Квадратичный закон взаимности

1. Пусть p – простое нечётное число, $t = \frac{p-1}{2}$, $0 < x \leqslant t$ и $(a, p) = 1$. Докажите, что **(а)** $ax \equiv_p (-1)^{[\frac{2ax}{p}]} \cdot r_x$, где $0 < r_x \leqslant t$; **(б)** $\left(\frac{a}{p}\right) = (-1)^{\sum_{x=1}^{t}[\frac{2ax}{p}]}$.

2. Пусть p – простое нечётное число, $t = \frac{p-1}{2}$, $0 < x \leqslant t$, a нечетно и $(a, p) = 1$. Докажите, что **(а)** $\left(\frac{2a}{p}\right) = (-1)^{\sum_{x=1}^{t}[\frac{ax}{p}]+\frac{p^2-1}{8}}$; **(б)** $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$; **(в)** $\left(\frac{a}{p}\right) = (-1)^{\sum_{x=1}^{t}[\frac{ax}{p}]}$.

3. **(а)** Пусть p и q — различные простые нечетные числа. Рассмотрим прямоугольник на целочисленной решетке с вершинами в точках $(1, 1)$, $(1, \frac{q-1}{2})$, $(\frac{p-1}{2}, 1)$, $(\frac{p-1}{2}, \frac{q-1}{2})$. Посчитав точки внутри и на границе этого прямоугольника, докажите, что

$$\sum_{i=1}^{\frac{p-1}{2}} \left[\frac{iq}{p}\right] + \sum_{j=1}^{\frac{q-1}{2}} \left[\frac{jp}{q}\right] = \frac{p-1}{2} \cdot \frac{q-1}{2}.$$

(б) (*Квадратичный закон взаимности Гаусса*) Пусть p, q — различные нечётные простые числа. Тогда выполнено равенство:

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.$$

4. Вычислите $\left(\frac{57}{179}\right)$.

5. Докажите, что простых чисел вида $10k - 1$ бесконечно много.

6. Докажите, что число $2^n + 1$ не имеет простых делителей вида $8k + 7$.

7. Последовательность $\{x_n\}$ определена рекурсивно: $x_1 = a$ при некотором натуральном a, а также $x_{n+1} = 2x_n + 1$. Пусть $y_n = 2^{x_n} - 1$. Какое максимальное количество подряд идущих простых чисел может быть в последовательности $\{y_n\}$?

8. Дано $k = 2^{2^n} + 1$. Докажите, что k простое тогда и только тогда, когда k является делителем числа $3^{\frac{k-1}{2}} + 1$.

9. Найдите все натуральные числа n, для которых $3^n - 1$ делится на $2^n - 1$.

10. Даны натуральные числа n и k. Оказалось, что $\varphi(5^n - 1) = 5^k - 1$. Докажите, что $(n, k) > 1$.

Другое доказательство

11. Умножение всех элементов приведенной системы вычетов по нечетному простому модулю p на вычет $a \not\equiv_p 0$ производит в ней перестановку.

(а) Докажите, что если a — квадратичный вычет по модулю p, то получившаяся перестановка четна.

(б) Докажите, что если a — квадратичный невычет по модулю p, то она нечетна.

12. Пусть p и q — различные нечетные простые числа. Рассмотрим два множества $M = \{0, 1, ..., pq-1\}$ и $M' = \{(a,b) | 0 \leqslant a < p, 0 \leqslant b < q\}$. Каждому элементу $x \in M$ поставим в соответствие пару $x' = (x_p, x_q) \in M'$, где $x_p \equiv_p x$ и $x_q \equiv_q x$. Заметим, что данное отображение будет биекцией между M и M'.

Рассмотрим пару отображений $f, g : M' \to M'$, заданную следующими равенствами: $f(a,b) = (a+pb)'$ и $g(a,b) = (qa+b)'$. Соответствующие им отображения из M в M мы также будем обозначать буквами f и g.

(а) Докажите, что f и g — перестановки на множестве M.

(б) Докажите, что перестановка f четна тогда и только тогда, когда $\left(\frac{p}{q}\right) = 1$.

(в) Рассмотрим перестановку $f \circ g^{-1}$ на множестве M . Вычислите число инверсий этой перестановки.

(г) При помощи предыдущих пунктов докажите квадратичный закон взаимности:

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.$$