Montgomeryho křivky ~ WK minimalizace

malé omezení substituce → vliv na výpočetní efektivitě

MK je křivka daná rovnicí

$$By^2 = x^3 + Ax^2 + x, \quad \mathrm{char}(K) \neq 2$$

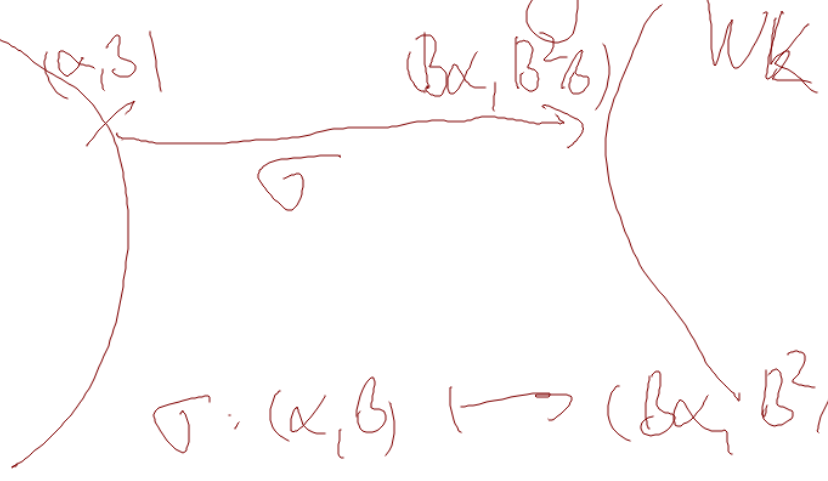
$$A \in K \quad B \in K^*$$

Píšeme velké A a B jen proto aby a, b v $y^2 = x^3 + ax + b$ nedošlo k záměně s

$$B y^2 = x^3 + Ax^2 + x \cdot 1 \cdot B^3$$

$$(B^2 y)^2 = (Bx)^3 + AB \cdot (Bx)^2 + B^2 (Bx)$$

2 MK dostanu WK $\quad y^2 = x^3 + AB x^2 + B^2 x$ WK



$\sigma : (\alpha, \beta) \longmapsto (B\alpha, B^2\beta)$ je bijekce $MK \longrightarrow WK$

$By^2 = x^3 + Ax^2 + x \longrightarrow y^2 = x^3 + ABx^2 + B^2x$

Když hladká $\Longleftrightarrow$ tato hladká

hladká $\Longleftrightarrow$

Polynom $x^3 + ABx^2 + B^2x = x(x^2 + ABx + B^2)$

nemá vícenásobné kořeny

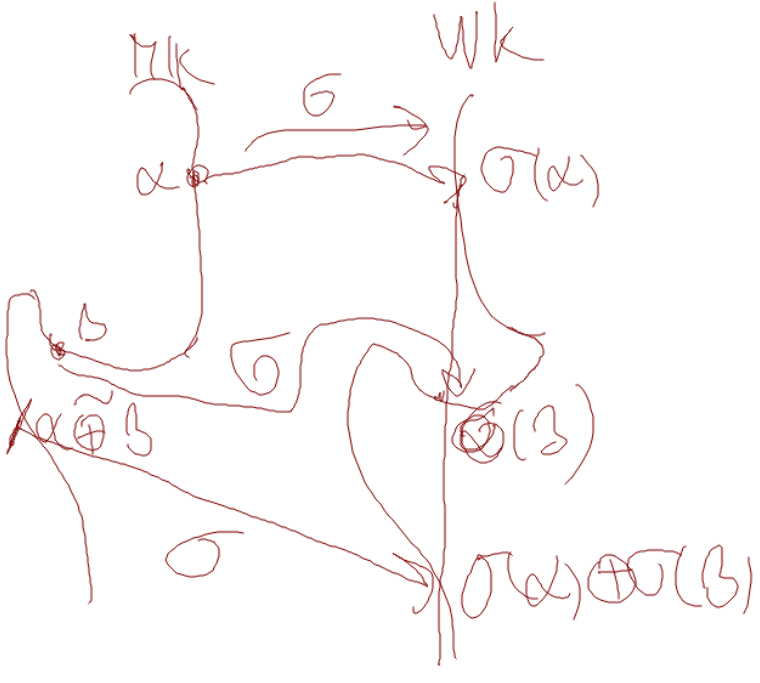
$B \neq 0$. Proto 0 není vícenásobný

$(AB)^2 - 4B^2 \neq 0$

$\Updownarrow$

$A^2 - 4 \neq 0 \Longleftrightarrow A \neq \pm 2$

Dále budeme předpokládat $A \neq \pm 2$



$$\alpha \widehat{\oplus} \beta = \sigma^{-1}(\sigma(\alpha) \oplus \sigma(\beta))$$

$$\widetilde{\ominus}\alpha = \sigma^{-1}(\ominus\sigma(\alpha))$$

$$\widetilde{\ominus}\alpha = \sigma^{-1}(\ominus(B\alpha_1, B^2\alpha_2))$$

$$= \sigma^{-1}(B\alpha_1, -B^2\alpha_2)$$

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

$\alpha = (\alpha_1, \alpha_2)$

$$\widetilde{\ominus}(\alpha_1, \alpha_2) = (\alpha_1, -\alpha_2)$$

$\widetilde{\ominus}$ produit point $\ominus$

$\alpha = (\alpha_1, \alpha_2) \quad B = (B_1, B_2)$

$\eta = (\eta_1, \eta_2) = (B\alpha_1, B^2\alpha_2) \oplus (BB_1, B^2 B_2)$

$a_2 = AB \quad a_1 = B^2 \quad a_0 = 0$

$(\eta_1, \eta_2) = \alpha \tilde{\oplus} B = (B^1\eta_1, B^2\eta_2)$

$(\eta_1, \eta_2) = (-B\alpha_1 - BB_1 + \lambda^2 - AB, \lambda(B\alpha_1 - \xi_1) - B^2\alpha_2)$

λ unsolvable. Predpostavljamo $\alpha \neq \ominus B$

$\alpha \neq B$

$\lambda = \dfrac{B^2 B_1 - B^2\alpha_1}{BB_1 - B\alpha_1} = B\dfrac{B_1 - \alpha_1}{B_1 - \alpha_1}$

$\tilde{\lambda}$

$\alpha = B$

$\lambda = \dfrac{3(B\alpha_1)^2 + 2AB(B\alpha_1) + B^2}{2B^2\alpha_2} = \dfrac{3\alpha_1^2 + 2A\alpha_1 + 1}{2\alpha_2}$

$\tilde{\lambda} = \lambda / B$

$\lambda = \tilde{\lambda} B$

$$\alpha \tilde{\oplus} \beta = (-\alpha_1 - \beta_1 + B\lambda^2 - A,\ \lambda(\alpha_1 - \gamma_1) - \alpha_2)$$

$$\lambda = \frac{\beta_2 - \alpha_2}{\beta_1 - \alpha_1} \quad \text{nebo} \quad \frac{3\alpha_1^2 + 2A\alpha_1 + 1}{2\alpha_2 B}$$

$$\alpha \tilde{\ominus} \beta = (-\alpha_1 - \beta_1 + (\tilde{\lambda})^2 - A,\ \tilde{\lambda}(\alpha_1 - \gamma_1) - \alpha_2) - \beta_2$$

$$\tilde{\lambda} = \frac{\alpha_2 + \beta_2}{\alpha_1 - \beta_1}$$

$\alpha_1 \neq \beta_1$

$\alpha \tilde{\oplus} (\ominus \beta)$

$M: By^2 = x^3 + Ax^2 + x$

TVRZENÍ M7 Ať $\alpha = (\alpha_1, \alpha_2)$, $\beta = (\beta_1, \beta_2) \in M$

$\gamma = \alpha \oplus \beta = (\gamma_1, \gamma_2)$ $\quad \delta = \alpha \ominus \beta = (\delta_1, \delta_2)$ Pak:

$$\gamma_1 \delta_1 (\alpha_1 - \beta_1)^2 = (\alpha_1 \beta_1 - 1)^2$$

D: $B\alpha_2^2 = \alpha_1^3 + A\alpha_1^2 + \alpha_1$ $\quad B\beta_2^2 = \beta_1^3 + A\beta_1^2 + \beta_1$

$\lambda = \frac{\beta_2 - \alpha_2}{\beta_1 - \alpha_1}$

$\lambda^2 = \frac{(\beta_2 - \alpha_2)^2}{(\beta_1 - \alpha_1)^2}$

$\gamma_1 (\alpha_1 - \beta_1)^2 = B(\alpha_2 - \beta_2)^2 - (\alpha_1 - \beta_1)^2 (\alpha_1 + \beta_1 + A)$

$= -2B\alpha_2\beta_2 + (\alpha_1^3 + A\alpha_1^2 + \alpha_1) + (\beta_1^3 + A\beta_1^2 + \beta_1)$

$-\alpha_1^3 - \beta_1^3 + \alpha_2^2 \beta_1 + \alpha_1 \beta_1^2 - A\alpha_1^2 - A\beta_1^2 + 2A\alpha_1\beta_1$ $\quad \gamma_1 = -\alpha_1 - \beta_1 + B\lambda^2 - A$

$= -2B\alpha_2\beta_2 + \alpha_1 + \beta_1 + \alpha_2^2 \beta_1 + \alpha_1 \beta_1^2 + 2A\alpha_1\beta_1$

$= -2B\alpha_2\beta_2 + \alpha_1\beta_1(\alpha_1 + \beta_1 + 2A) + (\alpha_1 + \beta_1)$

$$\gamma_1(\alpha_1-\beta_1)^2 = -2B\alpha_2\beta_2 + \alpha_1\beta_1(\alpha_1+\beta_1+2A) + (\alpha_1+\beta_1)$$

$$\gamma_1(\alpha_1-\beta_1)^2\alpha_1\beta_1 = -2B\alpha_1\alpha_2\beta_1\beta_2 + \beta_1^2(\alpha_1^3+\alpha_1^2+\alpha_1) + \alpha_1^2(\beta_1^3+A\beta_1+\beta_1)$$

$B\alpha_1^2$

$$= -2B\alpha_1\beta_1\alpha_2\beta_2 + B\beta_1^2\alpha_2^2 + B\alpha_1^2\beta_2^2 = B(\beta_1\alpha_2-\beta_2\alpha_1)^2$$

(δ_1,δ_2) nas stejné chovaps jako (γ_1,γ_2), ale místo β_2 je lepší použít $-\beta_2$

$$\delta_1(\alpha_1-\beta_1)^2\alpha_1\beta_1 = B(\beta_1\alpha_2+\beta_2\alpha_1)^2$$

$$\gamma_1\delta_1(\alpha_1-\beta_1)^4\alpha_1^2\beta_1^2 = B^2(\beta_1^2\alpha_2^2-\beta_2^2\alpha_1^2)^2$$

$$B(\beta_1^2\alpha_2^2-\beta_2^2\alpha_1^2)$$

UPRAVIT TAK, ABY
ZBYZELO $\alpha_1\beta_2$

POSHOD: $\alpha + \alpha^2\beta^2$

$$B(\beta_1^2\alpha_2^2 - \beta_2^2\alpha_1^2) = \beta_1^2(\alpha_1^3 + A\alpha_1^2 + \alpha_1) - \alpha_1^2(\beta_1^3 + A\beta_1^2 + \beta_1)$$

$$= (\alpha_1\beta_1)^2(\alpha_1 - \beta_1) + \alpha_1\beta_1(\beta_1 - \alpha_1) = (\alpha_1 - \beta_1)\alpha_1\beta_1(\alpha_1\beta_1 - 1)$$

$$\gamma_1\delta_1(\alpha_1 - \beta_1)^4\alpha_1^2\beta_1^2 = (\alpha_1 - \beta_1)^2\alpha_1^2\beta_1^2(\alpha_1\beta_1 - 1)^2$$

$$\gamma_1\delta_1(\alpha_1 - \beta_1)^2\alpha_1^2\beta_1^2 = (\alpha_1\beta_1 - 1)^2 \cdot \alpha_1^2\beta_1^2 \qquad (\alpha_1 \neq \beta_1)$$

POZOR JE TŘEBA OVĚŘIT ZDALI PŘÍPAD $\alpha_1 = 0$, $\beta_1 = 0$

$By^2 = x^3 + Ax^2 + x$ $\boxed{(0,0)}$

PLATÍ I PRO $\alpha = (0,0)$ NEBO PŘÍPAD $\beta = (0,0)$

Co je to Montgomeryho žebřík

Počítám $[n]P$ tak, že postupně od čísla n jdu

první souřadnice $[n_1]P$, $[n_2]P$, $[n_3]P$

kde společně udržuji první souřadnici $[n_i]P$ kde $n_i' = n_i + 1$

Čili znám vždy $[n_i]P \ominus [n_i']P = P = (\delta_1, \delta_2)$

$[n_i]P \quad [n_i']P \to \gamma_1 \to \delta_1$

Zbývá: Jak určit posloupnost $n_1, n_2, \ldots$

Jak ze znalosti $[n]P$ první souřadnice určit i

Lze tak učinit ze znalosti $[n]P$ a $[n+1]P$ prvních souřadnic | Ukážeme teď odvodit α_2 pomocí znalosti duhou $\alpha \oplus \beta = \gamma$

$\gamma_1 \quad (\gamma_1, \gamma_2) = [n+1]P$

$\beta \quad = (\beta_1, \beta_2) = P$

$\alpha_1 \quad (\alpha_1, \alpha_2) = [n]P$

lemat 12

$$\alpha_2' = \frac{\alpha_1\beta_1(\alpha_1+\beta_1+2A)+\alpha_1+\beta_1-\beta_1(\alpha_1-\beta_1)^2}{2B\beta_2}$$

Tuto platí na základě pravého vztahu odvozeného
v předchozím důkaze

$$\beta_1(\alpha_1-\beta_1)^2 = -2B\alpha_2\beta_2+\alpha_1\beta_1(\alpha_1+\beta_1+2A)+\alpha_1+\beta_1$$

Pokračuj $(n_i, n'_i = n_{i+1})$ se určuje tak, že

$(n_{i+1}, n'_{i+1}) = \begin{cases} (2n_i, n_i + n'_i) \\ (n_i + n'_i, 2n'_i) \end{cases}$

Který vybrat?
Jednoduše je jít pozadu. Začnu od
$(n_k, n'_k) = (n, n+1)$ a určuji $n_{k-1}, n_{k-2}, \ldots$

Je-li n_{i+1} sudé $\rightarrow n_i = n_{i+1}/2$
n_{i+1} liché $\rightarrow n'_i = n'_i/2$

Пусть $[n_i]P = (x_i, y_i)$ $\quad [n_i']P = (x_i', y_i')$

Тогда $(n_{i+1}, n'_{i+1}) = (2n_i, n_i + n_i')$, где

$$x_{i+1} = \frac{(x_i^2 - 1)^2}{4(x_i^3 + Ax_i^2 + x_i)} \qquad x'_{i+1} = \frac{(x_i x_i' - 1)^2}{x_1 (x_i' - x_i)^2}$$

$\beta_1 \quad \delta_1 \quad \alpha_1 \quad \beta_1$

Пусть $(n_{i+1}, n'_{i+1}) = (n_i + n_i', 2n_i')$

$$x_{i+1} = \frac{(x_i x_i' - 1)}{x_1 (x_i' - x_i)^2} \qquad x'_{i+1} = \frac{(x_i' - 1)^2}{4(x_i'^3 + Ax_i'^2 + x_i')}$$

$$y_k = \frac{x_1 x_k (x_1 + x_k + 2A) + x_1 + x_k - x_k' (x_k - x_1)^2}{2By_1}$$

JAK 2 WK ODĚLAT MK?

$By^2 = x^3 + Ax^2 + x$ je K-ekv. tvaru

$y^2 = x^3 + ABx^2 + B^2x$

Je li WK tvaru $y^2 = x^3 + a_2x^2 + a_4x$, pak

transformace WK → MK nemá problém

Podmínka je, aby a_4 byl čtverec

Pokud $a_4 = B^2$, pak stačí položit $A = a_2/B$

Jak převést $y^2 = x^3 + ax + b$ na tvar

$y^2 = x^3 + a_2 x^2 + a_4 x$, kde a_4 je čtverec?

A kdy to jde?

Nabízí se standardní postup:

Začít od hledaného rovnice $y^2 = x^3 + ABx^2 + B^2 x$ a převést ho na krátký W. tvar substitucí členem vyjádření $y^2 = (x + \frac{AB}{3})^3 + \dots$

Vznikne rovnice $y^2 = x^3 + B^2\left(1 - \frac{A^2}{3}\right)x - \frac{AB^3}{3} + \frac{2(AB)^3}{27}$

Vzniká otázka, při které $a = B^2\left(1 - \frac{A^2}{3}\right)$ $b = \frac{AB^3}{3}\left(-1 + \frac{2A^2}{9}\right)$

aby z (a, b) odvodila (A, B)

Kdyby $y^2 = f(x)$ a $f = x^3 + AB x^2 + B^2 x$

tak $\exists$ kořen ξ polynomu f, že

$f'(\xi)$ je čtverec.

To jistě stačí pokud $\xi = 0$

Proč? Mám f dané vlastnosti:

Vše z toho odvodit

Ať $y^2 = f(x)$, $f'(\xi)$ čtverec $f(\xi) = 0$ PK

Položme $\tilde{f}(x) = f(x + \xi)$ Pak $\tilde{f}(0) = f(\xi) = 0$

$\tilde{f}(x) = x^3 + \tilde{a}_2 x^2 + \tilde{a}_1 x$ $\tilde{f}'(0) = f'(\xi) = B^2$ dle

$\tilde{f}(0) = \tilde{a}_1 = B^2$ Tedíž $\tilde{f}$ tvaru $x^3 + AB x^2 + B^2 x$ vyřeší

$\tilde{f}$ nemá absolutní čtv.

Tvrzení: Ať $p \equiv 1 \bmod 4$, $f \in \mathbb{Z}_p[X]$ monický kubický separabilní rozkládající se nad $\mathbb{Z}_p$. Pokud $f(0) \neq 0$, tak $y^2 = f(X)$ je $\mathbb{Z}_p$-ekvivalentní Kartézského křivce

D: $f = (X-\xi_1)(X-\xi_2)(X-\xi_3)$, kde ξ_i jsou 3 různé kořeny

$$-\prod f'(\xi_i) = \prod (\xi_i - \xi_j)^2$$

-1 čtverec, čtverec

součin 3 čísel nad p dávajících čtverec

$\Rightarrow$ jedno z nich musí být čtverec

$By^2 = x^3 + Ax^2 + x$

$By^2 = (-x)^3 - A(-x)^2 + (-x)$

$\mathbb{K}$ dans (A, B) est équivalente à $\mathbb{K}$ dans $(-A, B)$

$B = \lambda^2 \hat{B}$ ici $\mathbb{K}$ dans (A, B)

est $\mathbb{K}$-équiv.

$\hat{B}(\lambda y)^2 = x^3 + Ax + x$ $\mathbb{K}$ dans $(A, B\lambda^2)$

$\forall \lambda \in \mathbb{K}^*$