Journal Homepage: - www.journalijar.com
INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)
Article DOI: 10.21474/IJAR01/2766
DOI URL: http://dx.doi.org/10.21474/IJAR01/2766
ISSN NO. 2320-5407

RESEARCH PAPER

AN APPROACH TO ELLIPTIC CURVES AND DISCRETE LOGARITHMIC PROBLEM.

Dr. S. Vasundhara.
Asst professor of Mathematics G. Narayanamma Institute of Technology and Science(Women). Shaikpet. Hyderabad.

Manuscript Info

Manuscript History

Received: 15 November 2016
Final Accepted: 17 December 2016
Published: January 2017

Key words:-
Cryptography, finite fields, Elliptic curves

Abstract

This paper studies the mathematics of elliptic curves, starting with their derivation and the proof of how points upon them form an additive abelian group. I then worked on the mathematics necessary to use these groups for cryptographic purposes, specifically results for the group formed by an elliptic curve over a finite field, E(Fq). I examine the mathematics behind the group of torsion points, to which every point in E(Fq) belongs, and prove Hasse's theorem along with a number of other useful results. I finish by describing how to define a discrete logarithmic problem using E(Fq) and showing how this can form public key cryptographic systems for use in both encryption and decryption key exchange.

Introduction:-

An elliptic curve is usually defined to be the graph of an equation

$y2 = x3 + Ax + B$

where x, y,A and B belong to a specified field. These curves are of great use in a number of applications, largely because it possible to take two points on such a curve and generate a third. In fact, we will show that by defining an addition operation and introducing an extra point, 1, the points on an elliptic curve form an additive abelian group. Such a group can then be used to create an analogue of the discrete logarithm problem which is the basis for several public key cryptosystems. This project will introduce the mathematics behind elliptic curves and then demonstrate how to use them for cryptography.

Elliptic curves:-

Elliptic curves have, over the last three decades, become an increasingly important subject of research in number theory and related fields such as cryptography. They have also played a part in numerous other mathematical problems over hundreds of years. For example, the congruent number problem of finding which integers n can occur as the area of a right angled triangle with rational sides can be expressed using elliptic curves .In this chapter we set out the basic mathematics of elliptic curves, starting with their derivation and definition followed by the proof that points upon them form an additive abelian group.

1. A study on cryptography technologies, which is the basis for the four security services that are authentication, confidentiality, data integrity and non-repudiation.
2. A study on Elliptic Curve Cryptography applications and its standards.
3. A study on algorithms, architectures and implementations of ECC.
4. A study on Binary Galois field and the implementations of Galois Field arithmetic units.

Corresponding Author:- Dr. S.Vasundhara.
Address:- Asst professor of Mathematics G. Narayanamma Institute of Technology and Science (women) Shaikpet Hyderabad.

5. The implementation of Scalar Multiplication.

In the mid-1980s, Miller and Koblitz introduced elliptic curves into cryptograph, and Lenstra showed how to use elliptic curves to factor integers. Since that time, elliptic curves have played an increasingly important role in many cryptographic situations. One of their advantages is that they seem to offer a level of security comparable to classical cryptosystems that use much larger key sizes. For example, it is estimated in that certain conventional systems with a 4096-bit key size can be replaced by 313-bit elliptic curve systems. Using much shorter numbers can represent a considerable saving in hardware implementations.

An elliptic curve E is the graph of an equation:-
E:$y^2 = x^3 + ax + b$, and denoted by Ep(a,b).

Where a, b are in whatever is the appropriate set(rational numbers, complex numbers, integers mod n, etc.).We also include a **"point at infinity,"** denoted □ , which is most easily regarded as sitting at the top of the y-axis. It can be treated rigorously in the context of projective geometry, but this intuitive notion suffices for what we need. The bottom of the y-axis is identified with the top , so □ also sits at the bottom of the y-axis.

When we are working with real numbers, the graph E has one of two possible forms, depending on whether the cubic polynomial in x has one real root or three real roots. In the figure below are shown example of elliptic curves illustrated using Matlab files

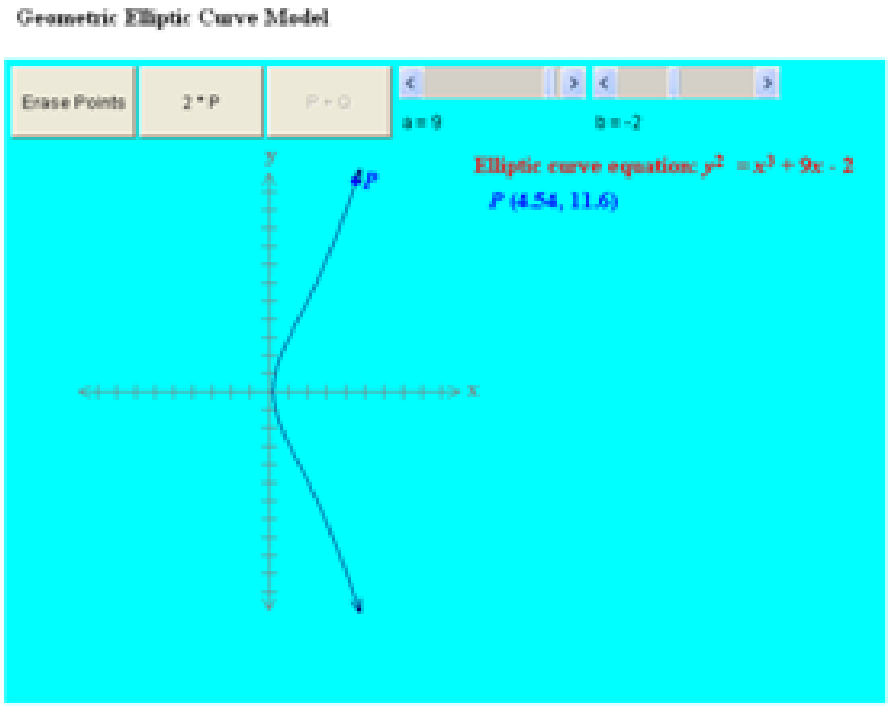
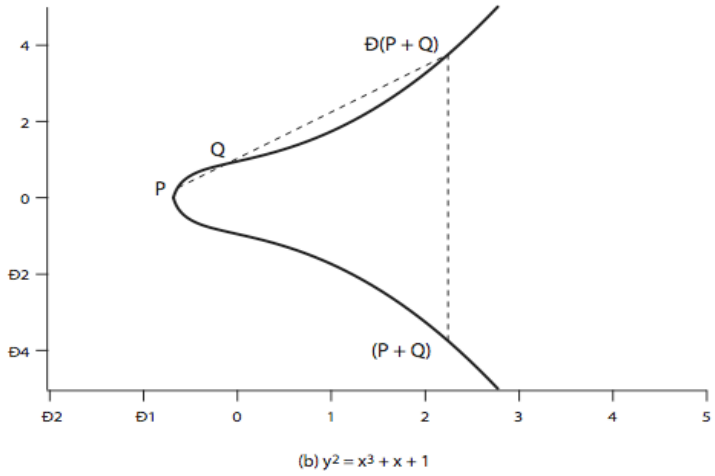


Figure 1

We assume that the cubic polynomial x 3+$ax + b$ has no multiple roots

Technical point:-
Given two points P1 and P2 on E, we can obtain a third point P3 on E as follows: Draw the line L through P1 and P2 (if P1 = P2, take the tangent line to E at P1). in third point Q. Reflect Q through the x-axis (i.e., change y to -y) to get P3. Define a law of addition on E by
P1 + P2 = P3
Note that this is not the same as adding points in the plane



(b) $y^2 = x^3 + x + 1$

Figure 2:-

Elliptic Curves Mod n:-

If n is an integer, we can work with elliptic curves mod n using the aforementioned ideas. For example, consider E: $y2 \equiv x3 + 2x + 3 (\text{mod } 5)$.

The points on E are the pairs (x, y) mod 5 that satisfy the equation, along with the point at infinity. These can be listed as follows. The possibilities for x mod 5 are 0, 1, 2, 3, 4 substitute each of these into the equation and find the values of y that solve the equation.

Historical point:- Elliptic curves are not ellipses. They received their name from their relation to elliptic integrals such as

$\int_{z_1}^{z_2} \frac{dx}{x^3+ax+b}$ and $\int_{z_1}^{z_2} \frac{xdx}{x^3+ax+b}$

Point addition: Elliptic Curve Addition:- A Geometric Approach:

1 P + Q = R is the additive property defined geometrically.

2 Elliptic curve groups are additive groups; that is, their basic function is addition. The addition of two points in an elliptic curve is defined geometrically.

3 The negative of a point P = (X_1,Y_1) is its reflection in the x-axis: the point -P is $(X_1,-Y_1)$. Notice that for each point P on an elliptic curve, the point -P is also on the curve.

Adding distinct points P and Q:- The resulted point of adding two different points on the elliptic curve is computed as shown below in figure 2

When P = (X_1,Y_1) and Q = (X_2,Y_2) are not negative of each other, $(X_1,Y_1)+ (X_2,Y_2)= (X_3,Y_3)$; where $X_1 \neq X_2$

P + Q = R where

$\lambda = (Y_2 - Y_1) / (X_2 - X_1)$

$X_3 = \lambda^2 - X_1 - X_2$ and

4 $Y_3 = -Y_1 + \lambda (X_1 - X_3)$

5 Note that λ is the slope of the line through P and Q.

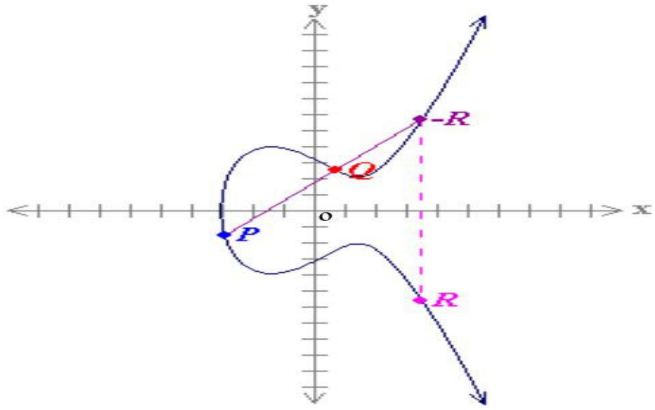


Figure 2:-

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

Arithmetic in Elliptic Curve Group over F_p

Point addition:-
Note that these rules are exactly the same as those for elliptic curve groups over real numbers, with the exception that computations are performed modulo p.

There are several major differences between elliptic curve groups over F_p and over real numbers. Elliptic curve groups over F_p have a finite number of points, which is a desirable property for cryptographic purposes. Since these curves consist of a few discrete points, it is not clear how to "connect the dots" to make their graph look like a curve. It is not clear how geometric relationships can be applied. As a result, the geometry used in elliptic curve groups over real numbers cannot be used for elliptic curve groups over F_p. However, the algebraic rules for the arithmetic can be adapted for elliptic curves over F_p. Unlike elliptic curves over real numbers, computations over the field of F_p involve no round off error - an essential property required for a cryptosystem.

The rules for addition over Ep (a,b):- Correspond to the algebraic technique described for elliptic curve defined over real numbers. For all points $P,Q \in E_p(a,b)$; P+O=P.

If $P=(x_p,y_p)$, then $P+(x_p,-y_p)=O$. The point $(x_p,-yp)$ is the negative of P, denoted as –P. For example , in $E_{23}(1,1)$, for P=(13,7), we have –P=(13,-7).But -7 mod 23=16.Therefore –P=(13,16), which is also in $E_{23}(1,1)$
if $P=(x_P,y_P)$ and $Q=(x_Q,y_Q0$ with $P \neq -Q$, then $R=P+Q=(x_R,y_R)$ is determined by the following rules: $X_R=(\lambda^2-x_P-x_Q) \bmod p$, $Y_R=(\lambda(x_P-x_R)-y_P) \bmod p$

Where
$\lambda=(\frac{y_Q-y_P}{x_Q-x_P}) \bmod p$ if $P \neq Q$
$(\frac{3x_P{}^2+a}{2y_P}) \bmod p$ if P=Q
Multiplication is defined as repeated addition; for example, 4P=P+P+P+P.

For example let P=(3,10) and Q=(9,7) in $E_{23}(1,1)$.Then
$\lambda=(\frac{7-10}{9-3}) \bmod 23=(\frac{-3}{6}) \bmod 23=(\frac{-1}{2}) \bmod 23=11$
$x_R=(112-3-9) \bmod 23=109 \bmod 23=17$
$y_R=(11(3-17)-10) \bmod 23=-164 \bmod 23=20$
so P+Q=(17,20).To find 2P
$\lambda\frac{=(3(32)+1}{2x10}) \bmod 23=(\frac{5}{20}) \bmod 23=(\frac{1}{4}) \bmod 23=6$

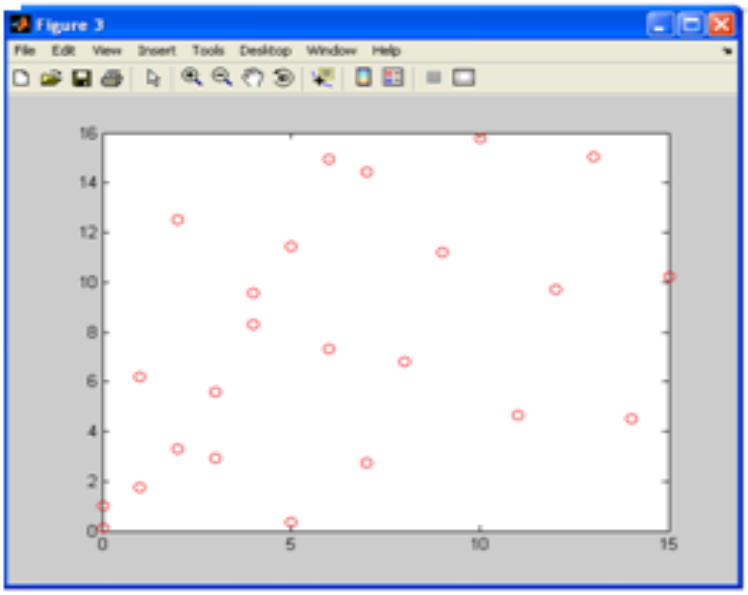


Figure 1.2:-

2 The Elliptic Curve Discrete Logarithm Problem:-

Discrete logarithms are fundamental to a number of public-key4algorithms,including, Diffie-Hellman key exchange and the digital signature algorithm(DSA).This section provides a brief overview of discrete logarithms.

The power of an Integer , modulo n
For $a^{\emptyset(n)} \equiv 1(\text{mod} n)$

Where $\emptyset(n)$,Euler's totient function, is the number of positive integers less than n and relatively prime to n.now consider the general expression:-
$a^m \equiv 1 \pmod n$ (1)

If a and n are relatively prime then there is at least one integer m that satisfies the Equation(1),namely , m=$\emptyset(n)$.The least positive exponent m for which equation holds is referred to in several ways:

- The order of a (mod n)
- The exponent which a belongs (mod n)
- The length of the period generated by a

To see the last point, consider the powers of 7, modulo 19:
$7^1 \equiv$ 7(mod 19)
$7^2=49=2x19+11 \equiv$ 11(mod19)
$7^3=343=18x19+1 \equiv$ 1(mod 19)
$7^4=2401=126x19+7 \equiv$ 7(mod19)
$7^5=16807=884x19+11 \equiv$ 11(mod19)

There is no point in continuing because the sequence is repeating. This can be proven by noting that $7^3 \equiv 1 \pmod{19}$ and therefore $7^{3+j} \equiv 7^3 7^j \equiv 7^j \pmod{19}$, and hence any two powers of7 whose exponents differ by 3 (or multiply by 3) are congruent to each other (mod 19).In other words the sequence is periodic and the length of the period is the smallest positive exponent m such that $7^m \equiv 1 \pmod{19}$

In the multiplicative group Zp*, the discrete logarithm problem is: given elements r and q of the group, and a prime p, find a number k such that r = qk mod p. 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

Example:-
In the elliptic curve group defined by:-
$y^2 = x^3 + 9x + 17$ over F_{23}, the discrete logarithm k of Q = (4,5) to the base P = (16,5)?

One (naïve) way to find k is to compute multiples of P until Q is found. The first few multiples of P are: P = (16,5) 2P = (20,20) 3P = (14,14) 4P = (19,20) 5P = (13,10) 6P = (7,3) 7P = (8,7)

8P = (12,17) 9P = (4,5)
Since 9P = (4,5) = Q, the discrete logarithm of Q to the base P is k = 9.

In a real application, k would be large enough such that it would be infeasible to determine k in this manner.
An Example of the Elliptic Curve Discrete Logarithm Problem

Discrete logarithmic problem:-
Consider the multiplicative group (Z_p^*, p^*), where p is a prime. Let g be a generator of the group ,i.e, successive powers of g generate all elements of the group .So

g^1 mod p,g^2mod p……..g^{p-1} modp

Is a re-arrangement of the integers in Z_p^*
Let x be an element in {0,1,2, ……..p-2}.The function
Y=g^x (modp)Is referred to a modular exponentiation with base g and modulus p.

The inverse operation is expressed as x=log_g^y (modp) And is referred to as the discrete logarithm. It involves computing x given the values of p,g and y∈ Z_p^*

Example Discrete logarithm in ($Z_p^*, 29^*$) with g=2

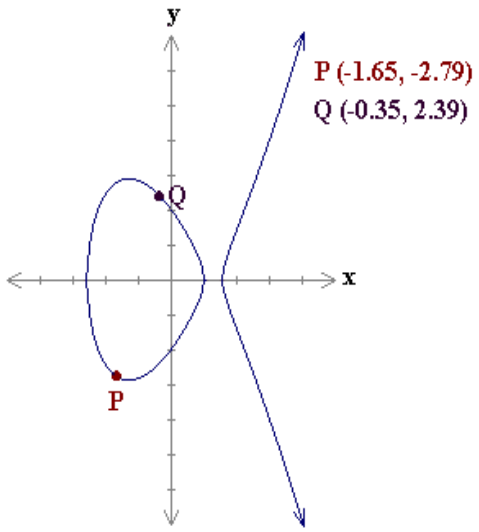
Y	log_2^y(mod29)	22	26
1	28	23	20
2	1	24	8
3	5	25	16
4	2	26	19
5	22	27	15
6	6	28	14
7	12		
8	3		
9	10		
10	23		
11	25		
12	7		
13	18		
14	13		
15	27		
16	4		
17	21		
18	11		
19	9		
20	24		
21	17		

From the above problem it gives value of x given p&g means that $2^7 \text{mod} 29=12$ i.e $log_2^{12} = 7$Similarly $2^{21} \text{mod} 29=17$ i.e $log_{29}^{17}=21$ and so on Example let p=131,g=2

Y	log_2^y(mod131)
1	2
2	4
3	8
4	16
5	32
6	64
7	128
8	125
9	119
10	107
11	83
12	35
13	70
14	9
15	18
16	36
17	72

The discrete logarithmic problem is $2^{17}(\text{mod } 131)=72$, *i.* e log_2^{72} (mod 131)=17,$2^{11}(\text{mod}131)=83$ i.e $log_2^{83}\text{mod}131)=11$

The discrete logarithm of Q(-0.35,2.39) to the base P(-1.65,-2.79) in the elliptic curve group $y^2 = x^3 - 5x + 4$ over real numbers is given by figure 3



Elliptic curve equation: $y^2 = x^3 - 5x + 4$

Figure 3:-

References:-

1. Certicom, "standards for Efficient Cryptography,SEC 1:Elliptic curve Cole, Eric, Jason Fossen, Stephen Northcutt, Hal Pomeranz. SANS Security Essentials with CISSP CBK, Version 2.1.USA: SANS Press, 2003.
2. J.Edge,an introduction to elliptic curve ,cryptography, http://Iwn.net/Articles/174127/.2006.
3. N.Koblitz,A course in Number theory and cryptography,2nd ed.,brookes/Cole,1997.
4. J.H.Silverman,The Arithmetic of Elliptic curves, Springer –Verlag,1986.
5. RSA" Wikipedia.wikipedia,n.d.web.09 feb 2011.Stalings,William. Cryptography and network security.fourth,pearson,2009.print.
6. Alfredj Menezes, paul c,vanoorschot and scott A.vanstone,guide to Elliptic curve Cryptography ,1996.
7. N.Koblitz.CM-curves with good cryptographic properties. In Advances in Cryptology: Crypto 91' volume 576 of in computer science, pages 279-287,springer-verlag,1992. Notes
8. The Thesis of on 2-Spreads in PG(5,3) by K. Hanumanthu under the super vision of Prof.K.Satyanarayana.
9. Thesis of Dr. K .V. Durga Prasad : "Construction ofTranslation planes and Determinition of their translation complements",Ph.D Thesis,Osmania University
10. Diffie, W., and M. E. Hellman. "New directions in cryptography." *IEEE Transactions on Information Theory,*, 1976: 644- 654.
11. A Scalar Multiplication in Elliptic Curve Cryptography with Binary Polynomial Operations in Galois Field Hero Modares(thesis of master science.