Квадратичный закон взаимности

Соглашение. Везде далее a и b — целые числа, p — *нечетное* простое число.

▷ **Определение 1.** Умножение на a дает перестановку множества $(\mathbb{Z}/p\mathbb{Z})^\times$ ненулевых вычетов по модулю p. Будем обозначать ее через m_a.

Задача 1. Выпишите явно перестановки m_a для $p = 11$ и $a = -1$, $a = -3$, $a = 3$.

Задача 2. $m_{ab} = m_a \circ m_b$.

Задача 3. а) Пусть a имеет порядок k по модулю p. Тогда m_a представляет собой произведение $\frac{p-1}{k}$ независимых циклов длины k.
б) Найдите четность этой перестановки.

▷ **Определение 2.** Если существует такое целое число x, что $x^2 \equiv a \pmod p$, и a не делится на p, то говорят, что a — *квадратичный вычет по модулю p*.

Задача 4. Если a — квадратичный вычет, то m_a — четная перестановка.

Задача 4$\frac{1}{2}$. Какие из остатков по модулю а) 11; б*) 57 являются квадратичными вычетами?

Задача 5. Каких остатков по модулю p больше: квадратичных вычетов или невычетов? (Указание: сколько прообразов может быть у элемента при отображении $x \mapsto x^2, \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$?)

Задача 6. а*) $x(x-1)(x-2)\dots(x-p+1) \equiv x^p - x \pmod p$.
(Указание: в поле $\mathbb{F}_p$ у этих многочленов совпадают все корни.)
Этим утверждением можно далее пользоваться без доказательства.
б) Как изменится правая часть в предыдущем тождестве, если в левой части оставить только те скобки $(x-a)$, в которых a — квадратичный вычет по модулю p?

▷ **Определение 3.** *Символ Лежандра* $\left(\frac{a}{p}\right)$ определяется как

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{если } a \text{ делится на } p; \\ 1, & \text{если } a \text{ квадратичный вычет по модулю } p; \\ -1, & \text{если } a \text{ квадратичный невычет по модулю } p. \end{cases}$$

Задача 7 (критерий Эйлера). $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$.

Задача 8. а) $\left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$ ("мультипликативность символа").
б*) $a \mapsto \left(\frac{a}{p}\right)$ — единственное непостоянное отображение $(\mathbb{Z}/p\mathbb{Z})^\times \to \{\pm 1\}$, обладающее мультипликативным свойством.

Задача 9 (лемма Золотарёва). $\left(\frac{a}{p}\right) \equiv \operatorname{sign} m_a$.

Задача 10. Вычислите $\left(\frac{-1}{p}\right)$ двумя способами.

Задача 11*. а) $\left(\frac{-3}{p}\right) = 1$ тогда и только тогда, когда сравнение $x^3 \equiv 1 \pmod p$ имеет нетривиальное решение.
б) Вычислите $\left(\frac{-3}{p}\right)$.
в) Вычислите $\left(\frac{3}{p}\right)$. Как связаны символы $\left(\frac{3}{p}\right)$ и $\left(\frac{p}{3}\right)$?

▷ **Определение 4.** Для нечетного числа n и взаимно простого с ним числа a определим *символ Якоби* $\left(\frac{a}{n}\right)$ как знак перестановки m_a множества $\mathbb{Z}/n\mathbb{Z}$.

Задача 12. $\left(\frac{a}{n}\right) \cdot \left(\frac{b}{n}\right) = \left(\frac{ab}{n}\right)$.

Задача 13. Верно ли, что если $\left(\frac{a}{n}\right) = 1$, то a — квадратичный вычет по модулю n? А обратное?

Задача 14 (лемма Гаусса). Будем называть вычет, сравнимый с числом из промежутка $(0, \frac{n}{2})$, положительным по модулю n, а число из промежутка $(-\frac{n}{2}, 0)$ — отрицательным.

Тогда $\left(\frac{a}{n}\right) = (-1)^s$, где s — число «перемен знака»: положительных вычетов, которые умножение на a переводит в отрицательные.

Задача 15. Вычислите $\left(\frac{2}{n}\right)$. При каких p число 2 является квадратичным вычетом по модулю p?

Задача 16. Если $m \equiv \pm n \pmod{4a}$, то $\left(\frac{a}{m}\right) = \left(\frac{a}{n}\right)$.

Задача 17 (квадратичный закон взаимности).
а) Если m и n — взаимно простые нечетные числа, сумма которых делится на 4, то $\left(\frac{m}{n}\right) = \left(\frac{n}{m}\right)$.
б) Если m и n взаимно простые нечетные числа, то

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}.$$

Задача 18. Выясните, является ли 57 квадратичным вычетом по модулю 2011.

Задача 19*. Если $p = a^2 + b^2$, a нечетное, то a — квадратичный вычет по модулю p.

Дополнительная часть: Суммы Гаусса

Соглашение. Везде далее p и q — различные нечетные простые числа.

▷ **Определение 5.** Пусть ζ — корень степени q из единицы. Выражение

$$S(\zeta; q) := \sum_{a \in \mathbb{F}_q^\times} \left(\frac{a}{q}\right) \zeta^a$$

называется *суммой Гаусса* по модулю q.

Задача 20. Вычислите суммы Гаусса
а) $S(\cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3}; 3)$; б) $S(\cos\frac{2\pi}{5} + i\sin\frac{2\pi}{5}; 5)$.

Задача 21. а) $S(\zeta, q)^2 = \left(\frac{-1}{q}\right) q$.
б*) Пусть $\zeta = \cos\frac{2\pi}{q} + i\sin\frac{2\pi}{q}$. Из предыдущего пункта следует, что

$$S(\zeta, q) = \begin{cases} \pm\sqrt{q}, & q = 4k+3; \\ \pm i\sqrt{q}, & q = 4k+1. \end{cases}$$

Найдите знаки.

Задача 22*. *Циклотомический многочлен* $\Phi_q(\zeta) := \frac{\zeta^q - 1}{\zeta - 1}$ неприводим над $\mathbb{F}_p$.

▷ Утверждением последней задачи можно далее пользоваться без доказательства.

▷ **Определение 6.** *Автоморфизмом Фробениуса* поля $\mathcal{F} := \mathbb{F}_p[\zeta]/\Phi_q(\zeta)$ называется отображение

$$\mathrm{Fr}\colon x \mapsto x^p.$$

Задача 23. а) Отображение Fr действительно является автоморфизмом поля $\mathcal{F}$.
б) Элемент x поля $\mathcal{F}$ лежит в поле $\mathbb{F}_p$ тогда и только тогда, когда $\mathrm{Fr}\, x = x$.
(Ср. с комплексным сопряжением для вложения $\mathbb{R} \subset \mathbb{C}$.)

Задача 24. Если $q^* := \left(\frac{-1}{q}\right) q$ — квадратичный вычет по модулю p, то $\mathrm{Fr}\, S(\zeta; q) = S(\zeta; q)$; в противном случае, $\mathrm{Fr}\, S(\zeta; q) = -S(\zeta; q)$. Другими словами,

$$\mathrm{Fr}\, S(\zeta, q) = \left(\frac{q^*}{p}\right) S(\zeta; q).$$

Задача 25. Убедитесь, что

$$\mathrm{Fr}\, S(\zeta; q) = \left(\frac{p}{q}\right) S(\zeta; q).$$

Задача 26. Равенство

$$\left(\frac{p}{q}\right) = \left(\frac{q^*}{p}\right)$$

эквивалентно обычному квадратичному закону взаимности (для простых m и n).