Kódoláselmélet 2020 szept 30

Def Jacobi szimbólum $a \in \mathbb{Z}$, P páratlan poz. egész

$P = p_1 p_2 \cdots p_k$
prímfelbontás

$$\left(\frac{a}{P}\right) = \left(\frac{a}{p_1}\right) \cdot \left(\frac{a}{p_2}\right) \cdots \left(\frac{a}{p_k}\right)$$

Tétel Tetszőleges $a, b \in \mathbb{Z}$ és $P, Q \in \mathbb{N}$ páratlan egészekre

(0) $\left(\frac{1}{P}\right) = 1$

(1) $\left(\frac{a}{PQ}\right) = \left(\frac{a}{P}\right) \cdot \left(\frac{a}{Q}\right)$ nevezőben multiplikatív

(2) $\left(\frac{ab}{P}\right) = \left(\frac{a}{P}\right) \cdot \left(\frac{b}{P}\right)$ számlálóban multiplikatív.

(3) $a \equiv b \mod P \Rightarrow \left(\frac{a}{P}\right) = \left(\frac{b}{P}\right)$

(4) $\left(\frac{-1}{Q}\right) = (-1)^{\frac{Q-1}{2}}$ (5) $\left(\frac{2}{Q}\right) = (-1)^{\frac{Q^2-1}{8}}$

(6) $\left(\frac{P}{Q}\right) \cdot \left(\frac{Q}{P}\right) = (-1)^{\frac{P-1}{2} \cdot \frac{Q-1}{2}}$ kvadratikus reciprocitás

Megj: Legendre szimbólum kiszámítása önmagában nehéz, mert $\left(\frac{a}{p}\right)$-nél a-t faktorizálni kell.

Áll: Legendre szimbólum kiszámítása Jacobi-szimbólum segítségével gyors ($\log_2 \max(P, Q)$ lépés)

Biz Hasonlóan az euklideszi algoritmushoz a (3) miatt vehetjük a előjeles maradékot, (6)-al tovább léphetünk páros számokat (5)-el, negatív számokat (4)-el kezeljük.

<u>Feladat</u> Számoljuk ki a $\left(\frac{30}{37}\right)$ Legendre szimbólumot a Legendre szimbólum számítási szabályaival.

$$\left(\frac{30}{37}\right) = \left(\frac{2}{37}\right)\cdot\left(\frac{3}{37}\right)\cdot\left(\frac{5}{37}\right)$$ mert $30 = 2\cdot 3\cdot 5$ <u>faktorizáció</u>!

$$\left(\frac{2}{37}\right) = -1^{\frac{37^2-1}{8}} = -1^{\frac{5^2-1}{8}} = -1^{3} = -1$$ mert $37 \equiv 5 \mod 8$

$$\left(\frac{3}{37}\right)\cdot\left(\frac{37}{3}\right) = +1^{\frac{3-1}{2}\cdot\underbrace{\frac{37-1}{2}}_{=18}} = -1^{1\cdot 18} = +1$$ kvadratikus reciprocitás

$$\left(\frac{37}{3}\right) = \left(\frac{1}{3}\right) = 1$$ mert $37 \equiv 1 \mod 3$

azaz $\left(\frac{3}{37}\right) = +1$

$$\left(\frac{5}{37}\right)\cdot\left(\frac{37}{5}\right) = -1^{\frac{5-1}{2}\cdot\frac{37-1}{2}} = -1^{2\cdot 18} = 1$$

$$\left(\frac{37}{5}\right) = \left(\frac{2}{5}\right) = -1^{\frac{5^2-1}{8}} = -1^{3} = -1$$

azaz $\left(\frac{5}{37}\right) = -1$ tehát $\left(\frac{30}{37}\right) = (-1)\cdot(+1)\cdot(-1) = +1$

$$\left(\frac{30}{37}\right) = \left(\frac{+7}{37}\right)\cdot\left(\frac{-1}{37}\right) = +1$$

$$\left(\frac{-1}{37}\right) = -1^{18} = +1$$

$$\left(\frac{37}{7}\right)\cdot\left(\frac{7}{37}\right) = +1$$

$$\left(\frac{37}{7}\right) = \left(\frac{2}{7}\right) = -1^{6} = 1$$

<u>Feladat</u> Ugyan ez de Jacobi szimbólumokkal

$$\left(\frac{30}{37}\right) = \left(\frac{2}{37}\right)\cdot\left(\frac{15}{37}\right), \quad \left(\frac{2}{37}\right) = -1$$ mint előbb

$$\left(\frac{15}{37}\right)\cdot\left(\frac{37}{15}\right) = -1^{7\cdot 18} = +1, \quad \left(\frac{37}{15}\right) = \left(\frac{7}{15}\right)$$

$$\left(\frac{7}{15}\right)\cdot\left(\frac{15}{7}\right) = -1^{3\cdot 7} = -1, \quad \left(\frac{15}{7}\right) = \left(\frac{1}{7}\right) = 1$$

azaz $\left(\frac{7}{15}\right) = -1$, $\left(\frac{15}{37}\right) = -1$, tehát $\left(\frac{30}{37}\right) = -1\cdot -1 = +1$.

<u>nem kell faktorizálni</u>

<u>Tétel (Solovay – Strassen)</u> Legyen $n > 1$ páratlan egész és $A = \{ a \mid 1 \le a \le n-1 \text{ és } \operatorname{lnko}(a,n) = 1 \} = \mathbb{Z}_n^*$

Ha n prím, akkor A minden elemére

$$\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} \pmod{n}.$$

Ha n nem prím, akkor A elemeinek legalább felére nem teljesül ez a feltétel.

<u>Áll:</u>

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p} \quad \text{ha } p \text{ páratlan prím.}$$

<u>Biz</u>

$$\underset{\text{test}}{\mathbb{Z}_p} = \{0, \underbrace{\overset{g^{p-1}}{\overset{\parallel}{1}}, g, g^2, g^3, \ldots, g^{p-2}}_{p-1 \text{ db}}\} \qquad g \text{ prím elem} \quad g^{p-1} = 1.$$

- ha $a = 0$, akkor $a^{\frac{p-1}{2}} = 0$
- ha $a = g^{2k}$, akkor $a^{\frac{p-1}{2}} = g^{2k \cdot \frac{p-1}{2}} = g^{(p-1)k} = 1^k = 1$

~~ka~~ ↑ itt a kvadratikus maradék, mert $(g^k)^2 \equiv a \mod p$.

- ha $a = g^{2k+1}$, akkor $a^{\frac{p-1}{2}} = g^{(2k+1)\frac{p-1}{2}} = g^{\frac{p-1}{2}} = -1$

és itt nem kvadratikus maradék, mert

$$(g^t)^2 = g^{2k+1} \iff 2t \equiv 2k+1 \mod p-1 \ \lightning \ \text{páros!}$$

Ez volt éppen a Legendre szimbólum definíciója. ∎

(4)

Biz (második rész) A "legalább a fele" lemma bizonyításához hasonló. Legyen

$$H = \left\{ a \in \mathbb{Z}_n^* \;\middle|\; \left(\frac{a}{n}\right) = a^{\frac{n-1}{2}} \right\}$$ zárt a szorzásra $1 \in H$

ez részcsoportja a $\mathbb{Z}_n^*$ multiplikatív csoportnak, tehát elegendő találni egyetlen $a \in \mathbb{Z}_n^*$ elemet, amelyre $a \notin H$. Indirekt gondolatmenettel tegyük fel, hogy $H = \mathbb{Z}_n^*$. Mivel $\left(\frac{a}{n}\right) \in \{-1, 1\}$ (mert $a \neq 0$) ezért minden $\mathbb{Z}_n^*$ elemre $a^{n-1} = 1$, azaz n Carmichael szám! Tehát n négyzetmentes, páratlan és legalább 3 prímosztója van $n = p_1 p_2 \dots p_k$. Legyen g primitív gyök mod p_1 és kínai maradéktétellel válasszunk $x \in \mathbb{Z}_n^*$ elemet, hogy

$$x \equiv g \pmod{p_1}, \quad x \equiv 1 \pmod{p_2}, \dots, x \equiv 1 \pmod{p_k}$$

$$x^{\frac{p_2-1}{2}} \equiv 1 \pmod{p_2}$$

$$\left(\frac{x}{p_1}\right) = -1, \left(\frac{x}{p_2}\right) = 1, \dots, \left(\frac{x}{p_k}\right) = 1 \quad \text{azaz} \quad \left(\frac{x}{n}\right) = -1$$

Ez azt jelenti, hogy $x^{\frac{n-1}{2}} \equiv -1 \pmod{n}$, mert $x \in H$. De akkor $x^{\frac{n-1}{2}} \equiv -1 \bmod p_2$, de ez ellentmond annak a feltevésünknek, hogy $x \equiv 1 \bmod p_2$. ∎

mert p_2 páratlan.

Fermat-faktorizáció

Áll: Egy páratlan n egészet ugyan olyan nehéz valódi szorzatként felírni mint két négyzetszám különbségeként.

Biz: $n = b^2 - c^2 = (b-c)(b+c)$

$$n = xy = \left(\frac{x+y}{2}\right)^2 - \left(\frac{x-y}{2}\right)^2.$$

Áll: Ha találunk olyan b, c egészeket, hogy
$b^2 \equiv c^2 \pmod n$, $b \not\equiv c \pmod n$ és $b \not\equiv -c \pmod n$
akkor $\text{lnko}(n, b+c)$ valódi osztója n-nek.

Biz: $\text{lnko}(n, b+c) \neq n$ mert $n \nmid b+c$
Ha $\text{lnko}(n, b+c) = 1$ akkor $n \mid (b-c)(b+c)$
miatt $n \mid b-c$, ami ellentmond $b \not\equiv c \pmod n$-nek.

Def: Legyen $\text{mod}(x, n)$ a legkisebb abszolútértékű maradékja ($-\frac{n}{2} <$ és $\leq \frac{n}{2}$) x-nek.

Algoritmus: Keressünk sok b_i egészet úgy, hogy $\text{mod}(b_i^2, n)$ abszolút értéke kicsi legyen.

Mindegyiket írjuk fel -1 és prímek szorzatára

$$\text{mod}(b_i^2, n) = p_1^{\alpha_{i1}} \cdot p_2^{\alpha_{i2}} \cdot p_3^{\alpha_{i3}} \cdot \ldots \cdot p_k^{\alpha_{ik}}$$

ahol $p_1, \ldots, p_k \in \{-1\} \cup \{\text{prímek}\}$ és $\alpha_{ij} \in \mathbb{N}$.

Ha több egyenletünk van mint prímünk, akkor $\mathbb{Z}_2$-feletti lineáris egyenletrendszert megoldva találunk egy

$$b = b_1^{x_1} b_2^{x_2} \cdot \ldots \cdot b_t^{x_t}, \qquad x_i \in \{0,1\}$$

egészt, hogy $\mathrm{mod}(b^2, n) \equiv$ négyzetszám.

Megj.: jó választás b_i-re $\lfloor\sqrt{kn}\rfloor$ és $\lceil\sqrt{kn}\rceil$ kis k egészekre. $b_i^2 \approx kn$ ($kn = d^2$ külön kezeljük)

Példa: $n = 6887$ faktorizálása

k	b_i	$\mathrm{mod}(b_i^2, n)$	-1	primek: 163	2	5	17	3	53
1	82	-163	1	1					
1	83	2	0	0	1				
2	117	-85	1	0	0	1	1		
2	118	150	0	0	1	2	0	1	
3	143	-212	1	0	2	0	0	0	1
3	144	75	0	0	0	2	0	1	0

$O\left(e^{c\sqrt{\log n \cdot \log\log n}}\right)$

vonatok $b = 83 \cdot 118 \cdot 144$ = 0 0 2 4 0 2 0

$$\mathrm{mod}(b^2, n) = \underbrace{2 \cdot 150 \cdot 75}_{150^2} = (-1)^0 \cdot 163^0 \cdot 2^2 \cdot 5^4 \cdot 17^0 \cdot 3^2 \cdot 53^0$$

$c = 150$

Ell. $n \nmid b-c,\ b+c$

$\mathrm{mod}(b, n) = 5388$ ($b - c \bmod n$)

$\mathrm{lnko}(n, b-c) = \mathrm{lnko}(6887, 5238) = 97$

Azaz $\boxed{n = 97 \cdot 71}$