

Примитивный вычет

! Пусть $a \perp m$. Говорят, что вычет a имеет порядок d по модулю n (при этом пишут $\text{ord}_m a = d$), если d — наименьшее натуральное число такое, что $a^d \equiv_m 1$. Далее $\psi(d)$ обозначает количество вычетов порядка d .

! Вычет g называется *примитивным* по модулю m , если $\text{ord}_m g = \varphi(m)$.

Таким образом, если g — примитивный вычет по модулю m , то вычеты

$$g, g^2, \dots, g^{\varphi(m)} = 1$$

все различны и образуют приведённую систему вычетов по модулю m .

1. Докажите, что если $a \perp m$ и a имеет порядок d по модулю m , то $\varphi(m):d$.
2. Пусть $m_1 \perp m_2$ и $a \perp m_1 m_2$. Пусть $\text{ord}_{m_1} a = d_1$ и $\text{ord}_{m_2} a = d_2$. Докажите, что $\text{ord}_{m_1 m_2} a = [d_1, d_2]$.
3. Докажите, что...

$$(a) \dots \forall n \in \mathbb{N} \quad \sum_{d|n} \varphi(d) = n; \quad (b) \dots \sum_{d|\varphi(m)} \psi(d) = \varphi(m).$$

4. Пусть $m = p \in \mathbb{P}$.

(a) Рассмотрим вычет a порядка d . Докажите, что

- i. $\text{ord}_p(b)|d$ тогда и только тогда, когда $b = a^k$ для некоторого k ;
- ii. для всякого k справедливо $\text{ord}_p(a^k) = \frac{d}{(d, k)}$.

(b) Докажите, что либо $\psi(d) = 0$, либо $\psi(d) = \varphi(d)$.

(c) Докажите, что для любого d , делящего $p-1$, существует ровно $\varphi(d)$ вычетов порядка d . (В частности, существует ровно $\varphi(p-1)$ примитивных вычетов.)

5. Можно ли записать по кругу числа $1, 2, \dots, 12$ так, чтобы для любых трех подряд стоящих чисел a, b, c число $b^2 - ac$ делилось на 13?
6. Запишите в таблицу 4×4 числа $1, 2, \dots, 16$ так, чтобы всевозможные произведения всех чисел, стоящих в одной строке, и всевозможные произведения чисел, стоящих в одном столбце, (т.е. всего 8 чисел) давали один и тот же остаток при делении на 17.

!! Примитивные вычеты существуют в точности по модулям $2, 4, p^\gamma$ и $2p^\gamma$ (где p — нечетное простое, а γ — натуральное число).

Удачных занятий математикой!



**Математическая
школа**

Шарич В.З.

sharich@mathschool.ru