Úvod do Schoofova algoritmu.

$|E(\mathbb{F}_q)| = q - t + 1 \qquad |t| \le 2\sqrt{q}$

Zásadní vztah – char. polynom Frob. end. se anuluje na křivce.

$$\varphi^2 \ominus [t]\varphi + [q] = \mathcal{O} \quad (=\infty)$$

Co je to φ^2. anuluje?

φ Frob. end. $\varphi : E \to E$ je def.

pomočo Frob. end $\lambda \mapsto \lambda^{q}$

$\forall P \in E$

$\varphi(\varphi(P)) - [t]\varphi(P) + [q]P = O$

def Frob. end. Potrebujemo na af. krivulje

tak $\varphi : (\alpha_1, \alpha_2) \mapsto (\alpha_1^{q}, \alpha_2^{q})$

def na proj. krivulje $(\alpha_1 : \alpha_2 : \alpha_3) \mapsto (\alpha_1^{q} : \alpha_2^{q} : \alpha_3^{q})$

E je definirana nad $\mathbb{F}_q$

Vztah $\varphi(P) \in C$ pro $\forall P \in C$ platí pro všechny křivky def. nad $\mathbb{F}_\Sigma$, [illegible]

$C = V_F \qquad F = \sum f_{ijk} X_1^i X_2^j X_3^k \qquad i+j+k=d$ (hom. polynom)

$(\alpha_1 : \alpha_1 : \alpha_3) \mapsto (\alpha_1^\Sigma : \alpha_2^\Sigma : \alpha_3^\Sigma)$

$0^\Sigma = \left(\sum f_{ijk} \alpha_1^i \alpha_2^j \alpha_3^k \right)^\Sigma \qquad 0 = \sum f_{ijk}^\Sigma (\alpha_1^{\Sigma i} \alpha_2^{\Sigma j} \alpha_3^{\Sigma k})$

$f_{ijk} \in \mathbb{F}_\Sigma \qquad f_{ijk}^\Sigma = f_{ijk} \qquad 0 = \sum f_{ijk} ((\alpha_1^\Sigma)^i (\alpha_2^\Sigma)^j (\alpha_3^\Sigma)^k)$

$(\alpha_1^\Sigma : \alpha_2^\Sigma : \alpha_3^\Sigma) \in C$

$P=(\alpha_1;\alpha_2;\alpha_3)$ nějaký K-rac. bod

$\mathbb{F}_5$-rac. bod

Frob. aut. k čemu užitečný

Vždyť $\mathbb{F}_5$-rac body jsou při aplikaci φ pevné.

MUSÍME OPUSTIT K-RAC BODY

ABYCHOM SPOČÍTALI KOLIK K-RAC

BUDEME PRACOVAT S BODY, KTERÉ K-RAC NEJSOU

Přesvědčíme se, že pro φ Frob. end. platí

$$\varphi(\alpha \oplus \beta) = \varphi(\alpha) \oplus \varphi(\beta)$$

je endomorfismem grupy $(E(\mathbb{F}_{q}), \oplus)$

(a tedy $(E(\overline{\mathbb{F}_q}), \oplus)$)

$$\gamma_1 = \lambda^2 - \alpha_1 - \beta_1$$

$$\gamma_2 = \lambda(\alpha_1 - \gamma_1) - \alpha_2$$

$$\lambda = \frac{\alpha_2 - \beta_2}{\alpha_1 - \beta_1} \qquad \lambda = \frac{3\alpha_1^2 + a}{2\alpha_2}$$

$$\lambda^q = \frac{\alpha_2^q - \beta_2^q}{\alpha_1^q - \beta_1^q} \text{ nebo } \frac{3(\alpha_1^q)^2 + a}{2\alpha_2^q}$$

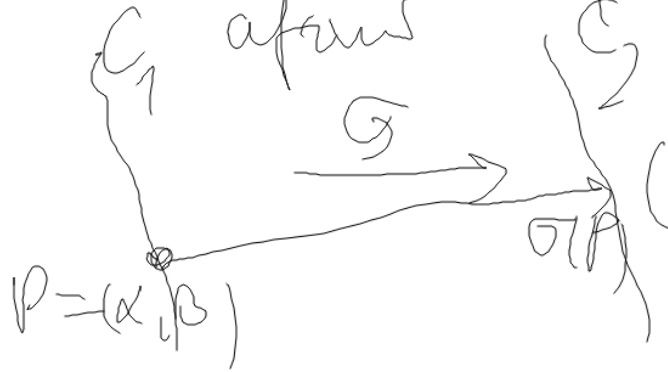
$$\gamma_1^q = \lambda^q - \alpha_1^q - \beta_1^q \qquad \gamma_2^q = \ldots$$

$$(\gamma_1^q, \gamma_2^q) = (\alpha_1^q, \alpha_2^q) \oplus (\beta_1^q, \beta_2^q)$$

φ je příklad
mnohem obecnějšího pojmu, a to <u>izogenie</u>

rac. zobraz. → projektivní verse (rational map)

σ rep. (s_1, s_2) $\quad s_i \in K(x_1, x_2)$



$(s_1(\alpha,\beta), s_2(\alpha,\beta))$

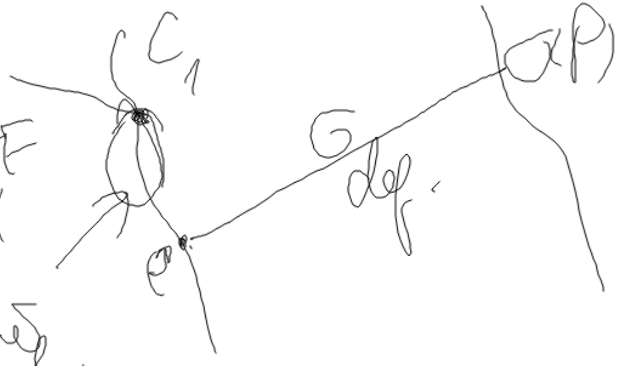
NĚKDY $s_1(P)$
NEBO $s_2(P)$
nemusí být def.

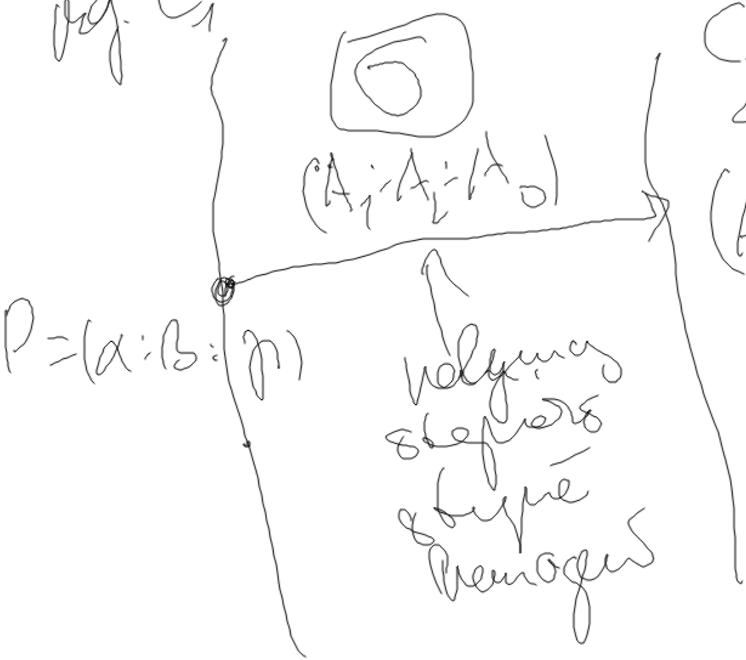
Pak ale může
σ mít jiného rep.
KVŮLI (r_1, r_2), že
$r(P)$ je def.

na C_1 se může $da_1 - b_1c_1$

$r_1 = \frac{a_1}{b_1}$ $\quad s_1 = \frac{c_1}{d_1}$

NEDEF
BODY
⇒
konečná
množina





$(B_1:B_2:B_0)$

$(A_1(\alpha):A_2(\alpha):A_3(\alpha))$

$A_iB_j - A_jB_i$ se anuluje na C_1

Ale pokud $A_i(\alpha)=0$ $\forall i$ tak nemůže tvořit definici $\sigma(P)$

Pokud $\gcd(B_1,B_2)=D$

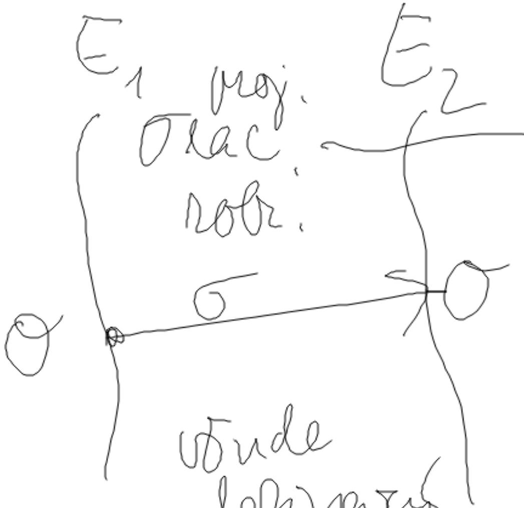
$\left(A_1\frac{B_2}{D} : A_2\frac{B_1}{D} : \frac{B_1B_2}{D}\right)$

Je-li C_1 hladká, lze rac. proj. zobr. $C_1 \to C_2$ definovat v každém bodě P

afinně $\left(\frac{a_1}{b_1}, \frac{a_2}{b_2}\right)$ $\quad \frac{a_1}{b_1} \to \frac{A_1}{B_1}$ $\quad \frac{a_2}{b_2} \to \frac{A_2}{B_2}$ $\quad \left(\frac{a_1}{a_2}, \frac{b_1}{b_2}\right) \to (A_1B_2 : A_2B_1 : B_1B_2)$

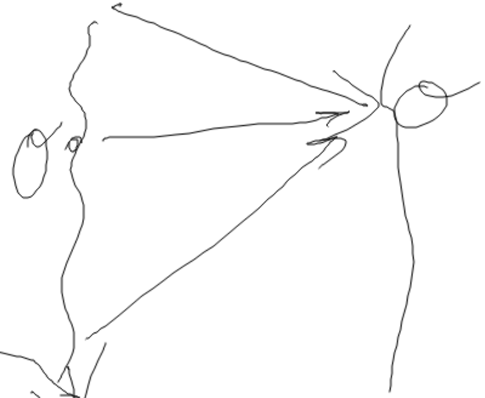
A_1 je hom. a_1, B_1 je hom. b_1, a $\deg(A_1) = \deg(B_1)$ $\quad X_3^2$

[illegible]



σ se nazývá izogenie, pokud $\sigma(O) = O$

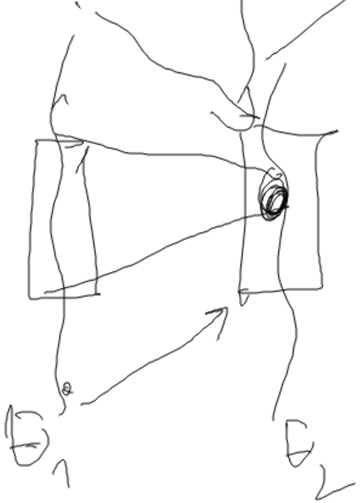
mezi izogeniemi bere ez člent izogenii konstantní triviální nulovou



všude definovaná

Všech ostatní izogenie jsou surjektivní

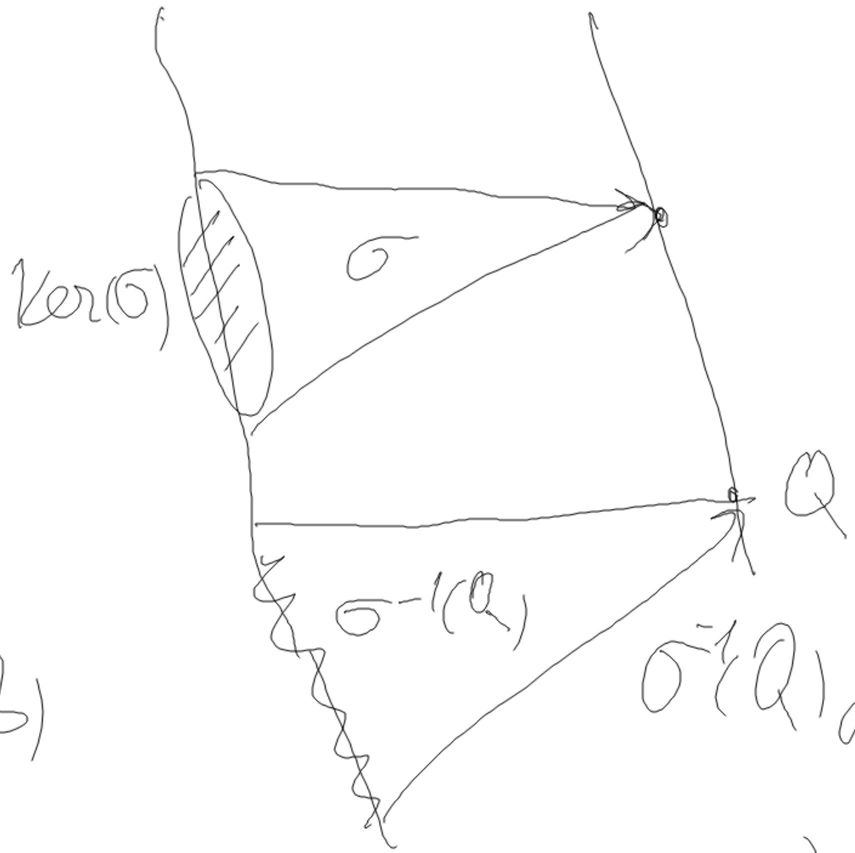
ALE POZOR TO NEZNAMENÁ, ŽE JSOU SURJEKTIVNÍ I NA K-RAC BODECH



ZÁKLADNÍ VLASTNOST ROZENÍ JE, ŽE TO JSOU HOMOMORFISMY GRUP

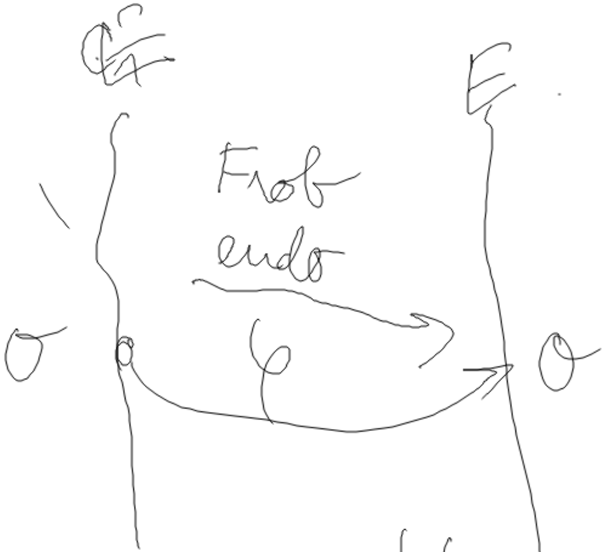
$\sigma(\alpha \oplus \beta) = \sigma(\alpha) \oplus \sigma(\beta)$

SLUČITELNÉ SE SČÍTÁNÍ



$\sigma^{-1}(Q)$ je rozkladová třída modulo Ker(σ)

$|\sigma^{-1}(Q)| = |Ker(\sigma)|$



avyzlows
avyzhws

bijekce

PRESTO NEEXISTUJE
INVERZNÍ IZOGENIE

Polynom $T^2 - tT + q \in \mathbb{F}_q[T]$ se nazývá charakteristický polynom Frob. end.

LIN. ALG.

t stopa Frob. end.

Pro $P \in E(\mathbb{F}_q)$ anulování char. polynom je kvadratické rovnice

$$\varphi^2(P) \ominus [t]\varphi(P) \oplus [q]P = O$$

Pokud $\varphi(P) = P$, tedy

to je totéž jako

$$P \ominus [t]P \oplus [q]P = O$$

$$[1+q-t](P) = O$$

$|E(\mathbb{F}_q)| = q+1-t$

V konečné ab. grupě $n \cdot x = O$, řád grupy

$P \longrightarrow P \oplus P$

$$\frac{R_1(X_1,X_2)}{S_1(X_1,X_2)} = \frac{(3x_1^2+a)^2 - 8x_1x_2^2}{4x_2^2}$$

$$\frac{R_2(X_1,X_2)}{S_2(X_1,X_2)} = \frac{(3x_1^2+a)\left(12x_1x_2^2 - (3x_1^2+a)^2\right) - 8x_2^4}{8x_2^3}$$

Homogenize

$$\frac{R_1(X_1,X_2,X_3)}{S_1(X_1,X_2,X_3)} = \frac{(3X_1^2+aX_3^2)^2 - 8X_1X_2^2X_3}{4X_2^2X_3^2}$$

$$\frac{R_2(X_1,X_2,X_3)}{S_2(X_1,X_2,X_3)} = \frac{(3X_1^2+aX_3^2)(12X_1X_2^2X_3 - (3X_1^2+aX_3^2)^2) - 8X_2^4X_3^2}{8X_2^3X_3^3}$$

$P \mapsto [2]P$ je jeho rozepsání

$(2X_2X_3R_1(X_1,X_2,X_3) : R_2(X_1,X_2,X_3) : 8X_2^3X_3^3)$

Chci ilustrovat, že i když v afinním případě odpovídá rac. zobrazení všude být def. na ... , tak [illegible] na bodech $(\alpha, 0)$, kde α kořen x^3+ax+b, tak jako proj rac. zobr. to možné je

$R_2(\alpha, 0, 1) = R_2(\alpha, 0)$

$= -(3x_1^2+a)^3$

$(\alpha : 0 : 1) \to (0 : -(3x_1^2+a)^3 : 0)$

$= (0 : 1 : 0) = \infty$

$(3x_1^2+a)(12x_1x_2^2 - (3x_1^2+a)^2) - 8x_2^4$

IZOGENIE SE DAJÍ SČÍTAT

$P \xrightarrow{\sigma} \sigma(P)$, $\quad P \xrightarrow{\tau} \tau(P)$

$P \xrightarrow{\sigma \oplus \tau} \sigma(P) \oplus \tau(P)$

Kdykoliv máme

$f: (G,+) \to (H,+)$

$g: (G,+) \to (H,+)$

$f+g: G \to H$

IZOGENIE $E \longrightarrow E$

ENDOMORFISMUS

$\sigma, \tau \in End(E) \longrightarrow$ sčítání $\sigma \oplus \tau \in End(E)$

Endomorfizmy tvoří okruh $End(E)$

$\sigma(\rho \oplus \tau)(P) = \sigma(\rho(P) \oplus \tau(P)) = \sigma\rho(P) \oplus \sigma\tau(P)$

$= (\sigma\rho \oplus \sigma\tau)(P)$

$\left\{ \xrightarrow[\text{reg. zobr.}]{\text{rac.}} \right\}$

id_E je jistě endomorfismus

$id_E \oplus id_E : P \longrightarrow P \oplus P = [2]P$

Iterováním vidíme, že $P \longrightarrow [m]P$ je $\forall m \in \mathbb{Z}$ izogenie

$[m] \oplus [n] = [m+n]$

$m \longmapsto [m]$ je homomorfismus $\mathbb{Z} \longrightarrow End(E)$ okruhů

$\varphi \in End(E)$

Určit počet bodů křivky, tedy najít $|E(\mathbb{F}_q)|$

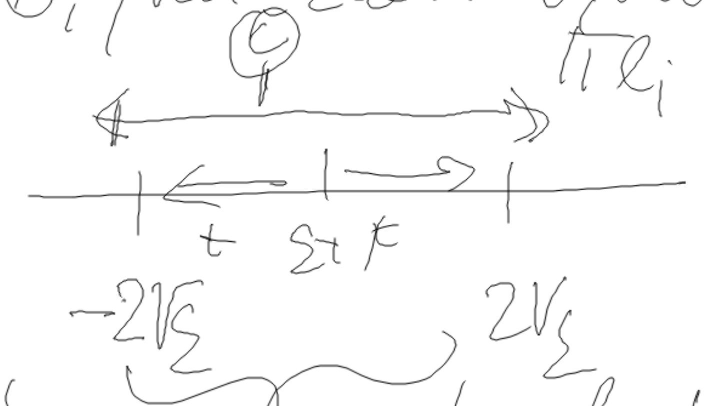
K tomu stačí znát stopu t $\quad = q+1-t \quad |t| < 2\sqrt{q}$

$t \bmod l$

Potřebuji počátečních prvočísel $l_1, \dots, l_r$ takových, že $\prod l_i > 4\sqrt{q}$

Pokud budu znát $t \bmod \prod l_i$, tak zvolím t, nebo $\prod l_i$ c

hledá v intervalu



v tomto intervalu je vyskytuje jediné číslo

c splývá $c \equiv t \bmod \prod l_i$

Podle čínské věty o zbytcích znalost $t \bmod \prod l_i$

STAČÍ ZNÁT $t \bmod l_i$ pro každé $i \in \{1, \dots, r\}$

$q = 101$ $\sqrt{q} \approx 10$ $41 > \sqrt[4]{101}$

$2 \cdot 3 \cdot 5 = 30$ $2 \cdot 3 \cdot 5 \cdot 7 = 210$ $3 \cdot 5 \cdot 7 > 41$

$t_\ell = t$ mod ℓ

$q_\ell \equiv q$ mod ℓ

t_2 — 0 involuce má / 1 involuce ne

$t_2 = 1 \iff \gcd(x^3 + ax - b, x^q - x) = 1$

t_ℓ mono $\mathbb{F}_q$-rac. body

ALE PRO ZJIŠTĚNÍ t_ℓ SE POUŽÍVAJÍ BODY KTERÉ NEJSOU K-RAC.

SOUČASNĚ PLATÍ, ŽE TY BODY, KTERÉ NEJSOU K-RACIONÁLNÍ NIKDY EXPLICITNĚ NEREPREZENTUJEME, VŠECHNA PRÁCE PŘES POLYNOMY NAD $\mathbb{F}_q$

Označme $E[\ell]^*$ všechny prvky $E[\ell]$ různé od $\mathcal{O}$

Každé $\alpha \in E[\ell]^*$ je řádu ℓ $\quad$ ℓ prvočíslo

$|E[\ell]^*| = \ell^2 - 1$ $\quad$ Pokud q prvočíslo, tak velikosti ℓ_i jsou výrazně menší než q $\quad$ $(\sqrt{q})$

$t_\ell \quad q_\ell$

$P \in E[\ell]^* \implies [\ell]P = \mathcal{O}$ a $[q]P = [q_\ell]P$

$[t]P = [t_\ell]P$

Čili $P \in E[\ell]^*$ splňuje

$$\boxed{\varphi^2(P) \oplus [q_\ell]P = [t_\ell]\varphi(P)}$$

TO PLATÍ PRO $\forall P \in E[\ell]^*$

POKUD PRO JEDNO JEDINÉ $P \in E[\ell]^*$

NAJDEME τ celé, že $\varphi^2(P) \oplus [q_\ell]P = [\tau]\varphi(P)$, tak už t_ℓ ZNÁME

STRATEGIE SCHOOFOVA ALGORITMU JE POSTUPNĚ BRÁT $z \in \{0, 1, \ldots, \ell-1\}$ $\frac{\ell-1}{2}$ A PRO KAŽDÉ z TESTOVAT

$\exists P \in E[\ell]^{*}$, že $\varphi(P) \oplus [z_\ell] P = [\pm z] \varphi(P)$

NEMÁME BODY $E[\ell]$ SPOČÍTANÉ

NĚCO VÍME $P = (\alpha, \beta) \in E[\ell] \iff \psi_\ell(\alpha, \beta) = 0$

Hledáme vlastnost, kterou $P \in E[\ell]^{*}$ musí mít, pokud

IDEA

UKAZUJE SE, ŽE $\exists$ polynom $h_x = h_{x,z}$, že x-ová souřadnice P se shoduje s $[z]P \iff h_x(\alpha) = 0$