EDWARDSOVA KŘIVKA $\quad x^2+y^2=1+dx^2y^2 \quad d\in\{0,1\}$

ZOBECNĚNÉ (TWISTED) $\quad ax^2+y^2=1+dx^2y^2 \quad a,d\in K^*$

$a\neq d$

$a=\delta^2 \quad (\delta x)^2+y^2=1+\frac{d}{a}(\delta x)^2y^2$

Pokud a je čtverec, ale a i d jsou „malé“ (do velikosti slova)

tak z výpočetních důvodů

může mít smysl pracovat s $a\neq 1$

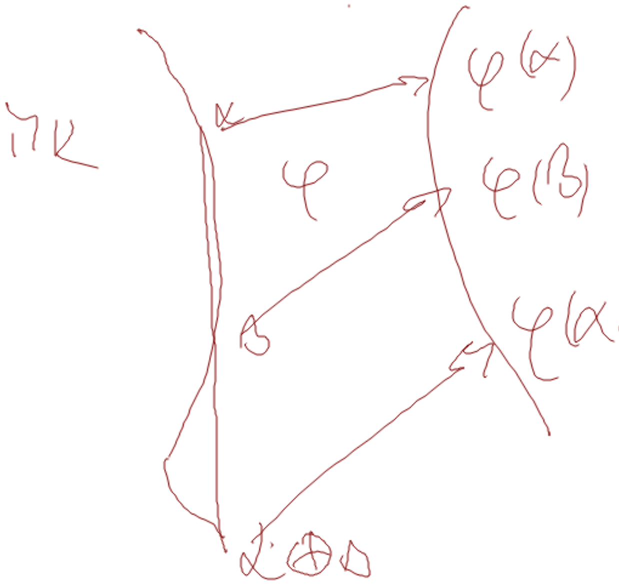
(d/a) může být „velké“

ZEK birac. ekv. MK

afd

$A \neq I_2$

EK



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

NENÍ ÚPLNĚ ZŘEJMÉ ANI Z TOHOTO VZTAHU, JAK PROVÁDĚT SČÍTÁNÍ BODŮ V NEKONEČNU

ZEK má 2 body v nekonečnu

↓

definované na místech stupně 1

K-racionální singularity

každý K-rac. bod

↕

místo stupně 1

singulární bod

- 1 místo stupně 2 ← NEVSTUPUJÍ DO GRUPY (v reálném případě odpovídá izolovaným bodům)
- 2 místa stupně 1

(0:1:0)

(1:0:0)

Pokud d není čtverec | Pak oba singulární body
ad^{-1} — 1 — | dávají místa stupně 2

PAK JE CELÁ GRUPA KŘIVKY REALIZOVANÁ NA AFINNÍCH

$$(\alpha_1,\alpha_2)\oplus(\beta_1,\beta_2)=\left(\frac{\alpha_1\beta_2+\alpha_2\beta_1}{1+d\alpha_1\alpha_2\beta_1\beta_2},\ \frac{\alpha_2\beta_2-a\alpha_1\beta_1}{1-d\alpha_1\alpha_2\beta_1\beta_2}\right)$$

NEUTRÁLNÍ PRVEK JE $(0,1)$

$$\ominus(\alpha_1,\alpha_2)=(-\alpha_1,\alpha_2)$$

$$\alpha_1\alpha_2+(-\alpha_1)\alpha_2=0 \qquad \alpha_2^2-a\alpha_1(-\alpha_1)=1-d\alpha_1\alpha_2(-\alpha_1)\alpha_2$$

Z HLEDISK ECC MÁ SMYSL $\{d, ad\}$ nejsou čtverce

PRO FAKTORIZACI ZEK SLOUŽÍ LÉPE NEŽ WK

ZDÁ SE, ŽE EK + ZEK JSOU VÝKONĚJŠÍ

ALE JE TO SLOŽITĚJŠÍ NEŽ TO VYPADÁ

4 dělí $|E(K)|$
↳ ZEK

$2 \nmid_2$

$\boxed{g+1}$

možná něco

11

VŠECHNY ELIPT. KŘIVKY NAD $\mathbb{F}_2$ → každá realizovaná WK

$23 \nmid 2$

$\exists\, |E(K)| \leftarrow (a,b) \in \mathbb{F}_2 \times \mathbb{F}_2 \quad 4a^3+27b^2 \neq 0$

$$(\alpha_1,\alpha_2)\oplus(\beta_1,\beta_2)=\left(\frac{\alpha_1\alpha_2+\beta_1\beta_2}{\alpha_2\beta_2+a\alpha_1\beta_1},\frac{\alpha_1\alpha_2-\beta_1\beta_2}{\alpha_1\beta_2-\alpha_2\beta_1}\right)$$

duality NEFUNGUJE $\alpha=\beta$

POKUD SE DAJÍ POUŽÍT OBA, DÁVAJÍ STEJNÝ VÝSLEDEK

$$\left(\frac{\alpha_1\beta_2+\alpha_2\beta_1}{1+d\alpha_1\alpha_2\beta_1\beta_2},\frac{\alpha_2\beta_2-a\alpha_1\beta_1}{1-d\alpha_1\alpha_2\beta_1\beta_2}\right)$$

VŽDY $(\alpha_1\alpha_2+\beta_1\beta_2)(1+d\alpha_1\alpha_2\beta_1\beta_2)=(\alpha_1\beta_2+\alpha_2\beta_1)(\alpha_2\beta_2+a\alpha_1\beta_1)$

STEJNĚ 2. souřadnice

POKUD REZIGNUJI NA VÝHODY ODOLNOSTI PROTI POSTR. KAN. LZE DUÁLNÍ VZOREC POUŽÍT PRO URYCHLENÍ

V projektivních souřadnicích

$$ax^2z^2 + y^2z^2 = z^4 + dx^2y^2$$

NÁŠ $10M + 1S + 1 \cdot a + 1 \cdot d$

↑ NÁSOBENÍ PRVKEM a

POČETNÍ $3M + 4S + 1a$

INVERTOVANÉ SOUŘADNICE

(α, β) ODPOVÍDÁ $(\alpha^{-1}, \beta^{-1})$

TZN., ŽE PRACUJI S ŘEŠENÍM ROVNICE

$$ax^{-2}z^{-2} + y^{-2}z^{-2} = z^{-4} + dx^{-2}y^{-2} \quad / \cdot z^4x^2y^2$$

$$ay^2z^2 + x^2z^2 = x^2y^2 + dz^4$$

násobení $9M + 1S + 1a + 1d$

mocnění $3M + 4S + 1a + 1d$

ROZŠÍŘENÉ SOUŘADNICE

$\mathbb{P}^2$

sféra se ztotožněnými protilehlými body

$\mathbb{P}^1 \times \mathbb{P}^1$

$\mathbb{P}^1$ kružnice

ŘEZ ANULOIDEM (TORUS)

2. EDW. KŘIVKA SE REALIZUJE NA $\mathbb{P}^1 \times \mathbb{P}^1$

$$((\alpha_1:\alpha_2),(\beta_1:\beta_2)) = ((\gamma_1:\gamma_2),(\delta_1:\delta_2))$$

$$\iff \mu,\nu \in K^*, \text{ že } \gamma_i = \mu\alpha_i,\ \delta_i = \nu\beta_i$$

AFINNÍ

$$(\alpha,\beta) \longmapsto ((\alpha:1),(\beta:1))$$

$$a x_1^2 + x_2^2 = 1 + d x_1^2 x_2^2 \longrightarrow a \frac{x_1^2}{y_1^2} + \frac{x_2^2}{y_2^2} = 1 + d \frac{x_1^2 x_2^2}{y_1^2 y_2^2}$$

$$a x_1^2 y_2^2 + y_1^2 x_2^2 = y_1^2 y_2^2 + d x_1^2 x_2^2$$

$y_2 = 0$ $\quad y_1^2 x_2^2 = d x_1^2 x_2^2$ $\quad y_2 = 0 \Rightarrow x_2 \neq 0$

$d = s^2$

SINGULARITA $\quad y_1^2 = d x_1^2 \quad$ BODY V NEKONEČNU

V PROJ. BODECH $\quad ((1:s),(1:0)) \quad ((1:-s),(1:0))$

SE ROZPADNE NA 2 BODY $\quad x_1 \; y_1$

$y_1 = 0$ $\quad a x_1^2 y_2^2 = d x_1^2 x_2^2 \longrightarrow a y_2^2 = d x_2^2 \quad a/d = t^2$

2 body $\quad ((1:0),(t:1)) \quad ((1:0),(-t:1))$

Jak vypadat $((\alpha_1;\alpha_2),(\beta_1,\beta_2)) \oplus ((\gamma_1;\gamma_2),(\delta_1,\delta_2))$

Zdroje $((\mu_1;\mu_2),(\nu_1;\nu_2))$ $((\mu_1';\mu_2'),(\nu_1';\nu_2'))$

$(\mu_1,\mu_2)=0$
NEBO
$(\nu_1,\nu_2)=0$
$\Longrightarrow$
$(\mu_1',\mu_2')\neq(0,0)$
$(\nu_1',\nu_2')\neq(0,0)$

ALESPOŇ JEDEN PŘÍPAD DÁVÁ KOREKTNÍ VÝSLEDEK

$(\mu_1',\mu_2')=0$
NEBO
$(\nu_1',\nu_2')=0$
$\Longrightarrow$
$(\mu_1,\mu_2)\neq(0,0)$
$(\nu_1,\nu_2)\neq(0,0)$

POKUD OBA, JSOU SHODNÉ

$$\mu_1 = \alpha_1\beta_2\gamma_2\delta_1 + \alpha_2\beta_1\gamma_1\delta_2 \qquad \mu_1' = \alpha_1\beta_1\gamma_2\delta_2 + \alpha_2\beta_2\gamma_1\delta_2$$

$$\mu_2 = \alpha_2\beta_2\gamma_2\delta_2 + d\alpha_1\beta_1\gamma_1\delta_1 \qquad \mu_2' = a\alpha_1\beta_2\gamma_1\delta_2 + \alpha_2\beta_1\gamma_2\delta_1$$

$$\nu_1 = \alpha_2\beta_1\gamma_2\delta_1 - a d_1\alpha_2\gamma_1\delta_2 \qquad \nu_1'$$

$$\nu_2 \qquad \nu_2' = \alpha_1\beta_2\gamma_2\delta_1 - \alpha_2\beta_1\gamma_1\delta_2$$

(σ_1, σ_2) (τ_1, τ_2) afurdbock $((\sigma_1 : 1), (\sigma_2 : 1))$ $((\tau_1 : 1), (\tau_2 : 1))$

$$\mu_1 = \frac{\sigma_1\tau_2 + \sigma_2\tau_1}{1 + d\sigma_1\sigma_2\tau_1\tau_2} \qquad \nu_1 = \frac{\sigma_2\tau_2 - a\sigma_1\sigma_2}{1 - d\sigma_1\sigma_2\tau_1\tau_2}$$

$\mu_2 =$ $\qquad \nu_2$

$((1:s),(1:0)) \oplus ((1:-s)),(1:0))$ (μ, ν) $((0:d),(-d:d)) = ((0:1),(1:1))$

$\cancel{((0:-d),(0,0))}$

STRUKTURA GRUPY A PŘÍKLADY NAD 5 PRVKY

E eliptická křivka nad $\mathbb{F}_q$

HASSEHO VĚTA

$$\left| q+1 - |E(\mathbb{F}_q)| \right| \le 2\sqrt{q}$$

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

r počet K-rac WR $\quad t = q - r$

$|t| \le 2\sqrt{q}$

$t > 0$ málo bodů

$t < 0$ hodně bodů

$K \subseteq L \subseteq \overline{K}$ $\qquad E(K) \le E(L) \le E(\overline{K})$

MNOHO FAKT O ELIPTICKÝCH KŘIVKÁCH SE DOKAZUJE PRO

$$E[m] = \{\alpha \in E;\ [m]\alpha = O\}$$

$P \in E;$

neutrální prvek

$$E[m](K) \le E[m]$$

$$= \{\alpha \in E(K);\ [m]\alpha = O\}$$

$[m](\alpha \oplus \beta) = [m]\alpha \oplus [m]\beta$

$[m](\ominus\alpha) = \ominus [m]\alpha$

$E[m]$ je podgrupa $\overline{E}(K)$

$[m](\alpha) = O$

$[m](\beta) = O$

$[m](\alpha \oplus \beta) = O$

A

konečná abelovská grupa

netriviálna konečná abelovská p-grupa

$$A \cong \bigoplus_{p \text{ prvočísla}} A_p$$

A_p p-primárna komponenta

$\|$

všetky prvky rádu p^r pre nejaké $r \geq 0$

p-grupy

$$\mathbb{Z}_p^{k_1} \times \dots \times \mathbb{Z}_p^{k_r}$$

$$k_1 \geq k_2 \geq \dots \geq k_r \geq 1$$

$$A \cong \mathbb{Z}_{d_1} \times \dots \times \mathbb{Z}_{d_r}$$

$$d_i \mid d_{i+1}$$

STRUKTURA $E[m]$

Ať $p = \mathrm{char}(K)$

$p \nmid m \Longrightarrow E[m] \cong \mathbb{Z}_m \times \mathbb{Z}_m$

$m = p^k,\ k \geq 1 \Longrightarrow E[m] \cong \mathbb{Z}_m$

$\cong 0$ ($\Longleftrightarrow E(K)$ neobsahuje žádný prvek řádu p)

$E[m_1 m_2] \cong E[m_1] \times E[m_2]$ pokud $\gcd(m_1, m_2) = 1$

Čvz

Pokud $m = n \cdot p^k$ $\quad E[m] \cong \mathbb{Z}_n \times \mathbb{Z}_n \times \begin{cases} \mathbb{Z}_{p^k} \\ 0 \end{cases}$

Každá konečná podgrupa $E(K)$ padne do nějaké $E[n]$ (lze např. položit $n = |H|$)

Ať $H \leq E(K)$ konečná

Podgrupy $\mathbb{Z}_n \times \mathbb{Z}_n$ tvaru $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$ $\quad n_1 \mid n_2$

Každá konečná grupa $E(K)$ je $\cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$ $\quad n_1 \mid n_2$

Eliptická křivka tvoří anuloidu

$E[n]$ a tedy může odpovídat podle vzoru anuloidu

$\cong$

$\mathbb{Z}_n \times \mathbb{Z}_n$

$n = 5$

Z hlediska ECC nás zajímají velká prvočísla l

že l dělí řád grupy

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

l dost velké atd. znamená

$l > 4\sqrt{q}$

l dělí číslo v rozmezí

$\langle q+1-2\sqrt{q},\ q+1+2\sqrt{q} \rangle$

Interval má délku max. $4\sqrt{q}$, leží v něm

jediný násobek prvočísla l!

#BodioWK

Je snadné si uvědomit

že hodnoty l se

shodují (téměř)

se znalostí $|E(\mathbb{F}_q)|$

c cofactor

l factor

$|E(\mathbb{F}_q)| = cl$

Křivky Weier. nad F_q
q prvočíslo
$q \neq 2,3$

Tohle se využívá ve faktorizaci Lenstrovou metodou

Náhodná volba parametrů
a,b $\quad y^2 = x^3 + ax + b$

každá volba dává ~~délku~~ počet bodů na křivce

Praxe ukazuje, že délky nejsou v žádné algoritmicky efektivně vyjádřitelné závislosti na (a,b)
(s výjimkou některých křivek)