View metadata, citation and similar papers at core.ac.uk
brought to you by CORE

ЧЕБЫШЕВСКИЙ СБОРНИК
Том 14 Выпуск 4 (2013)

ПЕРЕСТАНОВКИ И КВАДРАТИЧНЫЙ ЗАКОН ВЗАИМНОСТИ ПО ЗОЛОТАРЕВУ — ФРОБЕНИУСУ — РУССО

Е. А. Горин (Москва)

Аннотация

Приводится первое на русском языке корректное доказательство квадратичного закона взаимности, основанное на идее Золотарева.

Ключевые слова: Перестановки, символ Якоби, закон взаимности.

PERMUTATIONS AND RECIPROCITY LAW BY ZOLOTAREV — FROBENIUS — RUSSO

E. A. Gorin (c. Moscow)

Abstract

Given the first correct proof of the reciprocity law in Russian which based on the Zolotarev idea.

Keywords: Permutations, Jacobi symbol, reciprocity law.

Классический вариант квадратичного закона взаимности устанавливает связь между разрешимостью сравнений

$$x^2 \equiv q \pmod{p} \quad \text{и} \quad x^2 \equiv p \pmod{q},$$

где p и q — различные нечетные простые числа.

Для формулировки квадратичного закона взаимности требуется понятие *символа Лежандра*. Пусть a — целое число и $p \geqslant 3$ простое, причем a не делится на p. Тогда символ Лежандра определяется равенством

$$(a/p) \stackrel{\text{def}}{=} \begin{cases} +1, & \text{если сравнение } \ x^2 = a \pmod{p} \text{ разрешимо,} \\ -1, & \text{если сравнение } \ x^2 = a \pmod{p} \text{ не разрешимо.} \end{cases}$$

Часто удобно считать, что $(a/p) = 0$, если a делится на p.

Заметим, что обычно символ Лежандра изображают в столбик и используют горизонтальную черту, однако мы предпочитаем писать в строчку и использовать косую черту.

Простейший вариант квадратичного закона взаимности заключается в том, что

$$(p/q) \cdot (q/p) = (-1)^{(p-1)(q-1)/4}. \tag{1}$$

Формулировку квадратичного закона взаимности знал Эйлер. Попытку предъявить доказательство предпринял Лежандр, однако его рассуждение, как оказалось, содержало пробел.

Первое полное (но не простое) доказательство дал Гаусс в 1801 году. В дальнейшем в течение 30 лет Гаусс неоднократно возвращался к квадратичному закону взаимности и нашел еще 5 (или больше) доказательств, упрощающих исходное или основанных на других идеях.

В дальнейшем к квадратичному закону взаимности и его обобщениям обращались и многие другие авторы, и к настоящему времени известны сотни вариантов доказательства.

Интересное доказательство изобрел в свое время Е. И. Золотарев (1847–1878) [1]. Исходная идея Золотарева состоит в следующем. Пусть целое число a не делится на простое нечетное p. Пусть $\mathbb{Z}$ — кольцо целых чисел, (p) — идеал чисел, кратных p, и $\mathbb{Z}/(p)$ — поле вычетов по модулю p. Отображение $x \to ax$ биективно в $\mathbb{Z}/(p)$ и, стало быть, определяет перестановку этого конечного множества. Обозначим через $[a/p]$ четность *такой* перестановки. Исходная теорема Золотарева состоит в том, что $(a/p) = [a/p]$. Таким образом, дело сводится к сравнению четности перестановок (сравнение четности — отдельная и не вполне тривиальная задача).

В развитие идей Золотарева в начале XX–го века Фробениус [2] распространил квадратичный закон взаимности на символы Якоби.

Пусть $p = p_1 p_2 p_2 \ldots$ — (конечное) разложение нечетного положительного целого числа p в произведение (не обязательно различных) простых чисел p_i и пусть a взаимно просто с p. Напомним, что символ Якоби сводится к символу Лежандра, когда p — простое число, и в общем случае определяется равенством

$$(a/p) = (a/p_1) \cdot (a/p_2) \cdot (a/p_3) \cdot \ \ldots$$

(обозначение не меняется).

В небольшой прозрачной заметке [3] Руссо дал короткое, но полное доказательство теоремы Фробениуса. Вместе с тем, он заметил, что «it seems not to have been observed that a still greater simplification in the theory of quadratic residues is achieved when the ideas of [1] are given full weight».

На русском языке доказательство теоремы Гаусса по Золотареву (и уже́ в форме Фробениуса) впервые было опубликовано только в 2000-ом году в заметке В.В.Прасолова [4].

Прасолов ссылается на заметку Руссо, однако его рассуждения не полны, они приводят к теореме Гаусса, но не к теореме Фробениуса, так как он использует простоту и там, где её нет.

Цель данной работы — дать аккуратное и подробное изложение вопроса. В частности, я не стремлюсь к краткости. Кроме стандартных источников, я имею в виду обе указанные заметки. Некоторые классические результаты приведены с доказательствами, в небольшом числе случаев я заменяю фрагменты известных рассуждений собственными. Вместе с тем, статья в основном имеет методический характер.

1. Перестановки и подстановки

Пусть $X = \{a, b, c, \ \dots\}$ — конечное множество, содержащее $n \geqslant 2$ элементов. Биективное отображение $\sigma : X \to X$ называется *перестановкой* множества X. Простейшее изображение перестановки σ представляет строчка

$$(\sigma(a), \sigma(b), \sigma(c), \ \dots\ ).$$

Более детально ту же перестановку записывают в виде таблицы из двух строчек:

$$\begin{pmatrix} a & b & c & \dots \\ \sigma(a) & \sigma(b) & \sigma(c) & \dots \end{pmatrix}. \tag{2}$$

Таблица (2) называется *подстановкой*, отвечающей перестановке σ. При фиксированном порядке элементов исходного множества подстановка — это как бы перевернутый график перестановки. Вместе с тем, меняя местами (целиком) столбцы этой таблицы, мы будем получать подстановки, отвечающие той же перестановке.

Относительно суперпозиций множество $S(X)$ всех перестановок образует группу, которая называется *симметрической*. Операцию в этой группе мы будем обозначать по–простому, например, $\sigma_1\sigma_2$ или $\sigma_1 \cdot \sigma_2$.

Если $X = \{1, 2, 3, \ \dots\ , n\}$, то симметрическая группа обозначается $S(n)$. Симметрические группы из n элементов алгебраически изоморфны. Вместе с тем, при рассмотрении $S(n)$ мы можем использовать её арифметическую природу. Это предоставляет дополнительные возможности. Поэтому зачастую, особенно в элементарных текстах, другие симметрические группы игнорируют (см., например, [5] или [6]). Однако, нередко такой подход не проясняет дело, так как некоторые понятия за пределами $S(n)$ теряют наглядность или выглядят искусственными. Мы предпочитаем простые общие рассуждения, однако будем применять смешанную стратегию, по возможности упрощая формулировки и доказательства.

Пусть $a, b \in X$, причем $a \neq b$. *Транспозиция* $\tau = \tau_{a,b}$ — это перестановка, для которой

$$\tau(x) = \begin{cases} b, & \text{если } x = a, \\ a, & \text{если } x = b, \\ x & \text{в остальных случаях.} \end{cases}$$

Довольно часто вместо $\tau_{a,b}$ пишут (a, b) (и мы тоже будем так делать), однако не следует забывать, что аналогично обозначается и многое другое. Тождественная перестановка обозначается ϵ.

Теперь мы собираемся ввести понятие *четности перестановки*. Понятие четности обычно относят к самым элементарным, однако мы решили здесь дать аккуратное определение. По существу мы следуем по пути, указанному в [5, с.65], но несколько иначе расставляем акценты.

Лемма 1. *Пусть* $X = \{a, b, c, \ \dots\}$. *Тогда*

$$(b, c)(a, b) = (a, c)(b, c). \tag{3}$$

Тождество (3) легко проверяется. Смысл этого тождества в том, что транспозиция, включающая элемент a, смещается влево (см. ниже). □

Легко доказать, что каждая перестановка представляется в виде произведения конечного числа транспозиций. Такое представление, не единственно (пример, в частности, дает формула (3)).

Теорема 1. *Четность числа сомножителей представления перестановки в виде произведения транспозиций одинакова во всех представлениях.*

Схема доказательства. Предположим, что для каких–нибудь двух представлений четность различна. Убедимся, что это приводит к противоречию.

Пусть ϵ — тождественная перестановка. В указанном предположении приравняем друг другу представления. Так как $\tau^2 = \epsilon$ для каждой транспозиции, то получится, что

$$\epsilon = \tau_1 \cdot \tau_2 \cdot \ \dots \ \cdot \tau_{k-1} \cdot \tau_k \cdot \tau_{k+1} \cdot \ \dots \ \cdot \tau_m, \tag{4}$$

где m — *нечетное* натуральное число, а τ_i — транспозиции.

Мы проведем индукцию по m, чтобы установить *невозможность* представления ϵ в виде произведения нечетного числа транспозиций (и тем самым теорема 1 будет доказана).

Фиксируем какое–нибудь $a \in X$, присутствующее хотя бы в одной транспозиции τ_i. Для определенности будем считать, что $\tau_k = (a, b)$ при $k > 1$ в формуле (4), но τ_i оставляет на месте a при $i > k$. Кроме того, считаем, что $\tau_i = \varepsilon$, если $i < 1$.

При $m = 1$ возникает противоречие, так как ϵ не является транспозицией. Легко видеть, что и при каждом $m \geqslant 3$ противоречие также возникнет, если τ_1

перемещает a. Действительно, такое представление тождественной перестановки ϵ приводит к равенству

$$\tau_1 = \tau_2 \cdot \tau_3 \cdot \ \ldots \ \cdot \tau_m.$$

В этом равенстве справа стоит перестановка, оставляющая a на месте, тогда как транспозиция τ_1 перемещает. Эта информация о начальной перестановке произведения, представляющего ϵ как раз и позволит провести индукцию по m (а при фиксированном m — по k). В дальнейшем считается, что $m \geqslant 3$.

Если $\tau_{k-1} = \tau_k$, то $\tau_{k-1} \cdot \tau_k = \tau_k^2 = \epsilon$, и m меняется на $m-2$. По предположению индукции, такого представления нет.

При фиксированном m рассмотрим (снова по индукции) случай общего k.

Если перестановка τ_{k-1} оставляет на месте и a, и b, то $\tau_{k-1} \cdot \tau_k = \tau_k \cdot \tau_{k-1}$. Меняя местами τ_{k-1} и τ_k, мы получим представление, в котором m сохраняется, но самая левая перестановка, содержащая a, смещается на шаг влево. Однако это исключено, и остается рассмотреть случаи, когда $\tau_{k-1} = (b, c)$ или $\tau_{k-1} = (c, d)$, где все элементы a, b, c, d попарно различны. В первом случае можно применить лемму 1 и добиться аналогичного смещения влево. Во втором случае перестановки коммутируют.

Таким образом, во всех случаях, сохраняя m, удается заменить k на $k - 1$. □

Четность числа транспозиций, произведение которых представляет данную перестановку π, называется *четностью (знаком, сигнатурой) перестановки.* По теореме 1 это определение корректно. Для четности чаще всего используется обозначение $\operatorname{sgn}(\pi)$.

Из теоремы 1 сразу вытекает, что $\operatorname{sgn}(\pi_1 \cdot \pi_2) = \operatorname{sgn}(\pi_1) \cdot \operatorname{sgn}(\pi_2)$. Это означает, что $\chi : \pi \to \operatorname{sgn}(\pi)$ — гомоморфизм из $S(X)$ в $\{\pm 1, \times\}$ (мультипликативный вариант группы $\mathbb{Z}/(2)$). Других нетривиальных гомоморфизмов из $S(X)$ в $\{\pm 1, \times\}$ нет, и это означает, что понятие четности определяется в абстрактных терминах[1]. В частности, четные перестановки, составляют (единственный) нормальный делитель в $S(X)$. Эту подгруппу часто называют *знакопеременной.*

Вычислять четность перестановки при помощи приведенного определения, вообще говоря, утомительно. Однако есть довольно простой способ это сделать (детали см., например, в [5]).

Удобно рассмотреть вместо общей группы группу $S(n)$ (или записать элементы исходного множества в виде последовательности). Подстановку (2) можно выбрать в простейшей форме:

$$\begin{pmatrix} 1 & 2 & 3 & \ldots \\ \sigma(1) & \sigma(2) & \sigma(3) & \ldots \end{pmatrix}.$$

[1]Единственность такого гомоморфизма (характера) доказать легко. Однако совсем простого доказательства существования я не нашел.

Беспорядком (или инверсией) называется такая пара $\sigma(i), \sigma(k)$, что $i < k$, но $\sigma(i) > \sigma(k)$.

Легко проверить, что если поменять друг с другом места двух элементов второй строки, создающих беспорядок, то мы *уменьшим число беспорядков и изменим его четность*. Вместе с тем, эта процедура реализуется умножением на транспозицию. Отсюда легко вывести, что *четность перестановки совпадает с четностью числа беспорядков*. Заметим, что в числовом случае число беспорядков в перестановке совпадает с числом таких пар, в которых большее число стоит левее меньшего.

Однако вместо простейшей подстановки можно использовать любую другую, отвечающую той же перестановке. Поэтому дело не в расположении элементов (левее, правее), а в том, что для пары x, y верхней строки выполняется неравенство $x < y$, тогда как $\sigma(x) > \sigma(y)$ (*инверсия подстановки*).

Пусть p и q — нечетные целые числа $\geqslant 3$. Положим $X = \{0, 1, 2, 3, \ \dots\ , pq - 1\}$. Каждое число $x \in X$ можно разделить с остатком на p, т.е. однозначно представить в виде $x = a + bp$, где $0 \leqslant a < p$. Заметим, что $b < q$. Аналогичное представление возникает при замене p на q. Нечетность p и q пока не использовалась.

В результате возникает перестановка $\pi\colon a + bp = x \to y = b + aq$ множества X.

Лемма 2. *При нечетных p, q*

$$\operatorname{sgn}(\pi) = (-1)^{(p-1)(q-1)/4}. \tag{5}$$

Доказательство. Пусть

$$\begin{pmatrix} x_0 & x_1 & x_2 & \dots \\ y_0 & y_1 & y_2 & \dots \end{pmatrix} \tag{6}$$

— какая-нибудь подстановка, отвечающая перестановке π. Таким образом, строки таблицы (6) содержат по $pq - 1$ элементов (т.е. по разу все элементы множества X) и, в соответствии со сказанным выше, $x_i = a_i p + b_i$, $y_i = b_i q + a_i$.

Мы должны убедиться, что число инверсий в подстановке (6) является четным или нет в зависимости от знака правой части в (5).

Инверсия имеет место тогда и только тогда, когда $x_i < x_k$ и одновременно $y_i > y_k$. Легко проверить, что такое сочетание равносильно совокупности неравенств $a_i < a_k$ и $b_i > b_k$.

Числа a_i независимо принимают p различных значений, $0 \leqslant a_i < p$. Поэтому неравенство $a_i < a_k$ выполняется в $p(p-1)/2$ случаях (число сочетаний). Аналогично, второе неравенство выполняется в $q(q-1)/2$ случаях. Произведение r этих чисел и есть число инверсий. Четность этого числа определяется знаком числа $(-1)^r$. Так как p и q — нечетные числа, то множитель pq можно устранить из состава r в окончательной формуле. □

2. Классы вычетов по составному модулю

Напомним, что число 1 не считается простым, причисляется к делителям каждого натурального числа и одновременно — взаимно простым с каждым таким числом.

Пусть G — подгруппа группы $\mathbb{Z}$, причем $G \neq \{0\}$. Пусть d — наименьшее положительное число из G. Из правила деления с остатком вытекает, что d — делитель всех элементов группы G, т.е. $G = d \cdot \mathbb{Z}$.

Предположим теперь, что G порождается взаимно простыми числами p и q. Так как $\gcd(p, q) = 1$, то $d = 1$, т.е. $G = \mathbb{Z}$. В частности, $1 \in G$.

Поэтому найдутся такие $a, b \in \mathbb{Z}$, что

$$aq + bp = 1. \tag{7}$$

Пусть $X = \{\xi \in \mathbb{Z} \mid 0 \leqslant \xi < p\}$ и $Y = \{\eta \in \mathbb{Z} \mid 0 \leqslant \eta < q\}$. Множества X и Y суть (полные) множества минимальных неотрицательных вычетов по модулям p и q соответственно. Чтобы не отвлекаться на это в дальнейшем, положим еще $Z = \{\zeta \in \mathbb{Z} \mid 0 \leqslant \zeta < pq\}$ (это множество, иначе обозначенное, ужé появлялось перед леммой 2). Переходя от равенства (7) к сравнению по модулю pq, мы можем считать, что $a \in X$ и $b \in Y$. Тем самым возникает соотношение

$$aq + bp \equiv 1 \pmod{pq}. \tag{8}$$

Числа aq и bp в сравнении (8) оба содержатся в Z. При фиксированном модуле m (в нашем случае $m = pq$) их образы в $\mathbb{Z}/(m) = \mathbb{Z}/(pq)$ будут обозначаться e_1, e_2 соответственно.

Легко убедиться, что выполняются следующие соотношения:

(a) $aq \equiv 0 \pmod{q}$, $aq \equiv 1 \pmod{p}$ и $bp \equiv 0 \pmod{p}$, $bp \equiv 1 \pmod{q}$;

(b) $e_1 + e_2 = e$, где e — единица кольца $\mathbb{Z}/(pq)$;

(c) $e_1^2 = e_1$, $e_2^2 = e_2$ (т.е. e_1, e_2 — идемпотенты);

(d) $e_1 \cdot e_2 = 0$ («ортогональность»);

(e) $p \cdot e_1 = q \cdot e_2 = (pq) \cdot e = 0$.

Из этих соотношений, в частности, вытекает, что *для каждого $z \in \mathbb{Z}$ существуют такие однозначно определенные $x \in X$ и $y \in Y$, что $z \cdot e = x \cdot e_1 + y \cdot e_2$.*

Коротко сказанное можно переписать в виде

$$\mathbb{Z}/(pq) = \mathbb{Z}/(p) \oplus \mathbb{Z}/(q) \tag{9}$$

(*естественный* алгебраический изоморфизм).

Заметим, что прямые «слагаемые» $\mathbb{Z}/(p)$ и $\mathbb{Z}/(q)$ можно считать идеалами в $\mathbb{Z}/(pq)$ (со своими единицами e_1, e_2).

Формуле (9) можно придать «геометрический» вид:

$$Z = X \times Y \tag{10}$$

(*естественное* декартово произведение). Z становится «прямоугольником» в решетке $\mathbb{Z}^2$ евклидовой плоскости $\mathbb{R}^2$. Множество X располагается на оси абсцисс и изображает нижнее основание, а множество Y — на оси ординат и изображает левую сторону.

Алгебраические операции естественно переносятся с Z на $\mathbb{Z}/(pq)$. Представление (10), как мы увидим, делает наглядными некоторые рассуждения.

3. Закон взаимности для перестановок

Пусть $m \geqslant 3$ — нечетное натуральное число и пусть $a, b \in \mathbb{Z}/(m)$, причем a — обратимый элемент. Отображения $\alpha\colon x \to ax$ и $\beta\colon x \to ax+b$ оба биективны на $\mathbb{Z}/(m)$, т.е. являются перестановками.

Лемма 3. $\operatorname{sgn}(\alpha) = \operatorname{sgn}(\beta)$.

Схема доказательства. Пусть e — единица кольца $\mathbb{Z}/(m)$. Так как m — нечетное число, то перестановка $x \to x + e$, как легко проверить, является четной. Поэтому четной будет и перестановка $x + b$. Суперпозиция этой перестановки с α совпадает с β. □

Следующая теорема играет ключевую роль.

Теорема 2. *Если $p, q \geqslant 3$ — нечетные взаимно простые числа, то*

$$[p/q] \cdot [q/p] = (-1)^{(p-1)(q-1)/4}.$$

Доказательство. При переменных $x \in X,\ y \in Y$ зададим перестановку λ кольца $\mathbb{Z}/(pq)$ формулой

$$\lambda\colon (y + qx) \cdot e \to (x + py) \cdot e. \tag{11}$$

При делении с остатком на q или p каждое число из Z получает левое или правое представление соответственно из формулы (11). Это означает, что λ по существу совпадает с π из леммы 2. Следовательно, $\operatorname{sgn}(\lambda)$ вычисляется по той же формуле (5). Заметим, что $(y + qx)e = (y + qx)e_1 + ye_2$, так как $qe_2 = 0$. Зададим перестановку μ кольца $\mathbb{Z}/(pq)$ формулой

$$\mu\colon xe_1 + ye_2 \to (y + qx)e_1 + ye_2. \tag{12}$$

Для наглядности эту перестановку имеет смысл рассматривать как перестановку дискретного прямоугольника $Z = X \times Y$.

При фиксированном y перестановка (12) сводится к перестановке дискретного отрезка, «параллельного» отрезку X и расположенного на высоте y. По лемме 3, четность этой перестановки определяется числом $[q/p]$. По теореме 1 это же число определяет четность числа транспозиций, которые достаточно осуществить, чтобы привести данный отрезок «в порядок». Вместе с тем, количество таких отрезков равно q и, стало быть, нечетно. Следовательно, $\operatorname{sgn}(\mu) = [q/p]$.

Аналогично рассматривается перестановка

$$\nu\colon xe_1 + ye_2 \to (x + py)e_2 + xe_1,$$

и это дает: $\operatorname{sgn}(\nu) = [p/q]$. Очевидно, что $\nu \cdot \mu^{-1} = \lambda$. Четность перестановки μ и обратной к ней совпадают. В результате получается, что $[p/q] \cdot [q/p] = \operatorname{sgn}(\lambda)$.$\square$

Хотя мы получили закон взаимности для перестановок классов вычетов, мы пока не доказали даже исходную теорему Гаусса. Чтобы это сделать, надо убедиться, что $[p/q] = (p/q)$ хотя бы для простых p и q (что составляет одну из теорем Золотарева). В следующем разделе мы начнем с некоторой подготовки, затем рассмотрим случай простых p и q, после чего освободимся от простоты. В этой части фактически решающую роль и будет играть теорема 2.

4. Совпадение четности перестановки с символом Якоби

В этом разделе мы будем иметь дело с функциями $a \to f(a)$, определенными на некоторой полугруппе A полугруппы $\{\mathbb{Z}, \times\}$ множества целых чисел, рассматриваемого *как полугруппа по умножению*. Чаще всего будут появляться полугруппы $A \subset \{\mathbb{Z}, \times\}$ нечетных натуральных чисел, взаимно простых с некоторым фиксированным числом.

В качестве области значений функции f будут появляться также (мультипликативно записываемые) абелевы полугруппы, чаще всего натуральный ряд или группа $\{\pm 1, \times\}$.

По аналогии с терминологией, принятой в теории чисел, функция f называется *вполне мультипликативной*, если она является гомоморфизмом полугрупп. Если же f заведомо «сохраняет» произведение лишь для взаимно простых сомножителей в аргументе, то f называется (просто) *мультипликативной*.

Как мы увидим, в доказательстве (при определенных условиях) равенства $[p/q] = (p/q)$ (символ Якоби) решающую роль будет играть именно вполне мультипликативность этих функций по каждому из аргументов (из тех или иных полугрупп). Можно сказать, что в половине случаев она тривиальна, тогда как в другой — не совсем.

Функция $p \to [p/q]$ при натуральных p, взаимно простых с q значениях аргумента вполне мультипликативна, и это легко вытекает из определения.

Закон взаимности позволяет установить вполне мультипликативность и по аргументу q в дополнительном предположении нечетности обоих аргументов и условия $p, q \geqslant 3$.

Действительно, пусть $q = q_1 q_2$. Имеем

$$\begin{aligned} [p/q_1q_2] &= (-1)^{(p-1)(q_1q_2-1)/4}[q_1q_2/p] && \text{(теорема 2)} \\ &= (-1)^{(p-1)(q_1q_2-1)/4}[q_1/p]\cdot[q_2/p] && \text{(мультипликативность по } q\text{)}. \end{aligned}$$

Далее,

$$[q_1/p] = (-1)^{(q_1-1)(p-1)/4}[p/q_1] \ \text{ и } \ [q_2/p] = (-1)^{(q_2-1)(p-1)/4}[p/q_2].$$

Наконец,

$$q_1q_2 - 1 - q_1 - q_2 + 2 = (q_1-1)(q_2-1) \equiv 0 \pmod 4 \tag{13}$$

(последняя формула нам пригодится в дальнейшем).

Теперь мы займемся классическим символом Якоби. В этом случае в предположении $\gcd(p, q) = 1$ следствием определения является вполне мультипликативность функции $q \to (p/q)$, тогда как относительно первого аргумента доказательство не очень просто (хотя сам известен очень давно).

Напомним, что φ–функция Эйлера определена при натуральных значениях аргументов и принимает натуральные значения. По определению, $\varphi(1) = 1$. При $n > 1$ значение $\varphi(n)$ — это количество таких $k < n$, которые взаимно просты с n. Иначе говоря, $\varphi(n)$ — это число обратимых элементов в группе обратимых (по умножению) элементов кольца $\mathbb{Z}/(n)$. Легко убедиться, что функция φ мультипликативна но вполне мультипликативной не является. Например, $\varphi(2) = 1$, $\varphi(4) = 2$.

При простых $n = p$ вместо $\mathbb{Z}/(p)$ часто пишут $\mathbf{F}_p$. Очевидно, что $\mathbf{F}_p$ — поле. Группа его обратимых элементов состоит из $p-1$ элементов и обозначается $\mathbf{F}_p^*$. В частности, $\varphi(p) = p - 1$.

О функции Эйлера подробно сообщается практически во всех учебниках теории чисел, и мы вообще не будем давать никаких точных ссылок, хотя некоторые свойства приведем с эскизами доказательств. Заметим только, что в [9] основные свойства функции Эйлера выводятся из групповых соображений.

Согласно одной из теорем Эйлера, если m и a — натуральные числа, причем $\gcd(a, m) = 1$, то $a^{\varphi(m)} \equiv 1 \pmod m$. Доказательство удобнее всего провести, оставаясь в $\mathbb{Z}/(m)$ (в частности, тогда вместо сравнений можно писать равенства). Пусть a — обратимый элемент кольца $\mathbb{Z}/(m)$. Пусть $\{a_i\}$ — набор всех обратимых элементов в $\mathbb{Z}/(m)$ (их количество равно $\varphi(m)$). Пусть a — один из них. Тогда $\prod(aa_i) = \prod a_i$. Следовательно, $a^{\varphi(m)} \prod a_i = \prod a_i$, и это равенство можно сократить на $\prod a_i$. □

В частности, $a^{p-1} \equiv 1 \pmod p$ при простом p (теорема Ферма). Для доказательства следующей ниже леммы Гаусса нам потребуется теорема Эйлера в полном объёме.

Лемма 4. *Для каждого натурального n*

$$\sum_{d|n} \varphi(d) = n. \tag{14}$$

Доказательство. При каждом n обозначим через $\Phi(n)$ значение левой части в (14). Мы должны убедиться, что $\Phi(n) = n$.

Из мультипликативности функции φ не трудно вывести мультипликативность функции Φ. Поэтому формулу (14) достаточно проверить для целых вида p^α, где p простое.

Все делители числа p^α, кроме $d = 1$, имеют вид p^β, где $1 \leqslant \beta \leqslant \alpha$. Числа $k \leqslant p^\beta$, имеющие с p^β нетривиальный *общий множитель*, суть числа вида $l \cdot p$, где $l \cdot p \leqslant p^\beta$. Поэтому имеется $p^{\beta-1}$ таких чисел. Следовательно, $\varphi(p^\beta) = p^\beta - p^{\beta-1}$. Остается просуммировать такие числа по $1 \leqslant \beta \leqslant \alpha$ и добавить $\varphi(1) = 1$. □

Пусть G — конечная группа порядка n (т.е. состоящая из n элементов) и пусть H — подгруппа группы G порядка m. Тогда $m|n$ (теорема Лагранжа). Действительно, левые сдвиги $a \cdot H$ имеют по m элементов, причем либо совпадают, либо не имеют общих элементов.

Пусть $g \in G$. Рассмотрим последовательность $\{e, g, g^2, g^3, \ \dots\}$. Здесь e — единица группы. Так как группа G конечная, то все степени не могут оказаться различными. Отсюда легко вытекает, что последовательность является периодической. В частности, существуют такие натуральные k, что $g^k = e$. Если d — наименьшее из них, то d называется *порядком* элемента g, и то же самое имеют в виду, говоря, что g *принадлежит показателю* d.

Заметим, что $H \stackrel{\text{def}}{=} \{e, g, g^2, g^3, \ \dots \ g^{d-1}\}$ — циклическая группа порядка d. В частности, $d|n$. Ниже мы следуем [9, с.12, лемма 2], однако рассматриваем лишь основной частный случай.

Теорема 3. *Конечная (мультипликативная) подгруппа поля является циклической.*

Доказательство. Пусть G — конечная подгруппа порядка n группы обратимых элементов некоторого поля F. Пусть d — делитель числа n (равенство $d = n$ не исключается). Обозначим через G_d совокупность элементов $x \in G$, принадлежащих показателю d (априори пустота множества G_d допустима). Обозначим через $\psi(d)$ количество элементов в G_d. По определению (и по смыслу), $\psi(1) = 1$. Так как каждый элемент принадлежит в точности одному какому–то показателю d, то

$$\sum_{d|n} \psi(d) = n. \tag{15}$$

Теперь мы более детально исследуем множество G_d в предположении, что $d > 1$. Пусть $1 \neq x \in G_d$. Рассмотрим последовательность

$$e,\ x,\ x^2,\ \ \dots,\ x^{d-1}.$$

Эта последовательность является циклической группой Γ_d порядка d, причем все её элементы удовлетворяют уравнению $y^d - e = 0$. Последнее уравнение не может иметь в поле F более d решений. Поэтому Γ_d содержит все решения этого уравнения. В частности, в Γ_d содержатся все элементы из G, принадлежащие показателю d, т.е. $G_d \subset \Gamma_d$. Элементы из G_d и только они суть образующие циклической группы Γ_d. Но x^k, $1 \leqslant k \leqslant d-1$, тогда и только тогда является образующей, когда $\gcd(k, d) = 1$. Количество таких k равно $\varphi(d)$.

Мораль: если $d|n$, то $\psi(d) \leqslant \varphi(d)$.

Поэтому, имея в виду формулы (14) и (15), мы получаем

$$n = \sum_{d|n} \psi(d) \leqslant \sum_{d|n} \varphi(d) = n.$$

Отсюда и из предыдущего неравенства вытекает, что фактически $\psi(d) = \varphi(d)$, когда $d|n$. В частности, $\psi(n) > 0$, так что G — циклическая группа. □

Следующее утверждение называется теоремой Лежандра.

Лемма 5. *Если p — нечетное простое число и $a \notin (p)$, то*

$$(a/p) \equiv a^{(p-1)/2} \pmod{p}. \tag{16}$$

Доказательство. По теореме Эйлера, $a^{p-1} \equiv 1 \pmod{p}$.
Поэтому $a^{(p-1)/2} \equiv \pm 1 \pmod{p}$.

Рассмотрим отображение $x \to x^2$ группы $\mathbb{Z}/(p)^*$ в себя. Ясно, что это отображение является гомоморфизмом, и его образ G — подгруппа индекса 2 в $\mathbb{Z}/(p)^*$. Если $y \in G$, то (a) на всем классе вычетов $(a/p) = 1$ и (b) $y^{(p-1)}/2 = e$, т.е. на всем классе вычетов имеет место сравнение $a^{(p-1)/2} \equiv 1 \pmod{p}$. Поэтому формула (16) выполняется, когда $y \in G$.

Далее, соотношение (b) можно рассматривать как уравнение относительно y. Так как степень этого уравнения совпадает с порядком группы G, а $\mathbb{Z}/(p)$ — поле, то решениями этого уравнения служат в точности элементы из G. В частности, если $y \notin G$, то, по указанному следствию теоремы Эйлера, $y^{(p-1)}/2 = -e$ и $(a/p) = -1$ на всем классе вычетов. Таким образом, формула (16) выполняется и во второй половине случаев. □

Одно из следствий леммы 5 состоит в том, что символ Лежандра является гомоморфизмом в $\{\pm 1, \times\}$ по первому аргументу (иначе говоря, символ Лежандра вполне мультипликативен). Так как $\{\pm 1, \times\}$ — подгруппа единичной окружности комплексной плоскости, то можно еще сказать, что символ Лежандра — характер группы $\mathbb{Z}/(p)^*$.

Лемма 6. *Если p — нечетное простое число и $a \notin (p)$, то $(a/p) = [a/p]$. В частности, квадратичный закон взаимности выполняется для пар нечетных простых чисел.*

Доказательство. В данном случае $\mathbb{Z}/(p)$ — поле, так что по теореме 3 группа $\mathbb{Z}/(p)^*$ является циклической порядка $p-1$. На всех элементах класса вычетов символ Лежандра принимает одно и то же значение. Поэтому имеет смысл писать (x/p) при каждом $x \in \mathbb{Z}/(p)^*$ (вместо того, чтобы без конца повторять «на каждом классе вычетов»).

Пусть z — (циклическая) образующая группы $\mathbb{Z}/(p)^*$. Если $z = x^2$, то порядок z не превосходит $(p-1)/2$. В таком случае элемент z не мог бы выполнять роль образующей группы. Следовательно, $(z/p) = -1$. Далее, умножение на z порождает перестановку

$$(z,\ z^2,\ \ \ldots,\ z^{p-2},\ z^{p-1} = e).$$

Беспорядки создают пары, включающие e. Следовательно,

$$[z, p] = (-1)^{p-2} = -1$$

и, таким образом, $(z/p) = [z, p]$. Поэтому $(z^k/p) = [z^k/p]$ при каждом натуральном k, так как $x \to (x/p)$ и $x \to [x/p]$ суть гомоморфизмы по x. Поэтому

$(a/p) = [a/p]$ для каждого натурального $a \notin (p)$. Наконец, из этого равенства и теоремы 2 вытекает классическая теорема Гаусса о квадратичном законе взаимности для пар не совпадающих нечетных простых чисел. □

Из леммы 5 вытекает, что при нечетных простых p символ Якоби (a/p) вполне мультипликативен на полугруппе натуральных чисел $a \notin (p)$. Из определения следует, что это остается верным для всех нечетных $p \geqslant 3$. Вместе с тем, по (нечетному) аргументу p при фиксированном a также имеет место вполне мультипликативность (просто по определению).

Таким образом, для пар нечетных взаимно простых чисел $p, q \geqslant 3$ вполне мультипликативность по обоим аргументам имеет место и для $[p, q]$, и для (p, q).

Теорема 4. *Пусть $p, q \geqslant 3$ — нечетные взаимно простые числа. Тогда $(p, q) = [p, q]$ и поэтому квадратичный закон взаимности в случае таких пар имеет место для символов Якоби.*

Доказательство. Отмеченная выше вполне мультипликативность сводит дело к парам несовпадающих простых чисел, а эта ситуация включается в лемму 6. □

В заключение мы рассмотрим несколько примеров.

(a) $(1/p) = 1$ при простых p, так как $1 = 1^2$. Очевидно, что это равенство распространяется и на все символы Якоби.

(b) $(-1/p) = (-1)^{(p-1)/2}$ при простых p по теореме Лежандра (лемма 5). Это равенство также распространяется на символы Якоби. Действительно, достаточно доказать, что оно выполняется для $p = q_1 \cdot q_2$, если оно выполняется для нечетных сомножителей $q_1, q_2 \geqslant 3$. Но это вытекает из тождества (13).

(c) $(2/p) = (-1)^{(p^2-1)/8}$ для всех нечетных $p \geqslant 3$, т.е. для всех символов Якоби. Стандартные доказательства начинаются с простых p и не очень коротки. Однако это равенство можно получить по индукции, причем сразу для символов Якоби, применяя квадратичный закон взаимности (доказательство которого не использовало этого равенства). Довольно просто рассуждение по индукции оформлено в [4], и мы его напомним. В предположении, что равенство имеет место для данного p, устанавливается, что тогда оно имеет место и для $p + 2$. Доказательство можно осуществить «молча», не разбавляя последовательные тождества словами (неформального языка). Имеем:

$$\begin{aligned}(2/m+2) &= (2 - (m+2)/(m+2)) \\ &= (-m/(m+2)) = ((-1) \cdot m/(m+2)) \\ &= (-1)^{(m+1)/2} \cdot (-1)^{(m^2-1)/4}(2/m) \\ &= (-1)^{(m+1)/2}(2/m),\end{aligned}$$

так как $(m+1)^2/4$ имеет ту же четность, что и $(m+1)/2$, и остается использовать индуктивную предпосылку. □

Многочисленные числовые примеры вычисления символа Лежандра при помощи квадратичного закона взаимности для символов Якоби и двух последних примеров имеются в учебниках по элементарной теории чисел, и мы не будем на этом останавливаться. Заметим, что в обход квадратичного закона взаимности для символов Якоби вычисления быстро усложняются, так как тогда, вообще говоря, требуется находить разложения на простые множители больших натуральных чисел.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

1. Zolotareff G. Nouvell démonstration de la reciprocite de Legandre // Nouv. Ann. Math. (2), 1872. Vol. 11, P.109–111.

2. Frobenius G. Über das quadratische Recipprozitätsgesetz // I.S.–B.Preuss. Akad. Wiss., Berlin, 1914, P.335–349.

3. Rousseau G. On the Jacobi symbol // J. Number Theory, 1994. Vol. 48. P. 423–425.

4. Прасолов В. В. Доказательство квадратичного закона взаимности по Золотареву // Мат. просвещение. 2000. Серия 3, вып. 4. С. 140–144.

5. Кострикин А.И. Введение в алгебру (основы алгебры). М.: Наука, 1994. 320 с.

6. Шилов Г.Е Математический анализ (конечномерные линейные пространства). М.: Наука, 1969. 207 с.

7. Виноградов И.М. Основы теории чисел. М.: Наука, 1953. 180 с.

8. Сушкевич А.К. Теория чисел (элементарный курс). Харьков: Изд. Харьковского ун–та, 1956. 204 с.

9. Серр Ж.П. Курс арифметики. М.: Мир, 1972. 183 с.

Московский педагогический государственный университет
Поступило 6.11.2013