Software Implementation of Cyclic Abelian Elliptic Curve using Matlab.

Dipti Aglawe
M.E Scholar,CSVTU
Dept of Computer Science
Engineering
SSGI, Bhilai (C.G)

Samta Gajbhiye
Associate Professor ,CSVTU
Dept of Computer Science
Engineering
SSGI,Bhilai(C.G)

ABSTRACT

Majority of products and standards that use public-key cryptography for encryption and digital signature use RSA. The key length for secure RSA has increased over recent years ,and this has put heavier processing load on applications using RSA. Recently, a competing system has begun to challenge RSA: Elliptic curve cryptography (ECC).The principle attraction of ECC, compared to RSA, is that it appears to offer equal security for a far smaller key size, thereby reducing processor overhead. Cryptographers are interested only in elliptic curve that belongs to cyclic abelian group. This paper implements cyclic abelian elliptic curve in MATLAB. The properties of abelian group is proved over the coordinates satisfying the curve. Base points of elliptic curve are generated to prove that the elliptic curve belongs to cyclic abelian group.

Keywords

Elliptic Curve Cryptography (ECC), Cyclic abelian group, public key cryptography.

1. INTRODUCTION

Cryptography is the science of information security. Elliptic curve can be applied to cryptography as it is secure to the best of current knowledge. Elliptic curve cryptography provides the same level of security as RSA with smaller key size. Also it requires less storage and smaller bandwidth.[7][8]

Elliptic curve cryptography [ECC] is a public-key cryptosystem like RSA. In wireless networks and mobile devices such as cell phone, PDA and smart card, security of wireless networks and mobile devices are prime concern. An important issue is remote user authentication in insecure channel. Due to the limitation in the bandwidth, computational strength, power availability or storage in mobile devices, the public key cryptography-based remote authentication schemes are not suitable for mobile devices. So various authentication schemes based on elliptic curve cryptography (ECC) are proposed.[10]

The benefit of using elliptic curves is that similar level of security can be achieved with shorter keys than other public key cryptography which are based on the difficulties of solving discrete logarithms over integers or integer factorizations. The security of the key which is 160bit long is equivalent to the keys which are 1024bit long in the other two public key cryptographies. [7,8]

In cryptography cyclic abelian elliptic curve are required. To prove elliptic curve as an abelian group,the coordinates of elliptic curve should satisfy some properties.

Let G be a non empty set of coordinates of elliptic curve and ‘*’ be one or more binary operation in an algebraic structure. Then, (G,*) should observe following properties.[2]

1. G is closed w.r.t *
2. * is associative
3. Existence of identity element
4. Existence of inverse
5. * is commutative

The rest of our paper is organized as follows. Section 2 describes the related work which has been done in this area. Section 3 and 4 describes the method and implementation approach. Section 5 is the implementation of cyclic abelian elliptic curve using MATLAB.

2. RELATED WORKS

In the literature, many authors have tried to exploit the features of EC field to deploy for security applications. We have outlined some of the highlights of the relevant work in this section. Koblitz [7] and Miller [8] has first to introduce elliptic curve in cryptography. N.A. Saqib, F. Rodriguez-Henriquez and A. Diaz-perez et.al[9] in their work has explain that security of the ECC is based on the intractability of the elliptic curve discrete logarithm problem(ECDLP) [9]. Compared with RSA, ECC offers a better performance due to a smaller key size with the same security[9]. P.G. Shah, X. Huang and D. Sharma et al[11] have implemented ECC-based authentication algorithm in which they conclude that elliptic curve scalar multiplication is core operation, but this operation is the most time consuming operation. This operation takes 85% of executing time [11].

Abdalhossein Rezai and Parviz Keshavarzi et.al[10] have worked on the more efficient algorithm elliptic curve cryptosystem based on a novel finite field multiplication and a high performance scalar multiplication algorithm for wireless network authentication. Bin Yu et.al[6] has presented an efficient method to generate the elliptic curves which bases on the CM (composite method) algorithm. It may generate many elliptic curves which are suitable for building the cryptosystem.

A simple tutorial of ECC concept is very well documented and illustrated in the text authored by Williams Stallings et.al [1]. J.Nafeesa Begum, K. Kumar and Dr.V. Sumathy et.al[5] in their research has develop a multilevel access control for Defense messaging system using Elliptic curve cryptography. Defense messaging system takes a message and forwards it to the intending recipients or parties based on the message criteria for immediate action. This system should provide security assurance and should be manageable by central administrative authority instead of relying on the individual users. The paper presented by Guicheng shen, Xuefeng zheng et.al[4] mainly uses object-oriented technology as tools, and divides Elliptic Curve Cryptosystem into several layers, every of which corresponds a class.

3. METHOD DESCRIPTION

An elliptic curve is a plane curve defined by an equation of the form

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

where x, y are elements of GF(p), and each value of the ‘a’ and ‘b’ gives a different elliptic curve.

In equation $y^2 = x^3 + ax + b$, $a, b \in K$ and determinant$-16(4a^3 + 27b^2) \neq 0 (\text{mod } p)$. (2)

Here 'p' is known as modular prime integer making the EC finite field.

The condition that $-16(4a^3 + 27b^2) \neq 0$. implies that the curve has no “singular points”, means that the polynomial $y^2 = x^3 + ax + b$ has distinct roots

An elliptic curve E over GF(p) consist of the solutions(x, y) defined by (1) and (2), along with an additional element called 0, which is the point of EC at infinity. The set of points (x, y) are said to be affine coordinate point representation.

The basic EC operations are point addition and point doubling.

In Elliptic curves addition of points on a curve in the following manner: in order to find the sum of two points P and Q on elliptic curve E, we draw a line connecting P and Q. This line will intersect E at exactly one other point, which we will denote P * Q. P + Q will be defined as the reflection of P * Q across the x-axis.

There are certain cases for which this definition will not suffice. One such case is where P and Q are the same point. In this case, we draw the tangent line to E at P and find the second point where this line intersects E. We call this point P * P. Again, we reflect this point over the x-axis to obtain P + P. Another case is where the line connecting P and Q is vertical. In this case, we define P + Q to be O, the point at infinity. Note that the line connecting any point and O will be a vertical line, and reflecting O about the x-axis results in O

Let us start with P(xp,yp). To determine 2P, P is doubled. This should be an affine point on EC. Use the following equation, which is a tangent to the curve at point P.

$S = [(3x_p{}^2 + a)/2y_p] \text{ (mod p)}$ (3)

Then 2P has affine coordinates (x_r,y_r) given by:

$x_r = (S^2 - 2\,x_p) \text{ mod p}$

$y_r = [S\,(x_p - x_r) - y_p] \text{ (mod p)}$ (4)

Now to determine 3P, we use addition of points P and 2P, treating 2P=Q. Here P has coordinates $(x_{p,}y_p)$, Q=2P has coordinates (x_q,y_q). Now the slope is:

$S = [(y_q - y_p) / (x_q - x_p)] \text{ mod p}$

P+Q=-R

$x_r = (S^2 - x_p - x_q) \text{ mod p}$

$y_r = (S\,(x_p - x_r) – y_p) \text{ mod p}$ (5)

The value of kP can be calculated by a series of doubling and addition operation.

4. THE IMPLEMENTATION APPROACH FOR PROVING CYCLIC ABELIAN ELLIPTIC CURVE.

The implementation includes following modules:

(1) Generation of coordinates of elliptic curve.
(2) Elliptic curve as an algebraic structure.
(3) Finding all base points.
(4) elliptic curve as cyclic group.

(1) Generation of coordinates of elliptic curve

The implementation includes a function which is coded to generate all the coordinates of elliptic curves. Some in-built functions of MATLAB is used like mod, strcat, str2num, num2str. Plot is generated using these coordinates.

(2) Elliptic curve as an algebraic structure

Properties of abelian group ie Closure, associative, commutative, Inverse and identity element are to be proved. For proving the above addition and doubling operation is performed using formula equations (3),(4) and (5).

(3) Finding all base points

The base points or generating points are used in elliptic curve cryptography for public key generation and private key generation. Base points are the points which can generate all the coordinates of an elliptic curve. The order of all base points must be equal to ‘n’ where n is the total number of points for a particular elliptic curve.

(4) Elliptic curve as cyclic group

A non-empty set G equipped with one or more binary operations is denoted by (G,*).In elliptic curve this * is addition operation. If in a group G the underlying set G consists of a finite number of distinct elements then the group is called a “finite group” otherwise infinite group. The number of elements in a finite group is called the order of the group denoted as o(G) or #(G).Order of an element ‘a’ of a group i.e o(a):

$a^n = e$, where e is identity element in G (when composition is multiplication) na = e , where e is the identity in G (when composition is addition)

A group (G, *) is cyclic, if for a Є G , every element x Є G is of the form na , where n is some integer. Element '*a*' is called generator of G.

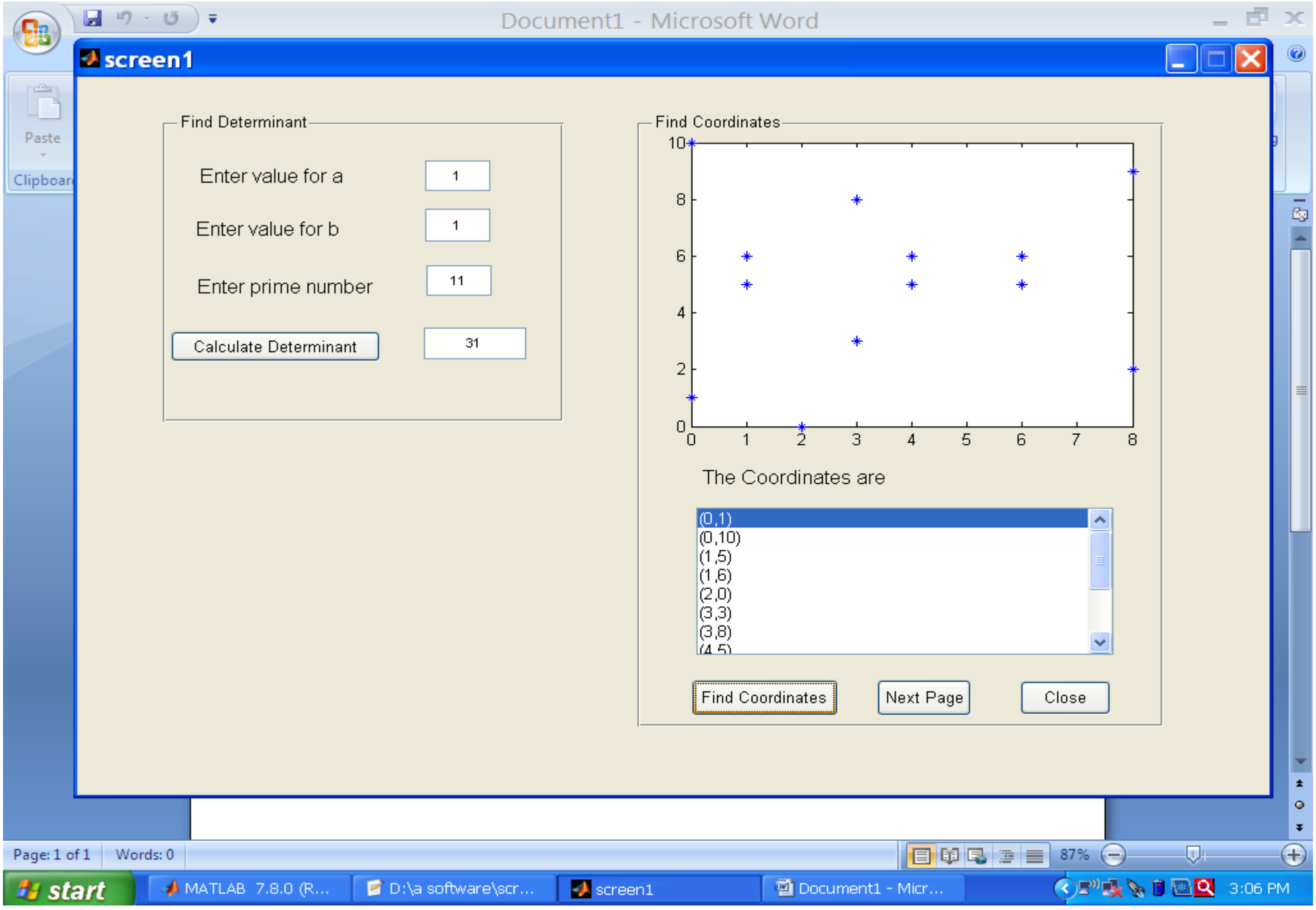
5. IMPLEMENTATION

Step 1: Finding coordinates of an elliptic curve in a finite field

In the equation $y^2=x^3+ax+b$, let the value of a and b are 1 and 1 respectively with the value of p=11. Using the program which is implemented in matlab generates the coordinates of elliptic curve.

Table 1. Points on elliptic curve E(1,1) with p=11

(0,1)	(0,10)	(1,5)	(1,6)	(2,0)
(3,3)	(3,8)	(4,5)	(4,6)	(6,5)
(6,6)	(8,2)	(8,9)		



Enter value for a 1

Enter value for b 1

Enter prime number 11

Calculate Determinant 31

The Coordinates are

(0,1)
(0,10)
(1,5)
(1,6)
(2,0)
(3,3)
(3,8)
(4,5)

Find Coordinates Next Page Close

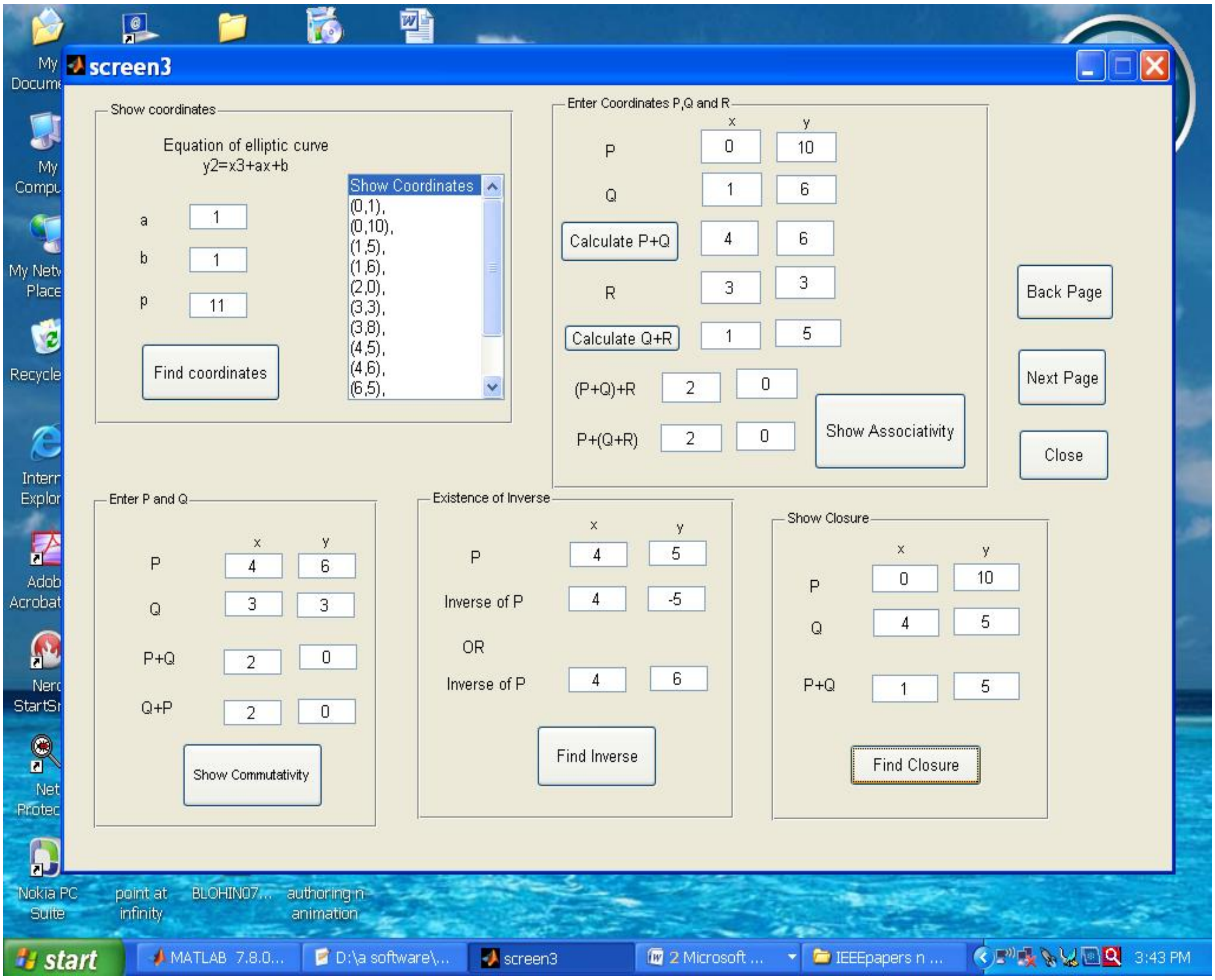
Fig.1: plot of coordinates of elliptic curve E(1,1) with p=11

Step 2: Elliptic curve as an algebraic structure

There are five properties of elliptic curves i.e. closure, associative, existence of identity, existence of inverse and commutative which are require to prove elliptic curve belonging to abelian group.

Closure Property: Let us take any two point of elliptic curve E(1,1) are (0,10) and (4,5)

By adding these point using the formulae (3),(4) and (5) .We get (1,5) which is one of the element of elliptic curve. In the implementation closure of every point is found and thus concluded that the set is closed.



screen3

Show coordinates

Equation of elliptic curve
y2=x3+ax+b

a 1

b 1

p 11

Show Coordinates
(0,1),
(0,10),
(1,5),
(1,6),
(2,0),
(3,3),
(3,8),
(4,5),
(4,6),
(6,5),

Enter Coordinates P,Q and R

	x	y
P	0	10
Q	1	6
Calculate P+Q	4	6
R	3	3
Calculate Q+R	1	5
(P+Q)+R	2	0
P+(Q+R)	2	0

Enter P and Q

	x	y
P	4	6
Q	3	3
P+Q	2	0
Q+P	2	0

Existence of Inverse

	x	y
P	4	5
Inverse of P	4	-5
OR		
Inverse of P	4	6

Show Closure

	x	y
P	0	10
Q	4	5
P+Q	1	5

Fig.2: Implementation of properties of an elliptic curve

Associativity:

P+(Q+R)=(P+Q)+R

If we take P=(0,10), Q=(1,6),R=(3,3)

The program will calculate (P+Q)=(4,6) and adding this value to R=(3,3) we get (2,0). Thus (P+Q)+R = (2,0). Also (Q+R) = (1,5), adding this point to P=(0,10) we get (2,0) Thus it proves that

(P+Q)+R=P+(Q+R)

In this way every combination of points we can take and prove the associativity property of elliptic curve.

Existence of inverse:

For every point of elliptic curve there exists an inverse coordinate.

If we take point (4,5),the inverse is (4,-5),which can be written as (4,-5mod11) that is (4,6).

Similarly we can find the inverse of each point using this software.

Commutative property:

It is written as P+Q=Q+P. Take any two coordinates P=(4,6) and Q=(3,3) and using the formulae defines above for addition we get P+Q=(2,0).Using the same formulae we can calculate Q+P=(2,0).Thus, we can prove commutative property for every possible pair of points.

Step 3: Finding all base or generator point

The base points or generating points are used in elliptic curve cryptography for public key generation and private key generation. Base points are the points which can generate all the coordinates of an elliptic curve. The order of all base points must be equal to 'n' where n is the total number of points for a particular elliptic curve.

For example:

In equation $y^2 = x^3 + ax + b$,

a=1,b=1,p=11 coordinates of curve are (0,1)(0,10)(1,5)(1,6)(2,0)(3,3)(3,8)(4,5)(4,6)(6,5)(6,6)(8,2)(8,9)

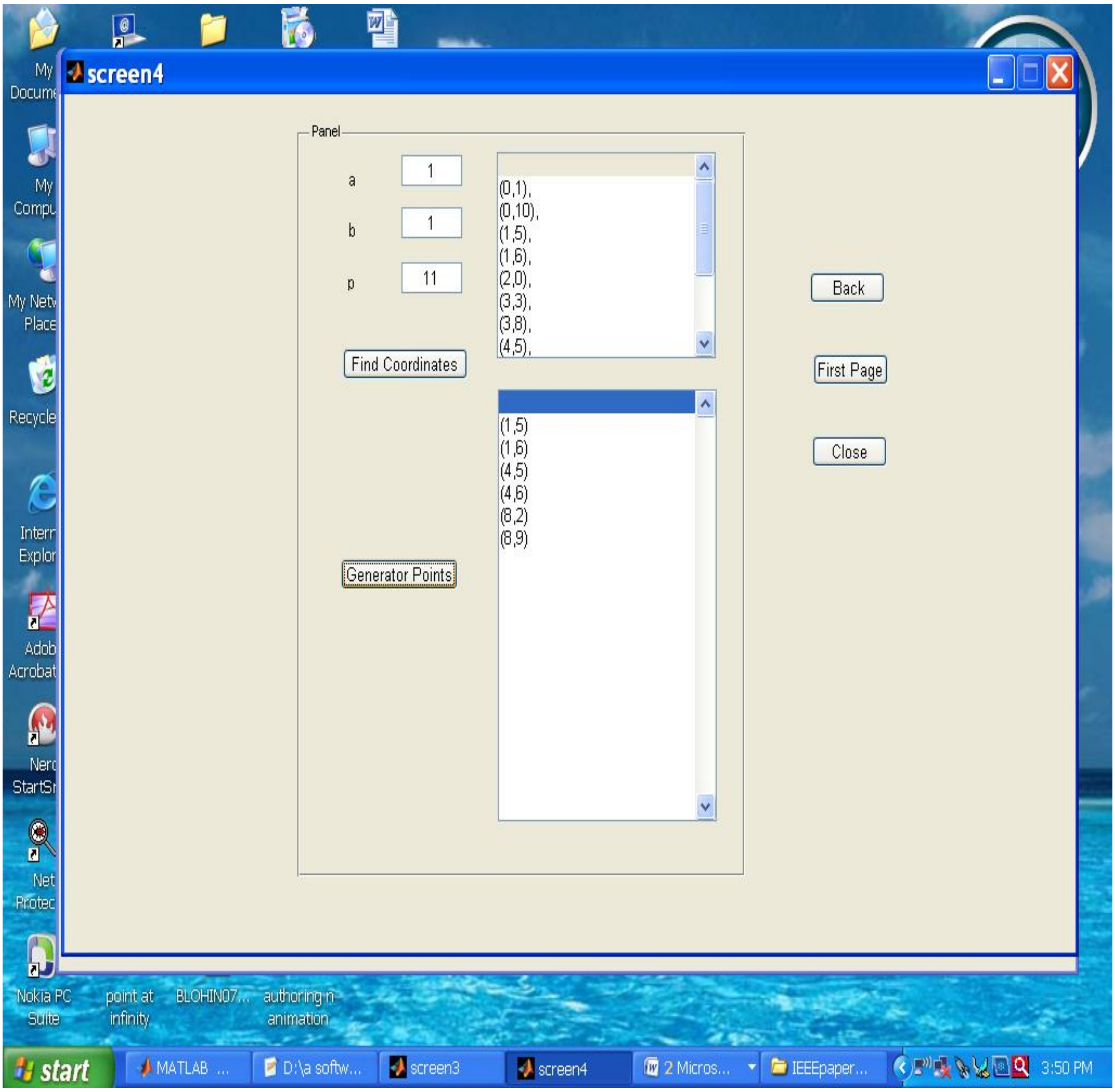
Let P=(0,1) then 2P=P+P=(3,3) 3P=(6,6) 4P=(6,5) 5P=(3,8) 6P=(0,10)

7P =(0,10)+(0,1) will not be calculated correctly as slope is infinity. The order is 7 which is not equal to the total number of coordinates of the example elliptic curve. This point cannot be taken as the base point.Now take P=(1,5) Using the formulae we can calculate

2P=(3,3) 3P=(8,2) 4P= (6,5) 5P= (4,6) 6P= (0,10) 7P= (2,0) 8P= (0,1) 9P=(4,5) 10P=(6,6) 11P=(8,9) 12P=(3,8) 13P=(1,6)

So the order is equal to 13 that is the total number of coordinates or elements of group.

The point (1,5) is generator point.
Similarly all the generator point can be calculated using the software.



a 1

b 1

p 11

(0,1),
(0,10),
(1,5),
(1,6),
(2,0),
(3,3),
(3,8),
(4,5),

(1,5)
(1,6)
(4,5)
(4,6)
(8,2)
(8,9)

Fig.3: Generating base points of elliptic curve $E_{11}(1,1)$

6. RESULTS AND CONCLUSION

In the elliptic curve equation $y^2 = x^3+ax+b$, E(1,1) ,p=11 coordinates of curve are in this sequence (0,1),(0,10),(1,5),(1,6),(2,0),(3,3),(3,8),(4,5),(4,6),(6,5),(6,6),(8,2),(8,9) which can be written as

Group

G={(0,1),(0,10),(1,5),(1,6),(2,0),(3,3),(3,8),(4,5),(4,6),(6,5),(6,6),(8,2),(8,9)}

We got six generator (base) points using this software as shown above. They are (1,5),(1,6),(4,5),(4,6),(8,2),(8,9)

Taking first base point (1,5) and rearranging the group we get

G={(1,5),(3,3),(8,2),(6,5),(4,6),(0,10),(2,0),(0,1),(4,5),(6,6),(8,9),(3,8),(1,6)} or

G={ P, 2P, 3P, 4P, 5P, 6P, 7P, 8P, 9P, 10P, 11P, 12P, 13P}

Taking second base point (1,6) and rearranging the group we get

G={(1,6),(3,8),(8,9),(6,6),(4,5),(0,1),(2,0),(0,10),(4,6),(6,5),(8,2),(3,3),(1,5)} or

G={ P, 2P, 3P, 4P, 5P, 6P, 7P, 8P, 9P, 10P, 11P, 12P, 13P}

Taking second base point (4,5) and rearranging the group we get

G={(4,5),(6,5),(1,6),(0,1),(8,2),(3,8),(2,0),(3,3),(8,9),(0,10),(1,5),(6,6),(4,6)} or

G={ P, 2P, 3P, 4P, 5P, 6P, 7P, 8P, 9P, 10P, 11P, 12P, 13P}

Taking second base point (4,6) and rearranging the group we get

G={(4,6),(6,6),(1,5),(0,10),(8,9),(3,3),(2,0),(3,8),(8,2),(0,1),(1,6),(6,5),(4,5)} or

G={ P, 2P, 3P, 4P, 5P, 6P, 7P, 8P, 9P, 10P, 11P, 12P, 13P}

Taking second base point (8,2) and rearranging the group we get

G={(8,2),(0,10),(4,5),(3,8),(1,5),(6,5),(2,0),(6,6),(1,6),(3,3),(4,6),(0,1),(8,9)} or

G={ P, 2P, 3P, 4P, 5P, 6P, 7P, 8P, 9P, 10P, 11P, 12P, 13P}

Taking second base point (8,9) and rearranging the group we get

G={(8,9),(0,1),(4,6),(3,3),(1,6),(6,6),(2,0),(6,5),(1,5),(3,8),(4,5),(0,10),(8,2)} or

G={ P, 2P, 3P, 4P, 5P, 6P, 7P, 8P, 9P, 10P, 11P, 12P, 13P}

Thus, the elliptic curve E(a,b) with a=1,b=1 and p=11 has six generator points and all are forming cyclic abelian group. This proves that the given elliptic curve belongs to cyclic abelian group

All the curves which is in the form of equation $y^2 = x^3 + ax + b$ is not mandatorily an elliptic curve and all the elliptic curve is not necessarily an elliptic curve belonging to cyclic abelian group. For example the curve $y^2 = x^3 -3x + 2$ is not an elliptic curve because its determinant value is equal to zero. Therefore, it cannot be used to form a group.

Also the elliptic curve E(1,1) with p=31,47,67 and so on are elliptic curves but they cannot be used for cryptography as they do not have generator points and therefore they do not form cyclic abelian group. We can find all the cyclic abelian elliptic curves using the software.

7. FUTURE SCOPE

All elliptic curves cannot be used for cryptography but elliptic curves which is proved that it belongs to cyclic abelian elliptic curve can be used. Using this software one can find the elliptic curves which belongs to cyclic abelian elliptic curve and can be used for cryptography. Elliptic curves are used as an extension to other cryptosystems that are being used currently like Elliptic Curve Diffie-Hellman Key Exchange and Elliptic Curve Digital Signature Algorithm.Elliptic curve can be extended to implement on hyperelliptic curves.

8. ACKNOWLEDGEMENTS

With deep sense of gratitude I express my sincere thanks to my esteemed and worthy Guide Prof. Samta Gajbhiye ,SSGI Bhilai for their valuable guidance in carrying out this work under their effective supervision, encouragement , enlighten and cooperation.

9. REFERENCES

[1] Williams Stallings, Cryptography and Network Security, *Prentice Hall,* 4th Edition, 2006

[2] Dr H. K Pathak, " Discrete mathematical structure"

[3] Stephen J. Chapman, "MATLAB programming for Engineers".

[4] Guicheng shen, Xuefeng zheng, "Research on Implementation of Elliptic Curve Cryptosystem in E-Commerce", 978-0-7695-3258-5/08 $25.00 © 2008 IEEE

[5] J.Nafeesa Begum,K. Kumar and Dr.V. Sumathy," Multilevel Access Control in Defense Messaging System Using Elliptic Curve Cryptography, Second International conference on Computing, Communication and Networking Technologies,2010Bin Yu

[6] , "Method to Generate Elliptic Curves Based on CM Algorithm", 978-1-4244-6943-7/10/$26.00 IEEE,2010

[7] N. Koblitz," Elliptic curve cryptosystem," matematics of computer, vol.48, pp.203-209, 1987.

[8] V.Miller," Uses of elliptic curves in cryptography," Advance in Cryptology (CRYPTO), LNCS vol.218, pp. 417–428, 1985.

[9] N.A. Saqib, F. Rodriguez-Henriquez and A. Diaz-perez, " A parallel architecture for fast computation of elliptic curve scalar multiplicationover GF(2m)", proceeding in the 18th international parallel and distributed processing symposium, USA, , vol. 4, pp.144a, April 2004.

[10] Abdalhossein Rezai and Parviz Keshavarzi,"High-performance implementation approach of elliptic curve cryptosystem for wireless network applications", 978-1-61284-459-6/11/$26.00 IEEE,2011

[11] P.G. Shah, X. Huang and D. Sharma, "Sliding window method with flexible window size for scalar multiplication on wireless sensor network nodes," proceeding in international conference on wireless communication and sensor computing, pp. 1-6, January 2010.