Samostatná úloha

Jak řešit $(\alpha^2, \beta^2) = [q](\alpha, \beta)$ pro $P = (\alpha, \beta) \in E[\ell]^*$

? Zjistit, ověřit, zda q je vlastní číslo Frobeniova endomorfismu, tj. lin. zobrazení $E[\ell]$ (máme $E[\ell] \cong \mathbb{Z}_\ell^* \times \mathbb{Z}_\ell^*$)

$$1 \leq q < \ell$$

equalx(ℓ)

$$[n]P = \left(x - \frac{\psi_{n-1}\psi_{n+1}}{\psi_n^2},\ \frac{\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2}{4y\psi_n^3}\right)$$

F

$$\boxed{[n](\alpha,\beta) = \left(\alpha - \frac{u_n(\alpha)}{v_n(\alpha)},\ \beta\frac{r_n(\alpha)}{s_n(\alpha)}\right)}$$

$$\frac{u_n(x)}{v_n(x)} = \frac{\bar f_{n-1}(x)\bar f_{n+1}(x)\cdot \mathcal{X}}{\bar f_n^2(x)}$$

$$\mathcal{X} \begin{cases} 4(x^3+ax+b) & n>1 \text{ lichö} \\ \dfrac{1}{4(x^3+ax+b)} & n\geq 2 \text{ sudo} \end{cases}$$

$$\frac{r_n(x)}{s_n(x)} = \frac{\bar f_{m+2}(x)\bar f_{m-1}^2(x) - \bar f_{m-2}(x)\bar f_{m+1}^2(x)}{\mathcal{Z}\,\bar f_m^3(x)}$$

$$\frac{u_1(x)}{v_1(x)} = \frac{0}{1}$$

$$\frac{r_1(x)}{s_1(x)} = \frac{1}{1}$$

$\mathcal{Z} = 1$ $\quad n\geq 3$ lichö

$\mathcal{Z} = 16(x^3+ax+b)^2$ $\quad n\geq 2$ sudo

Ověřit, zda p je vlastní číslo známou

1. Zjišťovat, zda lze ověřit rovnici $x^q = x - \frac{u_p(x)}{v_p(x)}$

$$\gcd\left(v_p(x)\,x^q - x\,v_p(x) + u_p(x),\ f_\ell\right) = g_\ell$$

2. $g_\ell > 1$ $\qquad g_\ell = 1 \Rightarrow$ p není vlastní číslo

2. Až $g_\ell > 1$ $\qquad y^q = y\,\frac{r_p(x)}{s_p(x)}$ $\qquad y^{q-1} = \frac{r_p(x)}{s_p(x)}$

$$\gcd\left((x^3+ax+b)^{\frac{q-1}{2}} s_p(x) - r_p(x),\ g_\ell\right) > 1 \qquad y^{q-1} = (x^3+ax+b)^{\frac{q-1}{2}}$$

Pokud ano — p je vlastní, pokud $=1$, není

Pokud ρ vlastní, tak v $E[\ell]$ má vlastní podprostor

Ten obsahuje $\ell-1$ nenulových bodů, a pak $\deg(g_\ell) = \frac{\ell-1}{2}$

Vlastní čísla kořeny $T^2 - t_\ell T + q_\ell$.

$T^2 - t_\ell T + q_\ell = (T-\rho)^2$, tak $\deg(g_\ell) = \frac{\ell^2-1}{2}$ $g_\ell = f_\ell$

Co když pár vlastní čísla $-\rho$ i ρ.

Pak $T^2 - t_\ell T + q_\ell = (T-\rho)(T+\rho) = T^2 - \rho^2$

$\Rightarrow t_\ell = 0$

Rozhodnuje, zda $\exists P \in E[l]^*$, že $\varphi^2(P)$ a $[q_l]P$ se shodují v x-ové souřadnici $\quad \tau = t_l$

$$g_l = \gcd(\xi_l, f_l) \qquad \text{if } (g_l > 1) \quad \tau = \underline{\text{equalx}(l)}$$

equalx(l) nejprve zjistí, zda $t_l = 0$ tedy zda $\varphi^2(P) \oplus [q_l]P = O$ $(\forall P \in E[l])$

Gpt. pom. pokud $\deg(g_l) < \frac{l^2-1}{2}$, tak $t_l \neq 0$

Abychom ověřili $t_l = 0$, stačí najít jeden bod $P \in E[l]^*$, že $\varphi^2(P) \oplus [q_l]P = O$. V první souřadnici to platí pro $\forall P = (\alpha, \beta)$, že $g_l(\alpha) = 0$

Stačí ověřit, že to platí i v druhé

$$\beta \frac{r_{q_l}(\alpha)}{s_{q_l}(\alpha)} \overset{?}{=} -\beta^{q^2} \qquad r_{q_l}(\alpha) = -(\alpha^3 + a\alpha + b)^{\frac{q^2-1}{2}} s_{q_l}(\alpha)$$

$$\gcd\left(g_l, r_{q_l}(x) + (x^3 + ax + b)^{\frac{q^2-1}{2}} s_{q_l}(x)\right) \overset{?}{>} 1$$

ANO $\tau = t_l = 0$

NE $t_l \neq 0$

$t_\ell \neq 0 \Rightarrow \exists$ vlastní číslo $\mu = \frac{2q_\ell}{\tau}$ $\tau^2 \equiv 4q_\ell \mod \ell$

JEDNO τ se vybere, jehož se přiřadí μ a zjišťuje se, zda μ je vlastní číslo. Pokud není, je vlastní číslo $= -\mu$
a místo vybraného τ bude brát $-\tau$

NEMŮŽE NASTAT, ŽE BY μ a $-\mu$ byla obě vlastní čísla

---

1. fázi zjišťování, že μ je vlastní číslo, můžeme vynechat a počítat $g_\ell = \gcd(f_\ell, \bar{f}_\ell)$.

Kořeny g_ℓ jsou všechna $P = (x, y) \in E[\ell]^*$, že $\varphi(P)$ a $[q_\ell]P$ se shodují v x-ové souřadnici. Všechna taková P tvoří podprostor $E[\ell]^*$.

na body z kolmého vlastního podprostoru nepadají do

Tento podprostor obsahuje vlastní podprostor odpovídající vl. číslu $\pm\mu$:

$\varphi^2(P) = [\mu^2]P = \left[\frac{4q_\ell^2}{\tau^2}\right] = [q_\ell]P$. Pokud vlastní prostor $\pm\mu$ má dim 2, je $g_\ell = f_\ell$

ODVOZENÍ Z VLASTNÍHO

Pokud vl. podprostor $\neq E[\ell]^*$, je dimenze 1. Pak tam $\exists$ ještě jiné vlastní číslo, řešíme χ a stačí ověřit, že

$\exists\,\lambda$ taková, že $\lambda^2 \equiv q^2$

$\lambda^2 = q_\ell$ odvození vede na $\lambda = \frac{2q_\ell}{\tau}$, kde $\frac{4q_\ell^2}{\tau^2} = q_\ell$

$\tau^2 \equiv 4q_\ell \mod \ell$

$\varphi(P) = [\lambda]_\ell P$

$\varphi^2(P) = [\lambda^2] P$

$[\lambda^2]P$ a $[q_\ell]P$ se shodují v první souřadnici

$g_\ell = \gcd(\bar{\psi}_\ell, f_\ell)$ popisuje vlastní podprostor

$\lambda^2 = -q_\ell$

$\gcd((x^3$

~~$g_\ell =$~~

$g_\ell = \gcd(\bar{s}_\ell, \bar{f}_\ell)$ popisuje skutečné vlastní podprostory čísla τ_p, takové odpovídající polynom z 1. kroku počáteční úvahy o výpočtu vlastního čísla.

Zbývá pouze rozhodnout, zda τ_p vyhovuje 2. kroku, tedy zda $\gcd\left((x^3+ax+b)^{\frac{q-1}{2}} s_p(x) - \tau_p(x), g_\ell\right) \geq 1$

Pokud ANO NAVRAŤ $\tau = t_\ell$ POKUD NE NAVRAŤ $-\tau = t_\ell$

```
IF gcd(s̄_ℓ, f̄_ℓ) ≠ 1
    THEN τ = equal(ℓ)
    ELSE DO
        τ = 0;                         /* τ = 1 ... (ℓ-1)/2 */
        do: τ = τ+1, r = nonequal(ℓ, τ)
        UNTIL r ≠ 0
        IF r == -1  THEN τ = -τ
    m = MUL(ℓ, τ) }
```

$$\tau = t_\ell$$

nonequal(x)

$$\text{if } (\gcd(h_x, \bar{f}_e) = 1) \text{ return } 0$$

$$\text{if } (\gcd(h_{y}, \bar{f}_e) = 1) \text{ return } -1$$

$$\text{return } 1;$$

VÍME, ŽE NA VSTUPU MŮŽEME PŘEDPOKLÁDAT,

ŽE $\varphi^2(P) \oplus [\xi_e]^P$ se liší vždy v prvosouřadnici

pro každé $P \in E[l]^*$

Řešíme, zda $\varphi^2(P) \oplus [\xi_e]^P = [\pm t]\varphi(P)$

$$[\xi_{\ell}](\alpha,\beta) = \left(\alpha - \frac{u(\alpha)}{v(\alpha)},\ \beta\,\frac{r(\alpha)}{s(\alpha)}\right) \qquad u = u_{\xi_\ell}\quad v = v_{\xi_\ell}\ \ldots$$

$q_\ell = 1$ — řeší 2 zobr. (triviální) $\qquad \varphi^2(P) \oplus [\xi_\ell]P = [\tau_\ell]\varphi(P)$

$$\varphi^2(P) \oplus [\xi_\ell]P = \left(\lambda^2 - \alpha^{q^2} - \alpha + \frac{u(\alpha)}{v(\alpha)},\ \lambda\left(2\alpha^{q^2} - \lambda^2 + \alpha - \frac{u(\alpha)}{v(\alpha)}\right) - \beta^{q^2}\right)$$

$$\lambda = \frac{\beta^{q^2} - \beta\, r(\alpha)/s(\alpha)}{\alpha^{q^2} - \alpha + u(\alpha)/v(\alpha)} = \beta\,\frac{v(\alpha)}{s(\alpha)}\left(\frac{(\alpha^3+a\alpha+b)^{\frac{q^2-1}{2}}\, s(\alpha) - r(\alpha)}{v(\alpha)(\alpha^{q^2}-\alpha) + u(\alpha)}\right)$$

V λ^2 vyměníme β^2 za $(\alpha^3+a\alpha+b)$ takže skutečnost, že nejde o $P = (\alpha,\beta) \in E[\ell]$ vyjadřuje rovnici v první souřadnici, znamená že $\lambda^2 - \alpha^{q^2} - \alpha + \frac{u(\alpha)}{v(\alpha)} = \alpha^2 - \frac{u_\tau(\alpha^2)}{v_\tau(\alpha^2)}$ h_x ~~...~~ je polynom, který popisuje souřadnici nebo

$\frac{q^2-1}{2}$

by se pak ~~pomocí~~ ~~s~~ shodovalo z y-ové souřadnice

NA LEVÉ STRANĚ $\beta\,(\beta^{q^2-1}$ nahradíme $(\alpha^3+a\alpha+b)^{\frac{q^2-1}{2}}$

NA PRAVÉ STRANĚ $\beta^2\,\frac{r_\tau(\alpha^2)}{s_\tau(\alpha^2)}$ $\qquad \beta^2 = \beta\,(\alpha^3+a\alpha+b)^{\frac{q^2-1}{2}}$

Bez konstant. Proto h_y pouze od x

Více o Weierstrassově křivce

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

$\mathrm{char}(K) \neq 2 \longrightarrow$ úprava na $y^2 = x^3 + a_2x^2 + a_4x + a_6$

$\mathrm{char}(K) \neq 3$ $\quad y^2 = x^3 + a_4x + a_6$

<u>úprava</u> $\quad y \longmapsto y + sx + t$

$\quad x \longmapsto x + r$

$\mathrm{char}(K) \neq 2, 3$ $\exists$ jediná trojice (r, s, t) takové, že

$$y^2 = x^3 + ax + b$$

$\mathrm{char}\,K = 3$:

- supersingulární $a_2 + a_1^2 = 0$ $\quad y^2 = x^3 + ax + b$ $\quad \bar{K} = K$ úprava $b = 0$
- $y^2 = x^3 + ax^2 + b$ $\quad a_2 + a_1^2 \neq 0$

$\mathrm{char}\,K = 2$:

- supersing. $a_1 = 0$ $\quad y^2 + a_3y = x^3 + a_4x + a_6$ $\quad K = \bar{K}$ $\quad a_4 = a_6 = 0$
- obecný $a_1 \neq 0$ $\quad y^2 + a_1xy = x^3 + a_2x^2 + a_6$ $\quad \bar{K} = K$ $\quad a_2 = 0$

$x \mapsto u^{-2}x \qquad y \to u^{-3}y$

$$y^2 = x^3 + a_4x + a_6 \longrightarrow (u^{-3}y)^2 = (u^{-2}x)^3 + a_4u^{-2}x + a_6$$

$$y^2 = x^3 + u^4a_4x + u^6x_6$$

char $k=3$ $\quad y^2 = x^3 + a_2x^2 + a_6 \longrightarrow y^2 = x^3 + u^2a_2x^2 + u^6a_6$

char $k=2$ $\quad y^2 + a_3u^3y = x^3 + u^4a_4x + u^6a_6$ supersing.

$$y^2 + \underbrace{a_1u}_{1}xy = x^3 + u^2a_2x^2 + u^6a_6$$

$\operatorname{char} K \neq 2,3$

$$(SH1) \quad y^2 = x^3 + a_4 x + a_6 \xrightarrow{K=\overline{K}} \begin{cases} y^2 = x^3 + x + a_6 \\ y^2 = x^3 + 1 \\ y^2 = x^3 \quad (\text{CUSP}) \end{cases}$$

$$(SH2a) \quad y^2 + xy = x^3 + a_2 x^2 + a_6 \longrightarrow y^2 + xy = x^3 + x^2 + a_6$$

$$(SH2b) \quad y^2 + a_3 y = x^3 + a_4 x + a_6 \longrightarrow y^2 + y = x^3 \text{ NEBO } \underset{\text{CUSP}}{y^2 = x^3}$$

$$(SH3a) \quad y^2 = x^3 + a_2 x^2 + a_6,\ a_2 \neq 0 \longrightarrow y^2 = x^3 + x^2 + a_6$$

$$(SH3b) \quad y^2 = x^3 + a_4 x + a_6 \longrightarrow y^2 = x^3 + x \text{ NEBO } y^2 = x^3$$

ZÁPIS NAD $\overline{K}$ JE JEDNOZNAČNÝ AŽ NA $\pm a_6$ v SH1

A AŽ NA $a_6 \to \eta a_6$ v SH3a, kde $\eta^3 = 1$

j-invariant je hodnota, která určí příslušnost k normálním tvarům nad $\overline{K}$ pro hladké W.K.

j-invariant se počítá pomocí diskriminantu $\Delta(C)$ a $\Delta(C) = 0 \iff C$ je singulární k definic $\Delta(C)$ se dopolnje [illegible] diskriminant polinom

$a = \sum a_i x^i$ $\quad D(a) = a_n^{2n-2} \prod_{i<j} (\alpha_i - \alpha_j)^2 \quad a(x) = (a-\alpha_1) \cdots (a-\alpha_n)$

$D(a)$ je tudi enako

$R(a, a')$ je matrika

$(-1)^{\binom{n}{2}} a_n^{-1} \det R(a, a')$

$$\begin{array}{c} \begin{pmatrix} a_n & a_{n-1} & \cdots & a_1 & a_0 & 0 & \cdots & 0 \\ 0 & a_n & a_{n-1} & \cdots & a_1 & a_0 & \cdots & \\ 0 & 0 & & a_n & \cdots & & a_1 & a_0 \\ na_n & (n-1)a_{n-1} & \cdots & & a_1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & na_n & \cdots & & 2a_2 & a_1 \end{pmatrix} \end{array} \begin{array}{l} \left.\vphantom{\begin{matrix} a \\ a \\ a \end{matrix}}\right\} n-1 \text{ vrstic} \\ \left.\vphantom{\begin{matrix} a \\ a \end{matrix}}\right\} n \text{ vrstic} \end{array}$$

$$D(ax^3+bx^2+cx+d) = -a^{-1} \begin{vmatrix} a & b & c & d & 0 \\ 0 & a & b & c & d \\ 3a & 2b & c & 0 & 0 \\ 0 & 3a & 2b & c & 0 \\ 0 & 0 & 3a & 2b & c \end{vmatrix}$$

$$= b^2c^2 - 4ac^3 - 4b^3d + 18abcd - 27a^2d^2$$

$y^2 = f(x)$ char$(K) \neq 2$

$$D(f) = a_2^2 a_4^2 - 4a_4^3 - 4a_2^3 a_6 + 18 a_2 a_4 a_6 - 27 a_6^2$$

$b_2 = 4a_2$ $b_4 = 2a_4$ $b_6 = 4a_6$

$$16 D(f) = -8 b_4^3 + 9 b_2 b_4 b_6 - 27 b_6^2 + b_2^2 \underbrace{(b_4^2 - b_2 b_6)}_{4}$$

Obecnie teraz WK w char$(K) \neq 2$. substytucja $\boxed{\begin{array}{l} x \mapsto x \\ y \mapsto y + sx + t \end{array}}$

prowadzi na $y^2 = x^3 + (a_2 + \frac{a_1^2}{4})x^2 + (a_4 + \frac{a_1 a_3}{2})x + (a_6 + a_3^2)/4$

$b_2 = 4a_2 + a_1^2$ $b_4 = 2a_4 + a_1 a_3$ $b_6 = 4a_6 + a_3^2$

char$(K) \neq 2$ $\frac{b_2 b_6 - b_4^2}{4} = 4a_2 a_6 + a_2 a_3^2 + a_1^2 a_6 - a_4^2 - a_1 a_3 a_4 = b_8$

$$\Delta(C) = -8 b_4^3 + 9 b_2 b_4 b_6 - 27 b_6^2 - b_2^2 b_8$$

Pokaži $\Delta(C)=0 \iff C$ je singularna

	b_2	b_4	b_6	b_8	$\Delta(C)$
St(1)	0	$2a_4$	$4a_6$	$-a_4^2$	$-8b_4^3-27b_6^2=-16(4a_4^3+27a_6^2)$
St(2a)	1	0	0	a_6	$b_8=a_6$
St(2b)	0	0	a_3^2	a_4^2	$b_6^2=a_3^4$
St(3a)	a_2	0	a_6	a_2a_6	$-b_2^3b_8=-a_2^3a_6$
St(3b)	0	$-a_4$	a_0	$-a_4^2$	$-b_4^3=-a_4^3$

$x\mapsto u^{-2}x \qquad y\mapsto u^{-3}y \qquad \Delta(\tilde{C})=u^{12}\Delta(C)$

$C\to\tilde{C}$

$j(C)$ definiran tako, da se efekt u^{12} nevtralizira

$$j(C) = \frac{c_4^3}{\Delta(C)} \qquad c_4 = b_2^2 - 24 b_4$$

<u>St1</u> $\quad 1728\left(\frac{4a_4^3}{4a_4^3 + 27a_6^2}\right) = j(C) \qquad 12^3 = 1728$

<u>St2a</u> $\quad \frac{1}{a_6}$ $\quad$ <u>St2b</u> $\quad 0$ $\quad$ <u>St3a</u> $\quad -\frac{a_2^3}{a_6}$ $\quad$ <u>St3b</u> $\quad 0$

$j(C) = j(\tilde{C}) \iff$ modele WK są K-ekwiwalentne.