11.05.2022

Generatori ai unui grup ciclic (An 1 zi)

Fie $(G, \cdot)$ un grup ciclic de ordinul n. Dacă se cunoaște un generator g al grupului atunci putem determina toți generatorii grupului $(G, \cdot)$: aceștia sunt elementele de forma g^k, unde $k \in \mathbb{N}$, $k < n$ și prim cu n; $(k, n) = 1$.

Numărul acestor generatori este egal cu $\varphi(n)$ = caracteristica lui Euler, = numărul elementelor inversabile din grupul $\mathbb{Z}_n$; = numărul elementelor lui $(U(\mathbb{Z}_n), \cdot)$ = grupul unităților lui $(\mathbb{Z}_n^*, \cdot)$.

Dacă $n = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_r^{k_r}$ unde p_i sunt numere prime, factorii primi ai lui n, atunci avem deci că

$$\frac{\varphi(n)}{n} = \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right) = \frac{\text{nr. cazurilor favorabile}}{\text{nr. cazurilor posibile}}$$

Raportul $\frac{\varphi(n)}{n}$ reprezintă probabilitatea de alegere a unui generator al grupului și această probabilitate nu depinde, constatăm că, de exponenții $k_1, k_2, \ldots, k_r$ ai factorilor primi distincți, ci numai de aceștia, $p_1, p_2, \ldots, p_r$ ai lui n.

Deci, dacă nu cunoaștem nici un generator al grupului și dorim să obținem unul, atunci alegem la întâmplare un element al grupului și verificăm dacă este generator. Acest lucru este posibil cu probabilitatea menționată anterior.

Pentru a verifica dacă un element g este generator va trebui să calculăm toate puterile lui g până la puterea $n-1$ și să constatăm că nici una nu este egală cu elementul neutru al grupului; conform teoremei următoare.

Teoremă: Dacă $p-1 = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_r^{k_r}$ este descompunerea în factori primi a numărului

$p-1$, atunci condiția necesară și suficientă ca g să fie generator este ca toate clasele $g^{d_i} \pmod p$ să fie diferite de clasa unitate, $d_i = \frac{p-1}{p_i}$, $i = \overline{1,k}$ pe unde p_i sunt divizorii primi ai numărului $p-1$.

Clasele $g^{d_i} \pmod p$ se pot obține prin calcule direct dacă p este mic. În practica criptografică însă, numărul p, prim, trebuie să fie foarte mare. În acest caz, pentru determinarea unui generator se utilizează un algoritm special unui algoritm polinomial de exponențiere modulo p.

Menționăm, însă, că algoritmul nu oferă un generator, ci doar permite verificarea faptului că elementul ales g este sau nu un generator. Când se știe p este foarte mare, este posibil să fie necesar un număr foarte mare de verificări și calcule pentru a obține un generator. Dacă nu există un algoritm polinomial pentru rezolvarea problemei:

În prezent s-au făcut și se fac pași importanți în următoarele direcții:

a) încercări de demonstrare a inexistenței unui astfel de algoritm polinomial

b) utilizarea unor artificii de rezolvare a problemei pentru numere suficient de mari, apropiindu-se astfel de glanța dintre polinomial și exponențial.

Algoritmul polinomial de exponențiere modulo p

Fie p un număr prim. De exemplu, $p = 101$ Se propune să calculăm clasa lui $3^{1000} \pmod{101}$. Evident că în loc de $g = 3$ se poate lua orice altă clasă de resturi modulo p al cărui $\gamma - 1$

a) în cât de mare numărul natural poate fi.

Etapele algoritmului

(1°) Se scrie exponentul 1000 în baza 2

$1000_{10} = 1111101000_2 = 2^9 + 2^8 + 2^7 + 2^6 + 2^5 + 2^3 \Rightarrow$

$3^{1000} = 3^{2^9 + 2^8 + 2^7 + 2^6 + 2^5 + 2^3} = 3^{2^9} \cdot 3^{2^8} \cdot 3^{2^7} \cdot 3^{2^6} \cdot 3^{2^5} \cdot 3^{2^3}$

(2°) Pornind de la ultimul $3^k \pmod{101}$ unde $k \in \{2^1, 2^2, 2^3, 2^4, \dots 2^8, 2^9\}$, rezultatele se trec într-un tabel de forma următoare:

k	2^1	2^2	2^3	2^4	2^5	2^6	2^7	2^8	2^9
3^k	9	81	97	16	54	88	68	79	80

$\Rightarrow 3^{1000} \pmod{101} = 3^{2^9} \cdot 3^{2^8} \cdot 3^{2^7} \cdot 3^{2^6} \cdot 3^{2^5} \cdot 3^{2^3} =$

$= \underbrace{97 \cdot 54 \cdot 88}_{460944} \cdot \underbrace{68 \cdot 79 \cdot 80}_{429760} = 81 \cdot 5 = 405 = 1 \pmod{101}$

Exemplu de calcul al generatorilor lui $(\mathbb{Z}_{17}^*, \cdot)$

(*) $p = 17 =$ nr prim.

(**) calculăm $p - 1 = 17 - 1 = 16 = 2^4 \Rightarrow$ ordinul elementelor maximal al lui $A - 1 = \frac{p-1}{2} = \frac{16}{2} = 8$

(***) Alegem un $g \in \{2, 3, 4, \dots, 16\} : g \in \mathbb{Z}_p^*$

Calculăm $g^8 \pmod{17}$.

Dacă $g^8 \pmod{17} \neq 1 \Rightarrow g$ este generator

Ex: $g = 2 \Rightarrow 2^8 = 256 = 1 \pmod{17}$

$\frac{256}{17} = 15 + \frac{1}{17} \Rightarrow g = 3$ nu este generator

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

$\Rightarrow 3^8 \pmod{17} = 16 \pmod{17} \neq 1 \Rightarrow$

$\Rightarrow g \Rightarrow$ este generator.

Deci sunt numerele 3, 5, 7, 9, 11, 13, 15 sunt

Știm că $16 = p-1 \Rightarrow$ ar $3^1, 3^5, 3^7, 3^9, 3^{11}, 3^{13}, 3^{15} \pmod{17}$ sunt de asemenea generatori (conform teoremei) dar se verifică printr-un calcul analog.

Algoritmul de verificare al unui generator (cazul general)

Rezultă din teorema 1:

(1°) Fie p un prim $\Rightarrow (\mathbb{Z}_p^*, \cdot)$ este grup ciclic.
$p-1 = p_1^{k_1} \cdot p_2^{k_2} \cdots p_n^{k_n}$ = descompunerea lui $p-1$ în factori primi (reducerea lui).

(2°) Se calculează divizorii proprii ai lui $p-1$:
$d_1 = \frac{p-1}{p_1}$; $d_2 = \frac{p-1}{p_2}$, ... $d_n = \frac{p-1}{p_n}$;

(3) Se alege un element $g \in \{2, 3, \dots, p-1\}$. Pentru a verifica dacă g este un generator al lui $\mathbb{Z}_p^*$, se calculează $g^{d_i} \pmod p$, pentru $\forall i \in \{1, 2, \dots, n\}$
→ dacă $\exists i$ a.î. $g^{d_i} \pmod p = 1$, atunci g nu este generator al lui $(\mathbb{Z}_p^*, \cdot)$
→ dacă $g^{d_i} \pmod p \neq 1$ pentru $\forall i = \overline{1,n}$, atunci g este generator al lui $(\mathbb{Z}_p^*, \cdot)$

Exemplu Fie $p = 631$ (nr. prim). Vrem să verificăm dacă $g = 5$ este generator pentru $(\mathbb{Z}_{631}^*, \cdot)$

Etapa 1. $p-1 = 630$ ⇒ se descompune în factori primi: $630 = 2 \cdot 3^2 \cdot 5 \cdot 7$

Etapa 2 Se calculează divizorii proprii ai lui $p-1 = 630$; $d_1 = \frac{630}{2} = 315$; $d_2 = \frac{630}{3} = 210$; $d_3 = \frac{630}{5} = 126$;
$d_4 = \frac{630}{7} = 90$.

Etapa 3: Se scrie fiecare divizor proprie în baza 2:

$315 = 100111011 = 2^8 + 2^5 + 2^4 + 2^3 + 2^1 + 2^0$
$210 = 11010010 = 2^7 + 2^6 + 2^4 + 2^1$
$126 = 1111110 = 2^6 + 2^5 + 2^4 + 2^3 + 2^2 + 2^1$
$90 = 1011010 = 2^6 + 2^4 + 2^3 + 2^1$

Avem $g=5$; verificăm dacă este generator.

Etapa 1: Se calculează, pornind de la clasa 5, și înlocuim consecutiv cu pașii, modulo 631:

	2^0	2^1	2^2	2^3	2^4	2^5	2^6	2^7	2^8
k	1	2	4	8	16	32	64	128	256
$5^k \pmod{631}$	5	25	625	36	34	525	509	371	83
3^k	3	9	81	251	532	336	578	285	457

pentru $g=5$: Se calculează 5^{d_i} pentru fiecare d_i cu algoritmul lui Rabin-Miller de exponențiere (mod 631)

$5^{90} = 5^{2+2^3+2^4+2^6} = 5^2 \cdot 5^{2^3} \cdot 5^{2^4} \cdot 5^{2^6} = 25 \cdot 36 \cdot 34 \cdot 509 = 427$

$5^{126} = 5^2 \cdot 5^{2^2} \cdot 5^{2^3} \cdot 5^{2^4} \cdot 5^{2^5} \cdot 5^{2^6} = 25 \cdot 625 \cdot 36 \cdot 34 \cdot 525 \cdot 509 =$

$= 15625 \cdot 1224 \cdot 267225 = 481 \cdot 593 \cdot 312 = 242 \pmod{631}$

$5^{210} = 5^2 \cdot 5^{2^4} \cdot 5^{2^6} \cdot 5^{2^7} = 25 \cdot 34 \cdot 509 \cdot 371 = 219 \cdot 170 = 1 \pmod{631}$

$5^{315} = \dots = 464 \pmod{631}$

Deoarece unul dintre rezultate este egal cu 1 (mod 631) $\Rightarrow g=5$ nu este generator.

Exemplu: Se verifică dacă $g=3$ este generator.

- Se calculează 3^{d_i}, $\forall d_i$:

$3^{90} = 269$
$3^{126} = 555$
$3^{210} = 587$
$3^{315} = 630$

$\Rightarrow$ toate rezultatele sunt diferite de clasa 1. $\Rightarrow g=3$ este generator al $(\mathbb{Z}_{631}^*, \cdot)$

Mai rezultă că 3^{d_i}, unde d_i sunt prime cu 630, sau, altfel spus, generatorii ai lui $(\mathbb{Z}_{631}^*, \cdot)$.