Доказательство квадратичного закона взаимности по Золотарёву

В. В. Прасолов

Квадратичный закон взаимности выражает связь между следующими двумя свойствами простых чисел p и q:

▷ число p сравнимо с некоторым квадратом целого числа по модулю q,

▷ число q сравнимо с некоторым квадратом целого числа по модулю p.

Первым эту связь обнаружил Эйлер и высказал соответствующую гипотезу, которую в некоторых частных случаях доказал Лежандр, а первое полное доказательство получил Гаусс. Сейчас известно много разных доказательств квадратичного закона взаимности. Одно из наиболее простых доказательств предложил в 1872 г. известный русский математик Егор Иванович Золотарёв[1)]. Его статья [12] опубликована по-французски. Идея Золотарёва обсуждалась довольно часто, но только в работах иностранных авторов (см. список литературы в конце статьи).

Для полноты мы докажем китайскую теорему об остатках, но следующие более элементарные сведения о сравнениях предполагаются известными:

▷ если числа m и n взаимно просты, то для любого целого числа a разрешимо сравнение $mx \equiv a \pmod{n}$,

▷ если p — простое, то для любого целого числа $a \not\equiv 0 \pmod{p}$ формула $x \bmod p \mapsto ax \bmod p$ задаёт перестановку множества $\{1, 2, \ldots, p-1\}$.

Несложно показать, что если p — простое число, то $a^p \equiv a \pmod{p}$ (*малая теорема Ферма*). Действительно, интересен лишь случай, когда $a \not\equiv 0 \pmod{p}$. В этом случае формула $x \bmod p \mapsto ax \bmod p$ задаёт перестановку множества $\{1, 2, \ldots, p-1\}$. Следовательно,

$$1 \cdot 2 \cdot \ldots \cdot (p-1) \equiv a \cdot (2a) \cdot \ldots \cdot (p-1)a \equiv a^{p-1}\bigl(1 \cdot 2 \cdot \ldots \cdot (p-1)\bigr) \pmod{p}.$$

После сокращения получаем $1 \equiv a^{p-1} \pmod{p}$.

[1)] Золотарёв (1847–1878) прожил только 31 год, но и за это короткое время он уже успел написать ряд работ первостепенной важности. 26 июня 1878 г. Золотарёв поехал на поезде на дачу к знакомым. На промежуточной станции он вышел из вагона и, когда поезд тронулся, попал под паровоз. Его извлекли из-под колес со смятой ступней и переломанной выше колена ногой. Он скончался после 12 дней тяжелых страданий.

Математическое просвещение, сер. 3, вып. 4, 2000(140–144)

Доказательство малой теоремы Ферма достаточно хорошо известно, но мы сочли нужным его напомнить, потому что оно имеет много общего с основной идеей Золотарёва.

1. Китайская теорема об остатках

Теорема 1. *Пусть числа $m_1, \ldots, m_k$ попарно взаимно простые и $m = m_1 \cdot \ldots \cdot m_k$. Тогда для любых целых чисел $a_1, \ldots, a_k$ система сравнений $x \equiv a_i \pmod{m_i}$, $i = 1, \ldots, k$, имеет решение, причём если x_1 и x_2 — два решения, то $x_1 - x_2$ делится на m.*

Доказательство. Положим $n_i = m/m_i$. Число n_i является произведением чисел, взаимно простых с m_i, поэтому $(n_i, m_i) = 1$. В таком случае можно выбрать целые числа r_i и s_i так, что $r_i m_i + s_i n_i = 1$. Положим $e_i = s_i n_i$ и $x = a_1 e_1 + \cdots + a_k e_k$. Ясно, что $e_i \equiv 1 \pmod{m_i}$ и $e_i \equiv 0 \pmod{m_j}$ при $j \neq i$, поэтому $x \equiv a_i \pmod{m_i}$, $i = 1, \ldots, k$.

Если x_1 и x_2 — решения рассматриваемой системы сравнений, то $x_1 - x_2 \equiv 0 \pmod{m_i}$, $i = 1, \ldots, k$. Числа $m_1, \ldots, m_k$ попарно взаимно простые, поэтому $x_1 - x_2$ делится на m.

2. Квадратичные вычеты и невычеты

Пусть p — простое число. Число a, не делящееся на p, называют *квадратичным вычетом* по модулю p, если $x^2 \equiv a \pmod{p}$ для некоторого целого числа x; в противном случае число a называют *квадратичным невычетом.*

Для простого числа p *символ Лежандра* $\left(\dfrac{a}{p}\right)$ определяется следующим образом:

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

Символ Лежандра мы иногда будем обозначать (a/p).

Теорема 2 (Лежандр). *Пусть p — нечётное простое число. Тогда*

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}.$$

Доказательство. Пусть $\mathbb{F}_p$ — поле вычетов по модулю p, обозначим $\mathbb{F}_p^* = \mathbb{F}_p \setminus \{0\}$. Рассмотрим отображение $\mathbb{F}_p^* \to \mathbb{F}_p^*$, заданное формулой $x \mapsto x^2$. Прообраз каждого элемента либо пуст, либо состоит из двух элементов x и $-x$, поэтому образ состоит из $(p-1)/2$ элементов. С другой стороны, если $a = x^2$, то $a^{(p-1)/2} = x^{p-1} = 1$, поэтому все элементы образа являются корнями уравнения $X^{(p-1)/2}=1$, которое не может иметь более $(p-1)/2$ корней. Остаётся заметить, что все элементы $\mathbb{F}_p^*$ являются корнями уравнения $X^{p-1}=1$, поэтому невычеты являются корнями уравнения $X^{(p-1)/2}=-1$.

Следствие 1. $\left(\dfrac{ab}{p}\right)=\left(\dfrac{a}{p}\right)\left(\dfrac{b}{p}\right)$.

Следствие 2.

$$\left(\frac{-1}{p}\right)=\begin{cases}1 & \textit{при } p=4k+1,\\ -1 & \textit{при } p=4k+3.\end{cases}$$

Обобщением символа Лежандра является *символ Якоби*, который обозначается точно так же и определяется следующим образом. Пусть $m = p_1\cdot\ldots\cdot p_k$, где $p_1,\ldots,p_k$ нечётные простые числа (не обязательно различные). Тогда

$$\left(\frac{a}{m}\right)=\left(\frac{a}{p_1}\right)\cdot\ldots\cdot\left(\frac{a}{p_k}\right).$$

Пример. $\left(\dfrac{2}{15}\right)=\left(\dfrac{2}{3}\right)\left(\dfrac{2}{5}\right)=(-1)(-1)=1$, *но* $2\not\equiv x^2 \pmod{15}$.

Золотарёв предложил следующую интерпретацию символа Лежандра, которую затем Фробениус [4] перенёс и на символ Якоби.

Теорема 3 (Золотарёв – Фробениус). *Пусть m — нечётное число, a — число, взаимно простое с m, и $\pi_{a,m}: i\mapsto ai \bmod m$ — подстановка на множестве остатков от деления на m. Тогда $\operatorname{sgn}\pi_{a,m}=(a/m)$, где $\operatorname{sgn}\pi_{a,m}$ — знак подстановки $\pi_{a,m}$.*

Доказательство. Рассмотрим многочлен

$$A(x_1,\ldots,x_m)=\prod_{1\leqslant i<j\leqslant m}(x_i-x_j).$$

Под действием чётной подстановки многочлен A не изменяется, а под действием нечётной подстановки он изменяет знак. Поэтому знак любой подстановки σ равен отношению $A(x_{\sigma(1)},\ldots,x_{\sigma(m)})$ к $A(x_1,\ldots,x_m)$. Положим $x_1=1,\ldots,x_m=m$. Тогда

$$\begin{aligned}\operatorname{sgn}\pi_{a,m} &= \prod_{1\leqslant i<j\leqslant m}\frac{\pi_{a,m}(i)-\pi_{a,m}(j)}{i-j}\equiv\prod_{1\leqslant i<j\leqslant m}\frac{ai-aj}{i-j}\equiv\\ &\equiv\prod_{1\leqslant i<j\leqslant m}a\equiv a^{m(m-1)/2}\pmod{m}.\end{aligned}$$

Учитывая, что $a^m\equiv a\pmod{m}$, получаем

$$\operatorname{sgn}\pi_{a,m}\equiv a^{(m-1)/2}\equiv(a/m)\pmod{m}.$$

3. Квадратичный закон взаимности

Теорема 4 (квадратичный закон взаимности). *Пусть m и n — нечётные взаимно простые числа. Тогда*

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

Доказательство. [11] Пусть $P = \{0, 1, \ldots, mn-1\}$ и $\overline{P} = \{\,(a, b) \mid 0 \leqslant a < m,\ 0 \leqslant b < n\}$. Согласно китайской теореме об остатках отображение $c \mapsto \bar{c} = (c \bmod m, c \bmod n)$ является взаимно однозначным отображением P на $\overline{P}$.

Рассмотрим отображения $\mu, \nu\colon \overline{P} \to \overline{P}$, заданные формулами $\mu(a, b) = \overline{a + mb}$ и $\nu(a, b) = \overline{na + b}$. Ясно, что $\mu(a, b) = (a,\ a + mb \bmod n)$, поэтому отображение μ переставляет элементы вида (a_0, b), где a_0 фиксировано. Следовательно, μ — подстановка множества $\overline{P}$ и $\operatorname{sgn}\mu = \left(\frac{m}{n}\right)^m = \left(\frac{m}{n}\right)$. Аналогично $\operatorname{sgn}\nu = \left(\frac{n}{m}\right)$.

Рассмотрим теперь на множестве P подстановку $\nu^{-1}\mu\colon na + b \mapsto a + mb$. Знак этой подстановки равен $(-1)^k$, где k — количество пар элементов множества $\overline{P}$, для которых выполняются неравенства $na + b > na' + b'$ и $a + mb < a' + mb'$. По условию $|b - b'| < n$ и $|a - a'| < m$, поэтому приходим к следующим неравенствам: $a > a'$ и $b < b'$. Таким образом, $k = \binom{n}{2}\binom{m}{2} = \frac{m-1}{2}\cdot\frac{n-1}{2}$. В итоге получаем

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = \operatorname{sgn}\mu \operatorname{sgn}\nu = \operatorname{sgn}\nu^{-1}\mu = (-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}.$$

Следствие. *Пусть m — нечётное число. Тогда*

$$\left(\frac{2}{m}\right) = (-1)^{(m^2-1)/8}.$$

Доказательство. При $m = 3$ требуемое равенство легко проверяется. Предположим, что $m \geqslant 3$ — нечётное натуральное число, для которого выполняется требуемое равенство. Тогда

$$\begin{aligned}\left(\frac{2}{m+2}\right) &= \left(\frac{-1}{m+2}\right)\left(\frac{m}{m+2}\right) = (-1)^{\frac{m+1}{2}}(-1)^{\frac{m-1}{2}\cdot\frac{m+1}{2}}\left(\frac{m+2}{m}\right) = \\ &= (-1)^{\frac{m+1}{2}}\left(\frac{2}{m}\right) = (-1)^{\frac{m+1}{2}}(-1)^{\frac{m^2-1}{8}} = (-1)^{\frac{(m+2)^2-1}{8}}.\end{aligned}$$

Отметим, что как правило в учебниках по теории чисел сначала доказывают равенство $\left(\frac{2}{m}\right) = (-1)^{(m^2-1)/8}$, а уже затем доказывают квадратичный закон взаимности. Но это равенство не требует отдельного доказательства, оно следует из квадратичного закона взаимности.

Список литературы

[1] *Brenner J. L.* Zolotarev's theorem on the Legendre symbol // Pacific J. Math., 1973. Vol. 45. P. 413–414.

[2] *Cartier P.* Sur unegénéralization des symboles de Legendre–Jacobi // L'Ens. Math., 1970. Vol. 16. P. 31–48.

[3] *Dressler R. E., Shult E. E.* A simple proof of the Zolotareff–Frobenius theorem // Proc. Amer. Math. Soc., 1975. Vol. 54. P. 53–54.

[4] *Frobenius G.* Über das quadratische Reziprozitätsgesetz, I. S.-B. Preuss. Akad. Wiss., Berlin, 1914, P. 335–349.

[5] *Lehmer D. H.* The characters of linear permutations // Linear and Multilinear Algebra, 1976. Vol. 4. P. 1–16.

[6] *Lerch M.* Sur un thórème arithmetique de Zolotarev // Česka Acad., Bull. Int. Cl. Math., 1986. Vol. 3. P. 34–37.

[7] *Morton P.* A generalization of Zolotarev's theorem // Amer. Math. Monthly, 1979. Vol. 86. P. 374–376.

[8] *Riesz M.* Sur le lemme de Zolotareff et sur la loi de réciprocité des restes quadratiques // Math. Scand., 1953. Vol. 1. P. 159–169.

[9] *Rousseau G.* Exterior algebras and the quadratic reciprocity law // L'Ens. Math., 1990. Vol. 36. P. 303–308.

[10] *Rousseau G.* On the quadratic reciprocity law // J. Austral. Math. Soc. (Series A), 1991. Vol. 51. P. 423–425.

[11] *Rousseau G.* On the Jacobi symbol // J. Number Theory, 1994. Vol. 48. P. 109–111.

[12] *Zolotareff G.* Nouvelle démonstration de la loi de réciprocité de Legendre // Nouv. Ann. Math. (2), 1872. Vol. 11. P. 354–362.