2. Działania na krzywej eliptycznej

Zad.1

$Y^2+a_1XY+a_3Y-(X^3+a_2x^2+a_4X+a_6)=0$

l: $y = \lambda x + \mu$

$$E(x, \lambda x + \mu) = 0 = -(x - x_1)(x - x_2)(x - x_3)$$

$(\lambda x + \mu)^2 + a_1 x(\lambda x + \mu) = a_2 x^2 \qquad (x_1 + x_2 + x_3) - x^2$

$$x^2(\lambda^2 + a_1\lambda - a_2)$$

$$x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2$$

$$\bar{y} = \lambda x_3 + \mu = \lambda x_3 + y_1 - \lambda x_1 = \lambda(x_3 - x_1) + y_1$$

$$-y_3 = \lambda(x_3 - x_1) + y_1 + a_1 x_3 + a_3$$

$$y_3 = -\lambda(x_3 - x_1) - y_1 - a_1 x_3 - a_3$$

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} dla\_P \neq Q$$

$$\lambda = \frac{3x^2 - a_1 y + 2a_2 x + a_4}{2y + a_1 + a_3} dla\_P = Q$$

zatem 1) E:y2=x3-x mod 5

p+Q….=(3,3)

Zad.2

Oblicz 2*(P+Q)

$$\lambda = \frac{3x^2 - a_1 y + 2a_2 x + a_4}{2y + a_1 + a_3} = \frac{3x^2 - 1}{2y} = \frac{27 - 1}{6} = \frac{26}{6} = \frac{1}{1} = 1$$

$$x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_1 = 1^2 - 2 * 3 = 1 - 6 = -5 = 0$$

$$y_3 = \lambda(x_1 - x_3) - y_1 - a_1 x_3 - a_3 = 1(3 - 0) - 3 = 0$$

2(P+Q)=(0,0)

Θ,(0,0), (1.0), (2.1), (3,3), (2,4)

Inny sposób P=(1,0) Q=(2,1) P+Q=(3,3) 2*(P+Q)=(0,0)

Znajdź generator grupy:

(0,0)

nie dają się mnożyć 2*(0,0)= Θ

(1,0)

(2,1)+(2,4)= Θ

P=(2,1) 2*P

$$\lambda = \frac{12 - 1}{2} = \frac{11}{2} = \frac{1}{2} (\mathrm{mod}\, 5) = 1 = 2^{-1} (\mathrm{mod}\, 5) = 3$$

x_3=9+4=0

y_3=3*(2-0)-1=0

P=(2,4) 2*P

$$\lambda = \frac{12 - 1}{9} = \frac{11}{3} = 1 * 3^{-1} = 2$$

x_3=4-4=0

y_3=2*(2-0)-4=0