Серия 30, квадратичный закон взаимности–1

20 июля

Определение 1. Напомним, что *символом Лежандра* называется выражение, обозначаемое $\left(\frac{a}{p}\right)$, равное 1, если a — квадратичный вычет по модулю p; -1, если a — невычет по модулю p; и 0, если a кратно p.

Также напомним, что $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$.

Теорема. Квадратичный закон взаимности. Пусть p и q — нечетные простые числа. Тогда выполнено

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

Приведем доказательство Е. И. Золотарёва, полученное им в 1872-м году. Для этого сначала введем понятие перестановки.

Определение 2. *Перестановкой* чисел $(1, 2, \ldots, n)$ будем называть их перестановку.

Определение 3. *Инверсией* перестановки $(a_1, a_2, \ldots, a_n)$ называется пара (a_i, a_k), где $i < k$, но $a_i > a_k$.

Определение 4. *Четностью* перестановки называется четность количества инверсий.

Лемма 0. Четность перестановки и обратной перестановки одинаковы.

Лемма 1. Пусть p — простое число, a — ненулевой остаток по модулю p. Определим перестановку $\pi := (a, 2a, 3a, \ldots, (p-1)a)$, где каждому числу соответствует его остаток по модулю p. Тогда эта перестановка четная, если a — квадратичный вычет по модулю p, и нечетная, если a — квадратичный невычет.

Чтобы доказать эту лемму, рассмотрим многочлен

$$P(x_1, x_2, \ldots, x_{p-1}) = \prod_{1 \leqslant i < j \leqslant p-1} (x_i - x_j).$$

Применим к переменным перестановку. Тогда многочлен не меняется, если π четна, и меняет знак на противоположный, если π нечетна.

Подставим $x_i = i$ и применим перестановку π, то есть подставим $x_i = ai$. Знак перестановки (1 для четной и -1 для нечетной) можно определить как

$$\frac{P(1, 2, \ldots, p-1)}{P(a, 2a, \ldots, (p-1)a)} = \prod_{1 \leqslant i < j \leqslant p-1} \frac{ai - aj}{i - j} \equiv a^{(p-1)p/2} \equiv a^{(p-1)/2} \pmod p,$$

что совпадает по знаку с символом Лежандра $\left(\frac{a}{p}\right)$.

Теперь зададим перестановку τ на числах $\{0, 1, 2, \ldots, pq-1\}$, где p и q — два нечетных простых числа, для которых мы доказываем КЗВ. Представим каждое число от 0 до $pq-1$ как $x = a + bp$, $0 \leqslant a \leqslant p-1$, $0 \leqslant b \leqslant q-1$ (такое представление единственно). Сопоставим $\tau : a + bp = x \to y = b + aq$.

1. Лемма 2. Четность перестановки τ определена как

$$\operatorname{sign} \tau = (-1)^{(p-1)(q-1)/4}.$$

2. Завершите доказательство КЗВ, связав четность перестановок π и τ.

3. Пусть $(n, k) = 1$. Пусть $(a, n) = 1$ и $(a, k) = 1$. Докажите, что число a является квадратичным вычетом по модулю nk тогда и только тогда, когда оно является квадратичным вычетом по модулям n и k.

4. Пусть p — нечетное простое число, $n \in \mathbb{N}$. Докажите, что a является квадратичным вычетом по модулю p^n тогда и только тогда, когда a является квадратичным вычетом по модулю p.

5. Докажите, что a является квадратичным вычетом по модулю 2^n (где $n > 3$) тогда и только тогда, когда a является квадратичным вычетом по модулю 8.