51. Сравнения второй степени. Квадратичные вычеты и невычеты. Тождество $\left(\frac{a}{p}\right) = (-1)^{\sum\limits_{x=1}^{\frac{p-1}{2}} \left[\frac{2ax}{p}\right]}$

Определение. $x^2 \equiv a \pmod m$ называется *сравнением второй степени.*

Будем считать, что $m = p$ – нечётное простое число, $(a, p) = 1$.

Замечание. *У сравнения второй степени либо нет решений, либо их два.*

▲. По теореме Лагранжа у сравнения второй степени не более 2.
Пусть x_0 – решение сравнения $x^2 \equiv a \pmod p$.
Тогда $-x_0$ – также решение, но $-x_0 \not\equiv x_0 \pmod p$ ■

Определение. Число a называется *квадратичным вычетом*, если у сравнения $x^2 \equiv a \pmod p$ два решения. Число a называется *квадратичным невычетом*, если у сравнения $x^2 \equiv a \pmod p$ нет решений.

Утверждение. *По модулю p есть ровно $\frac{p-1}{2}$ квадратичных вычетов и $\frac{p-1}{2}$ квадратичных невычетов.*

▲. Рассмотрим числа $1^2, 2^2, ..., (\frac{p-1}{2})^2$. Очевидно, что все они являются квадратичными вычетами. У каждого из сравнений с этими числами ровно два различных решения, причём у разных сравнений также получатся разные решения. Получается, что числами $1^2, 2^2, ..., (\frac{p-1}{2})^2$ исчерпываются все квадратичные вычеты. ■

Теорема. $a^{\frac{p-1}{2}} \equiv 1 \pmod p$, *если a – квадратичный вычет, и* $a^{\frac{p-1}{2}} \equiv -1 \pmod p$, *если a – квадратичный невычет.*

▲. По малой теореме Ферма $a^{p-1} \equiv 1 \pmod p$ для всех a. Тогда

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

Если a – квадратичный вычет, то

$$\exists x : x^2 \equiv a \pmod p \Rightarrow a^{\frac{p-1}{2}} \equiv (x^2)^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \pmod p$$

Доказательство для квадратичных невычетов аналогичное. ■

Определение. *Символ Лежандра*

$$\left(\frac{a}{p}\right) = \begin{cases} 1, \text{если } a \text{ – квадратичный вычет} \\ -1, \text{если } a \text{ – квадратичный невычет} \\ 0, \text{если } (a,p) \neq 1 \end{cases}$$

Замечание.

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

Следствие. Символ Лежандра мультипликативен.

Теорема. $\left(\frac{a}{p}\right) = (-1)^{\sum\limits_{x=1}^{\frac{p-1}{2}} \left[\frac{2ax}{p}\right]}$

▲. Пусть $x \in \{1, 2, ..., \frac{p-1}{2}\}$
$a \cdot x$ загоним в систему вычетов от $-\frac{p-1}{2}$ до $\frac{p-1}{2}$.

Переход в новую систему вычетов происходит следующим образом: левая часть системы вычетов $1, 2, ..., p-1$ остаётся такой же (то есть равна $\{1, 2, ..., \frac{p-1}{2}\}$), а правая будет равна $\{-\frac{p-1}{2}, ..., -2, -1\}$.

$$a \cdot x \equiv \varepsilon_x \cdot r_x \pmod p,$$

где $\varepsilon_x \in \{-1, 1\}, r_x \in \{1, 2, ..., \frac{p-1}{2}\}$

Если $a \cdot x$ попадет в левую часть системы вычетов {1, 2, ... p - 1}, тогда $\varepsilon_x = 1$, если в правую, то $\varepsilon_x = -1$.

Утверждается, что математически это записывается так:

$$\varepsilon_x = (-1)^{\left[\frac{2ax}{p}\right]}$$

Доказательство настолько скучное, что Райгородский не стал его рассказывать :)

Доказать можно примерно так:

Пусть $a \cdot x \in [kp+1; (k+1)p-1]$ для некоторого k. Тогда $\frac{ax}{p} \in (k, k+1)$. Соответственно, $\frac{2ax}{p} \in (2k, 2k+2)$.

Тогда если ax лежало в левой части, то $\left[\frac{2ax}{p}\right] = 2k$ (то есть чётному числу), иначе $\left[\frac{2ax}{p}\right] = 2k+1$ (то есть нечётному).

Покажем, что когда x пробегает значения от 1 до $\frac{p-1}{2}$, то r_x пробегает всю систему вычитов $1, 2, ..., \frac{p-1}{2}$:

Когда x пробегает значения от 1 до $\frac{p-1}{2}$, то значения ax не могут повториться, ведь иначе $(a, p) \neq 1$. Также r_x не может повториться, так как иначе $\exists x_1, x_2 \leq \frac{p-1}{2}$ т.ч. $x_1 \neq x_2, ax_1 \equiv_m r_x, ax_2 \equiv_m -r_x \Rightarrow ax_1 + ax_2 \equiv_m 0 \Rightarrow x_1 + x_2 \equiv_m 0$, чего быть не может так как x пробегает значения от 1 до $\frac{p-1}{2}$.

Показали. С учетом этого,

$$\prod_{x=1}^{\frac{p-1}{2}} (ax) \equiv \varepsilon_1 \cdot \varepsilon_2 \cdot ... \cdot \varepsilon_{\frac{p-1}{2}} \cdot \prod_{x=1}^{\frac{p-1}{2}} r_x \equiv \varepsilon_1 \cdot \varepsilon_2 \cdot ... \cdot \varepsilon_{\frac{p-1}{2}} \cdot \prod_{x=1}^{\frac{p-1}{2}} x$$

Разделив обе части на $\prod\limits_{x=1}^{\frac{p-1}{2}} x$ и используя выражение для ε_x, получаем:

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \equiv \varepsilon_1 \cdot \varepsilon_2 \cdot ... \cdot \varepsilon_{\frac{p-1}{2}} \equiv (-1)^{\sum\limits_{x=1}^{\frac{p-1}{2}} \left[\frac{2ax}{p}\right]}$$

■

52. Сравнения второй степени. Квадратичные вычеты и невычеты. Формула для $\left(\dfrac{2}{p}\right)$ (тождеством с суммой по $\left[\dfrac{2ax}{p}\right]$ можно пользоваться без доказательства).

Вся теория расписана в прошлом билете.

Теорема.

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

Доказательство. Для удобства введём обозначение $p_1 = \frac{p-1}{2}$.

Без доказательства можно пользоваться утверждением:

$$\left(\frac{a}{p}\right) = (-1)^{\sum\limits_{x=1}^{p_1}\left[\frac{2ax}{p}\right]}$$

Рассмотрим нечётное a.

$$\left(\frac{2a}{p}\right) = \left(\frac{4\cdot\frac{a+p}{2}}{p}\right) = \left(\frac{2^2}{p}\right)\cdot\left(\frac{\frac{a+p}{2}}{p}\right) = 1\cdot(-1)^{\sum\limits_{x=1}^{p_1}\left[\frac{2\cdot\frac{a+p}{2}\cdot x}{p}\right]}$$

Для удобства распишу отдельно показатель -1:

$$\sum_{x=1}^{p_1}\left[\frac{2\cdot\frac{a+p}{2}\cdot x}{p}\right] = \sum_{x=1}^{p_1}\left[\frac{ax}{p}+x\right] = \sum_{x=1}^{p_1}\left[\frac{ax}{p}\right]+\sum_{x=1}^{p_1}x = \sum_{x=1}^{p_1}\left[\frac{ax}{p}\right]+\frac{p_1(p_1+1)}{2} = \sum_{x=1}^{p_1}\left[\frac{ax}{p}\right]+\frac{p^2-1}{8}$$

Вернёмся к $\left(\frac{2a}{p}\right)$:

$$\left(\frac{2a}{p}\right) = (-1)^{\sum\limits_{x=1}^{p_1}\left[\frac{ax}{p}\right]}\cdot(-1)^{\frac{p^2-1}{8}}$$

Тождество верно для любого нечётного a, поэтому можно подставить $a = 1$.

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}\cdot(-1)^{\sum\limits_{x=1}^{p_1}\left[\frac{x}{p}\right]} = (-1)^{\frac{p^2-1}{8}},$$

так как $\left[\frac{x}{p}\right] = 0$ $(x \le p_1 < p)$. ∎