Квадратичні лишки. Символи Лежандра та Якобі

Означення. Число $a \in Z_n^*$ називається *квадратичним лишком* або *квадратом* за модулем n, якщо існує таке $x \in Z_n^*$, що $x^2 \equiv a \pmod n$. Якщо такого x не існує, то число a називається квадратичним нелишком. Множина усіх квадратичних лишків за модулем n позначається через Q_n, нелишків – через $\overline{Q}_n$. За означенням $0 \notin Z_n^*$, отже $0 \notin Q_n$ та $0 \notin \overline{Q}_n$.

Теорема. Нехай p – непарне просте число, g – генератор Z_p^*. Тоді число a є квадратичним лишком за модулем p тоді і тільки тоді, коли $a = g^i \pmod p$, де i – парне ціле.

Доведення. Якщо $a = g^{2k} \pmod p$, то $a = b^2 \pmod p$, де $b = g^k \pmod p$.

Нехай $a = g^k \pmod p$ – елемент Z_p^*. Піднесемо його до квадрату:

$a^2 = g^{2k} \pmod p \equiv g^i \pmod p$. Оскільки $2k \pmod{p-1} = i$ – парне число, то звідси і випливає твердження про те що квадрат довільного елемента $a \in Z_p^*$ представляється у вигляді $g^i \pmod p$ лише для парного i.

Наслідок. $|Q_p| = (p-1)/2$, $|\overline{Q_p}| = (p-1)/2$.

Тобто половина елементів Z_p^* є квадратичними лишками, а половина – ні.

Приклад. Число $a = 3$ є генератором Z_7^*. Степені a наведені у наступній таблиці

I	0	1	2	3	4	5	6
$a^i \bmod 7$	1	3	2	6	4	5	1

Звідси $Q_7 = \{1, 2, 4\}$, $\overline{Q}_7 = \{3, 5, 6\}$.

Схема множення кважратичних лишків та нелишків аналогічна схемі додавання парних та непарних цілих чисел:

лишок * лишок = лишок
лишок * нелишок = нелишок
нелишок * нелишок = лишок

Приклад. Дослідимо операції множення лишків та нелишків в групі Z_7^*.

$2 \in Q_7, 4 \in Q_7 : 2 * 4 = 8 \equiv 1 \in Q_7$
$2 \in Q_7, 5 \in \overline{Q}_7 : 2 * 5 = 10 \equiv 3 \in \overline{Q}_7$
$5 \in \overline{Q}_7, 6 \in \overline{Q}_7 : 5 * 6 = 30 \equiv 2 \in Q_7$

Твердження. Нехай n – добуток двох різних простих чисел p та q, $n = p * q$. Тоді число $a \in Z_n^*$ є квадратичним лишком за модулем n тоді і тільки тоді, коли $a \in Q_p$ та $a \in Q_q$. Звідси $|Q_n| = |Q_p| * |Q_q| = (p - 1)(q - 1) / 4$ та $|\overline{Q_n}| = 3 (p - 1)(q - 1) / 4$.

Приклад. Нехай $n = 21$. Тоді $|Q_{21}| = (2 * 6) / 4 = 3$, $Q_{21} = \{1, 4, 16\}$,
$|\overline{Q}_{21}| =. (3 * 2 * 6) / 4 = 9$, $\overline{Q}_{21} = \{2, 5, 8, 10, 11, 13, 17, 19, 20\}$.

Означення. Нехай $a \in Q_n$. Якщо $x \in Z_n^*$ задовольняє $x^2 \equiv a \pmod n$, то x називається *квадратним коренем* числа a за модулем n.

Означення. Нехай p – просте, a – ціле число. Символ Лежандра $\left(\frac{a}{p}\right)$ визначається так:

$$\left(\frac{a}{p}\right) = \begin{cases} 0, \textit{ якщо } a \textit{ ділиться на } p \\ 1, \textit{ якщо } a \in Q_p \\ -1, \textit{ якщо } a \in \overline{Q}_p \end{cases}$$

Критерій Ейлера. Число a, яке не ділиться на непарне просте p, є квадратичним лишком за модулем p тоді і тільки тоді, коли $a^{\frac{p-1}{2}} \equiv 1 \pmod p$, і квадратичним нелишком тоді і тільки тоді коли $a^{\frac{p-1}{2}} \equiv -1 \pmod p$.

Доведення. За теоремою Ферма $a^{p-1} \equiv 1 \pmod p$ при НСД(a, p) = 1 та НСД(2, p) = 1. Або:

$$\left(a^{\frac{p-1}{2}} + 1\right) * \left(a^{\frac{p-1}{2}} - 1\right) \equiv 0 \bmod p$$

Звідси вираз в одній із дужок ділиться на p. Обидві дужки не можуть ділитися на p, оскільки тоді на p ділилася б і їх різниця, яка дорівнює 2, а за умовою теореми p – непарне просте число. Якщо a є квадратичним лишком, то $a = x^2 \pmod p$ для деякого такого x, що НСД(x, p) = 1. Маємо: $a^{\frac{p-1}{2}} \equiv \left(x^2\right)^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \bmod p$, тобто $a^{\frac{p-1}{2}} \equiv 1 \bmod p$ або $a^{\frac{p-1}{2}} - 1$ ділиться на p. Якщо a є квадратичним нелишком, то $a^{\frac{p-1}{2}} - 1$ не ділиться на p, звідки $a^{\frac{p-1}{2}} + 1$ повинно ділитися на p, або $a^{\frac{p-1}{2}} \equiv -1 \bmod p$.

Наслідок. $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$. Якщо число a є квадратичним лишком за модулем p, то за означенням символа Лежандра $\left(\frac{a}{p}\right) = 1$, а за критерієм Ейлера $a^{\frac{p-1}{2}} \pmod{p} \equiv 1$. Відповідно якщо число a є квадратичним нелишком за модулем p, то $\left(\frac{a}{p}\right) = -1$ і $a^{\frac{p-1}{2}} \pmod{p} \equiv -1$, звідки і випливає твердження.

Приклад. Чи існує розв'язок рівняння $x^2 \equiv 5 \pmod 7$.

Якщо існує розв'язок рівняння, то число 5 повинно бути квадратичним лишком за модулем 7. Перевіримо це за критерієм Ейлера:

$5^{\frac{7-1}{2}} \equiv 5^3 \pmod 7 \equiv 25 * 5 \pmod 7 \equiv 4 * 5 \pmod 7 \equiv 20 \pmod 7 \equiv -1 \pmod 7$. Звідси випливає, що 5 є квадратичним нелишком за модулем 7 і рівняння розв'язків не має.

Властивості символа Лежандра.

1. $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$. Вказана властивість є наслідком критерія Ейлера.

Зокрема $\left(\frac{1}{p}\right) = 1$ та $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

Отже $-1 \in Q_p$ якщо $p \equiv 1 \pmod 4$ та $-1 \in \overline{Q}_p$ якщо $p \equiv 3 \pmod 4$.

2. $\left(\frac{a*b}{p}\right) = \left(\frac{a}{p}\right)*\left(\frac{b}{p}\right)$. Властивість випливає з послідовності очевидних порівнянь:

$$\left(\frac{a*b}{p}\right) \equiv (ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} * b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)*\left(\frac{b}{p}\right) \pmod{p}.$$

Зокрема, якщо $a \in Z_p^*$, то $\left(\frac{a^2}{p}\right) = 1$ та $\left(\frac{a^2 b}{p}\right) = \left(\frac{b}{p}\right)$.

3. Якщо $a \equiv b \pmod{p}$, то $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$. Властивість випливає з того, що числа одного класа є одночасно або квадратичними лишками, або нелишками. Випливаючи з цієї властивості, можна записати: $\left(\frac{a}{p}\right) = \left(\frac{a+pt}{p}\right)$, $t \in Z$.

4. $\left(\frac{1}{p}\right)$ = 1. Одиниця є квадратичним лишком для довільного непарного простого p. Ця властивість випливає з того, що порівняння $x^2 \equiv 1 \pmod p$ завжди має розв'язки $x = \pm 1 \pmod p$.

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

Якщо p = 8k ± 1, то $\frac{p^2-1}{8} = \frac{(8k\pm1)^2-1}{8} = \frac{64k^2\pm16k}{8}$ = $8k^2 \pm 2k$ – парне число.

Якщо $p = 8k \pm 3$, то $\frac{p^2-1}{8} = \frac{(8k\pm3)^2-1}{8} = \frac{64k^2\pm48k+8}{8}$ = $8k^2 \pm 6k + 1$ – непарне число.

Отже $\left(\frac{2}{p}\right)$=1, якщо $p \equiv 1$ або 7 (mod 8) та $\left(\frac{2}{p}\right)$= -1, якщо $p \equiv 3$ або 5 (mod 8).

6. Закон взаємності непарних простих чисел. Якщо p – просте непарне число, відмінне від q, то

$$\left(\frac{p}{q}\right) * \left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

Помноживши цю рівність на $\left(\frac{p}{q}\right)$, отримаємо: $\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} * \left(\frac{p}{q}\right)$. Якщо виконується хоча б одна з рівностей $p \pmod 4 \equiv 1$ чи $q \pmod 4 \equiv 1$, то $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$, інакше $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$.

Символ Якобі є узагальненням символу Лежандра на випадок коли n є непарним, але не обовя'язково простим.

Означення. Нехай n – непарне ціле число, n ≥ 3. Відомо, що $n = p_1^{k_1} p_2^{k_2} \ldots p_t^{k_t}$, де p_i – прості числа. Символ Якобі $\left(\frac{a}{n}\right)$ визначається так:

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{k_1}\left(\frac{a}{p_2}\right)^{k_2}\ldots\left(\frac{a}{p_t}\right)^{k_t}$$

Зазначимо, що якщо n просте, то символ Якобі стає символом Лежандра.

Властивості символа Якобі

1. $\left(\frac{a}{n}\right)$ може приймати одне з трьох значень: -1, 0 чи 1. При цьому $\left(\frac{a}{n}\right) = 0$ тоді і тільки тоді коли НСД(a, n) $\neq 1$.

2. $\left(\frac{a*b}{n}\right) = \left(\frac{a}{n}\right)*\left(\frac{b}{n}\right)$. Якщо $a \in Z_n^*$, то $\left(\frac{a^2}{n}\right) = 1$.

3. $\left(\frac{a}{m*n}\right) = \left(\frac{a}{m}\right)*\left(\frac{a}{n}\right)$.

4. Якщо $a \equiv b \pmod{n}$, то $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$.

5. $\left(\frac{1}{n}\right) = 1$.

6. $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$. Отже $\left(\frac{-1}{n}\right) = 1$, якщо $n \equiv 1 \pmod 4$ та $\left(\frac{-1}{n}\right) = -1$, якщо $n \equiv 3 \pmod 4$.

7. $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$.

Отже $\left(\frac{2}{n}\right) = 1$, якщо $p \equiv 1$ або $7 \pmod 8$ та $\left(\frac{2}{n}\right) = -1$, якщо $p \equiv 3$ або $5 \pmod 8$.

8. $\left(\frac{m}{n}\right) = \left(\frac{n}{m}\right)(-1)^{\frac{(m-1)(n-1)}{4}}$.

З властивостей символу Якобі випливає, що якщо n непарне, а число a подати у вигляді $a = 2^k a_1$, де a_1 – непарне число, то

$$\left(\frac{a}{n}\right) = \left(\frac{2^k}{n}\right)\left(\frac{a_1}{n}\right) = \left(\frac{2^k}{n}\right)\left(\frac{n \bmod a_1}{a_1}\right)(-1)^{\frac{(a_1-1)(n-1)}{4}}$$

Ця формула дає можливість обчислити значення символа Якобі не маючи розкладу числа n на прості множники.

На відміну від символу Лежандра, символ Якобі $\left(\frac{a}{n}\right)$ не визначає, чи є число a квадратичним лишком за модулем n. Справді, якщо $a \in Q_n$, то $\left(\frac{a}{n}\right) = 1$, але з того що $\left(\frac{a}{n}\right) = 1$ не випливає $a \in Q_n$.

Означення. Нехай n – непарне ціле число, n ≥ 3. Число a будемо називати псевдопростим за модулем n, якщо $\left(\frac{a}{n}\right) = 1$. Множину псевдопростих чисел позначатимо через $\widehat{Q}_n = J_n - Q_n$, де $J_n = \{a \in Z_n^* \mid \left(\frac{a}{n}\right) = 1\}$.

Теорема. Нехай p – просте, $p \equiv 3 \pmod 4$, $a \in Q_p$. Тоді розв'язком рівняння

$$x^2 \equiv a \pmod p$$

будуть числа r та $-r$, де $r = a^{\frac{p+1}{4}} \pmod p$.

Доведення. $r^2 \equiv a^{\frac{p+1}{2}} \pmod p \equiv \sqrt{a^{p+1}} \pmod p \equiv \sqrt{a^{p-1} \cdot a^2} \pmod p \equiv \sqrt{1 \cdot a^2} \pmod p \equiv a \pmod p$, оскільки за теоремою Ферма $a^{p-1} \pmod p \equiv 1$.

Доведення теореми можна провести, використовуючи критерій Ейлера. Оскільки a – квадратичний лишок за модулем p, то

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

Враховуючи що число p можна подати у вигляді $p = 4m + 3$ для деякого натурального m, то $\frac{p-1}{2} = 2m + 1$. Тобто $a^{\frac{p-1}{2}} = a^{2m+1} \equiv 1 \pmod p$, $a^{2m+2} \equiv a \pmod p$. Візьмемо квадратний корінь лівої та правої частини останньої рівності:

$$a^{m+1} \equiv \pm\sqrt{a} \pmod p$$

Приклад. Обчислити $\sqrt{5}$ та $\sqrt{3}$ в Z_{11}^*.

$p = 11$ – просте, $p \equiv 3 \pmod 4$, $\frac{p+1}{4} = 3$.

$\sqrt{5}$: $5^3 \pmod{11} \equiv 4$. $-4 \equiv 7 \pmod{11}$.

Перевірка: $4^2 \pmod{11} \equiv 5$, $7^2 \pmod{11} \equiv 5$.

$\sqrt{3}$: $3^3 \pmod{11} \equiv 5$. $-5 \equiv 6 \pmod{11}$.

Перевірка: $5^2 \pmod{11} \equiv 3$, $6^2 \pmod{11} \equiv 3$.

Теорема. Нехай $n = p * q$, де p, q – непарні прості числа. Число $a \in Z_n^*$ є квадратичним лишком за модулем n тоді і тільки тоді, коли a є квадратичним лишком за модулем p та q. Тобто

$$a \in Q_n \Leftrightarrow a \in Q_p \text{ та } a \in Q_q$$

Звідси $|Q_n| = |Q_p| * |Q_q| = (p - 1)(q - 1) / 4$.

Приклад. Нехай $n = 21 = 3 * 7$. $a \in Q_{21} \Leftrightarrow a \in Q_3$ та $a \in Q_7$.

$Q_3 = \{1\}$, поширимо остачі до 21 за модулем 3: {1, 4, 7, 10, 13, 16, 19}.

Q_7 = {1, 2, 4}, поширимо остачі до 21 за модулем 7: {1, 2, 4, 8, 9, 11, 15,16,18}.

$|Q_{21}| = |Q_3| * |Q_7| = 1 * 3 = 3$. Числа, спільні в двох множинах поширених остач, і є квадратичними лишками за модулем 21.

Q_{21} = {1, 4, 16}.

Алгоритм обчислення символа Лежандра/Якобі [Крэндал, алг.2.3.5, стор.118] $\left(\frac{a}{m}\right)$

1.[Цикл редукції]
```
a=a mod m;
t=1;
while(a≠0){
    while(a-парне){
        a=a/2;
        if(m mod 8∈{3,5}) t=-t;
    }
    (a,m)=(m,a); // Перестановка аргументів
    if(a≡m≡3(mod 4)) t=-t;
    a=a mod m;
}
```
2.[Завершення алгоритму]
```
if(m==1) return t;
return 0;
```