Curvas Elípticas

Nome: William Goulart Pacheco

soma

$P \neq Q$

$$L = \frac{(Y2 - Y1)}{(X2 - X1)}$$

$P = Q$

$$L = \frac{(3.\ (X1)^2 + A)}{(2.Y1)}$$

$$X3 = (L^2 - X1 - X2) \bmod p$$

$$Y3 = [L.(X1 - X3) - Y1] \bmod p$$

Negação

primo=11

P(0,2)

-P = (0,(11-2))

-P = (0,9)

Subtração

P-Q

P+ (-Q)

Multiplicação

3P=(P+P)+P

soma - lambda

P ≠ Q	P=Q
$L = \dfrac{(Y2 - Y1)}{(X2 - X1)}$	$L = \dfrac{(3.\ (X1)^2 + A)}{(2.Y1)}$

Soma - ajuste lambda

P ≠ Q

L= (Y2 -Y1) * ((X2-X1) modinverse p)

P=Q

L= (3. ((X1)² mod p) + A) * ((2.Y1) modinverse p)

modinverse - inverso modular

3 * 0 ≡ 0 (mod 7)
3 * 1 ≡ 3 (mod 7)
3 * 2 ≡ 6 (mod 7)
3 * 3 ≡ 9 ≡ 2 (mod 7)
3 * 4 ≡ 12 ≡ 5 (mod 7)
3 * 5 ≡ 15 (mod 7) ≡ 1 (mod 7) <------ RESTO 1 , ENCONTROU O INVERSO!
3 * 6 ≡ 18 (mod 7) ≡ 4 (mod 7)

5 é o inverso modular de 3 mod 7

$Y^2 = X^3 + 4X + 4 \bmod 11$

p=11
# qtd_residuos_quadraticos = (11-1) / 2
# qtd_residuos_quadraticos = 5

Y' = (i)² mod p	Y' = (p-i)² mod p	crivos
1² mod 11	10² mod 11	1
2² mod 11	9² mod 11	4
3² mod 11	8² mod 11	9
4² mod 11	7² mod 11	5
5² mod 11	6² mod 11	3

X	Crivo = X³ +4X +4 mod 11	Y'	Y''	PONTOS
0	(0³ + 4.0 + 4) mod 11 = 4	2	9	(0,2) (0,9)
1	(1³ + 4.1 + 4) mod 11 = 9	3	8	(1,3) (1,8)
2	(2³ + 4.2 + 4) mod 11 = 9	3	8	(2,3) (2,8)
3	(3³ + 4.3 + 4) mod 11 = 10			
4	(4³ + 4.4 + 4) mod 11 = 7			
5	(5³ + 4.5 + 4) mod 11 = 6			
6	(6³ + 4.6 + 4) mod 11 = 2			
7	(7³ + 4.7 + 4) mod 11 = 1	1	10	(7,1) (7,10)
8	(8³ + 4.8 + 4) mod 11 = 9	3	8	(8,3) (8,8)
9	(9³ + 4.9 + 4) mod 11 = 10			
10	(10³ + 4.10 + 4) mod 11 = 10			

E11={P∞ , (0,2),(0,9),(1,3),(1,8),(2,3),(2,8),(7,1),(7,10),(8,3),(8,8)}