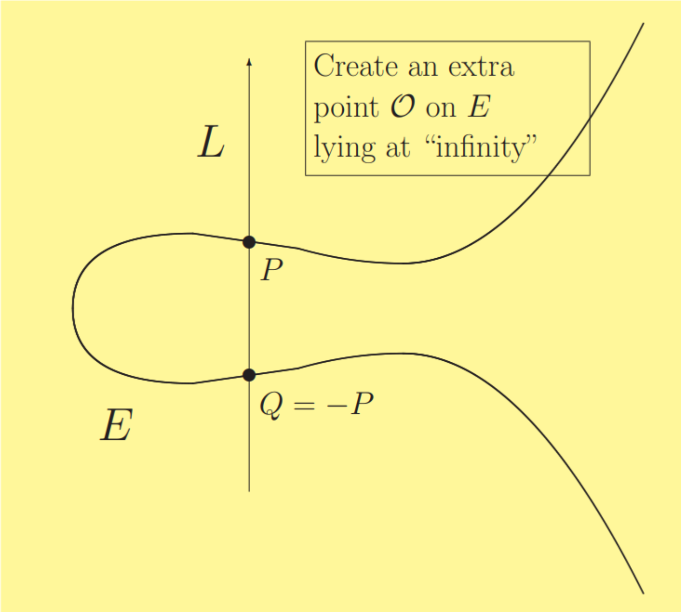
We define it as the sum of P and Q, and is denoted by P ⊕Q.



We can add P to itself. Since there are so many lines possible through P, we consider the tangent line through P which intersects E. So here L is the tangent line of E through P. L meets E at R and the reflected point of R gives P ⊕P or 2P.



The vertical line through P and –P does not meet at the third point. So, we create an extra point on that line O called ‘Point at Infinity’ to define P ⊕(-P).


Create an extra point $\mathcal{O}$ on E lying at "infinity"
L
P
$Q = -P$
E

1.3 Isogeny

Definition: Let E_1 and E_2 be elliptic curves. An isogeny from E_1 to E_2 is a morphism $\varphi: E_1 \to E_2$ satisfying $\varphi(O) = O$. Two elliptic curves E_1 and E_2 are isogenous if there is an isogeny from E_1 to E_2 with $\varphi(E_1) \neq \{O\}$.

Elliptic curves are abelian groups, so the maps between them form groups. We denote the set of isogenies from E_1 to E_2 by $\mathrm{Hom}(E_1, E_2) = \{\text{isogenies } E_1 \to E_2\}$.

The sum of two isogenies is defined by $(\varphi + \psi)(P) = \varphi(P) + \psi(P)$ implies that $\varphi+\psi$ is a morphism, so it is an isogeny. Hence $\mathrm{Hom}(E_1, E_2)$ is a group.

If $E_1 = E_2$, then we can also compose isogenies. Thus if E is an elliptic curve, we let $\mathrm{End}(E) = \mathrm{Hom}(E,E)$ be the ring whose addition law is as given above and whose multiplication is composition,

$(\varphi\psi)(P) = \varphi(\psi(P))$

The ring End(E) is called the endomorphism ring of E. The invertible elements of End(E) form the automorphism group of E, which is denoted by Aut(E).If E_1, E_2 and E are defined over a field K, then we can restrict attention to those isogenies that are defined over K. The corresponding groups of isogenies are denoted with the usual subscripts; thus $\mathrm{Hom}_K(E_1,E_2)$, $\mathrm{End}_K(E)$, $\mathrm{Aut}_K(E)$.

1.4 Weierstrass equation for an Elliptic curve

Let E be an elliptic curve over K. Any equation of the form

$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$ is called a Weierstrass equation for the elliptic curve.

To ease notation, we generally write the Weierstrass equation for our elliptic curve using non-homogeneous coordinates $x = X/Z$ and $y = Y/Z$,

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

always remembering that there is an extra point O = [0, 1, 0] out at infinity. As usual, if $a_1, a_2, \ldots, a_6 \in$ K, then E is said to be defined over K. If char(K) ≠ 2, then we can simplify the equation by completing the square. Thus the substitution

$$y \longmapsto \frac{1}{2}(y - a_1x - a_3)$$

gives an equation of the form

$$E : y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6,$$

Where, $b_2 = a_1^2 + 4a_4, \qquad b_4 = 2a_4 + a_1a_3, \qquad b_6 = a_3^2 + 4a_6.$

We also define the quantities

$$\begin{aligned} b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2, \\ c_4 &= b_2^2 - 24b_4, \\ c_6 &= -b_2^3 + 36b_2b_4 - 216b_6, \\ \Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6, \\ j &= c_4^3/\Delta, \\ \omega &= \frac{dx}{2y + a_1x + a_3} = \frac{dy}{3x^2 + 2a_2x + a_4 - a_1y}. \end{aligned}$$

These satisfies

$$4b_8 = b_2b_6 - b_4^2 \text{ and } 1728\Delta = c_4^3 - c_6^2.$$

If further char(K) ≠ 2, 3, then the substitution eliminates x^2 term and we get,

$$E : y^2 = x^3 - 27c_4x - 54c_6.$$

The quantity Δ is the discriminant of the Weierstrass equation, the quantity *j* is the *j*-invariant of the elliptic curve, and ω is the invariant differential associated to the Weierstrass equation.

Let P = (x_0,y_0) be a point satisfying a Weierstrass equation

$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$ and assume that P is a singular point.

Then we have $\frac{\partial f}{\partial x}(P) = \frac{\partial f}{\partial y}(P) = 0.$ It follows that there are α,β ∈ K such that the Taylor series expansion of E at P has the form

$$f(x,y) - f(x_0,y_0) \\ = \big((y-y_0) - \alpha(x-x_0)\big)\big((y-y_0) - \beta(x-x_0)\big) - (x-x_0)^3.$$

With notation as above, the singular point P is a node if α ≠ β. In this case, the lines $y - y_0 = \alpha(x- x_0)$ and $y - y_0 = \beta(x - x_0)$ are the tangent lines at P. Conversely, if α = β, then we say that P is a cusp, in which case the tangent line at P is given by $y - y_0 = \alpha(x - x_0)$.

A Weierstrass equation is in **Legendre form** if it can be written as $y^2 = x(x - 1)(x - \lambda)$. Assume that char(K) ≠ 2.Then, Every elliptic curve is isomorphic (over K) to an elliptic curve in Legendre form $E_\lambda : y^2 = x(x - 1)(x - \lambda)$ for some λ ∈ K with λ = 0, 1.

Since Char(K) ≠ 2, we know that E has a weirstrass equation of the form

$$E : y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6,$$

Replacing (x,y) by $(x,2y)$ and factorizing ,we get,

$$y^2 = (x - e_1)(x - e_2)(x - e_3) \text{ where } e_1, e_2, e_3 \in K$$

since $\Delta = 16(e_1 - e_2)^2(e_1 - e_3)^2 (e_2 - e_3)^2 \neq 0$, we see that the e_i 's are distinct. Now the substitution $x = (e_2 - e_1)x' + e_1$, $y = (e_2 - e_1)^{3/2}y'$ gives an equation in Legendre form with $\lambda = (e_3 - e_1)/(e_2 - e_1) \in K$, $\lambda \neq 0, 1$.

Take an elliptic curve E/Q and write it in Weierstrass form $y^2 = x^3 + ax + b$. The *j*-invariant is given by .

$$j(E) = 1728\frac{4a^3}{4a^3 + 27b^2}.$$

2. ELLIPTIC CURVES OVER A FINITE FIELD

2.1 No of Rational Points

Let E/F_q be an elliptic curve defined over a finite field. Here we try to determine the number of points in $E(F_q)$ or equivalently the number of solutions to the equation

$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$ with $(x, y) \in F_q^2$

Theorem 2.1 (Hasse)

Let E/F_q be an elliptic curve defined over a finite field. Then

$| \# E(F_q) - q - 1| \leq 2 \sqrt{q}$

Proof: Choose a Weierstrass equation for E with coefficients in F_q, and let $\varphi: E \to E$, $(x,y) \to (x^q,y^q)$, be the qth-power Frobenius morphism. Since the Galois group $G_{F_q^{al}/F_q}$ is (topologically) generated by the qth-power map on F_q, we see that for any point $P \in E(F_q^{\ al})$, $P \in E(F_q)$ if and only if $\varphi(P) = P$. Thus $E(F_q) = \ker(1 - \varphi)$, So we can find that,

$\#E(F_q) = \#\ker(1 - \varphi) = \deg(1 - \varphi)$.

Since the degree map on End(E) is a positive definite quadratic form and since $\deg \varphi = q$, we get the result by the theorem, Let A be an abelian group, and let $d: A \to Z$ be a positive definite quadratic form. Then for all $\psi,\varphi \in A$,

$$|d(\psi - \phi) - d(\phi) - d(\psi)| \leq 2\sqrt{d(\phi)d(\psi)}$$

Remark: Hasse's theorem gives a bound for the number of points in $E(F_q)$, but it does not provide a practical algorithm for computing $\# E(F_q)$ when q is large.

Example

Let F_q be a finite field with q odd. We can use Hasse's result to estimate the value of certain character sums on F_q. Thus let

$$f(x) = ax^3 + bx^2 + cx + d \in K[x]$$

be a cubic polynomial with distinct roots in F_q^{al}, and let $\chi : F_q^* \rightarrow \{\pm1\}$ be the unique nontrivial character of order 2, i.e., $\chi(t) = 1$ if and only if t is a square in F_q^* . Extend χ to F_q by setting $\chi(0) = 0$. We can use χ to count the F_q -rational points on the elliptic curve $E : y^2 = f(x)$

Each $x \in F_q$ yields zero, one, or two points $(x,y) \in E(F_q)$ according to whether the value f(x) is, respectively, a nonsquare, equal to zero, or a square in F_q. Thus in terms of χ we obtain (remember the extra point at infinity)

$$\begin{aligned} \#E(\mathbb{F}_q) &= 1 + \sum_{x\in\mathbb{F}_q} (1 + \chi(f(x))) \\ &= 1 + q + \sum_{x\in\mathbb{F}_q} \chi(f(x)). \end{aligned}$$

With notation as above,

$$\left|\sum_{x\in\mathbb{F}_q} \chi(f(x))\right| \leq 2\sqrt{q}.$$

We note that the sum shown above consists of q terms, each of which is ±1, so it says that as x runs through F_q, the values of the cubic polynomial f(x) tend to be equally distributed between squares and nonsquares. Indeed, if one takes a random sequence ($\varepsilon_1 ,\varepsilon_2 ,\ldots. \varepsilon_q$) of ones and negative ones, then the expected value of $| \varepsilon_1 + \varepsilon_2 +\ldots. +\varepsilon_q |^2$ is q, so the equation says that the set of values of $(\chi(f(x)))_{x\in\mathbb{F}_q}$ looks like a random sequence.

2.2 Supersingular Elliptic Curve

Definition: A point $P \in E$ is called a torsion point of order n if P has order n. Gathering all of the torsion points of a an elliptic curve C will form a finite subgroup of E, called E_{tor}: $E_{tor} = \{P \in E| \text{ P has finite order}\} \subseteq E$.

Let K be a (not necessarily finite) field of characteristic p, and let E/K be an elliptic curve. We know that there are two possibilities for the group of p-torsion points E[p], namely 0 and Z/pZ.

Theorem 2.2

Let K be a field of characteristic p, and let E/K be an elliptic curve. For each integer $r \geq 1$, let $\varphi_r : E \rightarrow E(p_r)$ and $\varphi\hat{}_r : E(p_r) \rightarrow E$ be the p_r -power Frobenius map and its dual.

(a) The following are equivalent.

(i) E[p_r]=0 for one (all) r ≥ 1.

(ii) $\varphi^\wedge{}_r$ is (purely) inseparable for one (all) r ≥ 1.

(iii) The map [p] : E → E is purely inseparable and j(E) ∈ F_{p2} .

(iv) End(E) is an order in a quaternion algebra.

(v) The formal group E/K ˆ associated to E has height 2.

(b) If the equivalent conditions in (a) do not hold, then E[p_r] = Z/ p_r Z for all r ≥ 1, and the formal group E/K has height 1. If further j(E) ∈ Fp^{al}, then End(E) is an order of a quadratic imaginary field. (For the case that j(E) is transcendental over F_p)

Definition: If E has the properties given in above theorem, then we say that E is supersingular, or that E has Hasse invariant 0. Otherwise, we say that E is ordinary, or that E has Hasse invariant 1.

Or we can say if an elliptic curve over a field of positive characteristic whose formal group law has height of a formal group equal to 2 is called a supersingular elliptic curve. Otherwise, the height equals 1 and the elliptic curve is called ordinary.

The next theorem gives a criterion to determine whether the given elliptic curve is supersingular or not.

Theorem 2.3

Let F_q be a finite field of characteristic p ≥ 3.

(a) Let E/ F_q be an elliptic curve given by a Weierstrass equation

E : $y^2 = f(x)$, where $f(x) \in F_q [x]$ is a cubic polynomial with distinct roots in F_q^{al}. Then E is supersingular if and only if the coefficient of x^{p-1} in $f(x)^{(p-1)/2}$ is zero.

(b) Let $m = (p - 1)/2$, and define a polynomial

$$H_p(t) = \sum_{i=0}^{m} \binom{m}{i}^2 t^i .$$

Let λ ∈ F_q^{al} with λ ≠ 0, 1. Then the elliptic curve

E : $y^2 = x(x - 1)(x - \lambda)$ is supersingular if and only if Hp(λ)=0.

(c) The polynomial Hp(t) has distinct roots in F_q^{al}. There is one supersingular curve in characteristic 3, and for p ≥ 5, the number of supersingular elliptic curves (up to F_q^{al} -isomorphism) is

$$\left[\frac{p}{12}\right] + \begin{cases} 0 & if\, p \equiv 1 \pmod{12}, \\ 1 & if\, p \equiv 5 \pmod{12}, \\ 1 & if\, p \equiv 7 \pmod{12}, \\ 2 & if\, p \equiv 11 \pmod{12}. \end{cases}$$

Example 1:

For p = 11 we have

$$H_{11}(t) \;\; = t^5 + 3t^4 + t^3 + t^2 + 3t + 1$$

$$= (t^2 - t + 1)(t + 1)(t - 2)(t + 5) \text{ (mod 11).}$$

The supersingular j-invariants in characteristic 11 are j = 0 and j = 1728 = 1

Example 2:

We compute for which primes p ≥ 5 the elliptic curve E : $y^2 = x^3 + 1$ with j = 0 is supersingular.

The criterion in theorem 2.3 says that we need to compute the coefficient of x^{p-1} in the polynomial $(x^3 + 1)^{(p-1)/2}$.

If p ≡ 2 (mod 3), then there is no x^{p-1} term, so E is supersingular.

On the other hand, if p ≡ 1 (mod 3), then the coefficient of x^{p-1} is $\binom{(p-1)/2}{(p-1)/3}$, which is nonzero modulo p, so in this case E is ordinary.

Example 3:

we compute for which primes p ≥ 3 the elliptic curve E : $y^2 = x^3 + x$ with j = 1728 is supersingular. This is determined by the coefficient of $x^{(p-1)/2}$ in the polynomial $(x^2 + 1)^{(p-1)/2}$.

This coefficient is equal to 0 if p ≡ 3 (mod 4) and $\binom{(p-1)/2}{(p-1)/4}$ if p ≡ 1 (mod 4). Hence E is supersingular if p ≡ 3 (mod 4) and ordinary if p ≡ 1 (mod 4).

Remark: These examples might suggest that for a given Weierstrass equation with coefficients in Z, the resulting elliptic curve is supersingular in characteristic p for half of the primes. This is in fact true, provided that the elliptic curve has complex multiplication over Q^{al} , as do the j = 0 and j = 1728 curves.

Example 4:

Let E be the elliptic curve given by the equation

$$E : y^2 + y = x^3 - x^2 - 10x - 20,$$

So $j(E) = -2^{12}31^3 / 11^5$. Then by the theorem, one finds that the only primes p < 100 for which E is supersingular in characteristic p are p ∈ {2, 19, 29}. More generally, D.H. Lehmer calculated that there are exactly 27 primes p < 31500 for which E is supersingular.

Remark: It is not hard to prove that for any elliptic curve E/Q, there are infinitely many primes p such that E is ordinary.

Theorem 2.4

Let E/Q be an elliptic curve without complex multiplication. Then the set of supersingular primes has density 0. More precisely, for every > 0 we have

$$\#\{p < x : E/\mathbb{F}_p \textit{ is supersingular}\} \ll x^{3/4+\epsilon}$$

Conjecture 2.5

Let E/Q be an elliptic curve without complex multiplication. Then

$$\#\{p < x : E/\mathbb{F}_p \textit{ is supersingular}\} \sim \frac{c\sqrt{x}}{\log x}$$

as x → ∞, where c > 0 is a constant depending on E.

Theorem 2.6

Let E/Q be an elliptic curve without complex multiplication. Then there are infinitely many primes p for which E/F_p is supersingular.

3. ELLIPTIC CURVES OVER C

3.1 Lattices and Fundamental Parallelogram

Definition: A lattice in C is the subgroup generated by two complex numbers that are linearly independent over R. Thus

$$\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2, \quad \text{some } \omega_1, \omega_2 \in \mathbb{C}, \;;$$

and since neither ω_1 nor ω_2 is a real multiple of the other, we can order them so that $\Im(\omega_1/\omega_2) > 0$. If $\{\omega_1', \omega_2'\}$ is a second pair of elements of , then

$$\omega_1' = a\omega_1 + b\omega_2, \quad \omega_2' = c\omega_1 + d\omega_2, \quad \text{some } a, b, c, d \in \mathbb{Z},$$

i.e., $\begin{pmatrix} \omega_1' \\ \omega_2' \end{pmatrix} = A \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix},$

with A a 2 x 2 matrix with integer coefficients. The pair $\{\omega_1', \omega_2'\}$ will be a Z-basis for if and only if A is invertible and so has determinant ±1. Let $z = \omega_1 / \omega_2$ and $z' = \omega_1' / \omega_2'$; then

$$\Im(z') = \Im\left(\frac{az+b}{cz+d}\right) = \frac{\Im(adz + bc\bar{z})}{|cz+d|^2} = \frac{(ad-bc)\Im(z)}{|cz+d|^2}$$

and so $\Im(\omega_1/\omega_2) > 0$ if and only if det A>0. Therefore, the group SL_2 (Z) of matrices with integer coefficients and determinant 1 acts transitively on the set of bases $\{\omega_1, \omega_2\}$ for Λ with $\Im(\omega_1/\omega_2) > 0$.

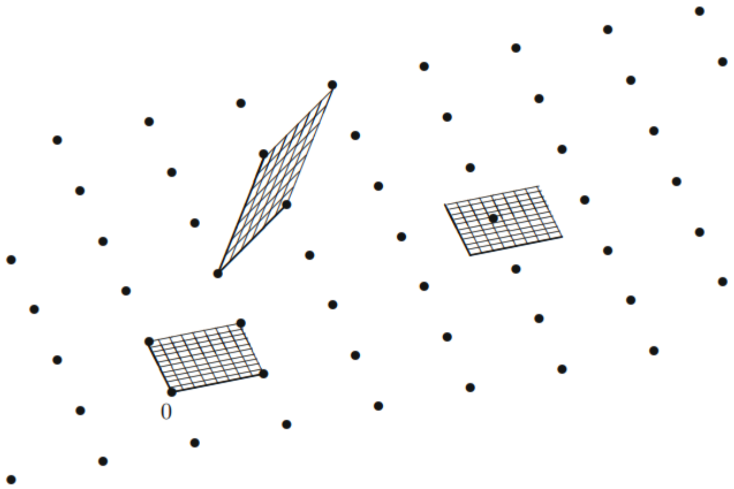
Proposition 3.1

Let M be the set of pairs of complex numbers $\{\omega_1, \omega_2\}$ such that $\Im(\omega_1/\omega_2) > 0$, and let *L* be the set of lattices in C. Then the map

$(\omega_1, \omega_2) \mapsto \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ induces a bijection SL_2 (Z)/M → *L*

Definition: An elliptic function (relative to the lattice Λ) is a meromorphic function $f(z)$ on C that satisfies $f(z + \omega) = f(z)$ for all $z \in$ C and all $\omega \in \Lambda$. The set of all such functions is denoted by $C(\Lambda)$. It is clear that $C(\Lambda)$ is a field.

Definition: A fundamental parallelogram for Λ is a set of the form $D = \{a + t_1\omega_1 + t_2\omega_2 : 0 \leq t_1 ,t_2 < 1\}$, where $a \in$ C and $\{\omega_1, \omega_2\}$ is a basis for Λ.



The figure shows a lattice and three fundamental parallelograms.

3.2 Analytic Maps

Let Λ_1 and Λ_2 be lattices in C, and suppose that $\alpha \in$ C has the property that $\alpha\Lambda_1 \subset \Lambda_2$. Then scalar multiplication by α induces a well-defined holomorphic homomorphism

$\varphi_\alpha : C/\Lambda_1 \rightarrow C/\Lambda_2$, $\varphi_\alpha(z) = \alpha z \pmod{\Lambda_2}$

Theorem 3.2

(a) With notation as above, the association

$\{\alpha \in C : \alpha \Lambda_1 \subset \Lambda_2\} \rightarrow \{$ holomorphic maps $\varphi : C/ \Lambda_1 \rightarrow C/ \Lambda_2$ with $\varphi(0) = 0 \}$

$\alpha \rightarrow \varphi_\alpha$ is a bijection.

(b) Let E_1 and E_2 be elliptic curves corresponding to lattices Λ_1 and Λ_2, respectively. Then the natural inclusion {isogenies $\varphi : E_1 \to E_2$} → { holomorphic maps $\varphi : C/\,\Lambda_1 \to C/\,\Lambda_2$ with $\varphi(0) = 0$ } is a bijection.

Corollary 3.3

Let E_1/C and E_2/C be elliptic curves corresponding to lattices Λ_1 and Λ_2 respectively. Then E_1 and E_2 are isomorphic over C if and only if Λ_1 and Λ_2 are homothetic, i.e., there exists some $\alpha \in C^*$ such that $\Lambda_1 = \alpha\, \Lambda_2$.

Remark: Since the maps φ_α are clearly homomorphisms, above corollary implies that every complex analytic map from E_1 (C) to E_2 (C) taking O to O is necessarily a homomorphism. This is the analytic analogue of the theorem which says that every isogeny of elliptic curves is a homomorphism.

3.3 Weirstrass ℘ function

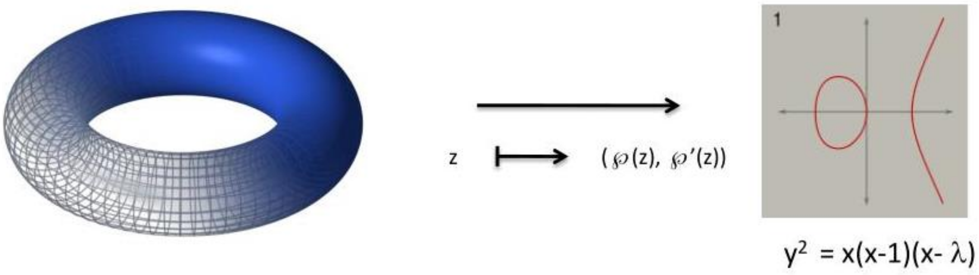
The points of an elliptic curve with coordinates in the complex numbers C form a torus.

The Weirstrass ℘ function gives a way of writing elliptic curves as a torus by C/L → E(C) such that $z \to (\wp(z),\ ½\ \wp'(z))$

Weirstrass ℘ function is given by

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega\in\Lambda,\,\omega\neq 0}\left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right)$$

$$\wp'(z) = \sum_{\omega\in\Lambda} \frac{-2}{(z-\omega)^{-3}}.$$



The Laurent Series expansion of $\wp$(z) around z = 0 is given by

$$\wp(z) = \frac{1}{z^2} + \sum_{k=1}^{\infty}(2k+1)G_{2k+2}z^{2k}.$$

And for all z ∈ C/Λ, the Weierstrass $\wp$-function and its derivative satisfy the relation

$$\wp'(z)^2 = 4\wp(z)^3 - 60G_4\wp(z) - 140G_6.$$

Now we can see that the function $f(z) = \wp'(z)^2 - 4\wp(z)^3 + 60G_4\wp(z) + 140G_6$

is holomorphic at z = 0 and satisfies f(0) = 0. But f(z) is an elliptic function relative to Λ, and it is holomorphic away from Λ, so f(z) is a holomorphic elliptic function.

Remark: It is standard to notate $g_2 = g_2(\Lambda) = 60G_4(\Lambda)$ and $g_3 = g_3(\Lambda) = 140G_6(\Lambda).$

Then we get

$$\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3.$$

3.4 Uniformization

Uniformization Theorem

Let A,B ∈ C be complex numbers satisfying $4A^3 - 27B^2 \neq 0$. Then there exists a unique lattice Λ ⊂ C satisfying g_2 (Λ) = A and g_3 (Λ) = B

Corollary 3.4

Let E/C be an elliptic curve. There exist a lattice Λ ⊂ C, unique up to homothety, and a complex analytic isomorphism

$$\phi : \mathbb{C}/\Lambda \longrightarrow E(\mathbb{C}), \qquad \phi(z) = [\wp(z,\Lambda), \wp'(z,\Lambda), 1],$$ of complex Lie groups.

Proposition 3.5

There are natural equivalences between the following categories:

(a) Objects: Elliptic curves E over C.

Morphisms: Regular maps E → E′ that are homomorphisms.

(b) Objects: Riemann surfaces E of genus 1 together with a point 0.

Morphisms: Holomorphic maps E → E′ sending 0 to 0′.

(c) Objects: Lattices Λ ⊂ C.

Morphisms: Hom(Λ, Λ′) = {α ∈ C | αΛ ⊂ Λ′}.

We now use the uniformization theorem to make some general deductions about elliptic curves over C.

Proposition 3.6

Let E/C be an elliptic curve and let m ≥ 1 be an integer.

(a) There is an isomorphism of abstract groups $E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$

(b) The multiplication-by-m map [m] : E → E has degree m^2.

Proof: (a) We know that E(C) is isomorphic to C/Λ for some lattice Λ ⊂ C. Hence

$$E[m] \cong \left(\frac{\mathbb{C}}{\Lambda}\right)[m] \cong \frac{\frac{1}{m}\Lambda}{\Lambda} \cong \left(\frac{\mathbb{Z}}{m\mathbb{Z}}\right)^2.$$

(b) Since char(C)=0 and the map [m] is unramified, the degree of [m] is equal to the number of points in $E[m]=[m]^{-1}$ {O}

Now let E/C be an elliptic curve then End(E) is a subring of C. Then we get, If $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$, then $\mathrm{End}(E) \cong \{\alpha \in \mathbb{C} : \alpha\Lambda \subset \Lambda\}.$

Since Λ is unique up to homothety this ring is independent of the choice of Λ.

Theorem 3.7

Let E/C be an elliptic curve, and let ω_1 and ω_2 be generators for the lattice Λ associated to E. Then one of the following is true:

(i) End(E) = Z.

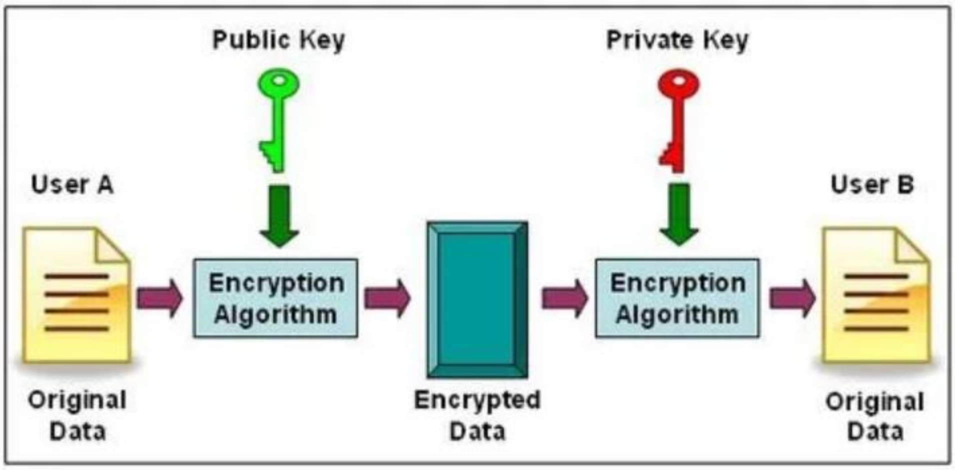
(ii) The field Q($\omega_2/\ \omega_1$) is an imaginary quadratic extension of Q, and End(E) is isomorphic to an order in Q($\omega_1/\ \omega_2$).

4. ELLIPTIC CURVE CRYPTOSYSTEMS

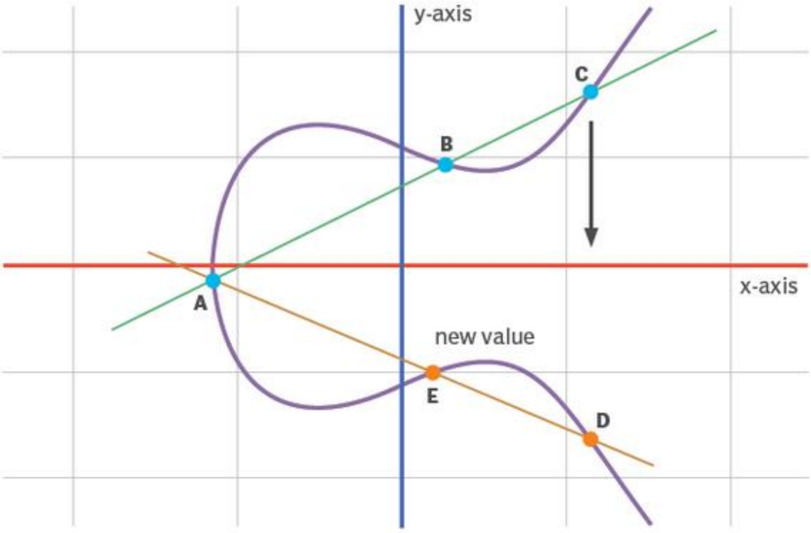
4.1 Elliptic Curve Cryptography

Elliptic curve cryptography [ECC] is a public-key cryptosystem just like RSA, Rabin, and ElGamal. Every user has a public and a private key. Public key is used for encryption/ signature verification while Private key is used for decryption/ signature generation.

The central part of any cryptosystem involving elliptic curves is the elliptic group. All public-key cryptosystems have some underlying mathematical operation. RSA has exponentiation (raising the message or ciphertext to the public or private values) and ECC has point multiplication (repeated addition of two points).



ECC is based on the properties of a set of values for which operations can be performed on any two members of the group to produce a third member, which is derived from points where the line intersects the axes as shown with the green line and three blue dots in the below diagram labeled A, B and C. Multiplying a point on the curve by a number produces another point on the curve (C). Taking point C and bringing it to the mirrored point on the opposite side of the x-axis produces point D. From here, a line is drawn back to our original point A, creating an intersection at point E. This process can be completed *n* number of times within a defined max value. The *n* is the private key value, which indicates how many times the equation should be run, ending on the final value that is used to encrypt and decrypt data. The maximum defined value of the equation relates to the key size used.



4.2 History of ECC

The properties and functions of elliptic curves in mathematics have been studied for more than 150 years. Their use within cryptography was first proposed in 1985, separately by Neal Koblitz from the University of Washington and Victor Miller at IBM.

ECC was first developed by Certicom, a mobile e-business security provider, and was then licensed by Hifn, a manufacturer of integrated circuitry and network security products. Vendors, including 3Com, Cylink Corp., Motorola, Pitney Bowes, Siemens, TRW Inc. (acquired by Northrop Grumman) and Verifone, supported ECC in their products.

The use of ECC in public and private sectors has increased over the past few years. While RSA continues to be more widely used and is easier to understand compared to ECC, the efficiency benefits of ECC make it appealing for many enterprise use cases. These include speeding up secure access to Secure Sockets Layer-encrypted websites and streaming encrypted data from IoT devices with limited computing power.

4.3 Example of ECC

- Suppose Alice wants to send to Bob an encrypted message.

  Both agree on a base point, B.

  Alice and Bob create public/private keys.

- Alice

  Private Key = a

  Public Key = P_A = a * B

- Bob

  Private Key = b

  Public Key = P_B = b * B

- Alice takes plaintext message, M, and encodes it onto a point, P_M, from the elliptic group
- Alice chooses another random integer, k from the interval [1, p-1]
- The ciphertext is a pair of points

  $P_C = [\ (kB), (P_M + k\ P_B\ )\ ]$

- To decrypt, Bob computes the product of the first point from P_C and his private key, b

  b * (kB)

- Bob then takes this product and subtracts it from the second point from P_C

  $(P_M + k\ P_B\ ) – [b(kB)] = P_M + k(bB) – b(kB) = P_M$

- Bob then decodes P_M to get the message, M.

5. ELLIPTIC CURVE DISCRETE LOGARITHM PROBLEM

5.1 Introduction to ECDLP

The elliptic curve discrete logarithm problem, which is abbreviated ECDLP, asks for a solution m to the equation $[m]P = Q$ for given points $P,Q \in E(Fq)$. If q is small, we can compute P, [2]P, [3]P,... until we find Q, but for large values of q it is quite difficult to find m. This has led people to create public key cryptosystems based on the difficulty of solving the ECDLP. Despite extensive research since the mid-1980s, the fastest known algorithms to solve the ECDLP on general curves are collision algorithms taking $O(\sqrt{q})$ steps. Thus the best known algorithms to solve the ECDLP in E(Fq) take exponential time, i.e., the running time is exponential in log q. This fact is the primary attraction for using elliptic curves in cryptography.

Let G be group, and let $x,y \in G$ be elements such that y is in the subgroup generated by x. The discrete logarithm problem (DLP) is the problem of determining an integer $m \geq 1$ such that $x^m = y$. The primary advantage of using elliptic curves is that at present, it is much harder to solve the ECDLP in E(Fq) than it is to solve the DLP in F_q^* . This means that elliptic curve cryptography has key and message sizes that are 5 to 10 times smaller than those for other systems.

5.2 Solving ECDLP

5.2.1 Exhaustive Search Method

Compute $[m_1]P$, $[m_2]P$, $[m_3]P$.... for randomly chosen values m_1, m_2, m_3 … until you get [m]P= Q. Since the field is Fq, and #E(Fq) = O(q). Hence the expected computational time is O(q). If P is of order n, then the running time will be n at the worst case and n/2 in average. Therefore, exhaustive search can be find out a way by selecting elliptic curve parameters with n sufficiently large to represent an infeasible amount of computation (e.g., $n \geq 2^{80}$).

5.2.2 Collision Search Method

Algorithms of the type collision algorithms, because they depend on the fact that it is easier to find collisions (elements that are common to two subsets) than it is to find specific elements in a set. This phenomenon is also known as the birthday paradox.

Compute two lists for randomly chosen values m_1, m_2, m_3, . . .

List 1: $[m_1]P$, $[m_2]P$, $[m_3]P$.....

List 2: $Q - [m_1]P$, $Q - [m_2]P$, $Q - [m_3]P$ . . . until finding a collision $[m_i]P = Q - [m_j]P$.

Expecting running time is $O(\sqrt{q})$ by birthday paradox.

5.2.3 Pollard's ρ Method

An alternative collision algorithm, due to Pollard, takes approximately the same number of steps and reduces the storage to essentially nothing. Pollard's algorithm and its variants, which are the most practical methods currently known for solving the ECDLP. The collision method has running time $O(\sqrt{q})$, but it takes about $O(\sqrt{q})$ space to store the two lists. Pollards ρ method for discrete logs achieves the same $O(\sqrt{q})$ running time while only requiring a very small amount of storage.

The idea is to traverse a "random" path through the multiples mP + nQ until finding a collision. This path will consist of a loop with a tail attached (just like the letter ρ!!).

That is, Pollard's rho algorithm is to find distinct pairs $(c', d')$and (c'', d'') of integers modulo n such that

$$c'P + d'Q = c''P + d''Q.$$

Then $(c' - c'')P = (d'' - d')Q = (d'' - d')lP$

and so $(c' - c'') \equiv (d'' - d')l \pmod{n}$.

Hence $l = log_P Q$ can be obtained by computing

$$l = (c' - c'')(d'' - d')^{-1} \bmod n.$$

A natural method to find those pairings (c', d') and (c'', d'') is just randomly select *c*, *d* from [0, n-1] and store the triples (*c*,*d*, *c*P + *d*Q) in a table sorted by third component until a point *c*P + *d*Q is obtained for a second time. By the birthday paradox, the expected number of iterations before a collision is obtained is approximately $\sqrt{\pi n/2} \approx 1.2533\sqrt{n}$. The drawback of this algorithm is the storage required for the $\sqrt{\pi n/2}$ triples.

Pollard's rho algorithm finds (c', d') and (c'', d'') in roughly the same expected time as the natural method, but has nearly zero storage requirements. The idea is to define an iterating function f : P→P so that given X ∈ P and *c*, *d* ∈ [0,n − 1] with X = *c*P + *d*Q, it is easy to compute X^* = f (X) and c^*, d^* ∈ [0,n−1] with $X^* = c^*P + d^*Q$ .Furthermore, f should have the characteristics of a random function.

Theorem 5.1

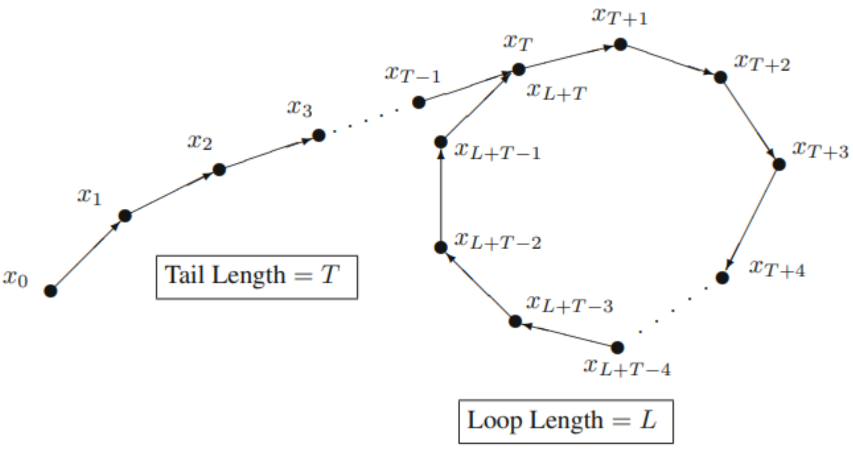
Let S be a finite set containing N elements, and let f : S → S be a function. Starting with an initial value x_0 ∈ S, define a sequence of points x_0, x_1, x_2 ,... by

$$x_i = f(x_{i-1}) = \underbrace{f \circ f \circ \cdots \circ f}_{i \text{ iterations of } f}(x_0).$$

Let T be the tail length and let L be the loop length of the orbit x_0, x_1, x_2 ,... of x, as illustrated in the figure below.

Formally, T = largest integer such that x_{T-1} appears only once in the sequence (x_i) i≥0,

L = smallest integer such that $x_{T+L} = x_T$



The orbit of x_0 in Pollard's ρ algorithm.

(a) There exist an index $1 \leq \boldsymbol{i} < T+L$ such that $x_{2i} = x_{i}$.

(b) If f : S → S and its iterates are "sufficiently random" at mixing the elements of S, then the expected value of T + L is $\sqrt{\pi N/2}$.

Remark: The path in the figure shows why the algorithm is called ρ algorithm.

Algorithm (Pollard's rho algorithm for the ECDLP (single processor))

INPUT: $P \in E(Fq)$ of prime order n, $Q \in \, < P >$.

OUTPUT: The discrete logarithm $l = \log_P Q$.

```
1. Select the number $L$ of branches (e.g., $L$ = 16 or $L$ = 32).
2. Select a partition function $H : < P > \rightarrow \{1,2,..., L\}$.
3. For $j$ from 1 to $L$ do
        3.1 Select $a_j , b_j \in_R [0, n-1]$.
        3.2 Compute $R_j = a_jP + b_jQ$.
4. Select $(c', d') \in_R [0, n-1]$ and compute $X' = c'P + d'Q$.
5. Set $X'' \leftarrow X', c'' \leftarrow c', d'' \leftarrow d'$.
6. Repeat the following:
        6.1 Compute $j = H(X')$.
            Set $X' \leftarrow X' + R_j, c' \leftarrow c' + a_j \bmod n, d' \leftarrow d' + b_j \bmod n$.
        6.2 For $i$ from 1 to 2 do
                Compute $j = H(X'')$.
                Set $X'' \leftarrow X'' + R_j, c'' \leftarrow c'' + a_j \bmod n, d'' \leftarrow d'' + b_j \bmod n$.
    Until $X' = X''$.
7. If $d' = d''$ then return("failure");
   Else compute $l = (c' - c'')(d'' - d')^{-1} \bmod n$ and return($l$)
```

Example: (*Pollard's rho algorithm for solving the ECDLP*)

Consider the elliptic curve defined over F_{229} by the equation:

$$E : y^2 = x^3 + x + 44.$$

The point $P = (5,116) \in E(F_{229})$ has prime order $n = 239$. Let $Q = (155,166) \in < P >$. We wish to determine $l = \log_P Q$.

We select the partition function $H : < P > \rightarrow \{1,2,3,4\}$ with $L = 4$ branches:

$H(x, y) = (x \bmod 4)+1$,

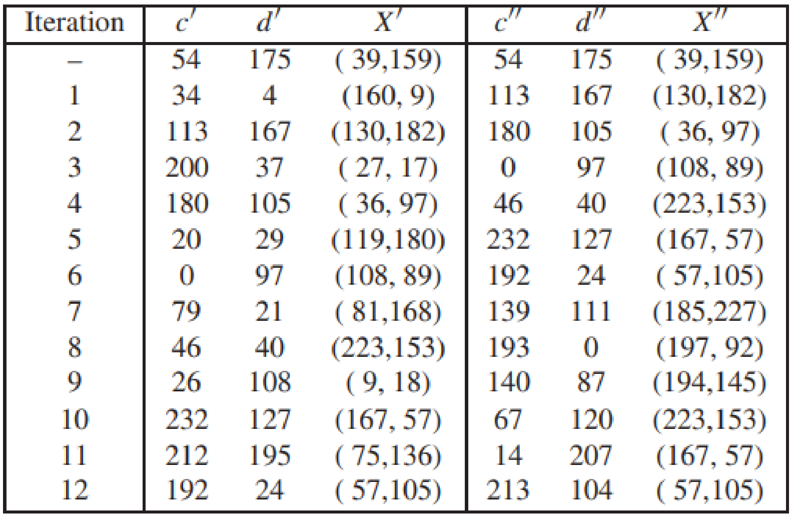
and the four triples $[a_1 ,b_1 ,R_1]=[79,163, (135,117)]$

$[a_2 ,b_2 ,R_2]=[206,19, (96,97)]$

$[a_3 ,b_3 ,R_3 =[87,109, (84,62)]$

$[a_4 ,b_4 ,R_4]=[219,68, (72,134)]$

The following table lists the triples (c', d', X') and (c'', d'', X'') computed in Algorithm above for the case (c', d') = (54,175) in step 4.



Iteration	c'	d'	X'	c''	d''	X''
–	54	175	(39,159)	54	175	(39,159)
1	34	4	(160, 9)	113	167	(130,182)
2	113	167	(130,182)	180	105	(36, 97)
3	200	37	(27, 17)	0	97	(108, 89)
4	180	105	(36, 97)	46	40	(223,153)
5	20	29	(119,180)	232	127	(167, 57)
6	0	97	(108, 89)	192	24	(57,105)
7	79	21	(81,168)	139	111	(185,227)
8	46	40	(223,153)	193	0	(197, 92)
9	26	108	(9, 18)	140	87	(194,145)
10	232	127	(167, 57)	67	120	(223,153)
11	212	195	(75,136)	14	207	(167, 57)
12	192	24	(57,105)	213	104	(57,105)

The algorithm finds $194P + 24Q = 213P + 104Q$, and hence

$$l = (194\text{-}213).(104\text{-}24)^{-1} \bmod 239 = 176.$$

5.2.4 Parallelized Pollard's ρ Method

Suppose now that M distinct starting points are available for solving an ECDLP instance. A better approach would be running Pollard's rho algorithm parallely on each processor (with different randomly chosen starting points W_0) until any one processor terminates. The analysis shows that the expected number of elliptic curve operations performed by each processor before one terminates is about $3\sqrt{n/M}$.. Thus the expected speedup is only by a factor of $\sqrt{M}$.

Van Oorschot and Wiener proposed a variant of Pollard's rho algorithm that yields a factor M speedup when M processors are employed. The idea is to allow the sequences $\{W_0^i\}i\geq0$ generated by the processors to collide with one another. More precisely, each processor randomly selects its own starting point W_0, but all processors use the same iterating function *f* to compute subsequent points W_0^i. Thus, if the sequences from two different processors ever collide, then, as illustrated in figure , the two sequences will be identical from that point on.

$$\begin{tikzcd}
W_i^0 \arrow[r, "f"] & W_{i+1}^0 \arrow[r, dashed] & W_j^0 \arrow[dddr, bend left, "f"] & \\
W_i^1 \arrow[r, "f"] & W_{i+1}^1 \arrow[r, dashed] & W_k^1 & \\
\vdots & & & \\
W_i^c \arrow[r, "f"] & W_{i+1}^c \arrow[rr, dashed] & & (W_j^0 = W_l^c) \arrow[d, "f"] \\
& & & (W_{j+1}^0 = W_{l+1}^c)
\end{tikzcd}$$

Let θ be the proportion of points in < P > having distinguishing property (a point may be distinguished if the leading t bits of its x-coordinate are zero.). Whenever a processor encounters a distinguished point, it transmits the point to a central server which stores it in a sorted list. When the server receives the same distinguished point for the second time, it computes the desired discrete logarithm by above methods and terminate all processor.

The expected number of steps per processor before a collision occurs is $(\sqrt{\pi n/2})/M$. subsequent distinguished point is expected after 1/θ steps. Hence the expected number of elliptic curve operations performed by each processor before a collision of distinguished points is observed is

$$\frac{1}{M}\sqrt{\frac{\pi n}{2}}+\frac{1}{\theta},$$

and this parallelized version of Pollard’s rho algorithm achieves a speedup that is linear in the number of processors employed.

Algorithm

```
INPUT: $P \in E(F_q)$ of prime order n, $Q \in \langle P \rangle$.

OUTPUT: The discrete logarithm $l = \log_P Q$.

1. Select the number $L$ of branches (e.g., $L = 16$ or $L = 32$).

2. Select a partition function $H : \langle P \rangle \rightarrow \{1,2,\dots, L\}$.

3. Select a distinguishing property for points in $\langle P \rangle$.

4. For $j$ from 1 to $L$ do

    4.1 Select $a_j, b_j \in_R [0, n-1]$.

    4.2 Compute $R_j = a_jP + b_jQ$.

5. Each of the M processors does the following:

    5.1 Select $c,d \in_R [0, n-1]$ and compute $X = cP + dQ$.

    5.2 Repeat the following:

        If $X$ is distinguished then send $(c,d, X)$ to the central server.

        Compute $j = H(X)$.

        Set $X \leftarrow X + R_j$, $c \leftarrow c + a_j \bmod n$, and $d \leftarrow d + b_j \bmod n$.

    Until the server receives some distinguished point $Y$ for the second time.

6. Let the two triples associated with $Y$ be $(c', d', Y)$ and $(c'', d'', Y)$.

7. If $d' = d''$ then return(“failure”);

   Else compute $l = (c' - c'')(d'' - d')^{-1} \bmod n$ and return($l$).
```

6.OTHER APPLICATIONS OF ELLIPTIC CURVE

6.1 Factorizing using Elliptic Curve

In mid 1980s it is found that elliptic curves are very effective for factoring numbers of around 60 decimal digits, and, for larger numbers, finding prime factors having around 20 to 30 decimal digits.

For example, We want to factor 4453. Let E be the elliptic curve $y^2 = x^3 + 10x - 2 \bmod 4453$ and let P = (1, 3).

We try to find 3P. First we compute 2P. The slope of line tangent at P is given by,

$$\frac{3x^2+10}{2y} = \frac{13}{6} \equiv 3713 \pmod{4453}.$$

We know that the gcd(6, 4453) = 1. So we can find that $6^{-1} \equiv 3711 \pmod{4453}$.

Using this we find the 2P = (x,y) as

$x \equiv 3713^2 - 2 \equiv 4332,\ \ y \equiv -3713(x-1) - 3 \equiv 3230$

To compute 3P, 3P = P+2P. Thus the slope is,

$$\frac{3230-3}{4332-1} = \frac{3227}{4331}.$$

But gcd(4331, 4453) = 61 $\neq 1$. Therefore, we cannot find 4331−1 (mod 4453), and we cannot evaluate the slope. However, we have found the factor 61 of 4453, and therefore

4453 = 61*73

Also we know that $E(\mathbf{Z}_{4453}) = E(\mathbf{F}_{61}) \oplus E(\mathbf{F}_{73}).$

If we look at the multiples of P mod 61 ,

we have P ≡ (1, 3), 2P ≡ (1, 58), 3P ≡ ∞, 4P ≡ (1, 3), ... (mod 61).

However, the multiples of P mod 73 are

P ≡ (1, 3), 2P ≡ (25, 18), 3P ≡ (28, 44), ..., 64P ≡ ∞ (mod 73).

Therefore, when we computed 3P mod 4453, we obtained ∞ mod 61 and a finite point mod 73.This is why the slope had a 61 in the denominator and was therefore infinite mod 61. If the order of P mod 73 had been 3 instead of 64, the slope would have had 0 mod 4453 in its denominator and the gcd would have been 4453, which would have meant that we did not obtain the factorization of 4453. But the probability is low that the order of a point mod 61 is exactly the same as the order of a point mod 73, so this situation will usually not cause us much trouble. If we replace 4453 with a much larger composite number n and work with an elliptic curve mod n and a point P on E, then the main problem we'll face is finding some integer k such that kP = ∞ mod one of the factors of n. In fact, we'll often not obtain such an integer k. But if we work with enough curves E, it is likely that at least one of them will allow us to find such a k. This is the key property of the elliptic curve factorization method.

Here is the **elliptic curve factorization method**. We start with a composite integer *n* (assume *n* is odd) that we want to factor and do the following.

1. Choose several (usually around 10 to 20) random elliptic curves $E_i : y^2 = x^3 + A_i x + B_i$ and points P_i mod *n*.

2. Choose an integer *B* (perhaps around 10^8) and compute $(B!)\ P_i$ on E_i for each *i*.

3. If step 2 fails because some slope does not exist mod *n*, then we have found a factor of *n*.

4. If step 2 succeeds, increase *B* or choose new random curves E_i and points P_i and start over.

Steps 2, 3, 4 can often be done in parallel using all of the curves E_i simultaneously.

The elliptic curve method is very successful in finding a prime factor *p* of *n* when $p < 10^{40}$. Suppose we have a random integer *n* of around 100 decimal digits, and we know it is composite (perhaps, for example, $2^{n-1} \not\equiv 1 \pmod{n}$, so Fermat's little theorem implies that *n* is not prime). If we cannot find a small prime factor (by testing all of the primes up to 10^7, for example), then the elliptic curve method is worth trying since there is a good chance that n will have a prime factor less than 10^{40}.

6.2 Primality Testing

We know the Pocklington-Lehmer primality test.

Proposition 6.1

Let $n > 1$ be an integer, and let $n - 1 = rs$ with $r \geq \sqrt{n}$. Suppose that, for each prim e |r ,there exists an integer a with,

$$a_\ell^{n-1} \equiv 1 \pmod{n} \text{ and } \gcd\left(a_\ell^{(n-1)/\ell} - 1, n\right) = 1.$$

Then n is prime.

Converese of this proposition is also true.

Proof: Let p be a prime factor of n and let l^e be the highest power of l dividing r. Let

$$b \equiv a_\ell^{(n-1)/\ell^e} \pmod{p}.$$

Then $$b^{\ell^e} \equiv a_\ell^{n-1} \equiv 1 \pmod{p} \text{ and } b^{\ell^{e-1}} \equiv a_\ell^{(n-1)/\ell} \not\equiv 1 \pmod{p},$$

Since $\gcd\left(a_\ell^{(n-1)/\ell} - 1, n\right) = 1.$ It follows that the order of b (mod p) is l^e . Therefore, l^e |$p - 1$. Since this is true for every prime power factor l^e of r, we have $r|p - 1$. In particular, $p > r \geq \sqrt{n}$. If n is composite, it must have a prime factor at most $\sqrt{n}$. We have shown this is not the case, so n is prime.

Theorem 6.2

Let $n > 1$ and let E be an elliptic curve mod n. Suppose there exist distinct prime numbers $l_1,l_2,..,l_k$ and finite points $P_i \in$ E(Z_n) such that,

1. $\ell_i P_i = \infty$ for $1 \leq i \leq k$
2. $\prod_{i=1}^k \ell_i > \left(n^{1/4} + 1\right)^2$.

Then n is prime.

Proof: Let p be a prime factor of n. Write $n = p^f n_1$ with $p \nmid n_1$ .Then,

$$E(\mathbf{Z}_n) = E(\mathbf{Z}_{p^f}) \oplus E(\mathbf{Z}_{n_1})$$

Since p_i is a finite point in $E(Z_n)$, it yields a finite point in $E(Z_{pf})$, namely P_i mod p^f . We can further reduce and obtain a finite point $P_{i,p} = P_i$ mod p in $E(F_p)$. Since $l_i\, P_i = \infty$ mod n, we have $l_i\, P_i = \infty$ mod every factor of n. In particular, $l_i\, P_{i,p} = \infty$ in $E(F_p)$, which means that $P_{i,p}$ has order l_i. It follows that

$l_i \mid \#\, E(F_p)$ for all i, so $\#\, E(F_p)$ is divisible by $\prod \ell_i$. Therefore,

$$\left(n^{1/4}+1\right)^2 < \prod_{i=1}^{k} \ell_i \leq \#E(\mathbf{F}_p) < p+1+2\sqrt{p} = \left(p^{1/2}+1\right)^2,$$

so $p > \sqrt{n}$. Since all prime factors of n are greater than $\sqrt{n}$, it follows that n is prime.

Example: Let $n = 907$. Let E be the elliptic curve $y^2 = x^3 + 10x - 2$ mod n. Let $l = 71$. Then,

$$\ell > \left(907^{1/4}+1\right)^2 \approx 42.1.$$

Let P = (819, 784). Then 71P = ∞. The above theorem implies that 907 is prime.

CONCLUSION

An elliptic curve is a curve that’s also naturally a group. The group law is constructed geometrically. An elliptic curve is not an ellipse in the sense of a projective conic. Ellipse has genus zero. Elliptic curves are especially important in number theory, and constitute a major area of current research; for example, they were used in Andrew Wiles's proof of Fermat's Last Theorem. They also find applications in elliptic curve cryptography (ECC) and integer factorization.

Elliptic curves over finite fields are notably applied in cryptography and for the factorization of large integers. It can be shown that elliptic curves defined over the complex numbers correspond to embeddings of the torus into the complex projective plane. The torus is also an abelian group, and this correspondence is also a group isomorphism. Note that the uniformization theorem implies that every compact Riemann surface of genus one can be represented as a torus. This also allows an easy understanding of the torsion points on an elliptic curve.

ECC is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. ECC allows smaller keys compared to non-EC cryptography (based on plain Galois fields) to provide equivalent security. It delivers a relatively more secure foundation than the first generation public key cryptography systems for example RSA.

REFERENCES

- Joseph H Silverman, The Arithmetic of Elliptic Curves, Second edition, Springer
- J S Milne, Elliptic Curves, Second edition, World Scientific
- Lawrence C Washington, Elliptic Curves Number Theory and Cryptography, Second Edition, Chapman & Hall/CRC
- Neal Koblitz, Introduction to Elliptic Curves and Modular Forms, Second Edition, Springer
- Darell Hankerson. Alfred Menezes. Scott Vanstone, Guide to Elliptic Curve Cryptography, Springer
- ecrypt-eu.blogspot.com/2016/02/parallelization-of-pollards-rho-method.html
- https://cse.iitkgp.ac.in/~debdeep/pres/TI/ecc.pdf