Dělicí polynom

Division polynomial

$P \in E[n] \iff [n]P = \infty$

křivka ≥ 2 $P \in E$ $P \in E(\overline{\mathbb{Z}})$

$E[n](K)$

K - naci body v $E[n]$

Def. pro každou el. křivku

Budeme se zabývat

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

char $K \neq 2, 3$ $4a^3 + 27b^2 \neq 0$

$p \nmid n \Rightarrow |E[n]| = n^2$

Tzn., že existuje $n^2 - 1$ afinních bodů

$P = (x, y)$ pro kterou $[n]P = \infty$

$P = (\alpha, \beta) \in E[n] \Rightarrow P = (\alpha, -\beta) \in E[n]$

Čili pokud $\beta \neq 0$, tak s α asociovaná 2 body

Kdy je $\beta = 0$? $\Longleftrightarrow$ právě když $[2]P = \infty$

$\Updownarrow$

α je kořen $x^3 + ax + b$

n liché – existuje $\frac{n^2-1}{2}$ hodnot α určujících prvek $E[n]$

n sudé – $\frac{(n^2-1)-3}{2} + 3 = \frac{n^2+2}{2}$ tolik různých hodnot α

Nechť

přetvarujme – ba musíme formu tak, aby, že

$\exists$ polynom $\tilde{\Psi}_m \in K[x]$, že $\deg(\tilde{\Psi}_m) < \begin{cases} \frac{m^2-1}{2} & m \text{ liché} \\ \frac{m^2+2}{2} & m \text{ sudé} \end{cases}$

$\tilde{\Psi}_m$ separabilní

Platí α kořen $\tilde{\Psi}_m \iff \exists \beta$, že $(\alpha, \beta) \in E[m]$

Pro $\tilde{\psi}_m$ existují rekurzivní formule, ze kterých vyplývá, že $\tilde{\psi}_m \in K[x]$ a že každý koeficient lze zapsat jako celočíselnou kombinaci prvků $a, b \in K$

Místo $\tilde{\psi}_m$ budeme používat

$$\psi_m = \begin{cases} \tilde{\psi}_m & m \text{ liché} \\ 2y\,\tilde{\psi}_m/(x^3+ax+b) & \end{cases}$$

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

DŮVOD: snadněji vyjádřitelné rekurzivní formule

Rekurzivní formule

$$\psi_0 = 0 \quad \psi_1 = 1 \quad \psi_2 = 2y \quad \psi_3 = 3x^4 + 6ax^2 + 12bx - a^2$$

$$\psi_4 = 4y\,(x^6 + 5ax^4 + 20bx^3 - 5a^2x^2 - 4abx - 8b^2 - a^3)$$

pokud a chápeme s váhou 2 a b s váhou 3, tak vidíme homogenitu

$$\psi_{2m+1} = \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3 \qquad m \geq 2$$

$$\psi_{2m} = \frac{(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2)\psi_m}{2y} \qquad m \geq 3$$

$$\begin{cases} m \text{ sudé} & y \mid \psi_{m+2}\ \psi_{m-2}\ \psi_m \\ m \text{ liché} & y \mid \psi_{m-1}\ \ y \mid \psi_{m+1} \end{cases}$$

Pro $P=(\alpha,\beta)\in E$ tedy platí

$$[n]P=\infty \iff \psi_n(\alpha,\beta)=0$$

(v našem označení jen když $\beta=0$)

Zdálo by se, že tohle platí jen když $\mathrm{char}(K)$ nedělí n.

Kupodivu to platí vždy!

To je divné, když $\deg\psi_n = \frac{n^2-1}{2}$ (n liché) a v případě $n=p$ může nast. p prvků v $E[p]$.

Vysvětlení: zmizí některé členy kvůli dělitelnosti — ukážeme na příkladu $K=\mathbb{F}_5$, $n=5$

$[2]P \neq \infty$

Dělicí polynomy dovolují počítat $[n]$ násobek bodu P který neleží v $E[n]$, tedy $\psi_n(P) \neq 0$

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

$P = (x, y)$

zkrácený zápis

ψ_{n-1} je zkratka pro $\psi_{n-1}(x, y)$

V dalším budeme pracovat s $\bar{f}_n$ na místě ψ_n

Další varianta def. dělicích polynomů

$$\bar{f}_n = \begin{cases} \psi_n & n \text{ liché} \\ \dfrac{\psi_n}{2y} & n \text{ sudé} \end{cases}$$

Čili platí. Ať $P=(\alpha,\beta)\in E$. Pokud $[2]P \neq \infty$

pak $P \in E[n] \iff \bar{f}_n(\alpha) = 0$

$\overline{f}_0 = 0 \quad \overline{f}_1 = 1 \quad \overline{f}_2 = 1 \quad \overline{f}_3 = 3x^4 + 6ax^2 + 12bx - a^2$

$\overline{f}_4 = 2(x^6 + 5ax^4 + 20bx^3 - 5a^2x^2 - 4abx - 8b^2 - a^3)$

$$\overline{f}_{2m+1} \begin{cases} \overline{f}_{m+2}\overline{f}_m^{\,3} - 16(x^3+ax+b)^2\,\overline{f}_{m-1}\overline{f}_{m+1}^{\,3} & m \geq 3 \text{ liché} \\ 16(x^3+ax+b)^2\,\overline{f}_{m+2}\overline{f}_m^{\,3} - \overline{f}_{m-1}\overline{f}_{m+1}^{\,3} & m \geq 2 \text{ sudé} \end{cases}$$

$$\overline{f}_{2m} = \overline{f}_m\left(\overline{f}_{m+2}\overline{f}_{m-1}^{\,2} - \overline{f}_{m-2}\overline{f}_{m+1}^{\,2}\right) \qquad m \geq 3$$

Odvození $\psi_3 = \overline{f}_3$

2 $(\alpha,\beta) \in E$, které leží na přímce $y = \lambda x + \mu$

$$(\lambda x+\mu)^2 = x^3+ax+b$$

$$(\lambda x+\mu-\beta)^2 = x^3+ax+b-2\beta(\lambda x+\mu)+\beta^2$$

α je 2-násobný kořen

pokud $3x^2+a-2\beta\lambda = 0$ od jde i zde o 2násobný kořen

$$\lambda = \frac{3\alpha^2+a}{2\beta}$$

derivace v (α,β)

pokud $y = \lambda x+\mu$ je tečna v (α,β), pak

je α ~~dvojnásobný~~ vícenásobný kořen $x^3+ax+b-(\lambda x+\mu)^2$

$[3](\alpha,\beta) = \infty \iff$ tečna v (α,β) křivku nikde neprotne

$$x^3+ax+b-(\lambda x+\mu)^2 = x^3-\lambda^2x^2+(a-2\lambda\mu)x+b-\mu^2$$

$$\|$$

$$(x-\alpha)^2(x-\beta) = (x^2-2\alpha x+\alpha^2)(x-\beta) = x^3-(2\alpha+\beta)x^2+\dots$$

Cíl: $\beta=\alpha \iff \lambda^2=3\alpha \iff [3](\alpha,\beta)=\infty$

$$\lambda=\frac{3\alpha^2+a}{2\beta} \qquad (3\alpha^2+a)^2 = 12\alpha(\alpha^3+a\alpha+b)$$

$$9\alpha^4+6a\alpha^2+a^2 = 12\alpha^4+12a\alpha^2+12b\alpha$$

$$0 = \underline{3\alpha^4+6a\alpha^2+12b\alpha-a^2} = \psi_3(\alpha) = f_3(\alpha)$$

(3α umocnit čtverec) má 8 bodů (α,β) řádu 3

Takové body $\exists \iff \psi_3$ se rozkládá na lineární činitele

Odvození $\overline{f_4}$ $\quad P=[\alpha,\beta]$

$[4]P=\infty \iff [2]P=(\alpha',0)$ $\quad \alpha'$ je kořen x^3+ax+b

$0=\beta'=\lambda(\alpha-\alpha')-\beta \qquad \alpha'=\lambda^2-2\alpha \qquad \lambda=\dfrac{3\alpha^2+a}{2\beta}$

$\lambda(3\alpha-\lambda^2)-\beta=$ $\qquad [2]P=(\alpha',\beta')$

$\dfrac{1}{(2\beta)^3}\Big(\big(3\alpha^2+a\big)\big(12\alpha\beta^2-(3\alpha^2+a)^2\big)\Big)-8\beta^4\Big)$

čili čitatel je $\ldots$ $-8\beta^4$ spolu s $(3\alpha^2+a)$ nesoudělné

$\alpha^3+a\alpha+\beta$

$$12x(x^3+ax+b)-(3x^2+a)^2 = 3x^4+6ax^2+12bx-a^2$$

$$(3x^2+a)(3x^4 - - a^2) = 9x^6+21ax^4+36bx^3+3a^2x^2+12abx+a^3$$

$$-8(x^3+ax+b)^2 = -8x^6-16ax^4-16bx^3-8a^2x^2-16abx-8b^2$$

$$x^6+5ax^4+20bx^3-5a^2x^2-4abx-a^3-8b^2$$

$$= \frac{f_4(x)}{2}$$

12 možných bodů řádu 4

3 ~~uvnitř~~ ... řádu

16 = |E[4]|

$Z_4 \times Z_4$ — f_4 má 6 kořenů

$Z_4 \times Z_2$, Z_4 — f_4 má 1 kořen

$b \neq 0$

$$[m]P = \left(\alpha - \frac{\psi_{m-1}\psi_{m+1}}{\psi_m^2}, \frac{\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2}{4\beta\psi_m^3}\right)$$

$\underline{m=2}$

$$[2](\alpha,\beta) = \left(\frac{(3\alpha^2+a)^2 - 8\alpha\beta^2}{4\beta^2}, \frac{3\alpha^2+a}{2b}(\alpha-\gamma) - \beta\right)$$

$\psi_0 = 0$

$\psi_1(\alpha,\beta) = 1$

$\psi_2^2(\alpha,\beta) = (2\beta)^2 = 4\beta^2$

$\psi_3(\alpha,\beta) = 3\alpha^4 + 6a\alpha^2 + 12b\alpha - a^2$

$= 12\alpha\beta^2 - (3\alpha^2+a)^2$

$$\frac{(3\alpha^2+a)(4\alpha\beta^2 - (3\alpha^2+a)^2 + 8\alpha\beta^2) - 8\beta^4}{8\beta^3} = \frac{f_4(\alpha)}{16\beta^3} = \frac{\psi_4(\alpha)\beta}{32\beta^4}$$

$$\alpha - \frac{\psi_1\psi_3}{\psi_2^2} = \alpha - \frac{12\alpha\beta^2 - (3\alpha^2+a)^2}{4\beta^2} = \frac{(3\alpha^2+a)^2 - 8\alpha\beta^2}{4\beta^2}$$

$$\beta = \frac{\psi_4(\alpha)}{32\beta^3} = \frac{\psi_4(\alpha)\beta}{4b\cdot(2\beta)^3}$$

Pokud se spolehneme na vzorec $\bar{f}_5 = 16(x^3+ax+b)^2 \bar{f}_4 \bar{f}_2^3 - \bar{f}_1 \bar{f}_3^3 = 16(x^3+ax+b)^2 \bar{f}_4 \bar{f}_3^3$

tak dostaneme že f_5 dává

$5x^{12}$ $\boxed{0}_{\bmod 5}$ $+ 62ax^{10}$ $\boxed{2ax^{10}}$ $+$

$380bx^9 - 105a^2x^8 - 240abx^7 - (240b^2+300a^3)x^6$ $\boxed{0}$

$-696ab^2x^5$ $\boxed{ab^2x^5}$ $-(1920ab^2+125a^4)x^4 - (1600b^3 - 80a^3b)x^3$ $\boxed{0}$

$-(240b^2a^2 - 50a^5)x^2 - (640ab^3 + 100a^4b)x$ $\boxed{0}$

$-256b^4 + 32a^3b^2 - a^6$ $\boxed{-b^4 + 2a^3b^2 - a^6}$

Nad tělesem 5 je f_5 rovno $2ax^{10} - ab^2x^5 - b^4 - 2a^3b^2 - a^6 = (rx^2+sx+t)^5$

mají prvky řádu 5 $\quad r^5 = 2a \quad s^5 = -ab^2 \quad t^5 = -b^4 - 2a^3b^2 + a^6$

TO JE VŽDY MOŽNÉ (perfektní těleso)