NAF-FORMY PRO VĚTŠÍ ZÁKLAD b

$b = 2^v$ $v = 1$ původní

Jak $k = \sum k_i 2^i$ PŘEVÉST DO NAF?

tak, aby platilo $0 \ldots 0$ $k_i \neq 0$ $k_i \in \{0, \pm 1, \ldots, \pm ?\}$

alespoň v nul

Zapiš při základu b, od daného jen 1 nula, pokud tam chceme binárně

$k = 2^v k'$ právě nuly zpět k'

$k = 2^{v+1} k' + w$ $|w| < 2^v$ k' [v nul] w

$k = 2^{v+1} k' - w$ k' v_{nul} $-w$

BARRETTŮV REDUKČNÍ ALGORITMUS

MÁME n (ODPOVÍDÁ p Z MNT. ARITM.)

JDE O REDUKCI, KTERÁ NEVYUŽÍVÁ PRVOČÍSELNOSTI

POUŽITÍ PRO NÁHODNÉ MODULO n

JE TŘEBA ŘEŠIT VÝPOČET x mod n, když $x < n^2$

AŤ $b^t > n > b^{t-1}$ PŘEDPOKLÁDÁME $b^{2t} > n^2$ více než $n^2 > x$

PŘEDPOČÍTANÁ HODNOTA $\mu = \left\lfloor \frac{b^{2t}}{n} \right\rfloor$

$b^t > n > b^{t-1}$ bx n $n^2 > x \geq 0$ $r = \left\lfloor \frac{b^{2t}}{n} \right\rfloor$

CÍL: SPOČÍTAT $x \bmod n$ „UMÍME EFEKTIVNĚ DĚLIT n“

POLOŽÍME $y = x - \left\lfloor \frac{xr}{b^{2t}} \right\rfloor n$

TVRZENÍ $0 \leq y < 2n$ (POKUD PLATÍ $x \bmod n \in \{y, y-n\}$)

D: $-2n < -y = -x + \left\lfloor \frac{xr}{b^{2t}} \right\rfloor n < 0$ ①

$x - 2n < \left\lfloor \frac{xr}{b^{2t}} \right\rfloor n \leq x$

$\frac{x}{n} - 2 < \left\lfloor \frac{x^2}{b^{2t}} \right\rfloor \leq \frac{x}{n}$

OVĚŘÍME

VÍME $x\left(\frac{b^{2t}}{n} - 1\right) \leq xr \leq \frac{b^{2t}}{n} x$

$\frac{x}{n} - \frac{x}{b^{2t}} \leq \frac{xr}{b^{2t}} \leq \frac{x}{n}$ $1 \geq \frac{x}{b^{2t}}$

$\frac{x}{n} - 1 \leq \frac{xr}{b^{2t}} \leq \frac{x}{n}$ ⇓

$\frac{x}{n} - 2 < \left\lfloor \frac{x}{n} - 1 \right\rfloor \leq \left\lfloor \frac{xr}{b^{2t}} \right\rfloor \leq \frac{x}{n}$

Jak $x - \left\lfloor \frac{x_k}{b^{2t}} \right\rfloor n$

EFEKTIVNĚ SPOČÍTAT

JAK SE ZBAVIT DLOUHÉHO

VÁHOVÁNÍ $x \cdot k$

rozkladu b^{2t} b^t

VZNIKNE NĚCO rozkladu b^{3t}

ale nižších než v x_k nepotřebuji

$\left\lfloor \frac{x_k}{b^{2t}} \right\rfloor$ vyšších než

JAK EFEKTIVNĚ VYUŽÍT

TECHTO POZOROVÁNÍ PRO VÝPOČET?

Navíc víme $l \leq 2n$

že u

$x - \left\lfloor \frac{x_k}{b^{2t}} \right\rfloor n < b^{t+1}$

stačí znát

dolních cca t cifer

b^{t+1}

Jacobiho souřadnice

Projektivní souřadnice vzniknou jako ekvivalence na $\mathbb{K}^3$, resp. $\mathbb{K}^3$ s odstraněnou $(0,0,0)$

$$[a:b:c] = [u:v:w] \iff \exists \lambda \in \mathbb{K}^* \quad u = \lambda a \quad v = \lambda b \quad w = \lambda c$$

LZE ZAPSAT TAKÉ POŽADAVKEM $aw = cu \quad bw = vc \quad av = bu$

Uvažujme podobný vztah

Jacobiho souřadnice

$[a|b|c] = [u|v|w] \iff$

$\exists \lambda \in K^*$, že $w = \lambda c \quad u = \lambda^2 a \quad v = \lambda^3 b$

Je to vůbec dobře def.? Je to ekvivalence?

$[u, v, w] = [x, y, z] \quad z = \gamma w \quad x = \gamma^2 u \quad y = \gamma^3 v$

$z = (\lambda\gamma) c, \; x = (\lambda\gamma)^2 a \quad y = (\lambda\gamma)^3 b$

EXISTUJE POPIS ROVNOSTI, KTERÝ NEUVÁDÍ λ

$[u|v|w] = [a|b|c] \iff a w^2 = c^2 u \quad b w^3 = v c^3 \quad b^2 u^3 = a^3 v^2$

$\Longrightarrow$ SNADNÝ V SKUTKU $\quad a \lambda^2 c^2 = c^2 \lambda^2 a \quad b \lambda^3 c^3 = \lambda^3 b^3 c^3$

$b^2 \lambda^6 a^3 = a^3 \lambda^6 b^2$

$aw^2 = c^2 u$ $bw^3 = vc^3$ $b^2u^3 = a^3v^2$

pokud $a = 0$ a $u \neq 0 \Longrightarrow b = 0, c = 0$ (spor s $(a,b,c) \neq (0,0,0)$)

$a = 0 \Longleftrightarrow u = 0$

$b = 0 \Longleftrightarrow v = 0$

$c = 0 \Longleftrightarrow w = 0$

Horní Ci v definici $[a|b|c]$ 2 každý vektor, což je třída $[\cdot\cdot]$ bod určen jednoznačně a λ řeší ($\lambda \in \mathbb{R}$, chceme ověřit)

Sledujme situaci s právě jednou nulou

$a = 0 = u$ $bw^3 = c^3 v$

$b = 0 = v$ $aw^2 = c^2 u$

$c = 0 = w$ $\lambda = \frac{av}{bu}$

$\lambda = w/c$ $v = (w/v)^3 c$

$\lambda = w/c$

$$\lambda^2 a = \frac{a^2v^2}{b^2u^2} \cdot a = \frac{a^3v^2}{b^2u^2} = \frac{b^2u^3}{b^2u^2} = u$$

$$\lambda^3 b = \frac{a^3v^3}{b^3u^3} \cdot b = \frac{b^2u^3}{b^2u^3} \cdot v = v$$

Vše nemluvě $\lambda = \frac{uc}{aw}$

$\frac{u^2c^2}{a^2w^2} a = \frac{a^2w^2 u}{a^2w^2} = u$

$\frac{u^3c^3}{a^3w^3} b = \frac{u^3c^3 v}{a^3w^3 v} \cdot b = \frac{u^3w^3 b^2}{a^3w^3 v} \frac{a^3v^2}{a^3v} = v$

$\frac{uc}{aw} c = \frac{uc^2}{aw} = \frac{aw^2}{aw} = w$

projektivní body

Jacobiho body

$(a:b:1) \to (a|b|1)$

$(a:b:c) \to (ac^2|bc^3|c)$, $c \neq 0$

Rovnost $(x|y|z)$, $z \neq 0$ $\Rightarrow \left(\frac{x}{z^2} : \frac{y}{z^3} : z\right)$

Jak naložit s body v nekonečnu

Čemu odpovídá $(a:b:0)$

TADY 1-1 korespondence není

$(a|b|0) = (c|d|0)$

$b^2c^3 = a^3d^2$!

PŘÍKLAD $(1|-1|0) = (1|1|0)$

S trochou míněné pravdy „Jacobiho homogenizace"

Chceme alg. vlastnosti body křivky byly nezávislé na tom, kterou z reprezentací $[a|b|c]$ zvolíme.

Potřebujeme vzít křivky s monomy $X_1^a X_2^b X_3^c$ kde $2a+3b+c$ je konstantní

Vyjádření křivky musí

homogenizovat na Jacobiho zvlášť

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

$$X_2^2 + a_1 X_1 X_2 X_3 + a_3 X_2 X_3^3 = X_1^3 + a_2 X_1^2 X_3^2 + a_4 X_1 X_3^4 + a_6 X_3^6$$

$$y^2 = x^3 + ax + b \Rightarrow Y^2 = X^3 + aXZ^4 + bZ^6$$

UKÁŽEME, JAK SE TO VÝPOČETNĚ VYUŽÍVÁ