Квадратичный закон взаимности. Два способа доказательства.

God does arithmetic.

Carl Friedrich Gauss

1. **Старая задача.** Рассмотрев $2 \cdot 4 \cdot 6 \cdot \ldots \cdot (p-1)$ докажите, что $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

2. Пусть p — нечётное простое число, $t = \frac{p-1}{2}$, $0 < x \leqslant t$ и $(a, p) = 1$. Докажите, что

   (a) $ax \equiv (-1)^{\left[\frac{2ax}{p}\right]} \cdot r_x \ (mod\ p)$, где $0 < r_x \leqslant t$; **(b)** $\left(\frac{a}{p}\right) = (-1)^{\sum_{x=1}^{t}\left[\frac{2ax}{p}\right]}$.

   Теперь будем считать, что a — нечётное число. Докажите, что

   (c) $\left(\frac{2a}{p}\right) = \left(\frac{(a+p)/2}{p}\right)$; **(d)** $\left(\frac{2}{p}\right)\left(\frac{a}{p}\right) = (-1)^{\frac{p^2-1}{8} + \sum_{x=1}^{t}\left[\frac{ax}{p}\right]}$; **(e)** $\left(\frac{a}{p}\right) = (-1)^{\sum_{x=1}^{t}\left[\frac{ax}{p}\right]}$.

3. **Квадратичный закон взаимности Гаусса.**
   Пусть p и q — два простых нечётных числа. Докажите, что

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

4. **Доказательство Руссо квадратичный закон взаимности Гаусса.**
   Пусть p и q — два простых нечётных числа.
   Пусть $\mathbb{Z}_{pq}^*$ — множество остатков по модулю pq взаимно простых с p и q. Рассмотрим три подмножества $\mathbb{Z}_{pq}^*$:

$$A = \{a \in \mathbb{Z}_{pq}^* | a \equiv 1, 2, \ldots, \frac{p-1}{2} \ (mod\ p), a \equiv 1, 2, \ldots, q-1 \ (mod\ q)\};$$

$$B = \{b \in \mathbb{Z}_{pq}^* | b \equiv 1, 2, \ldots, p-1 \ (mod\ p), b \equiv 1, 2, \ldots, \frac{q-1}{2} \ (mod\ q)\};$$

$$C = \{c \in \mathbb{Z}_{pq}^* | c \equiv 1, 2, \ldots, \frac{pq-1}{2} \ (mod\ pq)\}.$$

   (a) Докажите, что произведение всех элементов в каждом из подмножеств даёт ± 1 по модулям p и q.
   (b) Поймите, как отличаются «знаки» у множеств A и B (надо найти отличие двумя способами: напрямую и используя множество C). Выведите из этого квадратичный закон.