

Лекция 5. Теория чисел. Вычеты и невычеты. Расширенный алгоритм Евклида

#вшли

#дискретная_математика

#теория

#теория_чисел

Автор конспекта: Гридчин Михаил

Теорема Эйлера и алгоритм Евклида

Теорема (теорема Эйлера). Пусть дано n и число $a : (a, n) = 1$. Тогда $a^{\varphi(n)} \equiv 1 \pmod{n}$.

□

Выпишем все остатки от деления на n , взаимно простые с n :

$$r_1, r_2, \dots, r_{\varphi(n)}, \quad (r_i, n) = 1$$

Теперь умножим каждый из остатков на a :

$$a \cdot r_1, a \cdot r_2, \dots, a \cdot r_{\varphi(n)} \pmod{n}$$

Каковы остатки от деления этих чисел на n ? Они различные, т.к. если

$\exists r_i, r_j : a \cdot r_i \equiv a \cdot r_j \pmod{n}$, то $a(r_i - r_j) \equiv 0 \pmod{n} \implies r_i = r_j$, т.к. $(a, n) = 1$.

Перемножим все остатки:

$$(a \cdot r_1)(a \cdot r_2) \dots (a \cdot r_{\varphi(n)}) \equiv r_1 r_2 \dots r_{\varphi(n)} \pmod{n}$$

Но $(r_i, n) = 1$, поделим обе части на произведение r_i (т.к. они взаимно просты с n) и получим:

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

■

Замечание. Если n - простое, то $\varphi(n) = n - 1$ и тождество превращается в $a^{n-1} \equiv 1 \pmod{n}$. Это и есть малая теорема Ферма.

Алгоритм Евклида. Тождество $(a, b) = (a - b, b)$ очевидно. Чтобы найти (a, b) , воспользуемся следующим итеративным алгоритмом.

$$a_0 = a, \quad a_1 = b, \quad a_{i-1} = a_i q_i + a_{i+1}, \quad 0 \leq a_{i+1} < |a_i|$$

Строим эту цепочку, пока $a_{i+1} \neq 0$. Утверждается, что $a_{t+1} = (a_0, a_1)$ - последний ненулевой остаток.

Пример: 6 и 4. $6 = 4 \cdot 1 + 2 \implies 2 = 6 - 4 \cdot 1 = x \cdot 6 + y \cdot 4$.

Расширенный алгоритм Евклида. $d = xa + yb$.

Стартуем с $x_t = -1, y_t = q_{t+1}$ и "раскручиваем": $x_i = y_i + 1, y_i = x_{i+1} - q_{i+1}y_i$. На каждом шаге (можно показать) $x_i a_i + y_i a_{i+1} = (a_0, a_1)$. В конце получаем $x_0 a_0 + y_0 a_1 = (a_0, a_1)$

Решение Диофантовых уравнений. $ax + by = c, \quad d = (a, b)$. Если $c \nmid d$, То решений нет. Иначе $c = kd, k \in \mathbb{Z}$. Решим уравнение $a\tilde{x} + b\tilde{y} = d$. Тогда нашли \tilde{x}_0 и \tilde{y}_0 . Предположим, что у нас есть два решения:

$$\begin{aligned} a\tilde{x}_1 + b\tilde{y}_1 &= d \\ a\tilde{x}_2 + b\tilde{y}_2 &= d \end{aligned} (*) \implies a(\tilde{x}_1 - \tilde{x}_2) + b(\tilde{y}_1 - \tilde{y}_2) = 0$$

Заметим, что $a \mid d$ и $b(\tilde{y}_1 - \tilde{y}_2) \mid b$. Тогда $(\tilde{x}_1 - \tilde{x}_2) \mid \frac{b}{d}$. Тогда

$\tilde{x}_1 - \tilde{x}_2 = \frac{b}{d} \cdot t$ и $\tilde{y}_1 - \tilde{y}_2 = \frac{a}{d} \cdot (-t), t \in \mathbb{Z}$. Тогда общее решение:

$\tilde{x} = x_0 + \frac{b}{d} \cdot t, \quad \tilde{y} = y_0 - \frac{a}{d} \cdot t$. Чтобы получить из (*) необходимое, умножим уравнение на $\frac{c}{d}$.

Квадратичные вычеты

Def. Число a называют **квадратичным вычетом** по модулю n , если

$$\exists x \in \mathbb{Z} : x^2 \equiv a \pmod{n}.$$

p - простое > 2 .

Def. **Символ Лежандра.** $a \in \mathbb{Z}$.

$$\begin{aligned} \left(\frac{a}{p}\right) &= 0, & \text{если } a \mid p \\ \left(\frac{a}{p}\right) &= 1, & \text{если } a - \text{квадратичный вычет по } \pmod{p} \\ \left(\frac{a}{p}\right) &= -1, & \text{если } a - \text{квадратичный невычет по } \pmod{p} \end{aligned}$$

$x^2 \equiv (p - x)^2 \pmod{p}$. Рассмотрим все квадраты чисел:

$$1^2, 2^2, \dots, \left(\frac{p-1}{2}\right)^2 \pmod{p}$$

Каждое из них - квадратичный вычет по определению. Они все различны.

□ Пусть $\exists x_i, x_j :$

$$\begin{aligned} x_i^2 &\equiv x_j^2 \pmod{p} \\ (x_i - x_j) \cdot (x_i + x_j) &\equiv 0 \pmod{p} \\ \neq 0 &\quad < p \end{aligned}$$

Противоречие, значит $x_i = x_j$. ■

Следствие. Среди остатков от деления на p ровно $\left(\frac{p-1}{2}\right)$ квадратичных вычетов (все числа имеют близнецов $x = (p - x)^2$, числа, большие p тождественно равны рассмотренным нами квадратам чисел по модулю p) и ровно $\frac{p-1}{2}$ квадратичных невычетов (ненулевых).

Теорема. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$ - символ Лежандра мультипликативен.

□

СЛУЧАЙ 0. Если $a \mid p$ или $b \mid p$, то $ab \mid p$ и символ Лежандра равен 0. Пусть $a \nmid p$ и $b \nmid p$.

СЛУЧАЙ 1. $a \equiv x^2$, $b \equiv y^2$ - вычет, вычет. Возьмём произведение

$ab \equiv x^2 y^2 \pmod{p} \implies ab$ - квадратичный вычет. Тогда

$$\begin{aligned} \left(\frac{ab}{p}\right) &= \left(\frac{1}{p}\right) \cdot \left(\frac{b}{p}\right) \\ &= 1 \cdot 1 \\ 1 &= 1 \cdot 1 \end{aligned}$$

СЛУЧАЙ 2. Пусть a - квадратичный вычет, b - квадратичный невычет. То есть

$\left(\frac{a}{p}\right) = 1$, $\left(\frac{b}{p}\right) = -1$. Рассмотрим произведение $a \cdot b$. Как минимум $\left(\frac{ab}{p}\right) \neq 0$.

Предположим, что $\left(\frac{ab}{p}\right) = 1$. Тогда

$$\begin{aligned} \exists x : a &\equiv x^2 \pmod{p}, & (x, p) &= 1 \\ \exists y : ab &\equiv y^2 \pmod{p} & (*) \end{aligned}$$

По малой теореме Ферма $x \cdot x^{p-2} \equiv 1 \pmod{p}$. Обозначим $x_p^{-1} := x^{p-2} \in \mathbb{Z}$. Домножим (*) на $(x_p^{-1})^2$.

$$(x_p^{-1})^2 ab \equiv (x_p^{-1})^2 x^2 b \equiv b \equiv y^2 \pmod{p}$$

Значит, b - квадратичный вычет - противоречие, значит, $\left(\frac{ab}{p}\right) = -1$. Тогда $-1 = 1 \cdot (-1)$

СЛУЧАЙ 3. Пусть a - квадратичный невычет и b - квадратичный невычет. Рассмотрим все ненулевые остатки от деления на p : $1, 2, \dots, p-1$. Мы уже знаем, что среди них $\frac{p-1}{2}$ квадратичных вычетов и столько же квадратичных невычетов. Пусть V - множество всех вычетов, N - множество всех невычетов. $|V| = |N| = \frac{p-1}{2}$. Умножим все остатки на число $c : (p, c) = 1$:

$$\begin{array}{ccccccc} 1, & 2, & \dots, & p-1 \\ 1 \cdot c, & 2 \cdot c, & \dots, & (p-1) \cdot c \end{array}$$

Мы много раз уже показывали, что все эти остатки разные. Предположим, что $c \in N$.

Тогда по случаю 2 $\implies cV = N$. Мы получим все элементы из N (потому что во второй строке все числа различные). Но тогда и $cN = \{1, 2, \dots, p-1\} \setminus N = V$. Это следует из того, что все числа разные, все невычеты мы уже получили, значит, мы можем получить только то, что осталось, то есть только вычеты. То есть $\left(\frac{ab}{p}\right) = 1$, так как c - это невычет и N - это множество всех невычетов.

Получили доказательство мультипликативности символа Лежандра. ■

Теорема (критерий Эйлера).

a - квадратичный вычет по $\pmod{p} \iff a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.

a - квадратичный невычет по $\pmod{p} \iff a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.

□

ШАГ1. Доказываем слева направо первое утверждение. Пусть a - квадратичный вычет

$$\implies \exists x : a \equiv x^2 \pmod{p} \implies a^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \pmod{p}.$$

ШАГ2. Покажем, что вторая строка - в точности первая. Действительно

$$a^{p-1} \equiv 1 \pmod{p} \implies (a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1) \equiv 0 \pmod{p}$$

Значит, $a^{\frac{p-1}{2}} \in \{-1, 1\} \pmod{p}$.

ШАГ3. Доказательство в обратную сторону. Пусть a - квадратичный невычет. То есть $\left(\frac{a}{p}\right) = -1$. Тогда из мультипликативности $aV = N$, $aN = V$. Обозначим

$$v := \prod_{v_i \in V} v_i$$

$$n := \prod_{n_i \in N} n_i$$

Заметим, что

$$av_1 \equiv n_1 \pmod{p}$$

$$av_2 \equiv n_2 \pmod{p}$$

...

Возьмём произведение всех уравнений:

$$a^{\frac{p-1}{2}} v \equiv n \pmod{p}$$

По теореме Вильсона $v \cdot n \equiv (p-1)! \equiv -1 \pmod{p}$. Умножим на n :

$$a^{\frac{p-1}{2}} vn \equiv n^2 \pmod{p} \iff a^{\frac{p-1}{2}} \equiv -n^2 \pmod{p}$$