13.05.22

Problema logaritmului discret

- Se știe în orice corp finit și în mod deosebit în corpurile $\mathbb{Z}_p$, cu p = nr prim; $(\mathbb{Z}_p, +, \cdot)$ = corp comutativ faptul că fiecare număr în afară de 0 are un invers multiplicativ al acestuia corp finit există cel puțin un generator. În cazul corpului $(\mathbb{Z}_p, +, \cdot)$ acest grup este $(\mathbb{Z}_p^*, \cdot)$ și are $p-1$ elemente.

Fie g este unul dintre generatorii săi, atunci pentru orice clasă nenulă $a \pmod p$, există și este unic un număr x cuprins între 1 și $p-1$ astfel încât $g^x = a$. Numărul x cu această proprietate se numește logaritmul lui a în baza g:

$$g^x = a \iff x = \log_g a.$$

Funcția logaritmică astfel definită satisface proprietățile logaritmilor cunoscute din algebra clasică.

Trebuie menționat, însă următorul aspect: - în timp ce logaritmul (clasa nenulă $a \pmod p$) este de clasă mod. p, rezultatul se află în clasa resturilor $(p-1)$.

Deci problema logaritmului discret se poate formula astfel: „fiind dat generatorul g al corpului $(\mathbb{Z}_p, +, \cdot)$ și clasa nenulă $a \pmod p$, să se afle numărul x, cuprins între 1 și $p-1$, cu proprietatea $g^x = a \pmod p$.

Dacă numărul prim p este unic, atunci se pot găsi metode bune pentru calculul logaritmului discret. Dacă, însă, nr prim p este foarte mare, așa cum este în practică criptografică, nu există (încă) un algoritm potrivit pentru rezolvarea problemei:

Exemple

(1°) Fie un număr $p = 17$. Să se determine generatorii grupului $(\mathbb{Z}_{17}^*, \cdot)$ și pentru unul dintre generatorii găsiți să se rezolve problema logaritmului discret:

Rezolvare $p - 1 = 16$; $p - 1 = 16 = 2^4$,

- singurul divizor prim impar al lui $p - 1 = 16$, este $\frac{p-1}{d} = \frac{16}{2} = 8$.

$\mathbb{Z}_{17}^* = \{1, 2, 3, \dots, 16\}$. Pentru a verifica dacă $g \in \{2, 3, 4, \dots, 16\}$ este generator, vom calcula $g^8 \pmod{17}$. Dacă $g^8 \pmod{17} \neq 1$, atunci g este generator. Dacă $g^8 \pmod{17} = 1 \Rightarrow g$ nu este generator.

Fie $g = 2 \Rightarrow 2^8 = 256 = 1 \pmod{17} \Rightarrow g = 2$ nu este generator: $256 = 15 + \frac{1}{17} \Rightarrow 256 = 1 \pmod{17}$

Fie $g = 3 \Rightarrow g^8 = 3^8 = (3^4)^2 = 81^2 \pmod{17} = 6561 \pmod{17}$; $6561 = 385 + \frac{16}{17}$

$g^8 = 3^8 \pmod{17} = 16 \neq 1 \Rightarrow g = 3$ este generator.

Deoarece numerele 3, 5, 7, 9, 11, 13, 15 sunt prime cu $7 - 1 = 16$, rezultă că numerele $3^3, 3^5, 3^7, 3^9, 3^{11}, 3^{13}, 3^{15} \pmod{17} = \pmod{p}$ sunt, de asemenea, generatori.

Pentru $p = 17$ ($17 \in \mathbb{Z}_{17}^*$) și generatorul $g = 3$ logaritmii discreți vor rezulta din relația următoare: $g^x = a \Leftrightarrow x = \log_g a \Rightarrow x = \log_3 a$, unde $a \in \{1, 2, 3, \dots, 16\} = \text{celelalte } a \pmod{\frac{p-1}{2} = 16}$.

$\log_3 a$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$a = 3^k \pmod{17}$	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6	1

În prima linie a tabelului sunt elemente logaritmi în baza generatorului $g=3$ ai claselor a (modulo $p-1=16$).
$a \in \{1, 2, 3, \dots, 16\}$. Pe a doua linie sunt clasele $a = 3^x$ (mod. 17).
De constatat că 3 este generator al lui $(\mathbb{Z}_{17}^*, \cdot)$
$\{3^x \mid x \in \mathbb{N}\} = \mathbb{Z}_{17}^*$, a fiind de clasa mod.(17).

Exemplul (2)

Să se determine un generator pentru $(\mathbb{Z}_{13}^*, \cdot)$ și pentru el să se rezolve problema logaritmilor discreți.

→ $p=13 \Rightarrow p-1 = 12 = 4 \cdot 3 = 2^2 \cdot 3$

→ divizorii principali ai lui $p-1=12$ sunt:
$d_1 = \frac{12}{2} = 6$; $d_2 = \frac{12}{3} = 4$ $\left(\frac{p-1}{p_i}\right)$.

Fie $g \in \{2, 3, 4, \dots, 12\}$. Pt a vedea dacă g e generator, vom calcula $g^{d_1} = g^6 \pmod{13}$ și $g^{d_2} = g^4 \pmod{13}$.
Dacă $g^{d_i} \neq 1$ pt $i=\overline{1,2}$ ⇒ g este generator.
Dacă contrar nu și se alege alt g.
În cazul nostru
Fie $g=2 \Rightarrow \begin{cases} g^{d_1} = 2^6 = 64 \pmod{13} = 12 \neq 1 \\ g^{d_2} = 2^4 = 16 \pmod{13} = 3 \neq 1 \end{cases} \Rightarrow$

⇒ $g=2$ este generator. 5, 7, 11 ($< 12 = p-1$) sunt prime; deoarece numerele 5, 7, 11 sunt, de[?] cu $p-1=12$, rezultă că și 2^5, 2^7, 2^{11} sunt, de asemenea, generatori pt $(\mathbb{Z}_{13}^*, \cdot)$ ai unei clase

Problema logaritmilor discreți

$a \in \{1, 2, 3, \dots, 12\}$, și ecuația $g^x = a$; $g=2$
Fie $\in \{1, 2, \dots, 12\}$ și construim tabelul
⇒ $x = \log_g a \iff x = \log_2 a$.

$a = 2^x \pmod{13}$	2	4	8	3	6	12	11	9	5	10	7	1
$x = \log_2 a$	1	2	3	4	5	6	7	8	9	10	11	12

Pe prima linie sunt trecute puterile lui 2 pt $x \in \{1, 2, 3, \dots, 12\} \pmod{p-1}$.
Se constată că 2 este generator $\{2^n \mid n \in \mathbb{N}^*\} = \mathbb{Z}_{13}^* \pmod{13}$ și are 12 clase mod. 13.

Pe a doua linie sunt trecuți logaritmii discreți ai claselor $a \pmod{p-1 = 12}$; $x = \log_2 a$

Temă: Aceeași problemă pentru $(\mathbb{Z}_{19}, \cdot)$

Probleme propuse

(I) Să determine un generator pentru grupurile ciclice următoare: $(\mathbb{Z}_p^*, \cdot)$, unde:

$p = 109$; $p = 809$
$p = 211$; $p = 907$
$p = 661$; $p = 1009$
$p = 701$

(II) Să se determine indicatorul lui Euler pentru $n \in \mathbb{N}^*$, următoarele:

$n = 58$
$n = 64$
$n = 72$
$n = 88$
$n = 96$

Dacă $n = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_r^{k_r} \Rightarrow$
$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_r}\right)$$

Teorema lui Euler: Dacă $n \geq 2$ și $a \in \mathbb{Z}$, a este prim cu n, atunci $a^{\varphi(n)} \equiv 1 \pmod{n}$

Exemple rezolvate

Să se calculeze caracteristica lui Euler ($\varphi(n)$) pentru următoarele valori ale lui n:

1° $n = 18$; $(\mathbb{Z}_{18}^*, \cdot) = \{\hat{1}, \hat{2}, \hat{3}, \dots, \hat{17}\}$.

$n = 18 = 2 \cdot 9 = 2 \cdot 3^2 = p_1^{k_1} \cdot p_2^{k_2} \Rightarrow$
$p_1 = 2$; $p_2 = 3 \Rightarrow \varphi(18) = 18\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) =$
$= 18 \cdot \frac{1}{2} \cdot \frac{2}{3} = 6 \Rightarrow \varphi(18) = 6$;

= nr. natural care este prim cu 18 din $\mathbb{Z}_{18}^*$:

$U(\mathbb{Z}_{18}) = \{\hat{1}, \hat{5}, \hat{7}, \hat{11}, \hat{13}, \hat{17}\}$. Și $(U(\mathbb{Z}_{18}), \cdot)$ = grup abelian

$(\mathbb{Z}_{18}^*, \cdot)$ = monoid. $\text{card}(U(\mathbb{Z}_{18}^*)) = \varphi(18)$

2° $n = 100$; $\varphi(100) = ?$; $\mathbb{Z}_{100}^* = \{\hat{1}, \hat{2}, \hat{3}, \dots, \hat{99}\}$.

$\varphi(100)$ = nr. de elemente prime cu 100.

$100 = 4 \cdot 25 = 2^2 \cdot 5^2 \Rightarrow p_1 = 2;\ p_2 = 5$

$\varphi(100) = 100\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) = 100\left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{5}\right) =$

$= 100 \cdot \frac{1}{2} \cdot \frac{4}{5} = 40$

3° La se calculeze probabilitatea ca alegând, la întâmplare, un element din mulțimea $\{1, 2, 3, \dots, 1000\}$ acesta să fie număr prim.

$\varphi(1000)$ = nr. natural de elemente din $\mathbb{Z}_{1000}^*$, prime cu 1000 = nr. natural de numere naturale.

$1000 = 10^3 = 2^3 \cdot 5^3 \Rightarrow p_1 = 2;\ p_2 = 5$

$\varphi(1000) = 1000\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 1000 \cdot \frac{1}{2} \cdot \frac{4}{5} = \frac{4000}{10} = 400$

$P(E) = \frac{400}{1000} = \frac{4}{10} = \frac{2}{5}$