Е. Смирнов, О квадратичных вычетах, *Квант*, 2019, номер 10, 2–11

DOI: 10.4213/kvant20191001

О квадратичных вычетах

Е.СМИРНОВ

МНОГИЕ ЗНАЮТ, ЧТО С ОСТАТКАМИ при делении на данное натуральное число m – также говорят «с остатками по модулю m» и пишут «$\bmod m$» – можно делать почти то же самое, что с целыми числами: остатки можно складывать, вычитать, умножать… А если m равно простому числу p, то остатки можно даже и делить! Так, каждое линейное уравнение $ax = b \pmod p$ имеет единственное решение, если a – ненулевой остаток.

А как обстоит дело с квадратными уравнениями? Как выяснить, есть ли решения у уравнения $ax^2 = b$ по модулю простого числа p? Этому и посвящена настоящая статья. Главным утверждением, которое мы при этом докажем, будет знаменитый *квадратичный закон взаимности Гаусса* – теорема, устанавливающая связь между разрешимостью уравнений $x^2 = p \pmod q$ и $x^2 = q \pmod p$ для двух разных простых чисел p и q. С его помощью мы научимся выяснять, разрешимо ли квадратное уравнение по данному простому модулю.

Арифметика остатков

В этом разделе мы кратко напомним некоторые факты об арифметике вычетов по простому модулю. Читателю, который не знаком с арифметикой остатков, рекомендуем сначала прочесть, например, статьи: *Н.Виленкин*. Сравнения и классы вычетов («Квант» №10 за 1978 г.) или *А.Егоров, А.Котова*. Необыкновенные арифметики («Квант» №3–4 за 1993 г.).

Чтобы сложить два остатка a и b по модулю m, нужно сложить их как целые числа и взять у результата остаток по модулю m. Так же определяются и разность, и произведение остатков. Определенные таким образом операции удовлетворяют обычным законам арифметических действий: для них верны переместительный, сочетательный и распределительный законы, существуют ноль и единица. (Алгебраисты сказали бы, что они образуют *кольцо*.) Подробности читатель может восстановить сам или посмотреть в одной из упомянутых выше статей.

Для примера составим таблицы умножения остатков по модулю 6 и 7. При этом мы опускаем строчку и столбец, отвечающие

6	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1

7	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

умножению на ноль: они состоят из одних нулей.

Сопоставив эти таблицы, можно сделать некоторые наблюдения. Так, например, в первой из таблиц (по модулю 6) встречаются нули; иначе говоря, существуют такие два ненулевых остатка, произведение которых равно нулю. Такие остатки называются *делителями нуля*. Скажем, по модулю 6 делителями нуля будут числа 2, 3 и 4.

Ясно, что по составному модулю делители нуля всегда будут: так, если m составное, то существуют такие k и l, отличные от единицы, для которых $m = kl$. Поэтому числа k и l соответствуют ненулевым ос-

DOI: https://doi.org/10.4213/kvant20191001

таткам, произведение которых равно нулю по модулю m.

Чуть менее тривиален обратный вопрос: верно ли, что в арифметике остатков по простому модулю делителей нуля нет? (Например, по модулю 7 их нет, что подтверждается второй таблицей.) Оказывается, что это тоже верно.

Докажем это. Рассмотрим арифметику остатков по модулю p и предположим противное: пусть нашлись такие k и l, которые дают при делении на p ненулевые остатки – но при этом их произведение делится на p нацело, т.е. $kl = pm$. Однако если произведение двух чисел делится на простое число p, то на p делится хотя бы одно из этих чисел. Противоречие: ни k, ни l не делятся на p.

Мы получили следующее утверждение.

Предложение 1. *В арифметике остатков по модулю m нет делителей нуля тогда и только тогда, когда m является простым числом.*

Далее нас будет интересовать в основном тот случай, когда m простое; в этом случае будем обозначать его буквой p, а соответствующее множество остатков (с операциями сложения и умножения) будет обозначаться через $\mathbb{Z}/p\mathbb{Z}$.[1]

Можно сделать еще одно наблюдение: в каждой из строк второй таблицы записаны в каком-то порядке все ненулевые остатки по модулю 7; все числа от 1 до 6 встречаются в ней по одному разу, и ни одно не повторяется. Оказывается, что так обстоит дело и для произвольного простого модуля.

Предложение 2. *Пусть p простое, $a \in \mathbb{Z}/p\mathbb{Z}$ – некоторый ненулевой остаток. Тогда среди остатков $0, a, 2a, 3a, \ldots, (p-1)a$ нет повторяющихся.*

Доказательство. Пусть два остатка $k, m \in \mathbb{Z}/p\mathbb{Z}$ таковы, что $ak = am$. Тогда $a(k-m)$ равно нулю. Но мы только что доказали, что в $\mathbb{Z}/p\mathbb{Z}$ произведение двух ненулевых остатков отлично от нуля. Поскольку по условию $a \neq 0$, то это значит, что $k - m = 0$, т.е. $k = m$, что и требовалось.

Из этого несложного предложения вытекает несколько интересных следствий.

Следствие 1. *В $\mathbb{Z}/p\mathbb{Z}$ линейное уравнение $ax = 0$ при $a \neq 0$ имеет единственное решение.*

Доказательство. Действительно, переберем все возможные значения x, т.е. рассмотрим все остатки вида $0, a, 2a, \ldots$ Согласно предложению 2, среди них будет остаток, равный b, причем ровно один.

Частным случаем этого следствия является следующее утверждение.

Следствие 2. *Для каждого ненулевого остатка $a \in \mathbb{Z}/p\mathbb{Z}$ существует и единственный обратный, т.е. такой остаток x, что $ax = 1$.*

Этот остаток обычно обозначается a^{-1}.

Пример 1. Например, в $\mathbb{Z}/7\mathbb{Z}$ обратным к остатку 3 будет остаток 5: действительно, $3 \cdot 5 = 15$, что дает остаток 1 по модулю 7.

Замечание. Отметим, что в арифметике по составному модулю ни то, ни другое следствие не будет выполняться. Так, например, по модулю 6 уравнение $2x = 4$ будет иметь два решения: 2 и 5, а ни один из остатков 2, 3 и 4 не будет обратим.

Упражнение 1. Выясните, какие остатки будут обратимы в арифметике остатков по произвольному составному модулю m.

А что будет, если перемножить все остатки $a, 2a, \ldots, (p-1)a$? С одной стороны, $a^{p-1} \cdot 1 \cdot 2 \cdot \ldots \cdot (p-1) = a^{p-1}(p-1)!$. С другой стороны, согласно предложению 2, эти остатки – это те же $1, 2, \ldots, p-1$, только записанные в другом порядке. Значит, их произведение равняется $(p-1)!$. Тем самым мы получаем равенство

$$a^{p-1}(p-1)! = (p-1)!.$$

Поделив это равенство на $(p-1)!$ (контрольный вопрос: почему это можно сделать?), получаем следующую теорему.

Теорема 1 (малая теорема Ферма). *Пусть p простое. Тогда в $\mathbb{Z}/p\mathbb{Z}$ для*

[1] Смысл этого обозначения в том, что мы рассматриваем целые числа, множество которых традиционно обозначается через $\mathbb{Z}$, с точностью до прибавления чисел, делящихся на p, множество которых естественно обозначить через $p\mathbb{Z}$.

любого ненулевого a верно равенство

$$a^{p-1}=1.$$

Упражнение 2. Покажите, что остатки, обратные к самим себе, т.е. такие, для которых $a=a^{-1}$, это в точности 1 и $p-1$. Выведите отсюда *теорему Вильсона*:

$$(p-1)!=-1.$$

Квадратичные вычеты

Первая в истории человечества книга по алгебре, «Китаб аль-джебр ва-ль-мукабала», была написана средневековым ученым Мухаммадом ибн Мусой аль-Хорезми около 830 года н.э. Аль-Хорезми был уроженцем Хивы – сейчас это территория Узбекистана. В этой книге, в числе прочего, был изложен метод решения квадратного уравнения.

Основной метод решения квадратного уравнения (с вещественными коэффициентами) состоит в выделении полного квадрата, что сводит его к уравнению вида $x^2=a$. Такое уравнение легко решить: если $a>0$, то его корни равны $\pm\sqrt{a}$; если $a=0$, то единственный корень равен нулю; если же $a<0$, то корней у такого уравнения нет.

Квадратичные вычеты и невычеты. Наша ближайшая задача будет состоять в том, чтобы научиться искать число решений уравнения $x^2=a$, где $a\in\mathbb{Z}/p\mathbb{Z}$ – остаток по некоторому фиксированному простому модулю p. Будем считать, что $p>2$, т.е. p – *нечетное* простое число.

Заметим, что если уравнение $x^2=a$ при $a\neq 0$ имеет корень, то этих корней обязательно будет ровно два: а именно, если b – корень этого уравнения, то и $-b$ – тоже его корень. При этом, поскольку p нечетно, $b\neq -b$.

Поэтому получается, что $x^2-a=(x-b)(x+b)$. Отсюда следует, что других корней у уравнения $x^2=a$ нет: если c – корень уравнения, то $(c-b)(c+b)=0$, откуда $c=b$ или $c=-b$ (обратите внимание, что здесь мы опять пользуемся отсутствием делителей нуля в $\mathbb{Z}/p\mathbb{Z}$!).

Определение 1. Пусть $a\in\mathbb{Z}/p\mathbb{Z}$, $a\neq 0$. Будем называть a *квадратичным вычетом*, если уравнение $x^2=a$ разрешимо, и *квадратичным невычетом* в противном случае.

Пример 2. По модулю 7 квадратичными вычетами будут числа 1, 2 и 4: это в точности те числа, которые стоят на диагонали в таблице умножения остатков по модулю 7. Отметим, что каждое из них встречается там ровно два раза.

При этом число 0 мы не будем относить ни к квадратичным вычетам, ни к невычетам (так же, как вещественное число 0 не является ни положительным, ни отрицательным).

Предложение 3. *Количество как квадратичных вычетов, так и квадратичных невычетов в $\mathbb{Z}/p\mathbb{Z}$ равно $\dfrac{p-1}{2}$.*

Доказательство. Каждому квадратичному вычету a соответствуют два решения $\pm b$ уравнения $x^2=a$. Также ясно, что каждый ненулевой остаток из $\mathbb{Z}/p\mathbb{Z}$ является решением ровно одного квадратного уравнения такого вида. Поэтому получается, что квадратичных вычетов оказывается вдвое меньше, чем ненулевых элементов из $\mathbb{Z}/p\mathbb{Z}$, т.е. $\dfrac{p-1}{2}$. Все остальные элементы $\mathbb{Z}/p\mathbb{Z}$ тогда будут квадратичными невычетами, и их $(p-1)-\dfrac{p-1}{2}$, а значит, столько же.

Упражнения

3. Для всех нечетных простых чисел $p<20$ перечислите все квадратичные вычеты и невычеты по модулю p.

4. Докажите, что при нечетном простом p квадратное уравнение $ax^2+bx+c=0$, где $a,b,c\in\mathbb{Z}/p\mathbb{Z}$, $a\neq 0$,

- имеет два решения, равные $x_{1,2}=\dfrac{b\pm\sqrt{D}}{2a}$, если его дискриминант $D=b^2-4ac$ является квадратичным вычетом;
- имеет единственное решение, если $D=0$;
- неразрешимо над $\mathbb{Z}/p\mathbb{Z}$, если D – квадратичный невычет.

Указание. С помощью выделения полного квадрата сведите данное уравнение к виду $x^2=D$.

Символ Лежандра и его мультипликативность. Ясно, что произведение двух

квадратичных вычетов снова будет квадратичным вычетом. А что будет, если перемножить два квадратичных невычета? А вычет и невычет? Оказывается, верна следующая теорема.

Теорема 2. а) *Произведение двух квадратичных вычетов – квадратичный вычет;*

б) *произведение квадратичного вычета и квадратичного невычета – квадратичный невычет;*

в) *произведение двух квадратичных невычетов – квадратичный вычет.*

Доказательство. Пункт а) очевиден: если a и b квадратичные вычеты, т.е. существуют такие x и y, для которых $x^2 = a$ и $y^2 = b$, то ab тоже будет квадратичным вычетом, поскольку $(xy)^2 = ab$.

Докажем пункт б). Пусть a – квадратичный вычет, b – квадратичный невычет. Предположим противное: что ab – квадратичный вычет. Поскольку a – квадратичный вычет, найдется такое x, что $x^2 = a$. В таком случае и элемент a^{-1} будет квадратичным вычетом, так как $a^{-1} = \left(x^{-1}\right)^2$. Соответственно, в силу пункта а) элемент b как произведение квадратичных вычетов ab и a^{-1} будет квадратичным вычетом – противоречие.

Пункт в) аналогичными формальными манипуляциями доказать уже не удается. Однако его можно вывести из пункта б) при помощи подсчета числа элементов. А именно, пусть a – фиксированный квадратичный невычет. Рассмотрим все элементы вида $a, 2a, \ldots, (p-1)a$. Как обсуждалось ранее, в этой последовательности все элементы $1, 2, \ldots, (p-1)$ встречаются, причем ровно по одному разу – поэтому среди них $\frac{p-1}{2}$ квадратичных вычетов и $\frac{p-1}{2}$ квадратичных невычетов. Однако в силу пункта б) при умножении a на квадратичный вычет получается квадратичный невычет, и таких элементов будет $\frac{p-1}{2}$, т.е. все квадратичные невычеты будут получаться таким образом. Значит, при умножении a на все остальные элементы (т.е. невычеты) должны получаться квадратичные вычеты, что и требовалось.

Тем самым квадратичные вычеты и невычеты ведут себя при умножении примерно так же, как положительные и отрицательные числа. Это мотивирует следующее определение.

Определение 2. Пусть $a \in \mathbb{Z}/p\mathbb{Z}$, $a \neq 0$. *Символ Лежандра* $\left(\frac{a}{p}\right)$ определяется следующим образом:

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

Таким образом, символ Лежандра можно считать аналогом функции знака числа. Тогда предыдущая теорема принимает следующий компактный вид.

Теорема 3. *Символ Лежандра мультипликативен*:

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right).$$

Далее мы приведем другое доказательство этой теоремы, которое будет следовать из еще одного полезного утверждения, позволяющего вычислить символ Лежандра, – критерия Эйлера.

Критерий Эйлера. Прежде чем читать дальше, рекомендуем читателю выполнить следующее упражнение.

Упражнение 5. Возьмите какое-нибудь нечетное простое число, меньшее 20, и возведите каждый из ненулевых остатков $a \in \mathbb{Z}/p\mathbb{Z}$ в степень $\frac{p-1}{2}$. Убедитесь, что у вас всегда будет получаться ± 1. А когда получается 1, а когда -1?

Тем самым вы «экспериментально» проверите утверждение следующей теоремы.

Теорема 4 (критерий Эйлера). *Пусть* $p > 2$ *– простое число,* $a \in \mathbb{Z}/p\mathbb{Z}$. *Тогда*

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

Доказательство. При $a = 0$ утверждение теоремы очевидно. Дальше будем считать, что a отлично от 0.

Во-первых, сначала убедимся, что при

любом $a \neq 0$ будет иметь место равенство $a^{\frac{p-1}{2}} = \pm 1$. Действительно, $\left(a^{\frac{p-1}{2}}\right)^2 = a^{p-1} = 1$ по малой теореме Ферма. Но остаток, квадрат которого равен 1, может равняться только 1 или -1.

Далее, ясно, что если $\left(\frac{a}{p}\right) = 1$, то $a^{\frac{p-1}{2}} = 1$. Действительно, если a – квадратичный вычет, то существует такое b, что $b^2 = a$. Тогда $a^{\frac{p-1}{2}} = \left(b^2\right)^{\frac{p-1}{2}} = b^{p-1} = 1$ опять-таки в силу малой теоремы Ферма.

Осталось доказать, что если a – квадратичный невычет, то $a^{\frac{p-1}{2}} = -1$. Для этого рассмотрим уравнение $x^{\frac{p-1}{2}} - 1 = 0$. Это полиномиальное уравнение степени $\frac{p-1}{2}$, следовательно, по теореме Безу (которая верна и для многочленов с коэффициентами из $\mathbb{Z}/p\mathbb{Z}$) у него не может быть более $\frac{p-1}{2}$ корней. Но такое количество корней нам уже известно: это все квадратичные вычеты. Тем самым получается, что квадратичные невычеты не являются корнями этого уравнения, т.е. для них $a^{\frac{p-1}{2}} \neq 1$. Значит, для них $a^{\frac{p-1}{2}} = -1$. Теорема доказана.

Для полноты изложения докажем, что многочлен с коэффициентами из $\mathbb{Z}/p\mathbb{Z}$ степени d имеет не более d корней. Это доказывается точно так же, как и для многочленов с вещественными коэффициентами. Докажем это индукцией по d. База при $d = 1$ очевидна: это следствие 1. Для доказательства индуктивного перехода отметим, что если $p(x)$ – многочлен степени d, коэффициенты которого принадлежат $\mathbb{Z}/p\mathbb{Z}$, а остаток $a \in \mathbb{Z}/p\mathbb{Z}$ является его корнем, т.е. $p(a) = 0$, то $p(x)$ делится на двучлен $x - a$, значит, представляется в виде $p(x) = q(x)(x-a)$. Для доказательства этого факта разделим $p(x)$ на $x - a$ с остатком: $p(x) = q(x)(x-a) + r$ и подставим в качестве x значение a. Левая часть окажется равной нулю, стало быть, и $r = 0$. Степень многочлена $q(x)$ будет на единицу меньше, чем степень $p(x)$, а значит, и корней у него не более $d-1$ по предположению индукции. А корни многочлена $p(x)$ – это a и корни многочлена $q(x)$ (здесь мы используем отсутствие делителей нуля в $\mathbb{Z}/p\mathbb{Z}$). Поэтому их не больше d, что и требовалось.

Из критерия Эйлера очевидно следует мультипликативность символа Лежандра. Действительно,

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

Кроме того, с помощью критерия Эйлера легко понять, когда -1 является квадратичным вычетом, а когда – невычетом:

Следствие 3. *Имеет место равенство*

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1, & p = 4k+1, \\ -1, & p = 4k+3. \end{cases}$$

«Положительные» и «отрицательные» остатки. Выпишем все элементы из $\mathbb{Z}/p\mathbb{Z}$ в следующем порядке:

$$-\frac{p-1}{2}, \ldots, -2, -1, 0, 1, 2, \ldots, \frac{p-1}{2}.$$

Условимся называть те из них, которые выписаны слева от нуля, «отрицательными», а те, что справа – «положительными».[2]

Рассмотрим произвольный ненулевой элемент $a \in \mathbb{Z}/p\mathbb{Z}$ и умножим его на все «положительные» элементы. Получим элементы $a, 2a, \ldots, \frac{p-1}{2}a$.

Нетрудно доказать следующее утверждение.

Предложение 4. *Множество* $\left\{a, 2a, \ldots, \frac{p-1}{2}a\right\}$ *содержит ровно по одному элементу из каждой пары* $\pm 1, \pm 2, \ldots, \pm\frac{p-1}{2}$.

Доказательство. Ранее мы уже видели, что разные элементы из $\mathbb{Z}/p\mathbb{Z}$ при умно-

[2] Не надо путать положительные/отрицательные элементы в смысле этого обозначения с квадратичными вычетами/невычетами.

жении на произвольное ненулевое a не могут переходить в один и тот же элемент: это противоречило бы тому, что в $\mathbb{Z}/p\mathbb{Z}$ нет делителей нуля.

Докажем, что для различных «положительных» элементов $k \neq l$ элементы ak и al не могут быть противоположны друг другу. Действительно, это значило бы, что

$$0 = ak + al = a(k+l),$$

откуда $k+l = 0 \pmod p$. Но этого не может быть: поскольку $0 < k,l \le \frac{p-1}{2}$, то $0 < k+l < p$, значит, $k+l \neq 0 \pmod p$.

Поэтому среди элементов $a, 2a, \ldots, \frac{p-1}{2}a$ встречается не более одного элемента из каждой пары $\pm k$. Но элементов и пар по $(p-1)/2$ – стало быть, из каждой пары $\pm k$ войдет ровно один остаток.

Обозначим через $\varepsilon(a)$ количество «отрицательных» элементов во множестве $\left\{a, 2a, \ldots, \frac{p-1}{2}a\right\}$, т.е. число таких «положительных» элементов, которые при умножении на a становятся «отрицательными».

Предложение 5 (лемма Гаусса). *Имеет место равенство* $(-1)^{\varepsilon(a)} = \left(\frac{a}{p}\right)$. *Иначе говоря,* $\varepsilon(a)$ *четно, если* a – *квадратичный вычет, и нечетно в противном случае.*

Доказательство. Перемножим все остатки $a, 2a, \ldots, \frac{p-1}{2}a$. В силу предыдущего рассуждения мы получим, что это произведение равно

$$a \cdot 2a \cdot \ldots \cdot \frac{p-1}{2}a = (-1)^{\varepsilon(a)} \cdot 1 \cdot 2 \cdot \ldots \cdot \frac{p-1}{2}.$$

Но, с другой стороны, оно же равняется

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

(в последнем равенстве использован критерий Эйлера).

Поделив обе части на отличную от нуля величину $\left(\frac{p-1}{2}\right)!$, получаем требуемое равенство.

Это предложение позволяет вычислить символ Лежандра для некоторых значений a.

Пример 3. Убедимся еще раз, что $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$. Действительно, при умножении на -1 все «положительные» числа становятся «отрицательными» – а их всего $(p-1)/2$.

Выясним, когда число 2 является квадратичным вычетом по модулю p. Оказывается, что это зависит от остатка от деления p на 8: если он равен 1 или 7, то 2 будет квадратичным вычетом, а если 3 или 5, то невычетом.

Предложение 6. *Имеет место равенство*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1, & p = 8k \pm 1, \\ -1, & p = 8k \pm 3. \end{cases}$$

Доказательство. Умножим все «положительные» элементы на 2; получим элементы вида

$$2, 4, \ldots, p-3, p-1.$$

«Отрицательными» будут те из них, которые будут заключены между $p/2$ и $p-1$. Их количество, как нетрудно видеть, будет равно $\left\lceil \frac{p-1}{4} \right\rceil$ (т.е. числу $\frac{p-1}{4}$, округленному до ближайшего целого *вверх*).

Эта величина и будет равна $\varepsilon(2)$; мы хотим найти ее четность. Проще всего сделать это, разобрав четыре возможных случая:

- если $p = 8k+1$, то $\varepsilon(2) = \left\lceil \frac{p-1}{4} \right\rceil = 2k$;
- если $p = 8k+3$, то $\varepsilon(2) = \left\lceil 2k + \frac{1}{2} \right\rceil = 2k+1$;
- если $p = 8k+5$, то $\varepsilon(2) = \lceil 2k+1 \rceil = 2k+1$;
- наконец, если $p = 8k+7$, то $\varepsilon(2) = \left\lceil 2k + \frac{3}{2} \right\rceil = 2k+2$.

Гипотеза Эйлера. Посмотрим еще раз на предложение 6. Оно утверждает, что 2 является или не является квадратичным вычетом по модулю p в зависимости от

остатка, который p дает при делении на 8. Вообще говоря, это совершенно удивительно: оказывается, что при фиксированном нечетном r для всех простых чисел вида $8k+r$ двойка является или не является квадратичным вычетом одновременно!

Кстати, то же самое мы видели и для -1: является ли -1 вычетом или невычетом по модулю p, зависит лишь от остатка, который p дает при делении на 4.

Эйлер высказал гипотезу, что так будет и для любого числа a: символ Лежандра $\left(\frac{a}{p}\right)$ будет зависеть только от остатка, который p дает при делении на $4a$.

Сам Эйлер доказать эту гипотезу не смог; это было сделано Гауссом, который установил, как связаны между собой квадратичные вычеты по различным простым модулям. Это утверждение он назвал *золотой теоремой* (Theorema Aureum), а нам оно сегодня известно как *квадратичный закон взаимности*. В следующем разделе мы изложим одно из многочисленных доказательств этой теоремы, принадлежащее ученику Гаусса, Эйзенштейну.

Кстати, слово «многочисленные» – отнюдь не преувеличение. Существуют доказательства квадратичного закона взаимности, опирающиеся на самые разные идеи; сам Гаусс придумал около восьми разных доказательств. Немецкий математик Франц Леммермайер на своей странице https://www.rzuser.uni-heidelberg.de/~hb3/rchrono.html собрал 246 различных доказательств этой теоремы, последние 15 из которых были опубликованы в течение последнего десятилетия.

Теорема 5 (гипотеза Эйлера). *Число a одновременно будет квадратичным вычетом или невычетом для всех простых чисел, входящих в арифметическую прогрессию $4an+r$, где $n=0,\ 1,\ 2,\ \ldots$ и $0<r<4a$.*

Замечание. Понятно, что если первый член прогрессии r и ее разность $4a$ не взаимно просты, то таких простых чисел при $n\geq 1$ не будет (все члены прогрессии будут делиться на их общий делитель). *Теорема Дирихле* утверждает, что если первый член и разность арифметической прогрессии взаимно просты, то она будет содержать бесконечно много простых чисел.

Упражнение 6. Докажите, что количество простых чисел вида: а) $4k+3$; б*) $4k+1$ бесконечно.

Квадратичный закон взаимности Гаусса

Формула для $\varepsilon(a)$. В предыдущем разделе мы вычислили $\varepsilon(2)$, найдя число таких «положительных» элементов из $\mathbb{Z}/p\mathbb{Z}$, которые при умножении на 2 переходят в «отрицательные». А именно, эти элементы получаются из целочисленных x, удовлетворяющих двойному неравенству $p/4<x<p/2$. Напротив, целочисленные решения неравенства $0<x<p/4$ соответствуют «положительным» элементам, при умножении на 2 переходящим в «положительные».

Это можно представить себе следующим образом. Расположим остатки от 0 до $p-1$ в вершинах правильного p-угольника с координатами $(\cos 2\pi k/p;\sin 2\pi k/p)$. Тогда «положительные» остатки будут отвечать вершинам, лежащим в верхней полуплоскости (выше оси Ox), а «отрицательные» – соответственно, ниже Ox. Умножение элемента на 2 отвечает удвоению соответствующего угла, так что при этом вершина с номером k перейдет в вершину с номером $2k$. Поэтому в «положительные» элементы при этом отображении перейдут вершины, лежащие в I и III четвертях, а в «отрицательные» – соответственно, во II и IV. Поэтому интересующее нас число «положительных» элементов, переходящих в «отрицательные», есть не что иное, как количество вершин p-угольника, лежащих во II четверти.

Ясно, что это рассуждение можно обобщить для произвольного числа a, не только для 2. Для этого разобьем нашу плоскость на $2a$ одинаковых секторов и покрасим их поочередно в белый и серый цвета, как показано на рисунке 1. Вершины правильного p-угольника, попавшие в белые сектора, будут отвечать ненулевым элементам из $\mathbb{Z}/p\mathbb{Z}$, переходящим при умно-

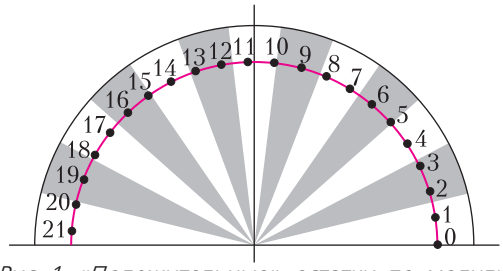

Рис. 1. «Положительные» остатки по модулю $p = 43$ (от 1 до 21), попавшие в серые сектора, переходят при умножении на $a = 13$ в «отрицательные»

жении на a в «положительные» элементы; те же вершины, которые попали в серые сектора, будут при умножении на a переходить в «отрицательные». На рисунке 1 показан пример, в котором $p = 43$ (т.е. «положительными» являются остатки от 1 до 21), а $a = 13$.

Отметим, что в силу простоты p (вернее, взаимной простоты p и a) на границу секторов попадет единственная вершина p-угольника – а именно, та, что отвечает элементу $0 \in \mathbb{Z}/p\mathbb{Z}$.

Итак, количество $\varepsilon(a)$ таких «положительных» элементов $\mathbb{Z}/p\mathbb{Z}$, которые при умножении на a переходят в «отрицательные», равняется количеству вершин p-угольника, лежащих выше оси абсцисс и при этом попадающих в серые сектора. Всего таких секторов будет $\left\lfloor \frac{a}{2} \right\rfloor$ (т.е. число $\frac{a}{2}$, округленное до ближайшего целого *вниз*). Ясно, что соответствующие вершины при этом будут иметь номера n, удовлетворяющие одному из следующих неравенств:

$$p/2 < an < p\,;$$

$$3p/2 < an < 2p\,;$$

$$5p/2 < an < 3p\,;$$

$$\dots$$

Тем самым, количество «положительных» элементов, переходящих при умножении на a в «отрицательные», есть в точности количество таких n, где $1 \le n \le \frac{p-1}{2}$ и $\left\lfloor \frac{2an}{p} \right\rfloor$ *нечетно*.

Это можно сформулировать в виде следующей леммы.

Лемма 1 (Эйзенштейн). *Имеет место равенство*

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{n=1}^{(p-1)/2} \left\lfloor \frac{2an}{p} \right\rfloor}.$$

Доказательство. Предыдущее обсуждение показывает, что $\left(\frac{a}{p}\right)$ равно 1 или -1 в зависимости от того, является ли количество *нечетных* чисел среди чисел вида $\left\lfloor \frac{2an}{p} \right\rfloor$ четным или нечетным. Теперь просуммируем все числа такого вида и воспользуемся простым наблюдением: сумма целых чисел нечетна тогда и только тогда, когда в нее входит нечетное число нечетных слагаемых.

Квадратичные вычеты и целые точки. В этом разделе мы установим взаимосвязь между квадратичными вычетами по *различным* модулям. Для этого зададимся различными простыми нечетными числами p и q.

Положим в предыдущей формуле $a = q$ и интерпретируем сумму в ее правой части геометрически. Нарисуем на координатной плоскости прямоугольник высоты q и ширины p с вершиной в начале координат, лежащий в первой четверти (рис.2). Коор-

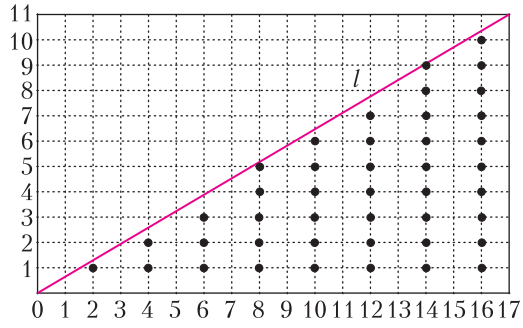

Рис. 2. Здесь $p = 17$, $q = 11$. Отмечены все точки с четными абсциссами, лежащие ниже прямой l

динаты его точек $(x; y)$ будут удовлетворять неравенствам $0 < x < p$, $0 < y < q$. Далее проведем в этом прямоугольнике диагональ l из левого нижнего в правый

верхний угол; она будет иметь уравнение $y = qx/p$.

Рассмотрим какое-нибудь целое число n, где $1 \le n \le (p-1)/2$. Возьмем все точки в прямоугольнике с абсциссой $2n$ и целой ординатой, лежащие ниже прямой l. Их ордината должна удовлетворять условию $y < \dfrac{2nq}{p}$. Таким образом, число этих точек равно $\left\lfloor \dfrac{2nq}{p} \right\rfloor$. Суммируя по n, получаем, что четность $\varepsilon(q)$ равна четности количества точек в прямоугольнике, которые лежат ниже прямой l и имеют *четные* абсциссы.

Оказывается, что существует еще более удобная интерпретация $\varepsilon(q)$:

Лемма 2. *Четность числа $\varepsilon(q)$ совпадает с четностью числа целых точек в треугольнике, заданном неравенствами $0 < x < p/2$, $0 < y < q/2$, $y < qx/p$ (на рисунке 3 этот треугольник выделен цветом).*

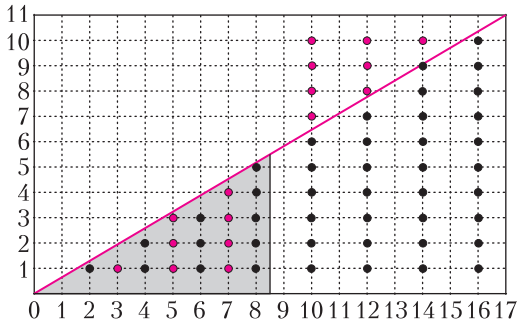

Рис. 3. Четность $\varepsilon(q)$ равна четности числа точек в выделенном треугольнике

Доказательство. Рассмотрим точки, отмеченные на рисунке 2, и добавим к ним еще некоторое количество точек: все точки в выделенном треугольнике, которые еще не отмечены, и центрально-симметричные им относительно центра прямоугольника. На рисунке 3 эти точки отмечены красным. При этом точке с координатами $(x; y)$ будет соответствовать точка с координатами $(p-x; q-y)$ – т.е. точке, лежащей *ниже* прямой l, будет отвечать точка *выше* этой прямой, а точке с *нечетной* абсциссой будет соответствовать точка, абсцисса которой *четна*. В результате у нас будут отмечены:

• во-первых, все целые точки в выделенном треугольнике;

• во-вторых, все точки с четными абсциссами, лежащие правее прямой $x = p/2$. В каждом таком столбце будет $q-1$ точка, т.е. четное число, а значит, общее число таких точек также будет четным.

Значит, четность $\varepsilon(q)$ равна четности числа целых точек в выделенном треугольнике, что и требовалось.

Отсюда немедленно получается квадратичный закон взаимности Гаусса:

Теорема 6 (квадратичный закон взаимности). *Для различных нечетных простых чисел имеет место равенство*

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

Доказательство. В предыдущих обозначениях рассмотрим прямоугольник $0 < x < p/2$, $0 < y < q/2$. Его делит пополам прямая l. Как показывает предыдущее обсуждение, число целых точек под ней будет четным или нечетным в зависимости от знака $\left(\dfrac{q}{p}\right)$. С другой стороны, четность числа точек *над* нею определяется знаком $\left(\dfrac{p}{q}\right)$. Но всего в прямоугольнике содержится $\dfrac{p-1}{2}\cdot\dfrac{q-1}{2}$ точек, что и дает нам требуемое утверждение.

На практике квадратичный закон взаимности удобно использовать в следующей форме:

Следствие 4. *Пусть p, q – различные нечетные простые числа. Символы Лежандра $\left(\dfrac{p}{q}\right)$ и $\left(\dfrac{q}{p}\right)$ равны, если хотя бы одно из чисел p, q имеет вид $4k+1$, и различны, если они оба имеют вид $4k+3$.*

Из квадратичного закона взаимности легко вывести гипотезу Эйлера (теорема 5).

Доказательство гипотезы Эйлера. Пусть a – такое число, что p и $4an+p$ одновре-

менно являются простыми. Докажем, что

$$\left(\frac{a}{p}\right)=\left(\frac{a}{4an+p}\right).$$

Поскольку символ Лежандра мультипликативен, можно считать, что число a тоже является простым (почему?). Если $a=2$, то это утверждение нам уже известно: это предложение 6. Если же нет, то a нечетно, и можно применить к обеим частям требуемого равенства квадратичный закон взаимности:

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

$$\left(\frac{a}{4an+p}\right)=(-1)^{\frac{a-1}{2}\cdot\frac{4an+p-1}{2}}\left(\frac{4an+p}{a}\right)=$$

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

Ясно, что эти величины равны. Гипотеза Эйлера доказана.

Рекомендуем читателю, который хочет узнать больше об истории гипотезы Эйлера и квадратичного закона взаимности, прочесть главу о Гауссе в замечательной книге С.Г.Гиндикина «Рассказы о физиках и математиках». В ней, в частности, изложено одно из первых доказательств квадратичного закона, полученное самим Гауссом.

Пример использования квадратичного закона взаимности. В качестве примера выясним с помощью квадратичного закона взаимности, разрешимо ли сравнение

$$x^2\equiv 57\pmod{179}.$$

Для этого нам нужно вычислить $\left(\frac{57}{179}\right)=\left(\frac{3}{179}\right)\cdot\left(\frac{19}{179}\right)$. Вычислим отдельно каждый из этих символов Лежандра.

Оба числа 3 и 179 дают при делении на 4 остаток 3. Поэтому

$$\left(\frac{3}{179}\right)=-\left(\frac{179}{3}\right)=-\left(\frac{-1}{3}\right)=1,$$

так как -1 является квадратичным невычетом по модулю 3. Значит, 3 – квадратичный вычет по модулю 179.

Далее, по той же причине (19 тоже имеет вид $4k+3$) получаем, что $\left(\frac{19}{179}\right)=-\left(\frac{179}{9}\right)=$ $=-\left(\frac{8}{19}\right)=-\left(\frac{2}{19}\right)$ (поскольку $8=2\cdot 4$, а 4 – полный квадрат). Но число 19 имеет вид $8k+3$, поэтому 2 является квадратичным невычетом по модулю 19. Стало быть, $\left(\frac{19}{179}\right)=1$, откуда $\left(\frac{57}{179}\right)=1$, и сравнение $x^2\equiv 57\pmod{179}$ разрешимо.

Прозрачное и непрозрачное

Л.АШКИНАЗИ

НА РИСУНКЕ 5 ПРЕДСТАВЛЕНЫ ФОТОграфии двух образцов – из монокристалла CaF_2 и нанокерамики (поликристала) $CaF_2:Ce^{3+}$. Оба образца – абсолютно прозрачные!

Теперь обсудим преломление. У газов коэффициенты преломления мало отличаются от единицы, и они вообще мало кого волнуют – кроме астрономов. Откройте зимой окно и посмотрите, как елозит пей-

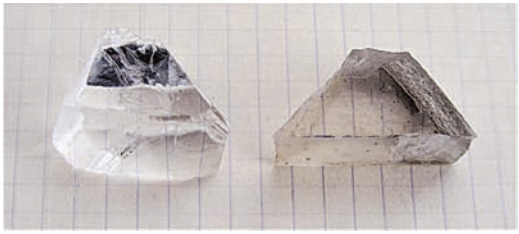

Рис. 5

заж, или просто посмотрите вверх, вспомнив не знаю кем сказанное «человек отличается от животного тем, что иногда под-

Окончание. Начало – в «Кванте» №8.