

③ Квадратичный закон Взаимности

Опр 1 Пусть $a, m \in \mathbb{Z}^*$ и $(a, m) = 1$. Число a наз-ся **квадратичным вычетом** по модулю m , если разрешимо сравнение $x^2 \equiv a \pmod{m}$, и **квадр. не вычетом** в противном случае.

Пример По модулю 7 $(\pm 1)^2, (\pm 2)^2, (\pm 3)^2$ сравнимы соот-но с $1, 4$ и $2 \Rightarrow 2$ -кв. вычет по $\text{mod } 7$, а 3 -кв.

Если x и mx , то 1 кв. вычет в случае, когда m - простое.

Предп 1 Пусть $m = 2^k p_1^{k_1} \dots p_s^{k_s}$ — разн. неупоряд. $u(a, m) = 1$.

a — квадрат. вычисл. $\bmod m \Leftrightarrow a) x^2 \equiv a \pmod{p_i}$

$\forall i = 1 \dots s \text{ и } 6) \quad a \equiv 1 \pmod{4} \quad k=2$

$a \equiv 1 \pmod{8} \quad k \geq 3$

Упр 1 $\Delta \rightarrow \mathbb{Q}$ предп. 1.

Сравнение $x^2 \equiv a \pmod{p}$ удовлетворяет в $\mathbb{F}_p$.

Предп 2 Для четного простого p и $a \in \mathbb{F}_p^*$,

или-то $(\mathbb{F}_q^*)^2$ всех невыр. кв-тов $\mathbb{F}_q \rightarrow \mathbb{F}_q$

для $\text{кон. зм. } x \mapsto x^{(q-1)/2}$ из $\mathbb{F}_q^* \in \{ \pm 1 \}$. В

каждом $\text{сл.}, |\mathbb{F}_q^* : (\mathbb{F}_q^*)^2| = 2$.

Д-во: Пусть $\mathbb{F} = \mathbb{F}_q$ и $\overline{\mathbb{F}}$ — то ад. зам. $\mathbb{F}$.

$\forall x \in F^* \exists y \in F : y^2 = x$. Тогда $y^{q-1} = x^{\frac{q-1}{2}} = \pm 1$,
 т.е. $x^{\frac{q-1}{2}} = \pm 1$ по правилу Лейбница. Значит x — квадрат в F
 $\Leftrightarrow y \in F$, т.е. $y^{q-1} = \pm 1$. Поэтому $(F^*)^2$ — подгруппа
 $x \mapsto x^{\frac{q-1}{2}}$. $\square$

Упр 2 Докажем, что при $p=2$, модуль $\mathbb{F}_q$ —
 квадрат.

Опр 2 Пусть $p \neq 2$ — простое и $x \in \mathbb{F}_p^*$. Символ Лежандра
 $\left(\frac{x}{p}\right) = x^{\frac{p-1}{2}} \in \{\pm 1\}$. По определению $\left(\frac{0}{p}\right) = 0$ и
 $\forall x \in \mathbb{Z} \left(\frac{x}{p}\right) = \left(\frac{\bar{x}}{p}\right)$, где $\bar{x}$ — образ x в $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$.

Презл 3 (св-ва дивизора Лежандра) Тук е p -кв.чрост.

$$1) \begin{pmatrix} x & y \\ 1 & p \end{pmatrix} = \begin{pmatrix} x \\ p \end{pmatrix} \begin{pmatrix} y \\ p \end{pmatrix}$$

$$2) \begin{pmatrix} 1 & 1 \\ 1 & p \end{pmatrix} = 1$$

$$3) \begin{pmatrix} -1 & 1 \\ 1 & p \end{pmatrix} = (-1)^{\varepsilon(p)} \quad \varepsilon(p) = \frac{p-1}{2} \quad \varepsilon(n) = \begin{cases} 0, & n \equiv 1(4) \\ 1, & n \equiv -1(4) \end{cases}$$

$$4) \begin{pmatrix} 2 & 1 \\ 1 & p \end{pmatrix} = (-1)^{\omega(p)} \quad \omega(p) = \frac{p^2-1}{8} \quad \omega(n) = \begin{cases} 0, & n \equiv \pm 1(8) \\ 1, & n \equiv \pm 5(8) \end{cases}$$

Л-во: $x \mapsto \begin{pmatrix} x \\ p \end{pmatrix}$ — зом-зм.

Из 3) очевидно $\Rightarrow \begin{pmatrix} x \\ p \end{pmatrix} = x^{\frac{p-1}{2}}$

Докажем 4)

Пусть $\alpha \in \overline{\mathbb{F}_p}$ — ненулев. корень 8-ой степени из 1.

Также $\alpha^7 = -1 \Rightarrow \alpha^2 + \alpha^5 = 0 \Rightarrow (\alpha + \alpha^5)^2 = 2$.

Обозн: $y = \alpha + \alpha^{-1}$. Тогда $y^p = \alpha^p + \alpha^{-p}$ и $y^{p-1} = \left(\frac{2}{p}\right)$.

Если $p \equiv \pm 1(8) \Rightarrow y^p = y \Rightarrow y^{p-1} = 1 = \left(\frac{2}{p}\right)$

Если $p \equiv \pm 5(8) \Rightarrow y^p = \alpha^5 + \alpha^{-5} = -(\alpha + \alpha^{-1}) = -y \Rightarrow$

$y^{p-1} = -1 = \left(\frac{2}{p}\right) \left[\alpha + \alpha^3 + \alpha^5 + \alpha^7 = 0 \right] \quad \square$

Теорема 1 (Гаусс) Пусть p и l — пр. пр. простые числа

Тогда $\left(\frac{p}{l}\right) \left(\frac{l}{p}\right) = (-1)^{\frac{p-1}{2} \frac{l-1}{2}} = (-1)^{\varepsilon(p)\varepsilon(l)}$.

КРАТКАЯ ЗАКОН ВЗ-СУ: p и l взаим. просты $\Leftrightarrow p^{l-1} \equiv 1(l)$
 $(p \nmid l \Leftrightarrow l \nmid p) \Leftrightarrow p, l \equiv \pm 1(4)$.

Д-во: $\omega \in \overline{\mathbb{F}_p}$ - ненулевой $(l-1)$ -ой ст. чл. в ант. зм. полин. $\mathbb{F}_p$.

Если $x \in \mathbb{F}_l$, то ω^x однозначно определен, т.к. $\omega^l = 1$.

Поэтому корректно введем "ант. ГАУССА":

$$y = \sum_{x \in \mathbb{F}_l} \left(\frac{x}{l} \right) \omega^x \quad (*)$$

Лемма 1 $y^2 = (-1)^{\varepsilon(l)} l$ $\varepsilon(l) = (l-1)/2$
 $l = \overline{l}$ - обратный l в $\mathbb{F}_p$.

Д-во: $y^2 = \sum_{t, z \in \mathbb{F}_l} \left(\frac{tz}{l} \right) \omega^{t+z} = \sum_{u \in \mathbb{F}_l} \omega^u \left(\sum_{t \in \mathbb{F}_l} \left(\frac{t(u-t)}{l} \right) \right)$
 $u = t+z \rightarrow z = u-t$

Если $t \neq 0$, то $\left(\frac{t(u-t)}{l} \right) = \left(\frac{-t^2}{l} \right) \left(\frac{1-ut^{-1}}{l} \right) =$
 $= (-1)^{\varepsilon(l)} \left(\frac{1-ut^{-1}}{l} \right) \Rightarrow (-1)^{\varepsilon(l)} y^2 = \sum_{u \in \mathbb{F}_l} \left(\frac{1-ut^{-1}}{l} \right) \omega^u, \text{ где}$

$$C_u = \sum_{t \in \mathbb{F}_\ell^*} \left(\frac{1 - ut^{-1}}{\ell} \right).$$

From $u=0$, $C_u = \sum_{t \in \mathbb{F}_\ell^*} \left(\frac{1}{\ell} \right) = \ell - 1.$

From $u \neq 0$, $s = 1 - ut^{-1}$ maps $\ell - 1$ to $\mathbb{F}_\ell \setminus \{1\} \Rightarrow$

$$C_u = \sum_{s \in \mathbb{F}_\ell} \left(\frac{s}{\ell} \right) - \left(\frac{1}{\ell} \right) = - \left(\frac{1}{\ell} \right) = -1, \text{ too. } |\mathbb{F}_\ell^*| \cdot |\mathbb{F}_\ell^*|^2 = 2.$$

Moreover $\sum_{u \in \mathbb{F}_\ell} C_u w^u = (\ell - 1) - \sum_{u \in \mathbb{F}_\ell^*} w^u = \ell \quad \square$
 $\therefore \sum_{u \in \mathbb{F}_\ell} w^u = 0!$

Lemma 2 $y^{p^{-1}} = \left(\frac{p}{\ell} \right).$

Proof: T.v. char $\overline{\mathbb{F}_p} = p \Rightarrow y^p = \sum_{x \in \mathbb{F}_\ell} \left(\frac{x}{\ell} \right) w^{xp} =$

$$\sum_{z \in \mathbb{F}_\ell} \left(\frac{zp^{-1}}{\ell} \right) w^z = \left(\frac{p^{-1}}{\ell} \right) \sum_{z \in \mathbb{F}_\ell} \left(\frac{z}{\ell} \right) w^z = \left(\frac{p^{-1}}{\ell} \right) y = \left(\frac{p}{\ell} \right) y \quad \square$$

Число ЗАКО имеет γ -во времени γ о сАТЮио ЗАМЕРЮ.

$$\left(\frac{p}{e}\right) \stackrel{1:2}{=} \gamma^{p-1} = \left(\gamma^2\right) \stackrel{1:2}{=} \left(\frac{(-1)^{\varepsilon(p)} e}{p}\right) = \left(\frac{e}{p}\right) \left(\frac{(-1)^{\varepsilon(e)}}{p}\right)$$

$$= \left(\frac{e}{p}\right) (-1)^{\varepsilon(p)\varepsilon(e)} \quad \boxed{\equiv}$$

Пример $\left(\frac{29}{43}\right) \stackrel{\varepsilon(29)=0}{=} \left(\frac{43}{29}\right) = \left(\frac{14}{29}\right) = \left(\frac{2}{29}\right) \left(\frac{7}{29}\right) \stackrel{\omega(29)=1}{=} -\left(\frac{7}{29}\right) =$

$$= -\left(\frac{29}{7}\right) = -\left(\frac{1}{7}\right) = -1.$$

Упр 3 Используя результат примера, покажите, что $29 \nmid \mathcal{O}_L$ — простой идеал в $L = (\mathbb{Q})[\sqrt{43}]$.