Примітивний елемент

Означення. Нехай $x \in Z_n^*$. ***Порядком*** числа x називається таке найменше натуральне число k, що $x^k \equiv 1 \pmod{n}$ та позначається $\text{ord}(x)$.

Твердження. Якщо $\text{ord}(x) = k$, $x^t \equiv 1 \pmod{n}$, то t ділиться на k. Зокрема, k ділить $\varphi(n)$.

Приклад. Нехай $n = 21$. $Z_{21}^* = \{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$. $\varphi(21) = \varphi(3) * \varphi(7) = 2 * 6 = 12$. Порядок елементів множини Z_{21}^* наведено у таблиці.

$x \in Z_{21}^*$	1	2	4	5	8	10	11	13	16	17	19	20
порядок x	1	6	3	6	2	6	6	2	3	6	6	2

Означення. Нехай $g \in Z_n^*$. Якщо порядок g дорівнює порядку групи Z_n^* ($\text{ord}(g) = |Z_n^*| = \varphi(n)$), то число g називається ***генератором*** або ***примітивним елементом або первісним коренем*** Z_n^*. Якщо Z_n^* має генератор, то множина Z_n^* називається ***циклічною***.

Властивості генераторів

1. Z_n^* має генератор тоді і тільки тоді, коли $n = 2, 4, p^k, 2 * p^k$, де p – непарне просте число та $k \geq 1$. Зокрема, якщо p просте, то Z_p^* має генератор.
2. Якщо g – генератор Z_n^*, то $Z_n^* = \{g^i \bmod n \mid 0 \leq i \leq \varphi(n) - 1\}$.
3. Нехай g – генератор Z_n^*. Тоді $b = g^i \bmod n$ є також генератором Z_n^* тоді і тільки тоді, коли НСД(i, $\varphi(n)$) = 1. Якщо множина Z_n^* є циклічною, то її кількість генераторів дорівнює $\varphi(\varphi(n))$.
4. Число $g \in Z_n^*$ є генератором Z_n^* тоді і тільки тоді, коли $g^{\phi(n)/p} \neq 1 \pmod{n}$ для кожного простого дільника p числа $\varphi(n)$.

Приклад. Множина Z_{21}^* не є циклічною, тому що вона не містить елементу, порядок якого дорівнює $\varphi(21) = 12$. Число 21 не задовольняє властивості 1 генераторів. Множина Z_{25}^* є циклічною, її генератором є 2.

Приклад. Множина Z_{13}^* має генератор g = 2.

n	1	2	3	4	5	6
$2^n \pmod{13}$	2	4	8	3	6	12

n	7	8	9	10	11	12
$2^n \pmod{13}$	11	9	5	10	7	1

$g = 4$ не є генератором множини Z_{13}^*, але є генератором її підмножини.

n	1	2	3	4	5	6
$4^n \pmod{13}$	4	3	12	9	10	1

Якщо група має генератор, то на поточний час не існує поліноміального алгоритму, який буде знаходити всі генератори групи.

Твердження. Нехай p – просте, g – генератор Z_p^*. Тоді рівність

$$g^a = g^b * g^c \pmod{p}$$

має місце тоді і тільки тоді, коли

$$a = b + c \pmod{p - 1}$$

Звідси випливає існування гомоморфізму f: $Z_p^* \to Z_{p-1}$.

Приклад. Розглянемо групу Z_{13}^*, генератором якої є $g = 2$. Тоді з рівності

$$2^{17} = 2^2 * 2^3 \pmod{13}$$

випливає рівність

$$17 = 2 + 3 \pmod{12}$$

Теорема 1. Нехай p – просте число, $p - 1 = p_1^{e_1} p_2^{e_2} ... p_k^{e_k}$ – розклад на множники порядка групи Z_p^* ($|Z_p^*| = \varphi(p) = p - 1$). Елемент g буде примітивним елементом групи Z_p^* тоді і тільки тоді, коли

$$g^{\frac{p-1}{p_i}} \neq 1 \pmod{p},\ 1 \le i \le k$$

Доведення. Елемент g буде примітивним елементом тоді і тільки тоді, коли його порядок дорівнює порядку групи: $\text{ord}(g) = |Z_p^*| = p - 1$. Якщо для деякого i, $1 \le i \le k$, має місце рівність

$$g^{\frac{p-1}{p_i}} = 1 \pmod{p},$$

то $\text{ord}(g) \le \frac{p-1}{p_i} < p - 1$, тобто порядок g не дорівнює порядку Z_p^* і в такому разі не може бути примітивним елементом.

Твердження. Z_p^* має точно $\varphi(p - 1)$ примітивних елементів.

Теорема 2. Нехай p та p_1 – прості числа, при чому $p = 2p_1 + 1$, $g \in Z_p^*$, $g \neq \pm 1 \bmod p$. Тоді g буде примітивним елементом тоді і тільки тоді, коли

$$g^{\frac{p-1}{2}} \neq 1 \pmod{p}$$

Доведення. $g^{\frac{p-1}{2}} \equiv g^2 \equiv 1$ тоді і тільки тоді, коли $g = \pm 1 \bmod p$. А дільниками порядка групи Z_p^* як раз і є значення 2 та $p_1 = \frac{p-1}{2}$.

Теорема 3. Нехай p та p_1 – прості числа, при чому $p = 2p_1 + 1$, $g \in Z_p^*$, $g \neq \pm 1 \bmod p$. Якщо g не примітивний елемент, то елемент $(-g)$ буде примітивним.

Доведення. Якщо $g \neq \pm 1 \bmod p$, але g не примітивний елемент, то $g^{\frac{p-1}{2}} = 1 \pmod p$. Тоді $(-g)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} * g^{\frac{p-1}{2}} \pmod p \equiv (-1)^{\frac{p-1}{2}} \pmod p \equiv -1 \pmod p$, тобто $(-g)$ є примітивним елементом.

Наслідок. Існує поліноміальний алгоритм обчислення примітивного елемента для Z_p^*, якщо p та $\frac{p-1}{2}$ є простими.

Для знаходження генератора групи достатньо обрати довільний елемент $g \in Z_p^*$ та перевірити, чи є він генератором. Якщо ні – то генератором буде елемент $(-g) \equiv p - g$.

Приклад. Знайти примітивні елементи в групі Z_{11}^*.

В даному випадку $p = 11$ та $(p - 1) / 2 = 5$ – прості. Значення g, для яких $g = \pm 1 \bmod 11$, генераторами не будуть (таких значення два: $g = 1$, $g = 10$). Кількість генераторів групи Z_{11}^* дорівнює $\varphi(10) = (2 - 1) * (5 - 1) = 4$.

Достатньо перевірити, чи є примітивними елементами $g = 2, 3, 4, 5$. Якщо це так, то елемент $11 - g$ примітивним не буде. І навпаки, якщо g не є примітивним елементом, то таким буде $11 - g$. Складемо таблицю $g^{\frac{p-1}{2}} \pmod p = g^5 \pmod{11}$:

g	2	3	4	5
g^5	10	1	1	1

Елемент $g = 2$ буде примітивним оскільки $2^5 \neq 1 \pmod{11}$, а $g = 3, 4, 5$ – ні. Отже всією множиною примітивних елементів у Z_{11}^* будуть $g = \{2, 11 - 3, 11 - 4, 11 - 5\} = \{2, 8, 7, 6\}$.

Відповідь: примітивними елементами в Z_{11}^* будуть $g = \{2, 6, 7, 8\}$.

Наступний алгоритм знаходить примітивний елемент в циклічній групі G та базується на теоремі 1: для того щоб едемент g був генератором G, необхідно і достатньо щоб значення виразу $g^{|G|/p_i}$ не дорівнювало 1 (p_i – дільники порядка групи G). Оскільки циклічна група G порядку n має $\varphi(n)$ генераторів, то ймовірність того що перше навмвння обране число $g \in G$ буде примітивним елементом, дорівнює $\varphi(n)/n$.

Алгоритм

Вхід: циклічна група Z_n^* порядку $\varphi(n) = p_1^{k_1} p_2^{k_2} ... p_s^{k_s}$.

Вихід: генератор g групи Z_n^*.

1. Обрати довільний елемент g із Z_n^*;
2. for $i \leftarrow 1$ to s do

    2.1. Обчислити $b \leftarrow g^{\varphi(n)/p_i} \bmod n$;

    2.2. if ($b = 1$) then goto 1;
3. return(g);

Приклад. Знайти генератор групи Z_{139}.

Обчислимо порядок групи Z_{139}: $|Z_{139}| = \varphi(139) = 138$. Розкладемо число 138 на прості множники: 138 = 2 * 3 * 23. Кількість генераторів Z_{139} дорівнює $\varphi(138) = \varphi(2) * (3) * (23) = 1 * 2 * 22 = 44$. Ймовірність того що взяте довільним чином число із Z_{139} є генератором, дорівнює 44 / 138 ≈ 0.31. Число 138 має три дільника. Тому для того, щоб превірити чи є генератором навмання обране $g \in Z_{139}$, достатньо обчислити значення $g^{138/2} \bmod n$, $g^{138/3} \bmod n$, $g^{138/23} \bmod n$ та впевнитися що вони не дорівнюють 1.

g	$g^{69} \bmod n$	$g^{46} \bmod n$	$g^{6} \bmod n$
64	1		
8	138	1	
99	1		
76	138	1	
70	138	42	63

[24] стор.138