4. Działania Weila

$$e(P,Q) = \frac{fp(\lambda Q)}{fq(\lambda P)} \; gdzie \_ \lambda q = (Q) - (\theta) \sim (Q + R_2) - (R_2)$$

fp: $(fp) \sim n(P) - n(\Theta) \sim n\{(P+R_1) - (R_1)\} \sim n(P+R_1) - n(R_1) \sim n(P+R_1) - n(R_1) - (nP) + (\Theta) := A_n := (fn)$

Po obliczeniu fp wystarczy policzyć fn

λ_n spełnia równanie nie-rekurencyjne

$$\lambda_{b+c} = \lambda_b + \lambda_c + (g_1) + (g_2) \text{ , gdzie } \begin{matrix} g_1 = (bP) + (cP) + (\overline{b + c(P)}) - 3(\theta) \\ g_2 = (b+c)P + (\overline{(b+c)P}) - 2(\theta) \end{matrix}$$

Stąd $f_{b+c}(\lambda_a) = fb(\lambda a) * fc(\lambda a) = \frac{g_1}{g_2}(\lambda a)$

Krzywa E_{11}: $y^2-(x^3+1)=0 (\text{mod } 11)$

Zad.1

Znaleźć 4 punkty na

E_{11}:={Θ,(0,1),(0,10),(2,3),(2,8),(5,4),(5,7),(7,5),(7,6),(9,2),(9,9),(10,0)}

x	x^3+1	y	y^2
3	6	0	0
4	10	1	1
5	5	2	4
6	8	3	9
7	3	4	5
8	7	5	3
9	4	6	3
10	0	7	5
		8	9
		9	4
		10	1

Zad.2

Obliczyć $f_3(\lambda_a)$ dla Q- podst. rzędu, 3 czyli 3Q=Θ

a) znajdź Q: 3Q=Θ

b) $f_1(\lambda a)$

c) $f_3(\lambda a)$

Dla 2P

Ad. A

$$\lambda(2P) = \frac{3x^2 + 2a_2x + a_4 - a_1y}{2y + a_1x + a_3}$$ czyli dla E_{11}: $\lambda = \frac{3x_1^2}{2y_1}$

P=(x_1,y_1)

$$x_3 = \lambda^2 + a_1\lambda - a_2 - 2x_1$$ (czyli $x_3 = \lambda^2 - 2x_1$)

$$y_3 = \lambda(x_1 - x_3) - y_1 - a_1x_3 - a_3$$ (czyli $y_3 = \lambda(x_1 - x_3) - y_1$)

(10,0) – rzędu 2

2*(0,1) $\lambda = 0$ x_3=, 0 y_3= 10 2*(0,1)=(10,0)

(0,10+ (0,10)=Θ 3*(0,1)=Θ

Ad. B

$f_1(\lambda a)$ (f1)~ (P+R_1)-(R_1)-(P)+Θ

Ustalamy P rzędu 3(inny)

12*(9,2)= Θ 3*(0,1)= Θ 3*(0,10)= Θ

4*(5,4)= Θ 6*(2,3)= Θ

P=(0,1) R_1=(0,1) Q=(0,-1)

(f_1)~ ((0,-1))- (0,1)- (0,1)+ Θ

$\lambda a = \lambda(0,1) = (Q + R_2) - R_2$

$\lambda q = Q - (\theta) = (0,-1) - (\theta)$

$f_1(\lambda a) = \prod f(P)^{ap} = f1(0,-1)^1$

Def. $\lambda = \sum ap(P)$

Trzeba znaleźć f_1) przy zadanym dywizorze

$$(f1) \sim (P+R_1)-(R_1)-(P)+\Theta \quad (\frac{1}{f_1}) \sim (P) + (R_1) + (\overline{P + R_1}) - 3\theta$$

szukamy stycznej w punkcie (0,1)

$$\left\{\begin{matrix} ax + by + c = 0 \\ y^2 = x^3 + 1 \end{matrix}\right\} \quad P=(0,1)$$