Лекция №4 «Сравнения». Курс A-I

Турашев Артём Сергеевич 619/2

30 сентября 2025

Определение 1. *$m, n \in \mathbb{Z}_{>0}$, $a \in \mathbb{Z}$, $(a, m) = 1$. Если сравнение $x^n \equiv a\,(m)$ разрешимо, то a называется вычетом степени $n \bmod m$.*
(То есть в $\mathbb{Z}/m\mathbb{Z}$ $a = b^n$)

Лемма 1. *Если $\exists$ первообразный корень $mod\, m$, $(a, m) = 1$. Тогда $a-$вычет степени n $\Leftrightarrow a^{\frac{\phi(m)}{d}} \equiv 1\,(m)$, $d = (n, \phi(m))$.*
$\square$ *Пусть $g-$первообразный корень. Введем обозначение $a = g^b$, $x = g^y$ в $\mathbb{Z}/m\mathbb{Z}$*
Тогда $x^n \equiv a\,(m) \Leftrightarrow g^{ny} \equiv g^b\,(m) \Leftrightarrow ny \equiv b\,(\phi(m)) -$ разрешимо $\Leftrightarrow d|b$
$\Rightarrow g^{b\frac{\phi(m)}{d}} \equiv 1\,(m) \qquad g^{b\frac{\phi(m)}{d}} = a^{\frac{\phi(m)}{d}}$
$\Leftarrow a^{\frac{\phi(m)}{d}} \equiv 1\,(m) \quad g^{b\frac{\phi(m)}{d}} \equiv 1\,(m) \quad \to \quad \phi(m)|b\frac{\phi(m)}{d}$. *Тогда получается, что*
$\to d|b$ $\blacksquare$

Определение 2. *Квадратичный вычет называется вычет с $n = 2$*

По КТО: Z/mZ - прямая сумма колец:

Z/mZ $= \bigoplus_{i=1}^{l} \mathbb{Z}/p^{a_i}\mathbb{Z}$

Рассмотрим самый простой случай: $\mathbb{Z}/p\mathbb{Z}$
Далее $p > 2 -$ простое, $\mathbb{Z}/p\mathbb{Z}$

Определение 3. *Символ Лежандра*

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & a - \textit{квадратичный вычет} \\ -1, & a - \textit{квадратичный невычет} \\ 0, & p|a. \end{cases}$$

Лемма 2. *1)* $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}}\,(p)$
2) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$
3) $a \equiv b\,(p) \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$
$\square$ *Пусть $p \nmid a$, $p \nmid b$, тогда*
$a^{p-1} \equiv 1\,(p) \qquad a^{p-1} - 1 \equiv 0\,(p)$
$(a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1) \equiv 0\,(p)$
$\Rightarrow$ *либо* $a^{\frac{p-1}{2}} - 1 \equiv 0\,(p)$
либо $a^{\frac{p-1}{2}} + 1 \equiv 0\,(p)$
Свойство: $a -$ *вычет* $\Leftrightarrow a^{\frac{\phi(m)}{d}} \equiv 1$, $d = (n, \phi(m))$ $\phi(m) = p - 1$, $n = 2$

$\Rightarrow d = 2$
то есть квадратичный вычет $\Leftrightarrow$ $a^{\frac{p-1}{2}} \equiv 1\,(p)$ *Из этого свойства следует верность 1)*
2) $\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} \equiv \dots$
3) *(очевидно, по определению)* $\blacksquare$

Замечание. *Число вычетов и невычетов одинаково*

Замечание. *a = -1* $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & p = 4k+1 \\ -1 & p = 4k+3 \end{cases}$

Лемма 3. *(Гаусс) p* $\not|\, a$ *Рассмотрим множество:* $\{ka : 1 \le k \le \frac{p-1}{2}\} = \{a,\, 2a,\, \dots,\, \frac{p-1}{2}a\}$
Обозначим $r_k \equiv ka\,(p)$ $-\frac{p-1}{2} \le r_k \le \frac{p-1}{2}$
Пусть $s = |\{k : r_k < 0\}|$
Тогда $\left(\frac{a}{p}\right) = (-1)^s$
$\square$ *Пусть* $u_1, \dots, u_s$ *– те* $r_k < 0$
Остальные $v_1, \dots, v_{\frac{p-1}{2}-s}$
$-u_1, \dots, -u_s \in [1, \frac{p-1}{2}]$
и к тому же $-u_i \ne v_j$ *(если* $-u_i = v_j$, $-u_i = ka$, $v_j = la$: $u_i + v_j \equiv 0\,(p) \Rightarrow$ *будет выполнено* $p(k+l)) \Rightarrow$ *получаем противоречие*
$\{-u_1, \dots, -u_s, v_1, \dots, v_{\frac{p-1}{2}-s}\} = \{1, 2, \dots, \frac{p-1}{2}\}$
$\prod(-u_i)\prod(v_j) = (\frac{p-1}{2})!$
$(-1)^s \prod u_i \prod v_j$
$(-1)^s \prod r_k\,(p)$
$(\frac{p-1}{2})! \equiv (-1)^s \prod r_k \equiv (-1)^s a^{\frac{p-1}{2}} (\frac{p-1}{2})!\ (p)$
$\Rightarrow (-1)^s \equiv a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\ (p)$ $\blacksquare$

Следствие. $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$
$\square$ $1 * 2,\, 2 * 2, \dots, \frac{p-1}{2} * 2$
$s = |\{k : \frac{p-1}{2} \le 2k \le p-1\}| = \frac{p-1}{2} - |\{k : 2k \le \frac{p-1}{2}\}|$ $|\{k : 2k \le \frac{p-1}{2}\}| = [\frac{p-1}{4}]$
$= \lceil \frac{p-1}{4} \rceil$ $\lceil \frac{p-1}{4} \rceil \equiv 0\,(2) \Leftrightarrow p = 8k \pm 1$

Лемма 4. $\left(\frac{a}{p}\right) = (-1)^{\sum_{k=1}^{\frac{p-1}{2}} [\frac{ak}{p}]}$ *для* $a \equiv 1\,(2)$
$\square$ $\left(\frac{a}{p}\right) = (-1)^s$
$s = |\{k : r_k < 0 \quad (r_k \equiv ka\,(p))\}|$
$[\frac{2ak}{p}] = [2([\frac{ak}{p}] + \{\frac{ak}{p}\})] = 2[\frac{ak}{p}] + [2\{\frac{ak}{p}\}]$ $[2\{\frac{ak}{p}\}] \equiv \begin{cases} 0 & r_k > 0 \\ 1 & r_k < 0 \end{cases}$
$\Rightarrow s \equiv \sum_{k=1}^{\frac{p-1}{2}} [\frac{2ak}{p}]\,(2)$
$a \equiv 1\,(2)$
$\left(\frac{2a}{p}\right) = \left(\frac{4\frac{a+p}{2}}{p}\right) = \left(\frac{\frac{a+p}{2}}{p}\right) = (-1)^{s'}$
$s' = \sum_{k=1}^{\frac{p-1}{2}} [\frac{2k\frac{a+p}{2}}{p}] = \sum_k [\frac{ka}{p} + k] = \sum_k [\frac{ka}{p}] + \sum_k k$ $\sum_k k = (\frac{p-1}{2}+1)\frac{p-1}{2}\frac{1}{2} = \frac{p^2-1}{8}$
$\left(\frac{2a}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{a}{p}\right) = (-1)^{\sum_k [\frac{ka}{p}]}(-1)^{\frac{p^2-1}{8}}$, *где* $(-1)^{\frac{p^2-1}{8}} = \left(\frac{2}{p}\right)$ $\blacksquare$

Теорема 1. *(квадратичный закон взаимности) p,q > 2 - простые, p+q*
$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$

$\square \quad P=\frac{p-1}{2} \quad Q=\frac{q-1}{2}$
Рассмотрим PQ *как пару* (qx,py)
$1\le x\le P \quad 1\le y\le Q$
$\forall x,y: \quad qx\neq py$
$PQ=S+T,$ *где* $S=|\{(qx,py): \quad qx<py \quad 1\le x\le P \quad 1\le y\le Q\}|$
$T=|\{(qx,py): \quad py<qx \quad 1\le x\le P \quad 1\le y\le Q\}|$
$S=|\{(x,y): \quad x<\frac{p}{q}y \quad 1\le x\le P \quad 1\le y\le Q\}|=\sum_{y=1}^{Q}[\frac{p}{q}y]$
Аналогично для $T=\sum_{x=1}^{P}[\frac{q}{p}x]$
По лемме:
$\left(\frac{p}{q}\right)=(-1)^S, \quad \left(\frac{q}{p}\right)=(-1)^T$
По построению получаем справедливость утверждений теоремы $\blacksquare$

Обобщенный символ Якоби

Определение 4. *Пусть* $p\in\mathbb{Z}_{>1}, \quad p\equiv 1\,(2), \quad p=p_1\dots p_r, \quad a\in\mathbb{Z} \quad \left(\frac{a}{p}\right)=\left(\frac{a}{p_1\dots p_r}\right)=\left(\frac{a}{p_1}\right)\dots\left(\frac{a}{p_r}\right)$

Замечание. $\left(\frac{a}{p}\right)=-1\Rightarrow a-$ *квадратичный невычет* (p)

Лемма 5. *1)* $\left(\frac{a_1a_2}{p}\right)=\left(\frac{a_1}{p}\right)\left(\frac{a_2}{p}\right)$
2) $\left(\frac{a}{PQ}\right)=\left(\frac{a}{P}\right)\left(\frac{a}{Q}\right)$
3) *если* $a_1\equiv a_2\,(P),$ *то* $\left(\frac{a_1}{P}\right)=\left(\frac{a_2}{P}\right)$
$\square$ *Упражнение* $\blacksquare$

Лемма 6. *1)* $\left(\frac{1}{p}\right)=1$
2) $\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}$
3) $\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}$
$\square$ *Упражнение* $\blacksquare$

Теорема 2. *P, Q (P,Q)=1*
$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right)=(-1)^{\frac{P-1}{2}\frac{Q-1}{2}}$
$\square$ *Упражнение* $\blacksquare$

Определение 5. *равномерное распределение последовательностей по mod 1 (р.р. по mod 1):* $(x_n)_{n=1}^{\infty} \quad x_n\in(0,1)$ *называется равномерно распределенной, если* $\forall$ *непрерывной измеримой по Лебегу функции, определенной на интервале* $(0,1)$
$\lim_{N\to\infty}\frac{1}{N}\sum_{n\le N}f(x_n)=\int_0^1 f(t)dt$

Эквивалентное определение: $(x_n)-$ *равномерно распределена по* $mod\,1\Leftrightarrow$
$\lim\frac{1}{N}|\{n<N: a\le x_n\le b\}|=b-a \quad 0<a<b<1$

Теорема 3. *Если* $\alpha-$ *иррациональная, то* $\{n\alpha\}-$ *равномерно распределена по* $mod\,1$

Теорема 4. *(Виноградов)* $\alpha-$*иррациональная* $\{p\alpha\}-$*равномерно распределена по* $mod\,1$

Теорема 5. *(80-е годы)* *Если в качетсве* (x_p)*−последовательность решений сравнения:*
$x_p^2 \equiv a\,(p),\quad p$ *− простое*
Тогда последовательность $\{\frac{x_p}{p}\}$ *− равномерно распределена по* $mod\,1$