Квадратичный закон взаимности

Квадратичный закон взаимности Гаусса. Если p, q — различные нечётные простые числа, то

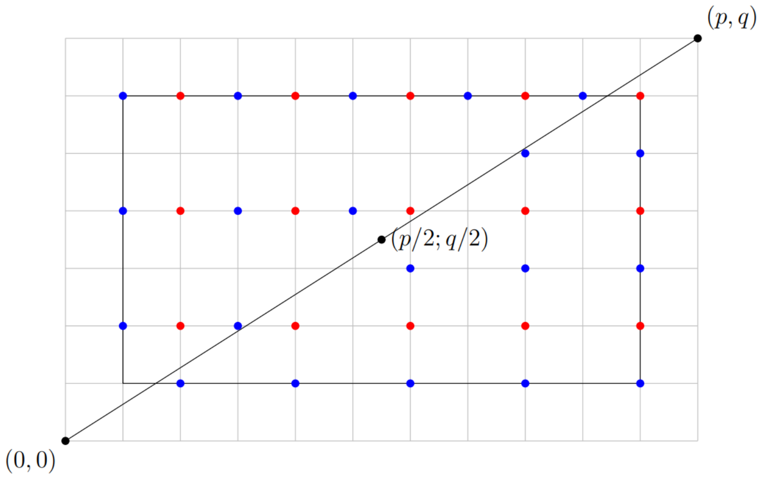
$$\left(\frac{p}{q}\right)\cdot\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

Давайте это докажем.

1. Рассмотрим множества остатков $P = \{1, 2, \dots, \frac{p-1}{2}\}$ и $S = \{-1, -2, \dots, -\frac{p-1}{2}\}$. Будем называть остатки из множества P «первичными», а остатки из множества S — «вторичными». Пусть также есть некоторое натуральное число a, взаимно простое с p.
(а) Докажите, что во множестве $\{a, 2a, \dots, \frac{p-1}{2}a\}$ есть ровно по одному остатку из каждой пары $\pm1, \pm2, \dots, \pm\frac{p-1}{2}$.
(б) Обозначим за $\varepsilon(a)$ число вторичных остатков во множестве $\{a, 2a, \dots, \frac{p-1}{2}a\}$. Докажите, что $\left(\frac{a}{p}\right) = (-1)^{\varepsilon(a)}$.
(в) Докажите, что первичный остаток i при умножении на a становится вторичным тогда и только тогда, когда $\left[\frac{2ai}{p}\right]$ — нечетное число. Выведите отсюда, что четность числа $\varepsilon(a)$ совпадает с четностью числа $\sum\limits_{i=1}^{\frac{p-1}{2}}\left[\frac{2ai}{p}\right]$.

То есть для доказательства закона взаимности достаточно проверить, что совпадают чётности чисел

$$\sum_{i=1}^{\frac{p-1}{2}}\left[\frac{2qi}{p}\right] + \sum_{i=1}^{\frac{q-1}{2}}\left[\frac{2pi}{q}\right] \quad \text{и} \quad \frac{p-1}{2}\cdot\frac{q-1}{2}.$$



2. Рассмотрим на координатной плоскости прямоугольник с вершинами $(0,0), (0,q), (p,q), (p,0)$ и прямую l с уравнением $py = qx$. Отметим целые точки строго внутри прямоугольника с чётной абсциссой, находящиеся ниже прямой l, и с чётной ординатой, находящиеся выше прямой l.
(а) Докажите, что число отмеченных точек ниже прямой l равно $\sum\limits_{i=1}^{\frac{p-1}{2}}\left[\frac{2qi}{p}\right]$, а выше — $\sum\limits_{i=1}^{\frac{q-1}{2}}\left[\frac{2pi}{q}\right]$.
(б) Отмеченные точки, у которых обе координаты чётные, покрасим в красный цвет, а остальные — в синий. Докажите, что синих точек чётно.
(в) Завершите доказательство квадратичного закона взаимности.

Теперь можно и задачи порешать

3. Найдите $\left(\frac{57}{179}\right)$.
4. Докажите, что -3 квадратичный вычет по модулю нечетного простого числа p тогда и только тогда, когда p дает остаток 1 при делении на 6.
5. Докажите, что при любом натуральном a все простые делители $a^2 - 5a + 5$ большие 5, имеют вид $5k \pm 1$.
6. Найдите наименьший простой делитель числа $12^{2^{15}} + 1$.
7. Найдите все натуральные n такие, что $3^n - 1 \,\vdots\, 2^n - 1$.
8. Найдите все такие простые p, что $p! + p$ — точный квадрат.