POJMY:

Dělicí polynom $\bar{f}_m$

nuly určují x-ové souřadnice prvků $E[m]$

pomocí $\bar{f}_m$ (či ψ_m) lze vyjádřit rac. fcí m-násobek prvků, které nejsou v $E[m]$

Rozšíření σ

rac. zobr.

σ

el. křivky nad el. křivku

jsou to homomorfismy vzhledem k $\oplus$

Endomorfismy $E[m]$ φ φ

Vztah $|E(\mathbb{F}_q)| = q - t + 1$ $\quad |t| \le 2\sqrt{q}$

$$\varphi^2 \ominus [t]\varphi \oplus q = 0$$

Cíl nalézt pro $y^2 = x^3 + ax + b$ hodnotu t — a tím i řád $E(\mathbb{F}_q)$

Metoda nalézt $\boxed{t_\ell \equiv t \bmod \ell}$ pro ℓ prvočísla, a to pro dostatek prvočísel $\ell_1, \dots, \ell_k$ takových, že $\prod \ell_i > 4\sqrt{q}$

z ČVZ z t_{ℓ_i} můžeme spočítat hodnotu $t \bmod \prod \ell_i$, a to vždy > určíme t podle Hasseovy rovnosti jednoznačně

Určit t_ℓ – k tomu stačí najít τ, že pro nějaký

$P \in E[\ell]^*$ je $\varphi^2(P) \oplus [q_\ell] P = [\tau] \varphi(P)$,

$\forall P$ je $\varphi^2(P) \oplus [q_\ell] P = [t_\ell] \varphi(P)$

Přitom $q_\ell \equiv q \bmod \ell$ $\quad t_\ell \equiv t \bmod \ell$ $\quad \varphi : (\alpha, \beta) \mapsto (\alpha^q, \beta^q)$

Volí se $\tau = 0, 1, \ldots, \frac{\ell-1}{2}$ a

zkoumá se rovnost $\varphi^2(P) \oplus [q_\ell] P = [\pm\tau] \varphi(P)$ $\quad \gcd(h_x, f_\ell) \neq 1$

$\exists$ nějaký polynom h_x, q_ℓ $\quad$ různý pravý $\quad q_\ell < \ell$

$h_x(\alpha) = 0 \iff \exists P = (\alpha, \beta)$ kolegové h_x $\quad$ f_{q_ℓ} v vyjádření $[q_\ell] P$ jako

V generických (nevýjimečných) případech postupujeme takto: Nalezneme h_x a provedeme $\gcd(h_x, f_\ell)$. Pokud $d>1$, víme, že $\exists P=(\alpha,\beta)\in E[\ell]^*$ takové, že

$$\varphi^2(P) \oplus [k_\ell]P = \begin{cases} [\tau]\varphi(P) \\ [-\tau]\varphi(P) \end{cases}$$

TŘEBA ROZHODNOUT

Postupuje se tak, že se předpokládá, že platí ten případ s τ, a ověřuje se, zda skutečně $\exists \beta$, že $P=(\alpha,\beta)\in E[\ell]^*$ splňuje rovnost.

$\gcd(h_{y,\tau}, f_\ell)>1$, umocníme β^2 $O^*_\beta = 0$ s ohledem mocnině $\Rightarrow (x^3+ax+b)\ h_{y,\tau}(x)$

Polynomy h_x i h_y jsou velmi vysokého stupně $\deg(\bar{f}_\ell) = \frac{\ell^2-1}{2}$ tak při vyčíslování h_x a h_y můžeme průběžně polynomy redukovat modulo $\bar{f}_\ell$.

$$h_x \bmod \bar{f}_\ell \qquad h_y \bmod \bar{f}_\ell$$

Výjimečné případy

ROZBOR, KDY

$\exists\ P \in E[\ell]^*$, že

pro $\varphi^2(P) \oplus [\xi_\ell]P$ NELZE POUŽÍT GENERICKÝ VZOREC

$$\varphi^2(P) \oplus [\xi_\ell]P = [z]\varphi(P)$$

zdvojení

generic- h_x, h_y

O opačné prvky

ZAHRNUJÍ SITUACI $\underline{z=0}$

V všech zbylých se počítá $z = 1, \dots, \frac{\ell-1}{2}$

JDE V PRVNÍM KROKU O ROZHODNUTÍ ZDA $\exists\ P \in E[\ell]^*$, že $\varphi^2(P)$ a $[\xi_\ell]P$ mají shodnou x-ovou souřadnici:

zda $\varphi^2(P) = \begin{cases} [\xi_\ell]P \\ [-\xi_\ell]P \end{cases}$

Pro počítání $[\zeta_e]^{-1}P$ můžeme použít formuli založenou na dělitelnosti polynomů.

Shoda v x-ové souř. znamená porovnat x^{ξ^2} a obrazem $P=(\alpha,\beta)$ při násobení $[\zeta_e]$

To lze opět vyjádřit polynomem — tedy ke existenci shody ~~lze~~ vyjádřit tím, že gcd f_e a tímto polynomem $\varphi > 1$. Příslušný gcd, pokud $\exists > 1$, se značí $\bar{S}_e$.

Pokud shoda v α existuje, tak buď dvě možnosti

$\varphi^{\ell}(P) = [\zeta_e]P$ NEBO $\varphi^{\ell}(P) \overset{!}{=} [-\zeta_e]P$ ← $\tau = 0$ $\tau_e = 0$

Rozhodnutí, zda $t_\ell = 0$ znamená opět řešit, zda předpoklad $t_\ell = 0$ lze podepřít existencí β.

Znovu to vede na nějaký polynom v x, který buď je nebo není násobek f_ℓ ($\iff \gcd(-, f_\ell) > 1$)

$\boxed{\beta^2}$

$\varphi^2[P] = [q_\ell] P$ důležitý $\longrightarrow$ SEA

Elkies

Atkin

$$t_\ell \neq 0 \implies \varphi^2(P) = [s_\ell]P$$

? $\exists\, P$, že shoda v x

$$\varphi^2[P] \oplus [s_\ell]P = [\tau]\varphi(P)$$

$$[2s_\ell]P = [\tau]\varphi(P)$$

$$\varphi(P) = \left[\frac{2s_\ell}{\tau}\right]P \qquad \tau = t_\ell$$

POČÍTÁNO MOD ℓ

$$[s_\ell]P = \varphi^2[P] = \varphi\left(\left[\frac{2s_\ell}{\tau}\right]P\right) = \left[\left(\frac{2s_\ell}{\tau}\right)^2\right]P \qquad \tau \to t_\ell$$

$$[s_\ell t_\ell^2]P = [4s_\ell^2]P \implies [t_\ell^2]P = [4s_\ell]P$$

Řekne $t_l^2 \equiv 4q_l \mod l$ Dvě možné hodnoty t_l

Jednu vyberu a označím τ.

2. $[2q_l]P = [\tau]\varphi(P) \iff \varphi(P) = [\gamma]P$

$\varphi^2(P) \oplus [q_l]P$

$$\boxed{\gamma = \frac{2q_l}{\tau}}$$

Rovnost vede na nový polynom, který vyjadřuje vztahy v y-ové souřadnice

Pokud polynom má $\gcd$ s f_l > 1, tak je výběr τ korektní, pokud vyjde $\gcd = 1$, je třeba zvolit $-\tau$.

TÍM JE ZHRUBA ALGORITMUS POPSÁN

$\varphi(P) = [\mu]P$

$E[l] \cong \mathbb{Z}_l \times \mathbb{Z}_l = V$ $\quad \dim V = 2$ nad $\mathbb{Z}_l = \mathbb{F}_l$

$\mu = \frac{2q_l}{t_l}$

φ zobrazí prvky řádu l na prvky řádu l, φ je injektivní.

$\exists P \in V$

Čili $\psi = \varphi|V$ je lineární automorfismus V

μ je vlastní číslo $\varphi|V$

∃ věta

Cayley-Hamiltonova věta

$$\psi^2 - tr(\psi)\cdot\psi + det(\psi) = 0$$

$$\varphi^2 \ominus [t_l]\varphi \oplus [q_l] = 0$$

$t_l = tr(\psi)$ $\quad q_l = det(\psi)$

STOPA FROBENIOVA ENDOMORFISMU

$$\varphi^2 \ominus [t]\varphi \oplus q = 0$$

SEA algoritmus rozlišuje

Elkiesova prvočísla $T^2 - t_\ell T + q_\ell$ má kořen v $\mathbb{Z}_\ell$

Atkinova prvočísla $T^2 - t_\ell T + q_\ell$ nemá kořen v $\mathbb{Z}_\ell$

Rozhodnout, zda jde o E. nebo A. prvočíslo není možné přímočaře, protože t_ℓ neznáme.

$\exists$ metody používající modulární polynomy, které to rozhodnout umožňují.

Elkiesovo pozorování $\exists \lambda \quad \varphi(P) = [\lambda]P$

Jedna z hlavních výhod SEA je v tom, že se λ dá spočítat efektivněji než procházení

$z = 0, 1, 2, \ldots$

Jakmile λ známe, takovou, že $\exists P \in E[\ell]^*$, že $\varphi(P) = [\lambda]P$, tak to

$$\underbrace{[\lambda^2]P}_{\varphi^{(2)}(P)} \oplus [q_\ell]P = \underbrace{[t_\ell \lambda]P}_{\varphi(P)\,[\lambda]P} \Rightarrow \lambda^2 + q_\ell = t_\ell \lambda$$

$$t_\ell = \lambda + \frac{q_\ell}{\lambda}$$

__Atkin__ $\exists$ metoda, jak získat množinu T_ℓ relativně malou, o které víme, že obsahuje t_ℓ.

Schoofov algoritmus formálne:

B je súčin prvočísel $l_1, l_2, \ldots$

M je zoznam (l, t_l)

$B = 2$; $l = 2$; if $\gcd(x^2 - x, x^3 + ax + b)$ $= 1$: $\tau = 1$; > 1: $\tau = 0$

$M = \{(2, \tau)\}$;

while $(B < 4\sqrt{q})$ do:

  $l = \text{nextprime}(l)$;

  $B = B * l$;

  ZISTI $\tau = t_l$

  $M = M \cup \{(l, \tau)\}$

ZISTI t POMOCOU M a ČVZ

VÝSLEDOK JE $q+1-t$

$\bar{s}_e$ – prowd ovrse byla sprawdzo (rozłączna kwadr. zajmuje)
skoda ($2^l P$) s $l_e P$

IF ($\gcd(\bar{s}_e, \bar{t}_e) \neq 1$)
    τ = equals(l)
ELSE DO
    $\tau = 0$;
    do: $\tau = \tau + 1$;
        r = nonequals(l, τ);
    until($r \neq 0$);
    If ($r == -1$) THEN $\tau = -\tau$;
RETURN τ;

$r = 0$: $t_e \notin I\tau$
$r = 1$: $t_e = \tau$
$r = -1$; $t_e = -\tau$

ODVOZENÍ ς_ℓ. Co chceme.

ZJISTIT PODMÍNKU, ŽE $\varphi^2(P)$ a $[\varsigma_\ell]P$ MAJÍ SHODNOU PRVNÍ SOUŘADNICI ALESPOŇ PRO JEDNO $P=(\alpha,\beta)$.

PŘIPOMEŇME, ŽE PRO $m=\varsigma_\ell$ je m-násobek ($m\geq 2$) $P=(\alpha,\beta)$ o prvé souřadnici rovna

$$\alpha-\frac{\psi_{m-1}(\alpha,\beta)\,\psi_{m+1}(\alpha,\beta)}{\psi_m^2(\alpha,\beta)}=\begin{cases}\alpha-\dfrac{\overline{f_{m-1}}(\alpha)\,\overline{f_{m+1}}(\alpha)}{4\beta^2\,\overline{f_m}^2(\alpha)} & \boxed{m \text{ sudé}} \quad \beta^2=x^3+ax+b\\[2ex] \alpha-\dfrac{\overline{f_{m-1}}(\alpha)\,\overline{f_{m+1}}(\alpha)\cdot 4\beta^2}{\overline{f_m}^2(\alpha)} & m \text{ liché}\end{cases}$$

$[q_\ell]P$ a $\varphi^2(P) = (x^{q^2}, y^{q^2})$ se pro $m = q_\ell$ sudé shodují v x-ové souřadnici pokud

$$\alpha^{q^2} 4\beta^2 \overline{f}_m^2(\alpha) = \alpha 4\beta^2 \overline{f}_m^2(\alpha) - \overline{f}_{m-1}(\alpha)\,\overline{f}_{m+1}(\alpha)$$

Když α je kořen $4(x^{q^2}-x)(x^3+ax+b)\overline{f}_m^2(x) + \overline{f}_{m-1}(x)\,\overline{f}_{m+1}(x)$

Pro $q_\ell > 1$ liché je podobně

$$\overline{s}_\ell(x) = 4(x^{q^2}-x)\,\overline{f}_{q_\ell}^2(x) + 4(x^3+ax+b)\,\overline{f}_{q_\ell-1}(x)\,\overline{f}_{q_\ell+1}(x)$$

Pro $q_\ell = 1$ $\quad \overline{s}_\ell(x) = x^{q^2} - x$.