Zp = {0, 1, 2, ..., p-1} = set of residues (integers) that are divisible by p

5P = **P + P** + P + P + P = (2P + P) + P + P = (3P + P) + P = 4P + P = 5P

k.P = P + P + ... + P (k times)

Optimization Method:

k = 7 = (111)_2 = 1 + 2 + 4

7.P = (1 + 2 +4).P = P + 2P + 4P = P + 2(P + 2P) -> 4 point additions

[2P = P +P -> 1 point addition
P + 2P = 3P -> 1 point addition
2(3P) = 2Q = Q + Q -> 1 point addition
P + 6P -> 1 point addition
Total point additions = 4]

No. of point additions: log_2(k)

P, K1.P, K2.P

ECDLP => K1

K1K2.P = K1. (K2.P)

a (mod p) => when a is devided by p, the remainder will be considered

a = b (mod p) => p | (a-b) => a mod p = b mod p

-5 = 10 (mod 5) => 5 | [-10-5] = -15

y^2 = a (mod p)

P + (-P) = O = (-P) + P

4a^3 + 27b^2 = 4 + 27 = 31 (mod 23) = 8 #0