$x_2^2 + a_1 x_1 x_2 + a_3 x_2 = x_1^3 + a_2 x_1^2 + a_4 x_1 + a_6$

$x_2^2 + g(x_1) x_2 = f(x_1)$

Zapisovat $(x_1, x_2) = (x_1 : x_2 : 1)$

Bod C hladkej, na K-rac. bodech C tvoří ab. grupu $(C(K), \oplus)$.

C

body projektivního uzavření hladké

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

∞ je neutrální prvek

$\infty \oplus x = x = x \oplus \infty$

POPÍŠEME $\oplus$

$(\alpha_1, \alpha_2) \in C$? kolik $\exists$?, že $(\alpha_1, ?) \in C$

$?^2 + g(\alpha_1)? - f(\alpha_1) = 0$

Jeden kořen dle rovnice zvolme. Jedno α_2

$\alpha_2 + ? = -g(\alpha_1) = -a_1\alpha_1 - a_3$

$? = -\alpha_2 - a_1\alpha_1 - a_3$

Platí $\ominus (\alpha_1, \alpha_2) = (\alpha_1, -\alpha_2 - a_1\alpha_1 - a_3)$

$2\alpha_2 = -a_1\alpha_1 - a_3$

$2\alpha_2 = -g(\alpha_1)$

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

Abz řešení (α_1, α_2) kořeny na kružnici, kde $\mathrm{char}(K) \neq 2$

$\left(\frac{g(\alpha_1)}{2}\right)^2 = f(\alpha_1)$

POKUD $g = 0$ JDE O KOŘENY f

$\mathrm{char}(K) = 2$

1 řešení

$a_1\alpha_1 = a_3$

$\mathrm{Valbar}(K) = 2$ 1 VO INVOLUCÍ

0 řešení ($a_1 = 0$)

MÁ NEJVÝŠE 3 ŘEŠ α_1 NEJVÝŠE 3 PRVKY ŘÁDU 2 (INVOLUCE)

$\beta \neq \ominus\alpha$ Lucene $\alpha \oplus \beta$ Pokud $\beta = \ominus\alpha$, tak $\alpha \oplus \beta = \infty$

$\beta = (\beta_1, \beta_2)$ $\alpha = (\alpha_1, \alpha_2)$

pokud $\beta_1 \neq \alpha_1$ tak i $\beta \neq \alpha$, $\beta \neq \ominus\alpha$

At $\alpha_1 = \beta_1$ Protože $\beta \neq \ominus\alpha$, tak $\beta_2 \neq -\alpha_2 - a_1\alpha_1 - a_3$

Protože $\exists n a$ (jeho 2) $\Rightarrow$ je-li $\alpha_1 = \beta_1$, musí být $\alpha = \beta$. Současně

β od $\wedge$ dokud α_1 α není involuce protože

Pro výpočet $\alpha \oplus \beta$ je třeba pokud $\beta_2 = \alpha_2 = -\alpha_2 - a_1\alpha_1 - a_3$

rozlišit případy

(1) $\alpha_1 \neq \beta_1$

(2) $\alpha = \beta$ a $2\alpha_2 + a_1\alpha_1 + a_3 \neq 0$

Pracuje se s přímkou procházející (1) body α a β

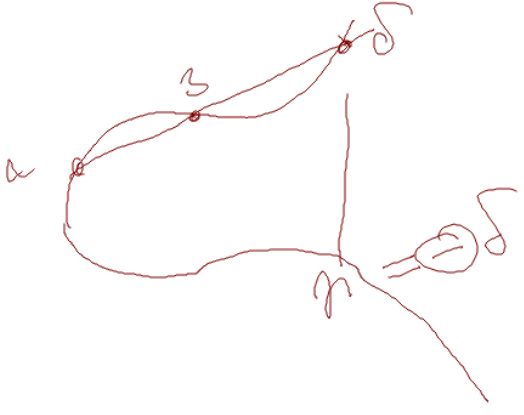
(2) bodem α

Její směrnice $\lambda = \begin{cases} \frac{\beta_2 - \alpha_2}{\beta_1 - \alpha_1} \\ \frac{3\alpha_1^2 + 2a_2\alpha_1 - a_1\alpha_2 + a_4}{2\alpha_2 + a_1\alpha_1 + a_3} \end{cases}$

$\alpha \oplus \beta = \gamma = (\gamma_1, \gamma_2)$

$\gamma_1 = -\alpha_1 - \beta_1 + \lambda^2 + a_1\lambda) - a_2$

$\gamma_2 = \lambda(\alpha_1 - \gamma_1) - \alpha_2 - a_1\gamma_1 - a_3$



$\alpha \oplus \beta \oplus \delta = \infty$

pokud α, β, δ leží na přímce a jdou po 2 různé

Pokud tečna v bodě P protne křivku v bodě Q
tak $[2]P \oplus Q = \infty$ čili $[2]P = \ominus Q$
Pokud tečna nepotne křivku v bodě P, pak $[3]P = \infty$

Na reálných číslech je situace $[3]P = \infty$ nejen
jako inflexní bod

$x_2^2 = x_1^3 + ax_1 + b$ $\quad \ominus(\alpha_1, \alpha_2) = (\alpha_1, -\alpha_2)$

$\alpha \oplus \beta = (\lambda^2 - \alpha_1 - \beta_1,\ \lambda(\alpha_1 - \beta_1) - \alpha_2)$

$\lambda = \frac{\alpha_2 - \beta_2}{\alpha_1 - \beta_1}$ $\quad \lambda = \frac{3x_1^2 + a}{2x_2}$

ZNÁTE-LI CENU VÝPOČTU λ JE CENA

SOUČTU $S + M$ Square $S \sim 8M$

Multiplikační. Inverze

CENA λ PROSTÉ SČÍTÁNÍ $I + M$

ZDVOJENÍ $I + M + S$

CENA SČÍT. $I + 2M + S$

ZDVOJ. $I + 2M + 2S$ ÚSILÍ O ODSTRANĚNÍ I

Projektivní souř.

$[n]P$ mnoho mezivýsledků

V nich můžu pracovat s proj. body $(\alpha_1 : \alpha_2 : \alpha_3)$, kde $\alpha_3 \neq 1$. Teprve na konci, při výstupu z procedury musím normalizovat

$$(\alpha_1, \alpha_2, \alpha_3) \longrightarrow \left(\frac{\alpha_1}{\alpha_3}, \frac{\alpha_2}{\alpha_3}\right)$$

Nad

$$X_2^2 X_3 = X_1^3 + aX_1 X_3^3 + bX_3^3$$

uspořádané body

$(\alpha_1 : \alpha_2 : \alpha_3)$ $(\beta_1 : \beta_2 : \beta_3)$

kde α_3 i $\beta_3 \neq 1$

Chceme upravit vzorec sčítání tak, abychom nemuseli dělit zlomky

Odvodení vzorce. Vyjdeme z toho, že $(\alpha_1 : \alpha_2 : \alpha_3) = \left(\frac{\alpha_1}{\alpha_3} : \frac{\alpha_2}{\alpha_3} : 1\right)$

$\alpha \neq \beta = \gamma = (\gamma_1 : \gamma_2 : \gamma_3) = \left(\frac{\gamma_1}{\gamma_3} : \frac{\gamma_2}{\gamma_3} : 1\right)$ $\quad (\beta_1 : \beta_2 : \beta_3) = \left(\frac{\beta_1}{\beta_3} : \frac{\beta_2}{\beta_3} : 1\right)$

$$\frac{\gamma_1}{\gamma_3} = \lambda^2 - \frac{\alpha_1}{\alpha_3} - \frac{\beta_1}{\beta_3} \qquad \frac{\gamma_2}{\gamma_3} = \lambda\left(\frac{\alpha_1}{\alpha_3} - \frac{\gamma_1}{\gamma_3}\right) - \frac{\alpha_2}{\alpha_3}$$

Pokud $\alpha \neq \beta$. Pak

$$\lambda = \frac{\alpha_2/\alpha_3 - \beta_2/\beta_3}{\alpha_1/\alpha_3 - \beta_1/\beta_3} = \frac{\alpha_2\beta_3 - \beta_2\alpha_3}{\alpha_1\beta_3 - \beta_1\alpha_3}$$

$\lambda = U/V \quad U = \alpha_2\beta_3 - \beta_2\alpha_3 \quad V = \alpha_1\beta_3 - \beta_1\alpha_3$

$\gamma_1 = \frac{U^2}{V^2}\gamma_3 - \frac{\alpha_1}{\alpha_3}\beta_3 - \frac{\beta_1}{\beta_3}\gamma_3$

$\gamma_2 = \frac{U}{V}\left(\frac{\alpha_2}{\alpha_3}\gamma_3 - \gamma_1\right) - \frac{\alpha_2}{\beta_3}\gamma_3$

2 VOLIT $A_i B_i$ JEDNOTLIVĚ = 1

Pro γ_1 vhodnou $V^2\alpha_3\beta_3$

Vzhledem ke NULTÉ $\gamma_3 = \gamma^2_3\alpha_3\beta_3$

$\gamma_1 = VW \quad W = U^2\alpha_3\beta_3 - V^2(\alpha_1\beta_3 + \alpha_3\beta_1)$

CENA: U 2M V 2M $W = 2S + 3M$

W SPOČÍTÁNÍ JINÝM DRAHÝM ZPŮSOBEM

$W = U^2\alpha_3\beta_3 - V^2(2\alpha_1\beta_3 - V) = U^2\alpha_3\beta_3 + V^3 - 2\alpha_1\beta_3 V^2$

2M M M

$W = 2S + 4M$

$y_3 = V^3 \alpha_3 \beta_3$ (1M) ($\alpha_3 \beta_3$ prodp. ve W)

$y_1 = V \cdot W$ (1M)

$y_2 = \frac{U}{V}\left(\frac{\alpha_1}{\alpha_3} V^3 \alpha_3 \beta_3 - VW\right) - \frac{\alpha_2}{\beta_3} V^2 \alpha_3 \beta_3$

$= U(\alpha_1 \beta_3 V^2 - W) - V^3 \alpha_2 \beta_3$

(1M) (2M+1M 2W) (1M)

(2M)

Case U, V (4M)

Case W (2S+4M)

y_i (4M)

2S+12M

Cena p_1 M+S

7M+5S CENA ZAVODENÍ

$$\alpha \oplus \alpha = \left(\lambda^2 - \frac{2\alpha_1}{\alpha_3},\ \lambda\left(\frac{\alpha_1}{\alpha_3} - \frac{p_2}{p_3}\right) - \frac{\alpha_2}{\alpha_3}\right)$$

p_1/p_3

$$\lambda = \frac{3(\alpha_1/\alpha_3)^2 + a}{2(\alpha_2/\alpha_3)} = \frac{3\alpha_1^2 + a\alpha_3^2}{2\alpha_2\alpha_3}$$

$$p_3 = 8\alpha_2^3\alpha_3^3$$

$$p_1 = 2\alpha_2\alpha_3\left((3\alpha_1^2 + a\alpha_3^2)^2 - 8\alpha_1\alpha_2^2\alpha_3\right)$$

$$p_2 = \frac{3\alpha_1^2 + a\alpha_3^2}{2\alpha_2\alpha_3}\left(8\alpha_1\alpha_2^3\alpha_3^2 - p_1\right) - 8\alpha_2^4\alpha_3^2$$

$$= (3\alpha_1^2 + a\alpha_3^2)\left(4\alpha_1\alpha_2^2\alpha_3 - \left((3\alpha_1^2 + a\alpha_3^2)^2 - 8\alpha_1\alpha_2^2\alpha_3\right)\right) - 8\alpha_2^4\alpha_3^2$$

(1) α_1^2 (2) α_3^2 (3) $U = 3\alpha_1^2 + a\alpha_3^2$ (4) U^2 (5) $V = 2\alpha_2\alpha_3$ (6) $\alpha_2 V$ (7) V^2 (8) $p_3 = V^3$

$p_1 = VW$, kde $W = U^2 - 4\alpha_1\alpha_2 V$

CENA $p_1 = 2M$

$p_2 = U(2\alpha_1\alpha_2 V - W) - 2(\alpha_2 V)^2$ (M, S)

UŠETŘÍME 4S + 4M

V projektových úrovních cena sčítání je
2S + 12M slogan 5S + 7M

Komentáře
① $a \cdot \alpha^2$ SE POČÍTÁ PŘI ZDVOJENÍ.
JE-LI a V ROZSAHU SLOVA, LZE 1M NAHRADIT 1m (DLOUHÉ × SLOVO)

② ALGORITMY ČASTO FUNGUJÍ TAK, ŽE SE PŘI ČÍTÁ BOD V ZÁKLADNÍM TVARU
$B = (B_1 : B_2 : 1) = P$

Pokud $B_3 = 1$
CENA SČÍTÁNÍ KLESNE NA 2S + 9M

$\alpha_1 B_3$, $\alpha_2 B_3$, $\alpha_3 B_3$ > SE NEBUDOU POČÍTAT

MONTGOMERYHO KŘIVKY

UVAŽME WR $y^2 + g(x)y = f(x)$

Pokud $\mathrm{char} K \neq 2$, tak je možno zapsat jako $\left(y + \frac{g(x)}{2}\right)^2 = f(x) + \left(\frac{g(x)}{2}\right)^2$

$\frac{g(x)}{2} = \frac{a_1 x + a_3}{2}$ Pokud $\bar{y} = y + \frac{a_1 x_1 + a_3}{2}$

$\bar{x} = x$

Tak vstupní WR se transformuje substitucí na $\bar{y}^2 = f(x)$

$y = x_2$
$x = x_1$

Uvažujeme zde pouze lineární substituce (afinní)

$x_i \to \lambda_{i1} x_1 + \lambda_{2i} x_2 + \mu_i \quad i \in \{1, 2\}$

$\det \begin{pmatrix} \lambda_{11} & \lambda_{12} \\ \lambda_{21} & \lambda_{22} \end{pmatrix} \neq 0$

REVERSIBILNÍ SUBSTITUCE

mající kořeny polynom f

NE KAŽDÁ LIN SUBT PŘEN. WR na WR

$y^2 = f(x)$ $\bar{y} = y$ $\bar{x} = x - y$ $\bar{y}^2 = f(\bar{x} + \bar{y})$

$\bar{y}$ se objeví v kvadr. mocnině

Pokud $\mathrm{char}(K) \neq 3$ tak

$y^2 = f(x)$ lze transformovat na tvar $y^2 = x^3 + ax + b$

$$f(x) = x^3 + a_2x^2 + a_1x + a_0 = \left(x + \frac{a_2}{3}\right)^2 + \left(a_1 - \frac{a_2^3}{3}\right)\left(x + \frac{a_2}{3}\right) + \left(a_0 - \frac{a_1a_2}{3} + \frac{2a_2^3}{27}\right)$$

Proč v $\mathrm{char}(K) \neq 2, 3$

LZE ZKOUMAT JEN $y^2 = x^3 + ax + b$

Dosavadní příklady měly tvar $X = X + \dots$ $\quad Y = Y + \dots$ $\quad \lambda_{11} = \lambda_{22} = 1$

Co když $X = \mu X + \dots$

$Y = \gamma Y \dots$

dosadím do WR

Co dostanu jistě nebude WR, ale může to být její skalární násobek

NAPŘ. $x = \lambda^2 x$

$y = \lambda^3 y$

$y^2 = x^3 + ax + b$ přejde na

$(\lambda^3 y)^2 = (\lambda^2 x)^3 + a\lambda^2 x + b \qquad \cdot 1/\lambda^6$

$y^2 = x^3 + a\lambda^{-4} x + b\lambda^{-6}$

Rovnice $y^2 = x^3 + ax + b$ $\quad y^2 = x^3 + \bar{a}x + \bar{b}$ lze lineární substitucí převést navzájem pokud $\bar{a} = \lambda^4 a$

$\bar{b} = \lambda^6 a$

Kvadr. $w(x,y)=0$ je K-ekvivalentní kvadr. $v(x,y)=0$ $\Leftrightarrow$ $\exists$ lineární substituce $\bar{x}=\dots$, $\bar{y}=\dots$

bere, že $w(\bar{x},\bar{y}) = \lambda\, v(x,y)$ pro $\lambda \in K^*$

$v(\alpha,\beta)=0 \Leftrightarrow \lambda v(\alpha,\beta)=0$

PLATÍ, ŽE

$y^2 = x^3+ax+b$ je K-ekvivalentní $y^2 = x^3+\bar{a}x+\bar{b}$

pravou když $\exists \lambda \in K^*$ pak, že $\bar{a} = \lambda^4 a$

$\bar{b} = \lambda^6 a$

MŮŽE BÝT, ŽE PRO $a,b,\bar{a},\bar{b}$ různé takové λ neexistuje, ale v nějakém $L \supseteq K$ $[L:K]<\infty$ TAKOVÉ λ ∃

PRO NĚJAKOU K-ekv., ale pro L-ekv.