Point multiplication: (OR) Elliptic curve scalar multiplication (ECSM)

Given a scalar k, and a point P, find kP.

$$\underbrace{P+P+\cdots+P}_{k \text{ times}}$$

which means adding a point P to itself k times.

the simple and efficient method to compute kP is double and add method.

Double-and-add Algorithm:-

Input: Scalar K, point P on elliptic curve E.

Output: kP, scalar multiplication.

Let binary representation of k is: $k_{m-1} k_{m-2} \cdots k_0$

1. Q = P
2. for i = m-2 to 0 do
3. begin
4. P = 2P
5. if (k_i == 1) then
6. R = P + Q
7. end for.
8. Return R.

eg: Find 11P

binary of 11 is: 1011

I^st Iteration

P = 2P

2^nd P = 4P, R = 4P + Q = 5P.

3^rd P = 10P, R = 10P + Q = 11P.

Let's consider the elliptic curve $E: y^2 = x^3 + x + 1$, prime 13.

$Z_p = Z_{13} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$

0 to $(p-1)/2$, 0 to 6

$0^2 \bmod 13 = 0$
$1^2 \bmod 13 = 1$
$2^2 \bmod 13 = 4$
$3^2 \bmod 13 = 9$
$4^2 \bmod 13 = 3$
$5^2 \bmod 13 = 12$
$6^2 \bmod 13 = 10$

perfect squares
$\{0, 1, 3, 4, 9, 10, 12\}$

$x=0$, $y^2 = x^3+x+1 = 1 \Rightarrow (0,1), (0,-1) \Rightarrow (0,1), (0,12)$

$x=1$, $y^2 = (1+1+1) \bmod 13 = 3 \Rightarrow (1,4)\ (1,-4) \Rightarrow (1,4), (1,9)$

$x=2$, $y^2 = 8+2+1 = 11 \Rightarrow$ 11 is not perfect square.

$x=3$, $y^2 = (27+3+1) \bmod 13 \Rightarrow 5 \Rightarrow 5$ "

$x=4$, $y^2 = (64+4+1) \bmod 13 = 4 \Rightarrow (4,2), (4,-2) \Rightarrow (4,2), (4,11)$

Similarly the other points $(5,1), (5,12), (7,0), (8,1), (8,12)$
$(10,6)\ (10,7)\ (11,2)\ (11,11), (\infty,\infty)$

are generated. And (∞, ∞) also.

Number of points:-

Due to Hasse's theorem, the number of points N

in E(a,b) satisfies $|N-p-1| < 2\sqrt{p}$

eg: $|16-13-1| < 2\sqrt{13} \Rightarrow 2 < 2\times 3 \Rightarrow 2 \not< 6$