$P+Q-(P\oplus Q)-O$

Normalizovaná priamka jednotková

$P=\ominus Q$ $\quad x-\alpha$ $\quad P=(\alpha,3)$ $\quad (X-X_P)=P+(\ominus P)-2O$

$X-X_P$

Ak $P\neq\ominus Q$ $\quad P+Q+R-3O=(\ell)$

ℓ je přímka procházející P a Q

$R=\ominus(P\oplus Q)$

$$P+Q-(P\oplus Q)-O=P+Q+R-3O-((P\oplus Q)+R-2O)=\left(\frac{\ell_{P,Q}}{X-X_{P\oplus Q}}\right)$$

AKLP

$0 \to 1$

$\ell = y - \lambda x - \mu \qquad v_O(\ell) = -3$

$$\frac{y - \lambda x - \mu}{z^3} = \frac{(y - \lambda x - \mu)x^3}{y^3} = \frac{(y - \lambda x - \mu)(y^2 - \alpha x - \beta)}{y^3}$$

$$= \frac{y^3 - \lambda x y^2 + \dots}{y^3} \longrightarrow (Y^3 - \lambda X Y^2 + Z(\dots) : Y^3)$$

$$(0:1:0) \longrightarrow (1:1)$$

$$\frac{y - \lambda x - \mu}{z^3}(\infty) = 1$$

$$\mu_{P,Q} = \frac{\ell_{P,Q}}{v_{P\oplus Q}} = \frac{y - \lambda(x - x_P) - y_P}{x - x_{P\oplus Q}}, \quad \lambda < \frac{y_P - y_Q}{x_P - x_Q}, \ \frac{3x_P^2 + a}{2y_P}$$

$$\mu_{P,Q} = x - x_P$$

$$\mu_{P,O} = \mu_{O,P} = 1$$

Ve všech párováních se vyskytuje v tole

Zjistěte normalizovaný prvek $u \in K(C)$
že $div(u) = rP - rO$, kde $P \in C[r]$

Cvičení úlohy

Pro $P \neq O$ $\quad P \in C(K)$ spočtěj $f_{r,P}(Q)$, $Q \neq P$

kde $f_{r,P}$ je normalizovaná pro $\overline{K}(C)$ $\quad \mathrm{div}(f_{r,P}) = rP - rO$

Postup se opírá o definice

Řešení úlohy $\quad \mathrm{div}(f_{j,P}) = jP - [j]P - (j-1)O$

TVRZENÍ $\quad f_{i+j,P} = f_{i,P} \cdot f_{j,P} \cdot \mu_{[i]P,[j]P}$

$$\mathrm{div}(\mu_{[i]P,[j]P}) = [i]P + [j]P - [i+j]P - O$$

$$jP - [j]P - (j-1)O + iP - [i]P - (i-1)O + \ldots$$

$$= (i+j)P - [i+j]P - (i+j-1)O$$

Millerův alg.

z tabule

Vstup $r \geq 1$ $I = \lfloor \log_2 r \rfloor$ $P \in C[r](K)$

$Q \in C(K)$

Výstup $f_{r,P}(Q)$

1. $r = \sum_{i=0}^{I} b_i 2^i$ binární dekompozice čísla r

Proměnné $T = P$; ← bod

$f = 1$; ← VÝSTUP

2. for $i = I-1, \dots, 0$

(a) $f = f^2 \mu_{T,T}(Q)$

2x

(b) $T = [2]T$

(c) if $b_i = 1$ $f = f \mu_{T,P}(Q)$

$T = T \oplus P$.

klasické

podobné

zleva doprava

Uvědomit si, že $f_{i,P}$ kde $i \in \mathbb{Z}$ tvoří grupu vůči ·

$\varphi: i \mapsto f_{i,P}$ je homomorfismus $\mathbb{Z} \to$ grupa

Operace v grupě je

$$f_{i+j,P} = f_{i,P} \boxed{+} f_{j,P} = f_{i,P} f_{j,P} \, (\ldots)_{i,j,P}$$

$$\varphi(i+j) = \varphi(i) + \varphi(j)$$

Pokud máme algoritmus na výpočet $f_{n,P}$, tedy $f_{n,P}$ umíme jako $\varphi(n)$ a tam algoritmus probíhá stejně. Millerův algoritmus počítá tam odsud násobení na Q, tak je vlastně výpočtem $\boxed{f_{n,P}} = \varphi(n)$

$f_{i,P}$ [illegible]

stačí se [illegible], když [illegible] aplikaci na Q

Q nastaví P [illegible]

Na $\mathbb{A}^1 = K$ je [illegible]

Na $\mathbb{P}^1$ [illegible] def. [illegible]

$$f_{i+j,P}(Q) = f_{i,P}(Q)\, f_{j,P}(Q)\, \mu_{[i]P,[j]P}(Q)$$

Pokud $\mu_{[i]P,[j]P}(Q) = \infty$

$j = 1$

$x - \alpha$

$y - \lambda x - \mu$

$x - p$

1

$[i+j]P = \pm Q$

$Q = [\pm(i+1)]P$