ELLIPTIC CALCULATOR

By :-
Md Saim Ahmad
Adil Reza

UNDER THE AEGIS OF :-
Prof Utpal Kumar Ray

Project Description

An android application of “Elliptic Calculator” in order to get the output of certain operation done on an elliptic curve which is mainly used in “Elliptic Curve Cryptography”.

The application is targeted to perform operations like :-

- Finding all the points in an elliptic curve on a finite field.
- Adding two points on the curve.
- Multiplying a point on the curve with a scalar quantity.
- Finding order of curve and any point on the curve.

Benefits of ECC

The foremost benefit of ECC is that it's simply stronger than RSA for key sizes in use today :-

Symmetric Key Size (bits)	RSA and Diffie-Hellman Key Size (bits)	Elliptic Curve Key Size (bits)
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	521

Table 1: NIST Recommended Key Sizes

Application of ECC

- Elliptic curves are applicable for encryption, digital signatures, pseudo-random generators.
- Used in several integer factorization algorithm that have applications in cryptography, such as Lenstra elliptic curve factorization.
- Bitcoin uses Elliptic Curve Cryptography (secp256k1 with the Elliptic Curve Digital Signature Algorithm)

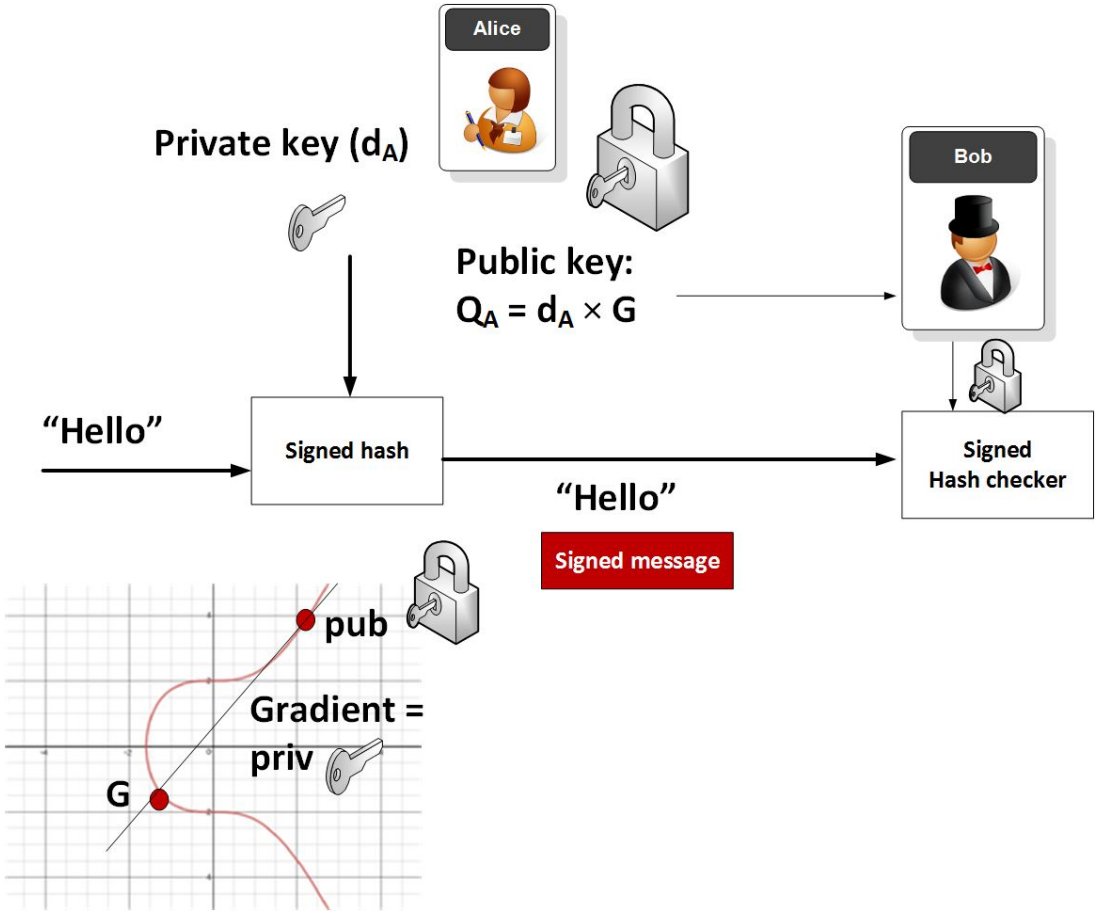
Components of ECC

- Private key :- A Random Number
- Public Key :- Point on a curve = Private Key * G
- Set of Operations :- These are defined over the curve
  $y^2 = x^3 + ax + b$,
  where $4a^3 + 27b^2 \neq 0$
- Domain Parameters :- G, a, b
  (Predefined constants)

ECC Discrete Logarithm Problem (ECCDLP)

- Let P and Q be two points on the elliptic curve
  Such that Q = kP, where k is a scalar value
- DLP: Given P and Q, find k?
  If k is very large, it becomes computationally infeasible
- The security of ECC depends on the difficulty of DLP
- Main operation in ECC is Point Multiplication

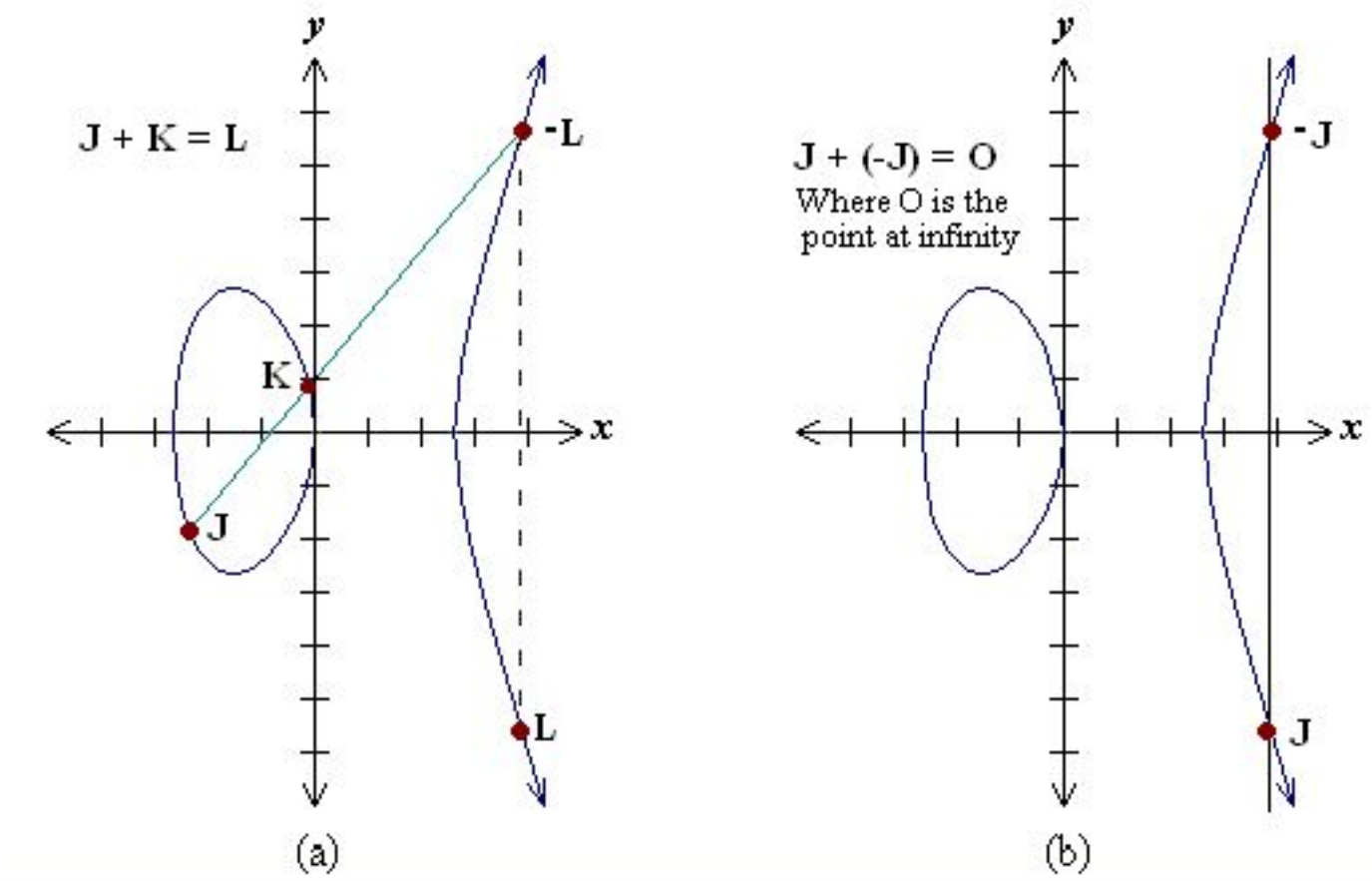
Working of ECC



Operations on Elliptic Curve

- Point Addition
- Point Multiplication
- Point Doubling
- Finding Curve Order
- Finding Point Order

Point Addition



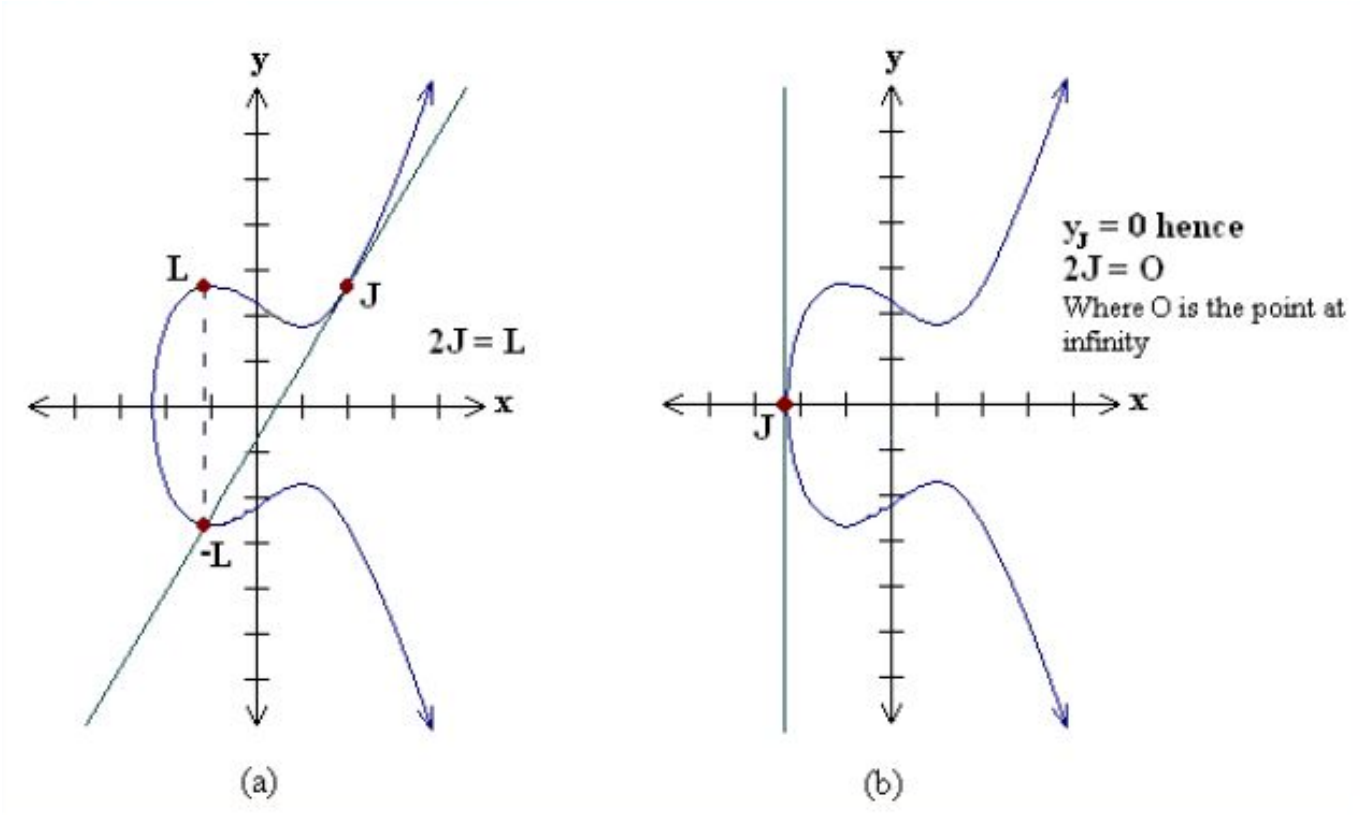
Point Multiplication

Point Multiplication is achieved by two basic curve Operations :-

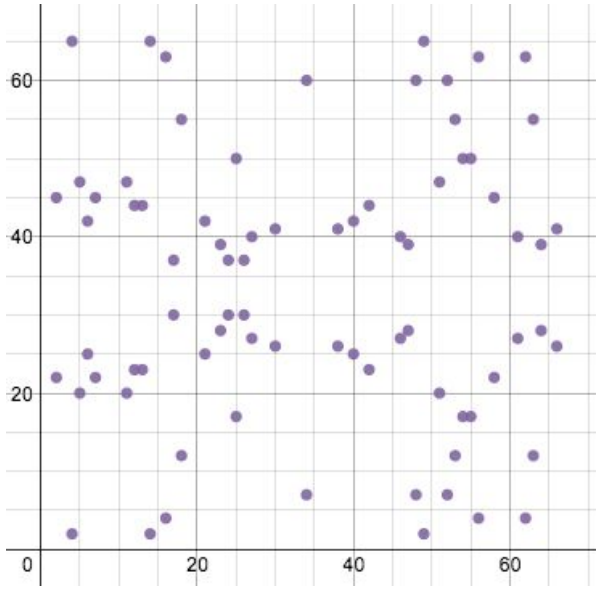
1. Point Addition, L = J + K
2. Point Doubling, L = 2J

Example:
If k = 23; then, kP = 23*P
= 2(2(2(2P) + P) + P) + P

Point Doubling



Order of Elliptic Curve



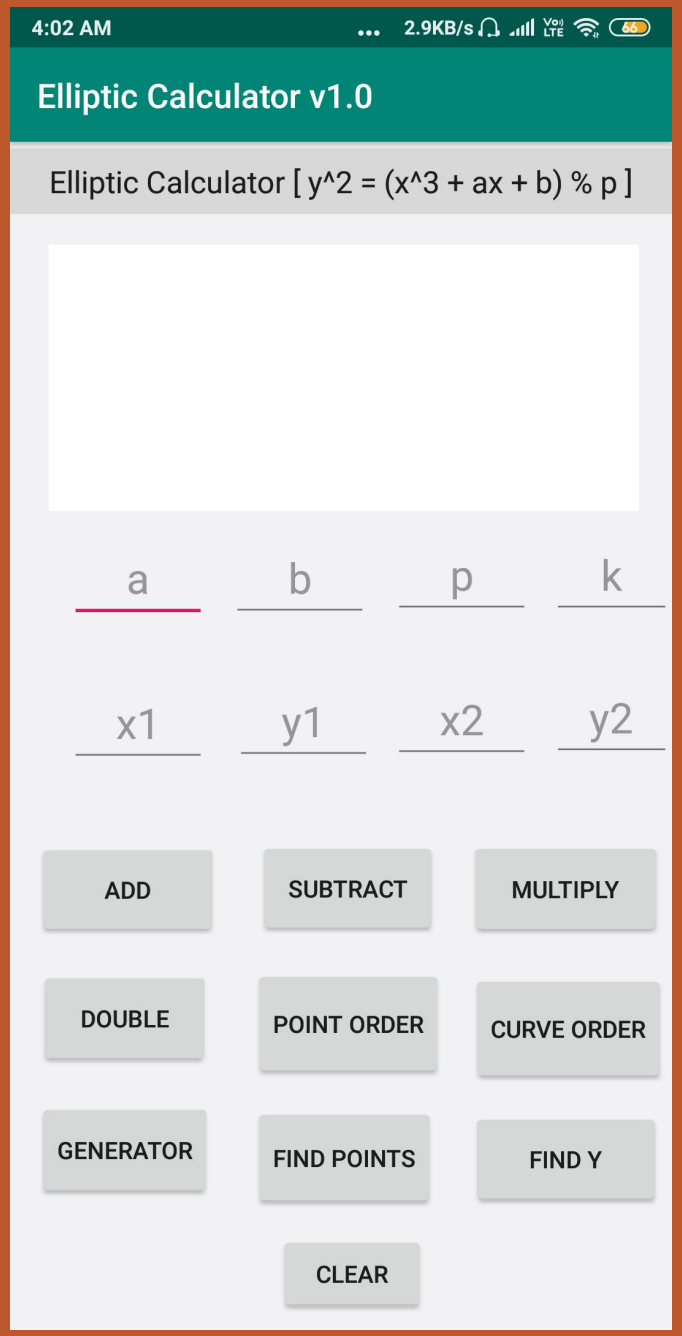
The number of integer points on the elliptic curve when
It is plotted in a finite field is called the order of the curve

List of ECC operations C programs

```
saim@saim-VirtualBox:~/Desktop/ECC$ ls
add_points                  find_order_of_a_point                find_y_given_x.c
add_points.c                find_order_of_a_point.c              point_multiply_adv.c
bsgs.c                      find_points                          point_multiply.c
bsgs_hasse.c                find_points.c                        quad_cong.c
double_points.c             find_points_N_order                  quad_cong_using_tonelli_shanks.c
find_curve-order.c          find_points_N_order.c                subgroup_generator.c
find_gen_point.c            find_points_N_order_no_to_shank      subtract_points.c
find_interval_MG.c          find_points_N_order_no_to_shank.c
find_max_interval.c         find_points_no_to_shank.c
```

Example....

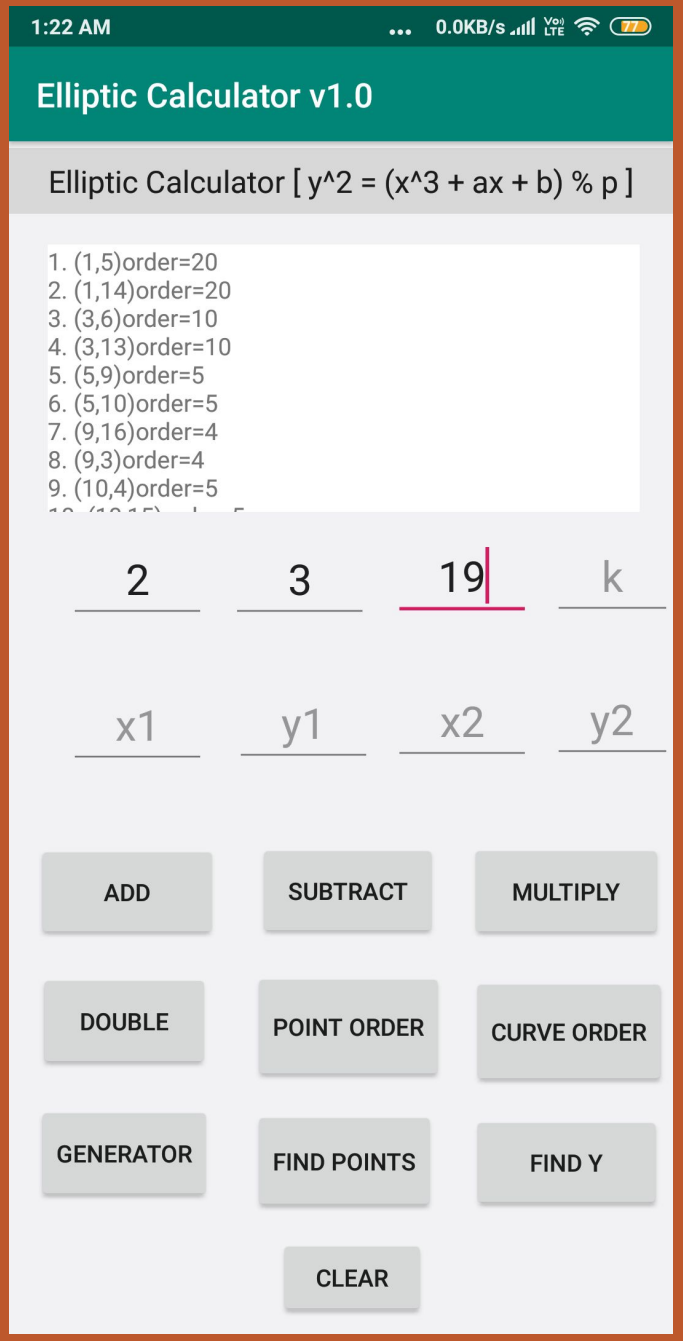
```
saim@saim-VirtualBox:~/Desktop/ECC$ ./find_points_N_order 2 3 19
19 is prime

(1 , 5) (1 , 14)          Order is 20
(3 , 6) (3 , 13)          Order is 10
(5 , 9) (5 , 10)          Order is 5
(9 , 16)          (9 , 3) Order is 4
(10 , 4)          (10 , 15)       Order is 5
(11 , 11)         (11 , 8)        Order is 20
(12 , 11)         (12 , 8)        Order is 20
(14 , 1)          (14 , 18)       Order is 20
(15 , 11)         (15 , 8)        Order is 10
(18 , 0):         Order is 2
Number of Total Points (including O point) is: 20
```



Application Layout

Here :-

- a, b & p are constants where p should be prime.
- K is the multiplication factor.
- (x1,y1) and (x2,y2) are coordinates of any two points on curve.

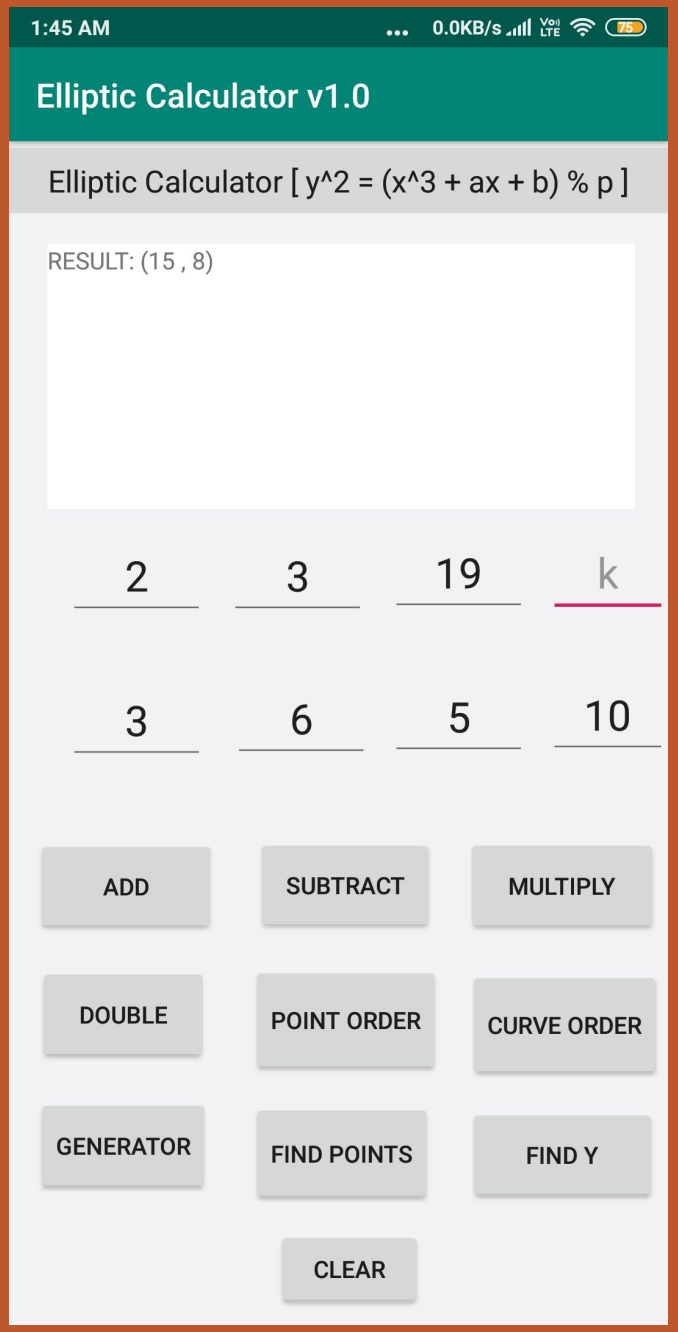


Working...

(finding all points on the curve)

Here :-

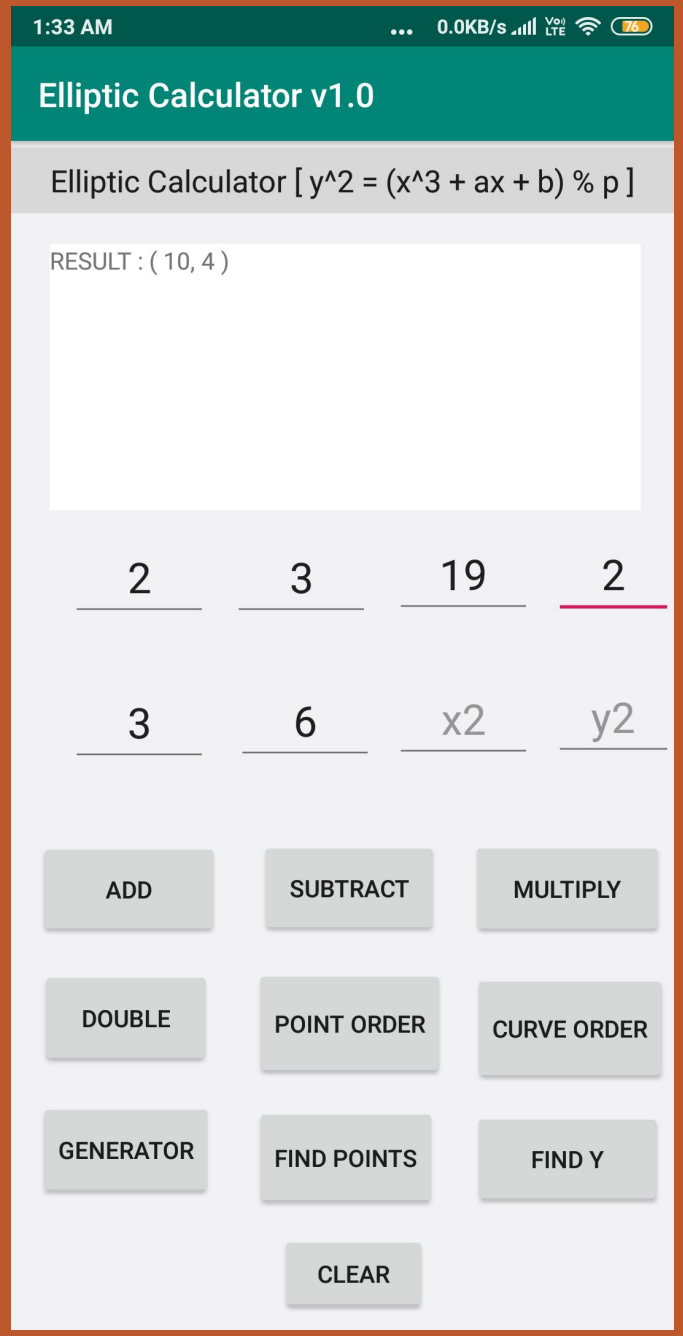
- a = 2
- b = 3
- p = 19



Working contd...
(point addition)

Here :-

- a = 2 , b=3 & p = 19
- (x1,y1) = (3,6)
- (x2,y2) = (5,10)
- Result = (15,8)



Working contd...

(point multiplication)

Here :-

- a = 2 , b=3 & p = 19
- (x1,y1) = (3,6)
- k = 2
- Result = (10,4)

Benefits : -

- This application enables performing various operations on an elliptic curve through an android device and hence is suitable for classroom environment.

Future scope for improvement :-

- More functions like finding quadratic residue can be added.
- Calculation speed can be improved.

References

- Lecture Notes & other materials supplied to us by our Mentor Prof. Utpal Kr. Ray.
- Cryptography & Network Security by B A Forouzan , D Mukhopadhyay
- Stallings, William, Cryptography and Network Security
- Cryptographic information from Wikipedia, URL http://en.wikipedia.org/wiki/Cryptography

Questions?

Thank You!!!