ВОКРУГ КВАДРАТИЧНОГО ЗАКОНА ВЗАИМНОСТИ

Д. Акимов, Д. А. Беляев, П. В. Бибиков, Г. Галяпин,
А. Приходько, П. Прохоров, Д. З. Хо[1]

Содержание

1. Предисловие

Данная книга написана по итогам сборов команды Москвы на Всероссийскую олимпиаду школьников по математике, проходивших с 19 по 29 июня 2022 г. Основной темой по теории чисел на этих сборах была такая классическая вещь, как *квадратичные вычеты*. Удивительно, но и в процессе подготовки к занятиям, и в процессе обсуждения задач со школьниками удалось обнаружить много новых, красивых и малоизвестных фактов, связанных с этим сюжетом. Отдельно хотелось бы отметить шесть (!) различных доказательств квадратичного закона взаимности, предложенных школьниками, являющимися авторами данного текста. (Нельзя не отметить, что столько доказательств придумал и сам Карл Фридрих Гаусс, впервые доказавший квадратичный закон взаимности.)

Впечатлившись таким энтузиазмом со стороны школьников, П. В. Бибикову захотелось сохранить эти результаты, в результате чего и родился данный текст. Его основу составляют два листка, составленных П. В. Бибиковым и А. Ю. Кушниром (эти листки приведены в конце текста), однако в текст добавлены и многие другие задачи, прежде всего из зарубежных олимпиад. Текст книги построен на развитии идей, представленных в этих листках, и построен в формате рассказа о наиболее известных и важных фактах из теории квадратичных вычетов, которые сопровождаются большим количеством задач.

Материал книги рассчитан на школьников, знакомых со следующими фактами из теории чисел:

- сравнения по модулю и их свойства;
- деление остатков по простому модулю;

[1]Лицей «Вторая школа»

- малая теорема Ферма: $a^{p-1} \equiv_p 1$ при $a \not\equiv_p 0$;
- теорема Вильсона: $(p-1)! \equiv_p -1$.

В отдельных задачах также полезно знать о порядках чисел по простому модулю, но эти знания необязательны. Мы стремились сделать данную книгу самодостаточной и кратко изложили эти результаты в тексте. Для более детального изучения основ теории чисел можно обратиться к [6].

2. Введение

Нашим основным объектом исследования будут остатки по модулю. Напомним, что множество остатков по модулю m обозначается через $\mathbb{Z}_m$ и называется *кольцом остатков*. Термин «*кольцо*» означает, что с остатками можно проводить различные арифметические операции, и свойства этих операций аналогичны свойствам операций над целыми или рациональными числами. А именно, остатки можно складывать, вычитать и умножать, и эти операции подчиняются известным законам коммутативности, ассоциативности и дистрибутивности, к которым мы привыкли, работая с обычными целыми числами. Другими известными примерами колец являются множества целых чисел $\mathbb{Z}$ и многочленов $\mathbb{Q}[x]$ и $\mathbb{R}[x]$ с рациональными или вещественными коэфициентами соответственно.

Кольцо $\mathbb{Z}_m$ состоит из остатков 0, 1, 2, …, $m-1$. Однако при работе с остатками часто бывает необходимо рассматривать и произвольные целые числа. Чтобы работать с остатками произвольных целых чисел, используется понятие *сравнения по модулю*. А именно, два целых числа a и b называются *сравнимыми по модулю* m, если они имеют одинаковые остатки при делении на m. Мы будем обозначать это следующим образом: $a \equiv_m b$. Несложно доказать, что $a \equiv_m b$ тогда и только тогда, когда разность $a-b$ делится на m. Таким образом, мы, во-первых, получаем удобный инструмент для работы с остатками произвольных целых чисел, во-вторых, можем использовать этот инструмент при изучении делимости, и в-третьих, само обозначение $\equiv_m$ очень похоже на знак обычного равенства $=$, и эта похожесть переносится и на различные свойства сравнений. Точнее говоря, сравнения можно складывать, вычитать и перемножать, точно так же, как мы складываем, вычитаем и перемножаем обычные равенства.

Учитывая это, мы часто будем заменять *остатки* из кольца $\mathbb{Z}_m$ на *целые числа*, имеющие те же остатки. При такой замене свойства делимости или сравнений никак не изменятся, поэтому, выбирая подходящие для замены числа, можно быстро проводить те или иные вычисления. Например, это дает возможность использовать отрицательные числа для работы с остатками: $7^{100} \equiv_8 (-1)^{100} \equiv_8 1$.

Если же в качестве модуля m взять *простое число* p, мы получим *поле остатков* $\mathbb{Z}_p$. Опять же, термин «*поле*» означает наличие дополнительной по сравнению с кольцом арифметической операции — операции *деления*. Точно так же, как и рациональные числа, остатки по простому модулю можно *делить*, и в частном вновь получается остаток. Например, если 1 поделить на 2 в поле $\mathbb{Z}_5$, получится 3, поскольку $2 \cdot 3 \equiv_5 1$. Разумеется, делить можно лишь на ненулевые остатки, что опять же привычно нам еще с начальной школы: «На нуль делить нельзя!». Ниже мы докажем, что операция деления действительно корректно определена для всех ненулевых остатков.

Учитывая указанное выше сходство кольца остатков $\mathbb{Z}_m$ и кольца целых чисел $\mathbb{Z}$, логично продолжить развивать это сходство, ставя какие-то вопросы для обычных целых чисел и затем перенося их в кольцо остатков. Оказывается, что во многих случаях даже простые для обычных целых чисел вопросы имеют далеко нетривиальные ответы в кольцах остатков.

Одному из таких вопросов и посвящена данная книга. Звучит этот вопрос следующим образом:

> *когда данное число a является точным квадратом*? (Иначе говоря, *когда уравнение $x^2 = a$ имеет решение*?)

В случае, если число a — это обычное целое число, никаких проблем нет: число a либо равно 0 или 1, либо оно положительно и в разложении на простые сомножители каждый сомножитель содержится в четной степени. Можно сформулировать и какие-то другие эквивалентные условия (например, число a либо равно 0, либо имеет нечетное количество натуральных делителей).

Совсем по-другому дело обстоит, когда a — элемент кольца $\mathbb{Z}_m$. Здесь ситуация становится существенно более сложной. Например, остаток 2 является точным квадратом в поле $\mathbb{Z}_7$, т.к. $3^2 \equiv_7 2$, но не является точным квадратом в поле $\mathbb{Z}_5$, т.к. $1^2 \equiv_5 4^2 \equiv 1$ и $2^2 \equiv_5 3^2 \equiv_5 4$. Если в целых (и даже в вещественных) числах есть не больше двух решений уравнения $x^2 = a$, то в кольцах остатков это не так: например, сравнение $x^2 \equiv_{15} 1$ имеет четыре решения 1, 4, 11 и 14.

Немного обобщая заданный выше вопрос, можно сформулировать его следующим образом: *как решать квадратные уравнения над кольцом $\mathbb{Z}_m$*? Отметим, что аналогичный вопрос для *линейных уравнений*, т.е. для уравнений вида $ax \equiv_m b$, допускает довольно простой ответ, кстати говоря, напрямую связанный с вопросом о корректности операции деления остатков.

Пусть $d = (a, m)$ — наибольший общий делитель чисел a и m, и пусть $a = a_1 d$, $m = m_1 d$. Если число b не делится на d, то решений нет, т.к. разность $ax - b$ должна делиться на m, а значит, и на d, но при этом первое слагаемое делится на d, а второе нет. Если же b делится на d, то $b = b_1 d$ и сравнение $ax \equiv_m b$ равносильно сравнению $a_1 x \equiv_{m_1} b_1$. Если x_0 — решение данного сравнения на отрезке от 0 до $m_1 - 1$, то оно порождает серию решений x_0, $x_0 + m_1$, $x_0 + 2m_1$, …, $x_0 + (d-1)m_1$ исходного сравнения $ax \equiv_m b$ (попробуйте доказать, что все решения сравнения $ax \equiv_m b$ устроены таким образом). Итак, разделив числа a, b и m на $d = (a, m)$, мы фактически сводим задачу к ситуации, когда $(a, m) = 1$.

В таком случае остаток a называется *делителем единицы* в кольце $\mathbb{Z}_m$, и уравнение $ax \equiv_m b$ на самом деле имеет единственное решение x_0. Рассмотрим доказательство этого утверждения, поскольку его ключевая идея еще не раз встретится нам в дальнейшем. Выпишем все ненулевые остатки из кольца $\mathbb{Z}_m$: 1, 2, 3, …, $m-1$. А теперь умножим каждый остаток на a и рассмотрим новый набор остатков: $1 \cdot a$, $2 \cdot a$, $3 \cdot a$, …, $(m-1) \cdot a$. Заметим, что остатков в этом наборе столько же, сколько и в исходном. Кроме того, все остатки во втором наборе также разные: если $k \cdot a \equiv_m \ell \cdot a$ для некоторых различных остатков k и ℓ, то $ka - \ell a$ делится на m. Но $(a, m) = 1$, поэтому на самом деле $k - \ell$ делится на m и $k \equiv_m \ell$, что невозможно. Значит, умножение на a как бы перемешивает (или, как говорят, переставляет) ненулевые остатки в кольце $\mathbb{Z}_m$. Но раз в исходном наборе остатков был остаток b, то он будет и во втором наборе. А значит, он получается умножением некоторого (и единственного) остатка x_0 на остаток a, т.е. $ax_0 \equiv_m b$. Таким образом, мы доказали, что при $(a, m) = 1$ наше уравнение $ax \equiv_m b$ имеет единственное решение x_0. Часто для остатка x_0 используется обозначение $x_0 \equiv_m ba^{-1}$, по аналогии с обычным знаком равенства и свойством отрицательной степени: $x_0 = ba^{-1} = b/a$. Отметим, что в случае, когда $m = p$ — простое число, любой ненулевой остаток a является делителем единицы, а значит, на него можно поделить любое сравнение. По сути, мы доказали, что множество $\mathbb{Z}_p$ действительно является полем, т.е. в нем можно делить.

Конечно, остается вопрос о том, как найти решение сравнения $ax \equiv_m b$ явно, если, например, нам заданы численные значения величин a, b и m. Для этого есть много способов (наиболее известный из которых — алгоритм Евклида), но поиск явного решения не будет играть для нас большого значения, так что пойдем дальше, отсылая заинтересованного читателя к книге [6].

Вернемся к уравнению $x^2 \equiv_m a$. Приведенные выше примеры показывают, что вопрос изучения разрешимости этого уравнения в произвольном кольце остатков $\mathbb{Z}_m$ является весьма

сложным, и сходу дать на него ответ не получится. Поэтому мы будем продвигаться к возможному ответу на этот вопрос постепенно, шаг за шагом, попутно исследуя возникающие на нашем пути конструкции. И начнем мы с рассмотрения уравнения не в кольце, а в поле. Иначе говоря, зафиксируем простое число p и будем решать уравнение $x^2 \equiv_p a$. Именно это уравнение и связанные с ним вопросы будут для нас основными на протяжении почти всего дальнейшего повествования. В случае $p = 2$ оно не представляет интереса, поэтому всюду далее мы обычно будем предполагать, что простое число p *нечетно*. (Это условие не всегда будет явно встречаться в тексте повествования, но всегда будет явно обозначено в формулировках предложений и теорем.)

3. Вычеты, невычеты и арифметические операции над ними

Зафиксируем нечетное простое число p и поле остатков $\mathbb{Z}_p$, в котором мы будем работать. Возьмем также произвольный ненулевой остаток $a \in \mathbb{Z}_p$ и рассмотрим уравнение $x^2 \equiv_p a$.

Определение 1. Остаток a называется *квадратичным вычетом* (или просто *вычетом*) по модулю p, если существует такое целое число x, что $x^2 \equiv_p a$. В противном случае число a называется *квадратичным невычетом* (или просто *невычетом*).

Допуская вольность речи, мы также будем говорить, что *произвольное целое число* a, не кратное p, является вычетом или невычетом в $\mathbb{Z}_p$, имея в виду наличие или отсутствие решений уравнения $x^2 \equiv_p a$.

Чтобы можно было обозначать свойство числа быть вычетом или невычетом, используется специальный символ, известный также как *символ Лежандра*. Он обозначается через $\left(\frac{a}{p}\right)$ и определяется следующим образом:

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{если } a \equiv_p 0, \\ 1, & \text{если } a \text{ — вычет в } \mathbb{Z}_p, \\ -1, & \text{если } a \text{ — невычет в } \mathbb{Z}_p. \end{cases}$$

Можно сказать, что символ Лежандра — это аналог знака вещественного числа (именно знак числа отвечает за наличие у него квадратного корня): в вещественных числах уравнение $x^2 = a$ разрешимо тогда и только тогда, когда $a \geq 0$, в то время как сравнение $x^2 \equiv_p a$ разрешимо тогда и только тогда, когда $\left(\frac{a}{p}\right) \geq 0$.

Первый вопрос, на который мы ответим, звучит следующим образом: *сколько существует квадратичных вычетов по модулю* p? Понятно, что, задавая этот вопрос, мы интересуемся количеством *остатков в поле* $\mathbb{Z}_p$, являющихся квадратичными вычетами, а не количеством целых чисел, для которых уравнение $x^2 \equiv_p a$ разрешимо (ясно, что таких чисел бесконечно много). Иначе говоря, сколько существует остатков $a \in \mathbb{Z}_p$, для которых $\left(\frac{a}{p}\right) > 0$?

Вспоминая, что поле $\mathbb{Z}_p$ является аналогом поля вещественных чисел $\mathbb{R}$, а среди вещественных чисел положительных ровно половина (если отбросить нуль), то можно предположить, что и квадратичных вычетов (т.е. остатков с положительным символом Лежандра) среди всех ненулевых тоже половина. И это действительно так! Верно следующее

Предложение 1. *Для нечетного простого числа* p *количество квадратичных вычетов в поле* $\mathbb{Z}_p$ *равно* $\dfrac{p-1}{2}$.

Доказательство. Заметим, что остатки x и $p-x$, не равные 0, при возведении в квадрат дают одинаковые остатки: $x^2 \equiv_p (p-x)^2$. Поэтому квадратичных вычетов не более $\frac{p-1}{2}$: мы отбросили остаток 0, а все остальные остатки разбили на пары $(x, p-x)$, квадраты которых дают одинаковые остатки, являющиеся квадратичными вычетами. Докажем, что все эти вычеты будут различны. В самом деле, если $x^2 \equiv_p y^2$, то, перенося y^2 в левую часть, получаем, что $(x-y)(x+y) \equiv_p 0$. Это означает, что произведение $(x-y)(x+y)$ делится на простое число p. Это возможно в одном из двух случаев: либо $x-y$ делится на p (и тогда $y \equiv_p x$), либо $x+y$ делится на p (и тогда $y \equiv_p -x$). Значит, не более двух различных остатков при возведении в квадрат могут совпасть. Но такие остатки мы знаем — это в точности пары остатков $(x, p-x)$. Каждая такая пара дает свой квадратичный вычет, и самих вычетов получается в точности $\frac{p-1}{2}$, что и требовалось доказать. □

Задача 3.1. Выпишите все квадратичные вычеты по модулям 3, 5, 7 и 11.

Задача 3.2. Чтобы увидеть квадратичные вычеты, можно применить следующую конструкцию. Рассмотрим граф на $p-1$ вершине и пронумеруем вершины графа ненулевыми остатками по нечетному простому модулю p. Далее, соединим вершины u и v ориентированным ребром $(u \to v)$, если $u^2 \equiv_p v$. Таким образом, у нас возникает ориентированный граф, стрелки в котором указывают на вершины, являющиеся квадратичными вычетами. Интересная задача — иследовать этот граф и проинтерпретировать его геометрические свойства в терминах квадратичных вычетов. Мы отсылаем заинтересованного читателя к замечательной статье [4], где исследуются такие графы.

Теперь давайте поймем, как свойство остатка быть квадратичным вычетом или невычетом связано с арифметическими операциями сложения, вычитания, умножения и деления. Можно ли, например, утверждать, что сумма двух квадратичных вычетов — снова квадратичный вычет? Оказывается, что операции сложения и вычитания с квадратичными вычетами связаны плохо: сумма двух вычетов может быть как вычетом, так и невычетом. Например, остаток 1 — это вычет по любому простому модулю, но $1+1=2$ — невычет по модулю 5 и вычет по модулю 7.

Плохую связь вычетов с операциями сложения и вычитания можно объяснить следующим образом. Определение квадратичного вычета связано с операцией возведения в квадрат, т.е. с *умножением* остатков. Логично предположить, что именно операция умножения (и двойственная ей операция деления) будет хорошо взаимодействовать с вычетами. Подобное наблюдается и в других задачах теории чисел. Например, открытая до сих пор проблема Гольдбаха утверждает, что любое четное число, большее 2, может быть представлено в виде суммы *двух* простых чисел. С другой стороны, определение простого числа связано с операцией *умножения* (число p называется простым, если его нельзя представить в виде ab, где a и b — натуральные числа, отличные от p). Возможно, именно это обстоятельство объясняет, почему гипотеза Гольдбаха до сих пор не доказана.

С другой стороны, операция умножения действительно хорошо связана с квадратичными вычетами. Например, произведение двух вычетов также должно быть вычетом. Однако можно утверждать даже большее:

- произведение двух вычетов — вычет;
- произведение вычета и невычета — невычет;
- произведение двух невычетов — вычет.

В некотором смысле эти свойства родственны свойствам произведения положительных и отрицательных вещественных чисел. Выше мы уже отмечали, что квадратичные вычеты можно считать аналогом положительных вещественных чисел (вещественное число $a > 0 \leftrightarrow$ квадратичный вычет $\left(\frac{a}{p}\right) > 0$), а квадратичные невычеты — отрицательных вещественных чисел. Тогда свойства, указанные выше, аналогичны простому свойству знаков вещественных чисел: произведение двух чисел с одинаковым знаком положительно, а произведение двух чисел с разными знаками отрицательно.

Сформулируем теперь эти свойства с помощью одной формулы.

Предложение 2. *Для любых ненулевых остатков a и b по нечетному простому модулю p имеет место равенство $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$. Иначе говоря, символ Лежандра* мультипликативен.

Доказательство. Мы по очереди докажем каждое из следующих утверждений:

- произведение двух вычетов — вычет;
- произведение вычета и невычета — невычет;
- произведение двух невычетов — вычет.

Начнем с первого утверждения. Оно является совсем простым. В самом деле, если остатки a и b являются вычетами, то существуют остатки x и y, такие, что $a \equiv_p x^2$ и $b \equiv_p y^2$. Перемножая эти сравнения, получаем $ab \equiv_p (xy)^2$. Это и означает, что остаток ab является вычетом.

Теперь докажем, что произведение вычета и невычета является невычетом. Предположим противное: пусть $a \equiv_p x^2$ — вычет, b — невычет и $ab \equiv_p z^2$ — вычет. Тогда разделим сравнение $ab \equiv_p z^2$ на число a (вспомним, что это можно сделать, т.к. модуль p является простым числом, а потому в поле $\mathbb{Z}_p$ деление корректно определено) и получим, что $b \equiv_p (zx^{-1})^2$ — тоже квадратичный вычет, что невозможно. Полученное противоречие завершает доказательство второго утверждения.

Остался самый сложный факт. Докажем, что произведение двух невычетов является вычетом. Здесь у нас не получится рассуждать так просто. Дело в том, что в общем случае нельзя записать в виде сравнения свойство остатка быть квадратичным *невычетом*. Отсюда нам следует запомнить важный принцип работы с невычетами: *полезно перемножить или разделить их, чтобы получить вычет.*

Но как же тогда доказать наше утверждение? Вспомним, что когда мы доказывали разрешимость сравнения $ax \equiv_m b$, где a — делитель единицы, мы тоже не написали явную формулу для остатка x, но тем не менее смогли доказать его существование, последовательно умножив все остатки на a и найдя среди получившихся произведений остаток b.

Попробуем реализовать эту идею в нашем случае. Для этого рассмотрим множество V всех квадратичных вычетов по модулю p, и множество N всех квадратичных невычетов по модулю p. Ясно, что эти множества не пересекаются, и их объединение дает все ненулевые остатки по модулю p: $V \cap N = \varnothing$ и $V \cup N = \mathbb{Z}_p \setminus \{0\}$ (кратко это такое объединение называется *дизъюнктным* и обозначается следующим образом: $V \sqcup N = \mathbb{Z}_p \setminus \{0\}$). Теперь рассмотрим произвольный невычет $a \in N$. Умножим все ненулевые остатки на a, точно так же, как мы поступали, когда доказывали разрешимость сравнения $ax \equiv_m b$. Но теперь мы проследим по отдельности за судьбой остатков из множеств V и N.

Обозначим через aV множество остатков, которые получаются из остатков множества V умножением на элемент a. Поскольку произведение вычета на невычет является невычетом, то $aV \subseteq N$. Но на самом деле $aV = N$. Действительно, в предложении 1 мы доказали, что

$|V| = \dfrac{p-1}{2}$, а значит, $|N| = |\mathbb{Z}_p \setminus \{0\}| - |V| = \dfrac{p-1}{2} = |V|$. Значит, множество aV содержится во множестве N, причем у них одинаковое число элементов. Это возможно, только если они совпадают, т.е. $aV = N$.

Итак, мы поняли, что умножение на невычет a переводит множество V во множество N. Во что же тогда перейдет множество N? Представим себе, что у нас есть два ящика, V и N, каждый вместимостью по $\dfrac{p-1}{2}$ мест. Мы берем ненулевой остаток, умножаем его на a и кладем либо в V, если получившееся произведение является вычетом, либо в N, если получившееся произведение является невычетом. Выше мы доказали, что весь ящик N уже занят вычетами. Значит, оставшиеся остатки (невычеты) могут попасть только в ящик V. Но это и означает, что произведение невычета a на любой невычет является вычетом! Таким образом, наше утверждение полностью доказано. □

Из доказательства этого предложения полезно запомнить два принципа работы с вычетами и невычетами, которые мы еще не раз встретим в задачах.

- Если мы работаем с вычетами, нужно искать полные квадраты.
- Если мы работаем с невычетами, полезно перемножить или разделить их, чтобы получить вычет.

Давайте потренируемся использовать эти принципы на практике.

Задача 3.3. (a) Докажите, что если простое число p является делителем числа $x^2 - 6x + 3$, где x — целое, то оно также является делителем числа $y^2 - 2y - 53$ для некоторого целого y.

(b) Докажите, что если простое число p является делителем числа $x^2 - x + 3$, где x — целое, то оно также является делителем числа $y^2 - y + 25$ для некоторого целого y.

Задача 3.4. Числа $a^2 + 5a + 1$ и $2a^2 - a + 2$ не делятся на простое число p ни при каких целых a. Докажите, что для некоторого натурального n число $n^2 + 3n + 11$ делится на p.

В заключение этого раздела поговорим немного о выражениях вида $ax^2 + bxy + cy^2$, где a, b и c — произвольные целые числа. Изучение таких выражений было одной из основных задач алгебры и теории чисел XIX в., а отдельные результаты о них содержались еще в работах Ферма, Эйлера и др. Так, например, хорошо известна теорема Ферма, утверждающая, что простое число p вида $4k + 1$ может быть представлено в виде суммы квадратов двух натуральных чисел, т.е. что уравнение $x^2 + y^2 = p$ имеет решение. Другие, более глубокие результаты в этой науке (которая называется *теорией бинарных квадратичных форм*) можно найти в книге [5].

Мы отметим лишь один факт, связанный с бинарными квадратичными формами, который будет связан с квадратичными вычетами и будет полезен нам в дальнейшем. Для этого свяжем с каждой формой $f = ax^2 + bxy + cy^2$ величину $D := b^2 - 4ac$, которая называется *дискриминантом* формы f. Связь с обычным дискриминантом квадратного уравнения заключается в следующем. Рассмотрим сравнение $ax^2 + bxy + cy^2 \equiv_p 0$. Предположим, что $y \not\equiv_p 0$. Тогда наше сравнение можно разделить на y^2, и, полагая $t = xy^{-1}$, можно переписать сравнение уже для одной переменной t: $at^2 + bt + c \equiv_p 0$. В таком виде аналогия с квадратным уравнением и его дискриминантом становится гораздо более понятной.

Продолжая аналогию с квадратным уравнением, подумаем, что мы вообще знаем про решения квадратных уравнений. Мы знаем, что на разрешимость квадратного уравнения (в вещественных числах) влияет знак дискриминанта D: если $D < 0$, то квадратное уравнение не имеет решений, а если $D > 0$, то решений ровно два. Вспоминая, что аналогом знака числа в остатках является знак символа Лежандра этого числа, можно предположить, что сравнение

$at^2 + bt + c \equiv_p 0$ неразрешимо в $\mathbb{Z}_p$ тогда и только тогда, когда $\left(\frac{D}{p}\right) < 0$. И это действительно так! Сформулируем это утверждение аккуратно.

Предложение 3. *Пусть a, b и c — произвольные целые числа, такие, что a не делится на нечетное простое число p. Докажите, что сравнение $ax^2 + bxy + cy^2 \equiv_p 0$ равносильно сравнениям $x \equiv_p y \equiv_p 0$ тогда и только тогда, когда $\left(\frac{D}{p}\right) = -1$, где $D = b^2 - 4ac$ — дискриминант бинарной формы $ax^2 + bxy + cy^2$.*

Доказательство. Ясно, что сравнение $ax^2 + bxy + cy^2 \equiv_p 0$ всегда имеет решение $(0, 0)$. Предположим теперь, что у него есть еще одно решение, для которого $y \not\equiv_p 0$. Тогда разделим сравнение на y^2, введем переменную $t = xy^{-1}$ и рассмотрим новое сравнение $at^2 + bt + c \equiv_p 0$. Чтобы решить его, выделим полный квадрат. Для этого нам будет удобно домножить сравнение на $4a$:

$$4a^2t^2 + 4abt + b^2 \equiv_p b^2 - 4ac \quad \Longrightarrow \quad (2at + b)^2 \equiv_p D.$$

Если $\left(\frac{D}{p}\right) = -1$, то остаток D является невычетом и у нашего сравнения нет решений. Если же $\left(\frac{D}{p}\right) \geq 0$, то существует такой остаток d, что $d^2 \equiv D$, поэтому можно взять $t \equiv_p (d - b)(2a)^{-1}$ (деление на $2a$ вновь законно, т.к. мы работаем в поле $\mathbb{Z}_p$ для нечетного простого p). Значит, при $\left(\frac{D}{p}\right) = -1$ ненулевых решений у сравнения $ax^2 + bxy + cy^2 \equiv_p 0$ не существует, а при $\left(\frac{D}{p}\right) = 0$ или 1 ненулевые решения существуют. Отсюда и следует наше утверждение. □

Из доказательства этого предложения следует, что квадратное сравнение $at^2 + bt + c \equiv_p 0$, где a не делится на p, либо имеет ровно два решения, если $\left(\frac{D}{p}\right) = 1$, либо имеет ровно одно решение, если $\left(\frac{D}{p}\right) = 0$, либо не имеет решений, если $\left(\frac{D}{p}\right) = -1$.

Мы научились работать с квадратичными вычетами и невычетами, совершая с ними различные арифметические операции и используя при этом символ Лежандра. Ниже приведены задачи для самостоятельного решения, с помощью которых можно отработать эти навыки на более высоком уровне. Отметим, что многие из этих задач крайне трудны. Тем не менее, пытаясь справиться с этими задачами, можно существенно повысить свой уровень владения материалом (даже несмотря на то, что пока что этого материала не так и много): именно борьба с такими задачами позволяет освоить материал на более глубоком уровне. Решения этих задач приведены в конце книги; тем не менее, стоит обращаться к этим решениям лишь после достаточно упорных самостоятельных попыток.

Задача 3.5. Пусть a и b — целые числа и p — нечетное простое число, такое, что a не делится на p. Докажите, что $\sum\limits_{x=0}^{p-1} \left(\frac{ax + b}{p}\right) = 0$.

Задача 3.6. Пусть p — нечетное простое число. Докажите, что наименьший квадратичный невычет по модулю p меньше $\sqrt{p} + 1$.

Задача 3.7. Докажите, что многочлен $x^4 + 1$ приводим над $\mathbb{Z}_p$ для любого простого p (т.е. он представим в виде произведения двух многочленов положительной степени с коэффициентами в $\mathbb{Z}_p$).

Задача 3.8. Пусть A — это множество ненулевых остатков $a \in \mathbb{Z}_p$, таких, что остатки a и $4-a$ являются невычетами по модулю p. Найдите остаток произведения всех элементов множества A по модулю p.

4. Критерий Эйлера и вычеты по простым модулям вида $4k \pm 1$

В прошлом разделе мы научились проводить арифметические операции с квадратичными вычетами и невычетами, а также использовать символ Лежандра для записи тех или иных фактов и результатов. Теперь поговорим о следующем вопросе: *как вычислить символ Лежандра* $\left(\frac{a}{p}\right)$? Вот, например, нам дано число $p = 31$ и остаток $a = 6$. Чему равен символ Лежандра $\left(\frac{6}{31}\right)$? Понятно, что можно ответить на этот вопрос, составив таблицу квадратов по модулю 31, но делать этого как-то не хочется...

Оказывается, есть более простой способ, основанный на утверждении, которое называется *критерием Эйлера*. Его мы сейчас и рассмотрим.

Прежде чем переходить к критерию Эйлера, напомним сначала формулировку и доказательство важного результата в теории остатков, который известен как *малая теорема Ферма*.

Теорема 1 (малая теорема Ферма)**.** *Для любого простого числа p и целого числа a, не кратного p, имеет место сравнение $a^{p-1} \equiv_p 1$.*

Можно убрать условие «a не делится на p» и записать малую теорему Ферма в виде $a^p \equiv_p a$, однако для нас будет важна именно первая форма записи.

Доказательство. Существует очень много различных доказательств малой теоремы Ферма. Например, есть очень красивое геометрическое доказательство, использующее перестановки и их диаграммы Юнга. О нем мы поговорим позже. А сейчас мы дадим классическое доказательство, основанное на идее перемножения остатков.

Выпишем все ненулевые остатки 1, 2, 3, ..., $p-1$ и умножим каждый из них на a. Мы получим два набора остатков:

$$\{1,\ \ 2,\ \ 3,\ \ \ldots,\ \ p-1\} \quad \text{и} \quad \{1 \cdot a,\ \ 2 \cdot a,\ \ 3 \cdot a,\ \ \ldots,\ \ (p-1) \cdot a\}.$$

Ранее мы уже доказывали, что эти два набора отличаются лишь порядком остатков, поэтому произведения остатков в этих наборы сравнимы по модулю p. Произведение остатков первого набора равно $(p-1)!$, а произведение остатков второго набора равно $a^{p-1}(p-1)!$. Таким образом, $a^{p-1}(p-1)! \equiv_p (p-1)!$. Сокращая обе части сравнения на число $(p-1)!$ (вновь мы пользуемся возможностью делить на ненулевые остатки в поле $\mathbb{Z}_p$), мы получаем в точности малую теорему Ферма: $a^{p-1} \equiv_p 1$. □

Каким образом малая теорема Ферма поможет нам вычислить символ Лежандра $\left(\frac{a}{p}\right)$? Можно привести следующее рассуждение. Поскольку мы рассматриваем квадратичные вычеты и невычеты для нечетных простых чисел p, степень $p-1$ является четной. Т.е. можно записать малую теорему Ферма в виде $\left(a^{\frac{p-1}{2}}\right)^2 \equiv_p 1$. Но мы знаем, что единственные остатки, чьи квадраты дают 1, — это 1 и -1 (мы пишем -1 вместо $p-1$, заменяя остаток на сравнимое с ним целое число). Поэтому $a^{\frac{p-1}{2}}$ сравнимо или с 1, или с -1 по модулю p. Нам нужно выбрать правильный

знак, стоящий перед единичкой. А с другой стороны, с остатком a мы можем связать другой знак— знак символа Лежандра $\left(\frac{a}{p}\right)$. Может быть, эти знаки совпадают?.. Это действительно так! Иначе говоря, справедливо следующее сравнение: $\left(\frac{a}{p}\right) \equiv_p a^{\frac{p-1}{2}}$. Именно это сравнение и называется *критерием Эйлера.*

Теорема 2 (критерий Эйлера)**.** *Для любого простого числа p и целого числа a имеет место сравнение* $\left(\frac{a}{p}\right) \equiv_p a^{\frac{p-1}{2}}$.

Доказательство. Для доказательства критерия Эйлера нам достаточно проверить два утверждения:

- если $\left(\frac{a}{p}\right) = 1$, то $a^{\frac{p-1}{2}} \equiv_p 1$;
- если $\left(\frac{a}{p}\right) = -1$, то $a^{\frac{p-1}{2}} \equiv_p -1$.

Доказательство первого утверждения не представляет особой сложности. Действительно, если a — квадратичный вычет, то найдется такой ненулевой остаток x, что $a \equiv_p x^2$. Тогда

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

по малой теореме Ферма.

Второе утверждение является более сложным. Мы приведем два его доказательства. Одно из них будет более длинным, но при этом будет использовать уже знакомые нам принципы работы с вычетами и остатками, а другое будет довольно коротким, но при этом идейно более сложным.

Доказательство 1. Основной идеей этого рассуждения является модификация доказательства малой теоремы Ферма с помощью уже рассматриваемых нами ранее множеств V и N вычетов и невычетов.

Зафиксируем невычет a и умножим все вычеты на a. Мы получим все невычеты, что кратко можно записать так: $aV = N$. Перемножим теперь все остатки из левого и правого множеств. Пусть v — произведение все вычетов (т.е. всех элементов множества V), а n — произведение всех невычетов (т.е. всех элементов множества N). Тогда имеет место сравнение $a^{\frac{p-1}{2}} v \equiv_p n$.

Таким образом, нам достаточно вычислить остатки чисел v и n. Для этого мы сначала вычислим их сумму и произведение. Сумму посчитать совсем просто, ведь это просто сумма всех ненулевых остатков по модулю p. Поэтому $v+n = 1+2+3+\ldots+(p-1) = p \cdot \frac{p-1}{2} \equiv_p 0$. Теперь вычислим произведение vn. Это произведение равно $(p-1)!$. Остаток этого числа по модулю p можно найти следующим образом. Разобьем все остатки из произведения $1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1)$ на пары (a, a^{-1}). Тогда произведение остатков в одной паре равно 1. Остается заметить, что остатки 1 и $p-1$ остаются без пары, поэтому $(p-1)! \equiv_p 1 \cdot (p-1) \equiv_p -1$. Таким образом, $vn \equiv_p (p-1)! \equiv_p -1$. Это сравнение называется *теоремой Вильсона.*

Отметим, что получить формулы $v + n \equiv_p 0$ и $vn \equiv_p -1$ можно было с помощью одной общей конструкции, аналог которой нам еще встретится во втором доказательстве. Для этого рассмотрим многочлен $f(t) = t^{p-1} - 1$ как многочлен с коэффициентами из поля $\mathbb{Z}_p$. Из малой теоремы Ферма следует, что все остатки 1, 2, 3, ..., $p-1$ являются корнями этого многочлена,

причем этих корней в точности $p-1$. А значит, по теореме Безу можно разложить многочлен $f(t)$ на множители:

$$f(t) = t^{p-1} - 1 \equiv_p (t-1)(t-2)(t-3)\dots(t-(p-1)).$$

Осталось применить к нашему многочлену теорему Виета: сумма его корней равна коэффициенту при t^{p-2}, т.е. равна 0, т.к. $p > 2$, а произведение корней равно свободному члену, умноженному на $(-1)^{p-1}$, т.е. равна -1. Таким образом, $v + n \equiv_p 0$ и $vn \equiv_p -1$.

Из этих сравнений следует, что либо $v \equiv_p 1$ и $n \equiv_p -1$, либо $v \equiv_p -1$ и $n \equiv_p 1$. В обоих случаях сравнение $a^{\frac{p-1}{2}} v \equiv_p n$, которое мы получили в начале доказательства, превращается в искомое сравнение $a^{\frac{p-1}{2}} \equiv_p -1$.

Доказательство 2. Пусть a — квадратичный невычет. Рассмотрим многочлен $f(t) = t^{\frac{p-1}{2}} - 1$ над полем $\mathbb{Z}_p$. По теореме Безу у этого многочлена есть не более $\dfrac{p-1}{2}$ корней. Но по первому утверждению все квадратичные вычеты являются корнями многочлена f, а вычетов, как мы помним, ровно $\dfrac{p-1}{2}$, т.е. их количество равно степени многочлена f. Значит, если a — невычет, то он не может быть корнем многочлена f, т.е. $f(a) \not\equiv_p 0$ и $a^{\frac{p-1}{2}} - 1 \not\equiv_p 0$. Но мы уже отмечали выше, что $a^{\frac{p-1}{2}} \equiv_p 1$ или -1. Раз случай 1 невозможен, остается только вариант с -1. Поэтому $a^{\frac{p-1}{2}} \equiv_p -1$, что и требовалось доказать. □

Отметим, что из критерия Эйлера сразу следует мультипликативность символа Лежандра, доказанная нами ранее в предложении 2:

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

Давайте посмотрим, как критерий Эйлера позволяет вычислять символы Лежандра. Вычислим, например, символ Лежандра $\left(\dfrac{6}{31}\right)$:

$$\left(\frac{6}{31}\right) \equiv_{31} 6^{15} = (6^2)^7 \cdot 6 \equiv_{31} 5^7 \cdot 6 \equiv_{31} (5^2)^3 \cdot 30 \equiv_{31} (-6)^3 \cdot (-1) = 6^2 \cdot 6 \equiv_{31} 5 \cdot 6 \equiv_{31} -1.$$

Таким образом, 6 — квадратичный невычет по модулю 31.

Приведенное выше вычисление показывает, что несмотря на конструктивный характер, критерий Эйлера не так просто применить: приходится работать с вычислениями больших степеней, и даже для не очень больших чисел счет может оказаться довольно трудным. И уж тем более непонятно, как использовать критерий Эйлера для переменных величин a и p. Хотя в некоторых ситуациях это все же возможно.

Задача 4.1. Пусть $p = 4k - 1$ — простое число. Докажите, что если сравнение $x^2 \equiv_p a$ имеет решение, то $x \equiv_p \pm a^k$.

К счастью, в некоторых случаях критерий Эйлера работает очень быстро. Наиболее важный случай следующий. Давайте подумаем, степени какого целого числа a считать очень просто? Ясно, что легко считаются степени чисел 0 и 1, но они совсем уж неинтересны. Но есть еще одно число, чьи степени устроены просто — это число $a = -1$. Значение степени числа -1 зависит от четности этой степени: в четной степени мы получаем 1, а в нечетной — -1.

Отсюда вытекает следующая важная теорема.

Теорема 3 (о корне из -1)**.** *Число -1 является квадратичным вычетом по нечетному простому модулю p тогда и только тогда, когда $p \equiv_4 1$, т.е. p имеет вид $4k+1$.*

Доказательство. Мы вновь приведем два доказательства этой важной теоремы. Одно из них будет использовать критерий Эйлера, а другое — малую теорему Ферма и теорему Вильсона.

Доказательство 1. По критерию Эйлера имеем $\left(\dfrac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$. Правая часть этого равенства равна 1 тогда и только тогда, когда число $\dfrac{p-1}{2}$ четно, т.е. когда $p \equiv_4 1$, что и требовалось доказать.

Доказательство 2. Вначале докажем, что если p имеет вид $4k+3$, число -1 является невычетом по модулю p. В самом деле, преоположим противное: пусть найдется такой остаток x, что $x^2 \equiv_p -1$. Возведем это сравнение в степень $\dfrac{p-1}{2}$:

$$(x^2)^{\frac{p-1}{2}} \equiv_p (-1)^{\frac{p-1}{2}} \quad \Longrightarrow \quad x^{p-1} \equiv_p -1,$$

что противоречит малой теореме Ферма. Таким образом, при $p \equiv_4 3$ число -1 является невычетом по модулю p.

Осталось доказать, что если p имеет вид $4k+1$, число -1 является вычетом. Для этого запишем теорему Вильсона: $(p-1)! \equiv_p -1$. Наша цель — перегруппировать множители в левой части так, чтобы там получился точный квадрат. Для этого разобьем эти множители на две половины:

$$1,\ \ 2,\ \ 3,\ \ \ldots,\ \ \frac{p-1}{2} = 2k \quad \text{и} \quad \frac{p+1}{2} = 2k+1,\ \ \frac{p+3}{2} = 2k+3,\ \ \ldots,\ \ p-1 = 4k.$$

Заметим, что остатки из второго набора сравнимы с числами $-\dfrac{p-1}{2} = -2k$, $-\dfrac{p-3}{2} = -(2k-1)$, $\ldots$, -1, т.е. с остатками из первого набора, записанными со знаком «$-$» в обратном порядке. Сгруппируем теперь сомножители a и $-a$ и преобразуем получившееся произведение:

$$-1 \equiv_p (p-1)! = \big(1\cdot(-1)\big)\cdot\big(2\cdot(-2)\big)\cdot\ldots\cdot\Big(\frac{p-1}{2}\cdot\big(-\frac{p-1}{2}\big)\Big) = (-1)^{\frac{p-1}{2}}\cdot\big(1\cdot 2\cdot\ldots\cdot 2k\big)^2 = \big((2k)!\big)^2.$$

Таким образом, мы явно предъявили число (равное $(2k)!$), чей квадрат сравним с -1 по модулю $p = 4k+1$. Наше доказательство закончено. □

Из теоремы о корне из -1 следует так называемая теорема Жирара, связанная с теорией бинарных квадратичных форм.

Предложение 4 (теорема Жирара)**.** *Если целые числа x и y таковы, что $x^2 + y^2 \equiv_p 0$ для некоторого простого числа p вида $4k+3$, то $x \equiv_p y \equiv_p 0$.*

Доказательство. Предположим, что существуют такие x и y, что $y \not\equiv_p 0$ и $x^2+y^2 \equiv_p 0$. Разделив это сравнение на y^2 и полагая $t = xy^{-1}$, запишем сравнение в виде $t^2 \equiv_p -1$. Но это сравнение невозможно в силу теоремы о корне из -1. □

В частности, из теоремы Жирара сразу следует, что простые числа вида $4k+3$ не представимы в виде суммы квадратов двух натуральных чисел.

В различных задачах теорема о корне из -1 очень часто используется в следующей формулировке:

> *для любого натурального n нечетные простые делители числа n^2+1 имеют вид $4k+1$.*

Таким образом, часто бывает полезно создать в задаче выражение вида $n^2 + 1$ и доказать (предварительно предположив противное), что у него существует нечетный простой делитель вида $4k + 3$. Давайте потренируемся это делать на примере следующих задач. ни при каких натуральных числах m и n.

Задача 4.2. Существуют ли 18 последовательных натуральных чисел, которые можно разбить на две группы с одинаковыми произведениями?

Задача 4.3. (a) Докажите, что простых чисел вида $4k + 1$ бесконечно много. (*Указание*: рассмотрите многочлен $f(x) = x^2 + 1$.)

(b) Докажите, что существует бесконечно много натуральных чисел n, для которых число $n^2 + 1$ имеет не менее 2022 различных простых делителей

Задача 4.4. Докажите, что число $4mn - m - n$ не является точным квадратом ни при каких натуральных числах m и n.

Задача 4.5. Докажите, что число $\dfrac{x^2+1}{y^2-5}$ никогда не является целым при натуральных x, $y > 2$.

Задача 4.6. Докажите, что уравнение $x^2 = y^3 + 7$ не имеет решений в целых числах.

В заключение этого раздела мы докажем следующий важный результат, активно использующийся в различных аспектах теории чисел. Выглядет он довольно странно, и догадаться до него, заранее не зная, непросто. Поэтому мы сначала приведем пример задачи, которая подведет нас к основному вопросу.

Задача 4.7. Пусть p — нечетное простое число. Сколько существует пар соседних друг с другом квадратичных вычетов? Иначе говоря, какова мощность множества

$$\{x^2 + 1 : x \in \mathbb{Z}_p\} \cap \{y^2 : y \in \mathbb{Z}_p\}?$$

Решить эту задачу можно и без применения каких-то новых фактов (попробуйте сделать это!). Однако мы попробуем с ее помощью сформулировать тот общий вопрос, который играет очень важную роль во могих задачах из теории чисел.

Начнем с того, что немного упростим нашу задачу. Давайте рассмотрим сравнение $x^2 + 1 \equiv_p y^2$ и спросим, *сколько пар решений* (x, y) имеет это сравнение. Обратите внимание, это не то же самое, что и количество пар соседних квадратичных вычетов! Но посчитать количество пар решений оказывается проще.

Чего от нас хотят? По сути происходит следующее. Мы берем произвольный остаток x и смотрим, является ли число $x^2 + 1$ квадратичным вычетом. Если является, то это добавляет нам ровно два решения в общее количество (они соответствуют парам (x, y) и $(x, -y)$). Если $x^2 + 1 \equiv_p 0$, то такой x добавляет нам ровно одно решение (а именно, пару $(x, 0)$). Наконец, если $x^2 + 1$ является невычетом, то новых решений соответствующий x не добавляет.

Все эти три случая можно объединить следующей формулой. При фиксированном x количество решений сравнения $x^2 + 1 \equiv_p y^2$ равно $1 + \left(\dfrac{x^2+1}{p}\right)$. В самом деле, если символ Лежандра в этой формуле равен 1, то $x^2 + 1$ — вычет, и мы получаем два решения, если символ Лежандра равен 0, то мы получаем одно решение, и если он равен -1, то решений мы не получаем.

Таким образом, мы приходим к следующему утверждению. *Количество пар решений сравнения* $x^2 + 1 \equiv_p y^2$ *равно сумме* $\displaystyle\sum_{x=0}^{p-1} \left(1 + \left(\frac{x^2+1}{p}\right)\right)$.

Чему равна эта сумма? Ясно, что вклад единичек будет равен p, поэтому нам достаточно вычислить сумму $\displaystyle\sum_{x=0}^{p-1} \left(\frac{x^2+1}{p}\right)$. Почему можно надеяться, что эта сумма в принципе разумно

считается? Например, на это намекает задача **3.5.** Кроме того, ясно, что если вместо выражения $x^2 + 1$ записать любой другой квадратный трехчлен, то, научившись считать суммы символов Лежандра значений квадратных трехчленов $ax^2 + bx + c$, мы научимся находить количество решений сравнений вида $ax^2 + bx + c \equiv_p y^2$, а такая общая постановка вопроса выглядит весьма интересно.

И действительно, существует формула, вычисляющая соответствующую сумму символов Лежандра для произвольного квадратного трехчлена. Выглядит она следующим образом.

Теорема 4. *Пусть a, b и c — произвольные целые числа, такие, что числа a и $b^2 - 4ac$ не делятся на p. Тогда справедливо равенство* $\sum\limits_{x=0}^{p-1} \left(\dfrac{ax^2 + bx + c}{p}\right) = -\left(\dfrac{a}{p}\right)$.

Прежде чем доказывать эту теорему, завершим с ее помощью решение задачи **4.7.** Формула из теоремы 4 гласит, что $\sum\limits_{x=0}^{p-1} \left(\dfrac{x^2+1}{p}\right) = -1$, а потому количество пар решений сравнения $x^2 + 1 \equiv_p y^2$ равно $p - 1$.

Вычислим теперь количество *пар соседних квадратичных вычетов*. Чем это количество отличается от количества решений сравнения $x^2 + 1 \equiv_p y^2$? Тем, что некоторые пары решений дают одинаковые соседние пары вычетов. Даже более точно, каждая четверка решений $(\pm x, \pm y)$ дает одну пару соседних квадратичных вычетов. Поэтому кажется, что правильным ответом в нашей задаче будет число $\dfrac{p-1}{4}$.

Немного подумав, можно понять, что эта формула не может быть верной. Хотя бы потому, что для простых чисел p вида $4k + 3$ она дает нецелый ответ. Давайте поймем, в чем ошибка. На самом деле в некоторых исключительных случаях у нас получаются не четверки решений, в пары. Происходит это в одном из двух случаев: если $x = 0$ или если $y = 0$. В случае $p = 4k+3$ вариант $y = 0$ невозможен, т.к. сравнение $x^2 + 1 \equiv_p 0$ не имеет решений по теореме о корне из -1, а при $x = 0$ мы получаем пару $(0, \pm 1)$, которую надо учесть отдельно. Таким образом, при $p = 4k + 3$ ответ выглядит так: $\dfrac{(p-1)-2}{4} + 1 = k + 1$. Смысл это формулы следующий. Из общего количества пар решений сравнения $x^2 + 1 \equiv_p y^2$, равного $p - 1$, мы убираем две особые пары решений $(0, \pm 1)$, все остальные пары решений группируем в четверки $(\pm x, \pm y)$, каждая из которых порождает свою пару соседних вычетов, а затем добавляем еще одну пару соседних вычетов, соответствующую исключительным парам решений $(0, \pm 1)$.

Давайте теперь проведем аналогичные рассуждения для случая $p = 4k + 1$. В этом случае исключительных пар будет больше: уже знакомые нам пары $(0, \pm 1)$ и еще пары $(\pm a, 0)$, где $a^2 \equiv_p -1$. Тогда подсчет количества пар соседних вычетов дает следующий результат: $\dfrac{(p-1)-2-2}{4} + 1 + 1 = k + 1$.

Полученные в этих случаях ответы можно объединить в один: $\left\lceil \dfrac{p}{4} \right\rceil$ (проверьте это!). Это и есть ответ в нашей задаче.

Ответ. Существует в точности $\left\lceil \dfrac{p}{4} \right\rceil$ пар соседних квадратичных вычетов по модулю нечетного простого числа p.

Давайте потренируемся использовать теорему 4.

Задача 4.8. Даны нечетное простое число p и натуральное число $d > 1$. Выразите через p и d количество пар решений сравнения $dx^2 + y^2 \equiv_p 1$.

Задача 4.9. Для нечетного простого числа p вычислите количество неупорядоченных пар квадратичных вычетов с суммой 1.

Задача 4.10. Используя результат предыдущей задачи, вычислите символ Лежандра $\left(\frac{2}{p}\right)$. (В следующем разделе мы вычислим этот символ другим способом.)

Завершая этот раздел, докажем теорему 4.

Доказательство. Нам нужно доказать равенство $\sum\limits_{x=0}^{p-1}\left(\frac{ax^2+bx+c}{p}\right) = -\left(\frac{a}{p}\right)$. Пользуясь мультипликативностью символа Лежандра, разделим это сравнение на $\left(\frac{a}{p}\right)$ и положим $B \equiv_p ba^{-1}$ и $C \equiv_p ca^{-1}$. Тогда наше равенство примет следующий вид: $\sum\limits_{x=0}^{p-1}\left(\frac{x^2+Bx+C}{p}\right) = -1$. Именно с ним мы и будем работать.

Мы дадим два доказательства этого равенства. Одно из них будет использовать работу с квадратными сравнениями, а другое — критерий Эйлера.

Доказательство 1. Зафиксируем остаток x и попробуем понять, когда выражение x^2+Bx+C является вычетом. Если $\left(\frac{x^2+Bx+C}{p}\right) = 1$, то существует такой остаток α, что $x^2+Bx+C \equiv_p (x+\alpha)^2$. Более того, таких остатков α ровно два, поскольку существуют ровно два остатка, чьи квадраты сравнимы по модулю p с остатком x^2+Bx+C: это $x+\alpha$ и $-(x+\alpha) = x+(-2x-\alpha)$.

Теперь исследуем связь между остатками x и α. Если мы зафиксируем остаток α, то либо существует ровно один остаток x, для которого выполнено сравнение $x^2+Bx+C \equiv_p (x+\alpha)^2$, либо таких остатков x вообще не существует. В самом деле, раскрывая скобки и приводя подобные, получаем $x(B-2\alpha) \equiv_p \alpha^2 - C$. Если $\alpha \equiv_p B/2$, то левая часть равна 0, а правая нет, поскольку в противном случае $C \equiv_p \alpha^2$ и $b^2-4ac \equiv_p a^2(B^2-4C) \equiv_p a^2(4\alpha^2-4\alpha^2) \equiv_p 0$, что невозможно. Значит, при $\alpha \equiv_p B/2$ не существует остатка x, для которого выполнено сравнение $x^2+Bx+C \equiv_p (x+\alpha)^2$. Во всех остальных случаях сравнение $x(B-2\alpha) \equiv_p \alpha^2-C$ можно разделить на остаток $B-2\alpha$, не равный 0, и найти соответствующий x, являющийся решением этого сравнения.

Сказанное выше можно сформулировать следующим образом. Рассмотрим p сравнений на переменную x:

$$x^2+Bx+C \equiv_p x^2,\ \ x^2+Bx+C \equiv_p (x+1)^2,\ \ x^2+Bx+C \equiv_p (x+2)^2,\ \ \ldots,\ \ x^2+Bx+C \equiv_p \big(x+(p-1)\big)^2.$$

Среди этих сравнений есть ровно одно, у которого нет решений, а у всех остальных сравнений решение ровно одно. Кроме того, если при фиксированном остатке x остаток x^2+Bx+C является вычетом, то существуют в точности два остатка α_1 и α_2, такие, что $x^2+Bx+C \equiv_p (x+\alpha_1)^2 \equiv_p (x+\alpha_2)^2$.

Теперь мы готовы вычислить искомую сумму символов Лежандра. Чтобы сделать это, нам потребуется рассмотреть два случая: когда у квадратного трехчлена x^2+Bx+C есть два различных корня в поле $\mathbb{Z}_p$ (т.е. когда дискриминант $D = B^2-4C$ является вычетом) и когда у него нет корней в поле $\mathbb{Z}_p$ (т.е. когда дискриминант D является невычетом).

Случай 1: $\left(\frac{D}{p}\right) = 1$. Тогда у сравнения $x^2+Bx+C \equiv_p 0$ существуют ровно два различных корня x_1 и x_2. Вновь рассмотрим сравнения

$$x^2+Bx+C \equiv_p x^2,\ \ x^2+Bx+C \equiv_p (x+1)^2,\ \ x^2+Bx+C \equiv_p (x+2)^2,\ \ \ldots,\ \ x^2+Bx+C \equiv_p \big(x+(p-1)\big)^2.$$

Каждое сравнение, кроме одного, имеет единственное решение относительно величины x. При этом ровно два сравнения $x^2+Bx+C \equiv_p (x-x_1)^2$ и $x^2+Bx+C \equiv_p (x-x_2)^2$ имеют решения x_1 и x_2 соответственно, для которых $\left(\frac{x^2+Bx+C}{p}\right) = 0$, а для всех остальных остатков x

имеем $\left(\frac{x^2+Bx+C}{p}\right) = 1$. Однако таких остатков x на самом деле не $p-3$, а $\frac{p-3}{2}$, потому что для каждого x, удовлетворяющего условию $\left(\frac{x^2+Bx+C}{p}\right) = 1$, существуют в точности два различных остатка α_1 и α_2, для которых $x^2+Bx+C \equiv_p (x+\alpha_1)^2 \equiv_p (x+\alpha_2)^2$. Таким образом, среди слагаемых суммы $\sum\limits_{x=0}^{p-1}\left(\frac{x^2+Bx+C}{p}\right)$ есть ровно два нуля, ровно $\frac{p-3}{2}$ единиц и ровно $p-2-\frac{p-3}{2} = \frac{p-1}{2}$ минус единиц. В итоге наша сумма действительно равна -1, и первый случай разобран.

Случай 2: $\left(\frac{D}{p}\right) = -1$. Здесь все даже проще, поскольку не требуется исключать два особых остатка x, для которых $\left(\frac{x^2+Bx+C}{p}\right) = 0$ (таких остатков x просто нет). В этом случае у нас будет ровно $\frac{p-1}{2}$ слагаемых, равных 1, и ровно $p-\frac{p-1}{2} = \frac{p+1}{2}$ слагаемых, равных -1. Вновь получаем, что наша сумма равна -1. Таким образом, наша формула полностью доказана.

Доказательство 2. Возьмем формулу $\sum\limits_{x=0}^{p-1}\left(\frac{x^2+Bx+C}{p}\right) = -1$ и сделаем в ней замену $y \equiv_p x + B/2$. Для переменной y мы получим следующую формулу: $\sum\limits_{y=0}^{p-1}\left(\frac{y^2+d}{p}\right) = -1$, где $d \equiv_p C - B^2/4$. Заметим, что $d \not\equiv_p 0$.

Выберем произвольное слагаемое $\left(\frac{y^2+d}{p}\right)$ и применим критерий Эйлера. Мы получим следующее:

$$\left(\frac{y^2+d}{p}\right) \equiv_p (y^2+d)^{\frac{p-1}{2}} \equiv_p y^{p-1} + P(y),$$

где $P(y) = a_{p-2}y^{p-2} + a_{p-3}y^{p-3} + \ldots + a_1 y + a_0$ и $\deg P \le p-2$. Суммируя теперь слагаемые $y^{p-1}+P(y)$ по всем остаткам y, мы получаем, во-первых, сумму $\sum\limits_{y=0}^{p-1} y^{p-1} = p-1 \equiv_p -1$ (в этой сумме по малой теореме Ферма все слагаемые, кроме $y=0$, сравнимы с 1), а во-вторых, сумму

$$\sum_{y=0}^{p-1} P(y) = a_{p-2}\sum_{y=0}^{p-1} y^{p-2} + a_{p-3}\sum_{y=0}^{p-1} y^{p-3} + \ldots + a_1\sum_{y=0}^{p-1} y^1 + a_0\sum_{y=0}^{p-1} 1.$$

Докажем, что каждая сумма $\sum\limits_{y=0}^{p-1} y^k$ при любом $k = 1, \ldots, p-2$ равна 0.

Положим $S_k := \sum\limits_{y=0}^{p-1} y^k$. Умножим левую и правую части на a^k, где a — некоторый остаток по модулю p, отличный от 0. Заметим, что правая часть равенства при таком умножении не изменится, поскольку умножение остатков на a просто переставляет их. Значит, $a^k S \equiv_p S$ и $(a^k-1)S \equiv_p 0$. Докажем, что можно выбрать такое a, что $a^k \not\equiv_p 1$ (тогда отсюда сразу следует, что $S \equiv_p 0$).

Предположим, что существует такое $k \le p-2$, что $a^k - 1 \equiv_p 0$ для всех ненулевых остатков a. Рассмотрим многочлен $f(t) = t^k - 1$ над полем $\mathbb{Z}_p$. У этого многочлена есть $p-1$ корень (это все ненулевые остатки по модулю p), но при этом его степень k строго меньше $p-1$. Это противоречит теореме Безу. Значит, найдется остаток a, такой, что $a^k \not\equiv_p 1$. Проведя рассуждения для такого остатка, мы получаем, что $S \equiv_p 0$.

Таким образом, окончательно получаем:

$$\sum_{x=0}^{p-1}\Big(\frac{ax^2+bx+c}{p}\Big) \equiv_p \sum_{y=0}^{p-1}\Big(\frac{y^2+d}{p}\Big) \equiv_p \sum_{y=0}^{p-1} y^{p-1} + \sum_{y=0}^{p-1} P(y) =$$
$$= a_{p-2}\sum_{y=0}^{p-1} y^{p-2} + a_{p-3}\sum_{y=0}^{p-1} y^{p-3} + \ldots + a_1\sum_{y=0}^{p-1} y^1 + a_0\sum_{y=0}^{p-1} 1 \equiv_p -1.$$

Остается заметить, что наша сумма лежит в диапазоне от $-p$ до p, поэтому она может быть равна или -1, или $p-1$. Докажем, что случай $p-1$ невозможен. В самом деле, если сумма равна $p-1$, то в этой сумме все слагаемые, кроме одного, равны 1, а одно равно 0. Это означает, что существует единственный остаток y_0, такой, что $y_0^2+d \equiv_p 0$. Но это возможно только в случае, когда $y_0 \equiv_p 0$, и тогда $0 \equiv_p d \equiv_p C - B^2/4 \equiv_p (4ac-b^2)/4$, что невозможно по условию. Таким образом, искомая сумма равна -1, что и требовалось доказать. □

Замечание 1. В общем случае задача вычисления (или хотя бы оценки сумм вида $\sum\limits_{x=0}^{p-1}\Big(\frac{f(x)}{p}\Big)$), где f — заданный приведенный многочлен, очень важна в связи с оценкой количества решений сравнения $y^2 \equiv_p f(x)$. Например, в случае $\deg f = 3$ эта задача тесно связана с изучением эллиптических кривых, свойства которых используются в самых разных областях математики (например, именно с помощью эллиптических кривых была доказана Великая теорема Ферма). Самая простая (и самая известная) оценка называется *оценкой Хассе* и имеет следующий вид:

$$\left|\sum_{x=0}^{p-1}\Big(\frac{f(x)}{p}\Big)\right| \le (d-1)\sqrt{p}, \quad \text{где } d := \deg f.$$

На даже ее доказательство весьма непросто.

5. Квадратичный закон взаимности

В этом разделе мы рассмотрим центральный результат в элементарной теории квадратичных вычетов — *квадратичный закон взаимности*. Прежде чем сформулировать его, расскажем немного об истории его открытия.

Многие факты и результаты в классической теории чисел, ныне хорошо известные, обязаны своим появлением французскому математику Пьеру Ферма. Несмотря на то, что Ферма работал юристом (живя в небольшом городе Тулуза, он был одновременно и прокурором, и адвокатом, и судьей), много свободного времени он тратил на занятия математикой, в частности, теорией чисел (возможно, потому, что для открытия чего-то нового в ней тогда не требовалось каких-либо специальных познаний, а нужно было быть наблюдательным и в некоторой степени терпеливым человеком, проводя большое количество численных экспериментов и обрабатывая полученный эмпирический материал). Стиль Ферма был далек от привычного нам сейчас подхода к изложению новых утверждений: Ферма обычно не записывал доказательства найденных им фактов (так, без доказательства остались малая и Великая теоремы Ферма), а вместо этого посылал письма со своими открытиями профессиональным математикам, предлагая доказать сформулированные в этих письмах факты. Надо сказать, что очень часто математикам того времени не удавалось найти доказательств, так что по отношению к Ферма математическое сообщество того времени испытывало, мягко говоря, недобрые чувства. Возможно, именно поэтому многие факты, открытые Ферма, не смогли заинтересовать научное сообщество XVII

века, и пришлось ждать более 100 лет, пока математики нового поколения не взглянули на эти результаты по-новому...

Одним из математиков, сумевших понять и доказать многие результаты Ферма, стал российский математик Леонард Эйлер. Несмотря на то, что Эйлер родился в швейцарском городе Базель, более четверти века он жил и работал в Петербурге, а потому по праву его можно считать российским. Стиль работы Эйлера очень хорошо соответствовал стилю результатов, найденных Ферма. Неудивительно, что многие работы Эйлера по сути были посвящены развитию и обобщению этих результатов.

И вот один из таких результатов, сформулированных Ферма и оставленных им без доказательства, мы сейчас и рассмотрим. Речь идет о представимости квадратов в виде $\ell p - 1$, где p — простое число. Ферма утверждал, что для всякого простого p вида $4k+1$ существует квадрат вида $\ell p - 1$, а для p вида $4k+3$ таких квадратов не существует. Это утверждение по сути является теоремой о корне из -1. В 1747 г. Эйлер после нескольких безуспешных попыток (невероятно: у Эйлера не сразу получилось доказать это...) доказывает это утверждение Ферма и продолжает движение в естественном направлении: для каких p число $\ell p + 2$ может быть квадратом и, шире, для каких p при фиксированном a число $\ell p + a$ может быть квадратом? При $a = 2$ гипотеза состоит в том, что квадраты такого вида существуют при $p = 8k \pm 1$ и не существуют в остальных случаях (это результат задачи **4.10.**). Общая гипотеза, сформулированная Эйлером, звучит так.

Гипотеза (Гипотеза Эйлера)**.** *Число a является квадратичным вычетом или невычетом по модулю p одновременно для всех простых p из арифметической прогрессии $b + 4at$ (где $t = 1$, 2, ...). Иначе говоря, если $p \equiv_{4a} q$ — нечетные простые числа, то $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$.*

Эйлер смог доказать свою гипотезу, кроме $a = -1$, лишь для $a = 3$. Затем Лагранж доказал гипотезу при $a = 2, 5, 7$; Лежандр в 1785 г. предложил доказательство гипотезы для общего случая, которое, однако, содержало существенные пробелы. И наконец, 8 апреля 1796 г. немецкий математик Карл Фридрих Гаусс, которому на тот момент было всего 19 лет, нашел полное доказательство.

Вначале Гаусс, как и его предшественники, заметил утверждение для $a = -1$, затем, уже угадав результат для общего случая, он последовательно разобрал случай за случаем, продвинувшись дальше других: им вручную рассмотрены $a = \pm 2, \pm 3, \pm 5, \pm 7$. Восемь разных случаев, каждый из которых требовал отдельной работы! Общий случай (гипотеза Эйлера) не поддался первой атаке; Гаусс писал в своем дневнике: «Эта теорема мучила меня целый год и не поддавалась напряженнейшим усилиям». Впрочем, усилия крупнейших математиков того времени, пытавшихся доказать гипотезу Эйлера, также были безрезультатными.

Наконец, 8 апреля 1796 г. он находит общее доказательство, которое Кронекер (1823 – 1891) очень метко назвал «пробой сил гауссова гения». Доказательство проводится двойной индукцией по a и p; Гауссу приходится придумывать существенно различные соображения для рассмотрения восьми (!) различных случаев. Нужно было иметь не только поразительную изобретательность, но и удивительное мужество, чтобы не остановиться на этом пути. Позднее Гаусс нашел еще шесть доказательств гипотезы Эйлера (ныне их известно около пятидесяти).

Как это часто бывает, после того как теорема доказана, удается найти доказательства много более простые, чем первоначальное. Мы приведем далее семь различных доказательств гипотезы Эйлера (впрочем, шесть из них будут иметь общую природу), а также поговорим о том, как этот важный результат применяется при решении задач.

Нам будет удобно доказывать не гипотезу Эйлера, а несколько иное, эквивалентное ему утверждение, сформулированное В 1798 г. Лежандром и названное им *квадратичным законом взаимности.*

Теорема 5 (Квадратичный закон взаимности)**.** *Пусть p и q — различные нечётные простые числа. Тогда имеет место равенство*

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

Задача 5.1. Считая, что гипотеза Эйлера справедлива, выведите из нее квадратичный закон взаимности.

Все же мы будем доказывать квадратичный закон взаимности независимо от гипотезы Эйлера (а после выведем ее как следствие КЗВ). В этом разделе мы рассмотрим так называемое *геометрическое* доказательство этой теоремы. Оно будет основано на общей идее рассмотрения так называемых отрицательных остатков. Однако реализовать эту идею можно по-разному, и мы покажем шесть возможных способов для этого.

Итак, начнем. Для нечётного простого p запишем следующий ряд из $p-1$ числа:

$$1,2,3,\ldots,\frac{p-3}{2},\frac{p-1}{2},-\frac{p-1}{2},-\frac{p-3}{2},\ldots-3,-2,-1.$$

Заметим, что остатки этих чисел различны и отличны от 0, и потому можно сравнивать произвольные числа не с обычными остатками от 1 до $p-1$, а числами из этого набора. Поэтому, допуская вольность речи, также будем называть числа нашего набора *остатками*, причем остатки $1,2,3,\ldots,\frac{p-3}{2},\frac{p-1}{2}$ будем называть *положительными*, а остальные остатки — *отрицательными*. Подчеркнем, что по сути мы просто поделили все остатки на две равные части (убрав предварительно нулевой остаток), и первую половину назвали положительной, а вторую — отрицательной. Для нас будет важно именно наличие знака «$-$» перед отрицательными остатками; сравнивать их с нулем мы не будем (вообще сравнивать остатки — довольно странная идея...).

Теперь выберем произвольное целое число a, не кратное p, и попробуем понять, как свойство числа a быть квадратичным вычетом или невычетом по модулю p можно проинтерпретировать в терминах положительных и отрицательных остатков. Имеет место следующее утверждение, которое также известно как *лемма Гаусса*.

Предложение 5 (лемма Гаусса)**.** *Целое число a, не кратное нечетному простому числу p, является квадратичным вычетом по модулю p тогда и только тогда, когда среди остатков a, $2a$, $3a$, ..., $\frac{p-1}{2}a$ чётное число отрицательных.*

Доказательство. Рассмотрим набор остатков a, $2a$, $3a$, ..., $\frac{p-1}{2}a$. Ясно, что все эти остатки различны. Но верно даже более сильное утверждение: среди этих остатков присутствует ровно один остаток для каждой пары $(t,-t)$. Действительно, если $ax\equiv_p -ay$ для каких-то положительных остатков x и y, то, сокращая это сравнение на a, получаем, что $x\equiv_p -y$, что невозможно, т.к. сумма любых двух положительных остатков лежит в диапазоне от 2 до $p-1$.

Далее, обозначим количество отрицательных остатков среди остатков a, $2a$, $3a$, ..., $\frac{p-1}{2}a$ через s. Вновь, как и при доказательстве малой теоремы Ферма и критерия Эйлера, перемножим эти остатки. Заметим, что в произведении $a\cdot 2a\cdot 3a\cdot\ldots\cdot\frac{p-1}{2}a$ участвует ровно по одному остатку из каждой пары $(t,-t)$, а потому это произведение можно преобразовать следующим образом: $a\cdot 2a\cdot 3a\cdot\ldots\cdot\frac{p-1}{2}a=(-1)^s\cdot\left(1\cdot 2\cdot 3\cdot\ldots\cdot\frac{p-1}{2}\right)$. С другой стороны,

$$a\cdot 2a\cdot 3a\cdot\ldots\cdot\frac{p-1}{2}a=a^{\frac{p-1}{2}}\cdot\left(1\cdot 2\cdot 3\cdot\ldots\cdot\frac{p-1}{2}\right)\equiv_p\left(\frac{a}{p}\right)\cdot\left(1\cdot 2\cdot 3\cdot\ldots\cdot\frac{p-1}{2}\right).$$

Таким образом, $(-1)^s \cdot \left(1 \cdot 2 \cdot 3 \cdot \ldots \cdot \frac{p-1}{2}\right) \equiv_p \left(\frac{a}{p}\right) \cdot \left(1 \cdot 2 \cdot 3 \cdot \ldots \cdot \frac{p-1}{2}\right)$. Сокращая обе части сравнения на произведение положительных остатков, получаем, что $\left(\frac{a}{p}\right) = (-1)^s$, что и требовалось доказать. □

Видно, что в каком-то смысле лемма Гаусса аналогична ранее доказанному нами критерию Эйлера. Важное отличие между этими утверждениями заключается в том, что в критерии Эйлера нам приходится возводить в степень число a, и это очень неудобно. А в лемме Гаусса нужно возможить в степень число -1, что, конечно, гораздо удобнее. Надо отметить, что Эйлер не смог применить свой критерий в случае $a = 2$. А мы сейчас применим предложение 5 для этого случая и увидим, что оно довольно несложно работает.

Предложение 6. *Для нечётного простого p что число 2 является квадратичным вычетом тогда и только тогда, когда p имеет вид $8k \pm 1$. Иными словами,* $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

Доказательство. Применим лемму Гаусса, выбрав $a = 2$. Нам нужно понять, сколько чисел среди набора 2, 4, 6, …, $p-1$ имеют отрицательные остатки. Ясно, что отрицательные остатки будут иметь числа, которые строго больше, чем $\frac{p-1}{2}$, т.е. которые получаются при умножении на 2 остатков, строго больших, чем $\frac{p-1}{4}$. Значит, это в точности все четные числа на отрезке от $2\left\lceil\frac{p-1}{4}\right\rceil$ до $p-1$. Нас интересует четность количества четных чисел на этом отрезке, поэтому нужно смотреть остатки числа p по модулю 8. Сделаем это, разобрав четыре случая.

Случай 1: $p = 8k+1$. Тогда нам нужны четные числа на отрезке от $4k$ до $8k+1$. Количество четных чисел на нём равно $2k$, поэтому в этом случае число 2 — вычет по модулю p.

Случай 2: $p = 8k+3$. Тогда нам нужны четные числа на отрезке от $4k+2$ до $8k+2$. Количество четных чисел на нём равно $2k+1$, поэтому в этом случае число 2 — невычет по модулю p.

Случай 3: $p = 8k+5$. Тогда нам нужны четные числа на отрезке от $4k+4$ до $8k+4$. Количество четных чисел на нём равно $2k+1$, поэтому в этом случае число 2 — невычет по модулю p.

Случай 4: $p = 8k+7$. Тогда нам нужны четные числа на отрезке от $4k+4$ до $8k+6$. Количество четных чисел на нём равно $2k+2$, поэтому в этом случае число 2 — вычет по модулю p. □

Что ж, теперь настало время перейти к доказательству квадратичного закона взаимности. Учитывая значимость и важность этого результата, мы приведем сразу шесть доказательств. Но все они будут основаны на общей идее, которую мы сейчас и обсудим.

Расмотрим два различных нечетных простых числа p и q. Наша цель — вычислить символы Лежандра $\left(\frac{p}{q}\right)$ и $\left(\frac{q}{p}\right)$, используя лемму Гаусса. Для этого нам нужно вычислить количество отрицательных остатков по модулю q среди чисел $1 \cdot p$, $2 \cdot p$, …, $\frac{q-1}{2} \cdot p$ и количество отрицательных остатков по модулю p среди чисел $1 \cdot q$, $2 \cdot q$, …, $\frac{p-1}{2} \cdot q$. Ясно, что эти вычисления так или иначе будут отличаться заменой переменных p и q друг на друга, поэтому можно сосредоточиться на вычислении первого количества. Ключевым соображением, которое используется практически во всех вычислениях, является геометрическая интерпретация чисел, имеющих

отрицательные остатки. Посмотрим, как выглядит эта интерпретация в самом естественном и прямом доказательстве.

Доказательство 1. Рассмотрим набор чисел $1\cdot q$, $2\cdot q$, $\ldots$, $\dfrac{p-1}{2}\cdot q$. Мы хотим увидеть среди них те числа, остаток которых по модулю p отрицательный. Пусть у числа xq, где $1 \le x \le \dfrac{p-1}{2}$, остаток по модулю p отрицательный. Число xq лежит на отрезке, концы которого кратны p. Пусть yp — правый конец этого отрезка. Тогда тот факт, что остаток числа xq по модулю p отрицательный, означает, что число xq лежит в *правой половине* этого отрезка, т.е. выполнено двойное неравенство $-p/2 < xq-py < 0$. Наоборот, если найдутся такие x и y, что $1 \le x \le \dfrac{p-1}{2}$ и $-p/2 < xq - py < 0$, число xq имеет отрицательный остаток.

Наличие двух переменных x и y подсказывает ввести декартову систему координат Oxy и отметить на ней точки с натуральными координатами. Среди них нам нужно выбрать точки (x, y), чьи координаты удовлетворяют неравенствам $1 \le x \le \dfrac{p-1}{2}$ и $-p/2 < xq - py < 0$. Таким образом, мы получаем важную геометрическую интерпретацию чисел с отрицательными остатками:

> *числа с отрицательными остатками соответствуют некоторым специальным точкам на координатной плоскости.*

К сожалению, точки с координатами (x, y), удовлетворяющими неравенствам $1 \le x \le \dfrac{p-1}{2}$ и $-p/2 < xq-py < 0$, не очень удобны для изучения. Вспомним, однако, что эти точки нам нужны для вычисления только одного символа Лежандра $\left(\dfrac{q}{p}\right)$. Удивительно, но именно вычисление сразу двух символов Лежандра $\left(\dfrac{q}{p}\right)$ и $\left(\dfrac{p}{q}\right)$ и изучение точек, соответствующих сразу двум этим символам, гораздо более удобно!

Давайте проведем те же самые рассуждения для набора чисел $1 \cdot p$, $2 \cdot p$, $\ldots$, $\dfrac{q-1}{2} \cdot p$ и их отрицательных остатков по модулю q. Наша цель — сновь поставить в соответствие числам из этого набора, имеющим отрицательный остаток по модулю p, точку (x, y) на координатной плоскости Oxy. Поскольку в предыдущем рассуждении мы умножали на q координату y, то сейчас введем координаты следующим образом. Рассмотрим число yp, где $1 \le y \le \dfrac{q-1}{2}$ и запишем с помощью двойного неравенства тот факт, что у этого числа отрицательный остаток: $qx - q/2 < yp < qx$. В дальнейшем нам будет удобнее работать с эквивалентным двойным неравенством $-q/2 < yp - qx < 0$.

Видно, что условия, накладываемые на координаты точек, соответствующих числам с отрицательными остатками *сразу из двух наборов*, выглядят очень похожи; эти множества точек выглядят следующим образом:

$$S_1 := \{(x, y) : 1 \le x \le \frac{p-1}{2},\ -p/2 < xq-py < 0\} \quad \text{и} \quad S_2 := \{(x, y) : 1 \le y \le \frac{q-1}{2},\ -q/2 < yp-qx < 0\}.$$

Естественно предположить, что множество отрицательных остатков в обоих наборах соответствует следующему множеству точек на координатной плоскости:

$$S := \{(x, y) : 1 \le x \le \frac{p-1}{2},\ 1 \le y \le \frac{q-1}{2},\ -q/2 < yp - qx < p/2\}.$$

Для доказательства этого факта нам по сути достаточно показать, что для кооординат точек из множества S_1 выполнено неравенство $1 \le y \le \dfrac{q-1}{2}$, и наоборот, для кооординат точек из множества S_2 выполнено неравенство $1 \le x \le \dfrac{p-1}{2}$.

Давайте докажем, что если точка (x, y) лежит в S_1, то $1 \le y \le \dfrac{q-1}{2}$, а для множества S_2 рассуждение будет аналогичным. Это следует из несложных преобразований неравенств: $y > \dfrac{xq}{p} > 0$, откуда $y \ge 1$, и

$$y < \frac{xq}{p} + \frac{1}{2} \le \frac{(p-1)q}{2p} + \frac{1}{2} = \frac{q+1}{2} - \frac{q}{2p} < \frac{q+1}{2},$$

откуда $y \le \dfrac{q-1}{2}$, что и требовалось.

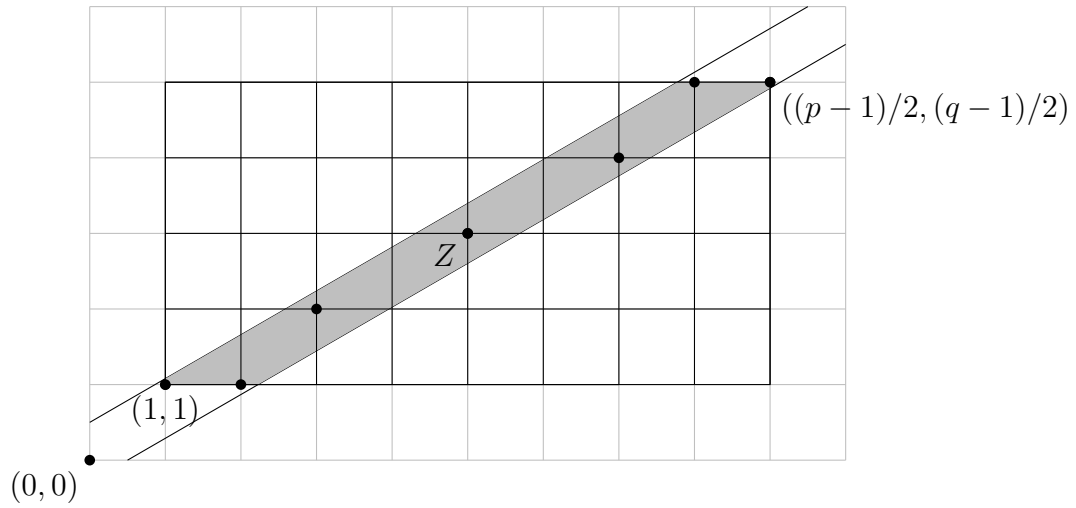
Это рассуждение и аналогичное ему рассуждение для множества S_2 показывают, что множества точек S_1 и S_2 можно объединить и получить множество S: $S_1 \cup S_2 = S$, причем $S_1 \cap S_2 = \varnothing$. Такое объединение (объединение непересекающихся множеств) называется *дизъюнктным* и обозначается следующим образом: $S_1 \sqcup S_2 = S$. То, что множества S_1 и S_2 не пересекаются, следует из того, что знак выражения $xq - yp$ для координат точек из этих множеств разный. Поясним, почему дизъюнктное объединение этих множеств дает S. Рассмотрим точки (x, y) множества S, для которых $yp - xq = c$, где $-q/2 < c < p/2$ — фиксированное целое число. Если $c > 0$, то все такие точки лежат во множестве S_1, если $c < 0$, то в S_2. Случай $c = 0$ невозможен, т.к. не существует натуральных чисел $x < p$, $y < q$, таких, что $xq = yp$.

Давайте свяжем множества S_1, S_2 и S с символами Лежандра $\left(\dfrac{p}{q}\right)$ и $\left(\dfrac{q}{p}\right)$. Для этого положим $s_1 := |S_1|$, $s_2 := |S_2|$, $s := |S| = |S_1| + |S_2| = s_1 + s_2$ и применим лемму Гаусса. Получается, что $\left(\dfrac{q}{p}\right) = (-1)^{s_1}$, $\left(\dfrac{p}{q}\right) = (-1)^{s_2}$ и $\left(\dfrac{q}{p}\right)\left(\dfrac{p}{q}\right) = (-1)^{s_1+s_2} = (-1)^s$. Таким образом, доказательство квадратичного закона взаимности сводится к проверке следующего утверждения:

четности чисел s и $\dfrac{(p-1)(q-1)}{4}$ совпадают.

В других доказательствах мы также будем пользоваться аналогичными переформулировками.

Итак, докажем наше утверждение о совпадении четностей чисел s и $\dfrac{(p-1)(q-1)}{4}$. Рассмотрим число s. Это число равно количеству точек с натуральными координатами, лежащими внутри прямоугольника, ограниченного прямыми $x = 1$, $y = 1$, $x = \dfrac{p-1}{2}$, $y = \dfrac{q-1}{2}$, и внутри полосы, заданной неравенствами $-q/2 < yp - qx < p/2$.



Заметим, что эта полоска симметрична относительно центра Z прямоугольника, имеющего координаты $\left(\frac{p+1}{4}, \frac{q+1}{4}\right)$. Это проверяется непосредственно в координатах (хотя геометрически это выгляжит очень правдоподобно, но простого доказательства без применения координат найти не удалось...): точка (x, y) при центральной симметрии с центром в Z перейдет в точку $\left(\frac{p+1}{2} - x, \frac{q+1}{2} - y\right)$. Тогда прямая $yp - xq = -q/2$, ограничивающая нашу полоску, перейдет в прямую

$$\left(\frac{q+1}{2} - y\right)p - \left(\frac{p+1}{2} - x\right)q = -\frac{q}{2} \quad \Longleftrightarrow \quad yp - xq = \frac{p}{2},$$

также ограничивающую нашу полоску.

Значит, все точки множества S симметричны относительно точки Z. Это означает, что если точка Z сама не лежит во множестве S, то все точки из S разбиваются на пары симметричных, а потому число s четно. Нечетным число s будет, если и только если координаты точки Z будут натуральными числами, что возможно лишь когда $p \equiv_4 q \equiv_4 3$. Т.е. если оба числа p и q имеют вид $4k+3$, то число s нечетно, а во всех остальных случаях s четно. Но ровно так же устроена четность числа $\dfrac{(p-1)(q-1)}{4}$: если оба числа p и q имеют вид $4k+3$, то оно нечетно, а во всех остальных случаях оно четно. Это означает, что четности чисел s и $\dfrac{(p-1)(q-1)}{4}$, что и завершает первое доказательство квадратичного закона взаимности. □

Мы постарались изложить первое доказательство квадратичного закона взаимности максимально подробно и аккуратно. Чтобы лучше проиллюстрировать его ключевую идею — сопоставление числам с отрицательными остатками точек с натуральными координатами на координатной плоскости, — мы приведем еще несколько доказательств, уже не проговаривая их настолько подробно.

Зафиксируем еще раз конструкцию сопоставления числам точек на координатной плоскости: мы сопоставили остатку числа xq по модулю p точку (x, y) на координатной плоскости, где $1 \leq x \leq \dfrac{p-1}{2}$, а $y = \left[\dfrac{xq}{p}\right]$. Наоборот, остатку числа yp по модулю q мы сопоставили точку (x, y) на координатной плоскости, где $1 \leq y \leq \dfrac{q-1}{2}$, а $x = \left[\dfrac{yp}{q}\right]$. Сейчас мы немного изменим эту конструкцию. Прежде всего докажем следующее утверждение.

Предложение 7. *Целое число a, не кратное нечётному простому числу p, является квадратичным вычетом по модулю p тогда и только тогда, когда число $\sum\limits_{x=1}^{(p-1)/2} \left[\dfrac{ax}{p/2}\right]$ четно.*

Доказательство. В самом деле, данная сумма есть не что иное, как количество чисел в наборе $1 \cdot a$, $2 \cdot a$, $\ldots$, $\dfrac{p-1}{2} \cdot a$, имеющих отрицательные остатки. Чтобы увидеть это, возьмем числовую прямую и разобьем ее на отрезки, концы которых расположены в точках 0, $\pm p/2$, $\pm 2 \cdot p/2$, $, 3 \cdot p/2$, $\ldots$ Пронумеруем отрезки, считая отрезок $[0, p/2]$ имеющим номер 0. Тогда подходящие нам числа из набора $1 \cdot a$, $2 \cdot a$, $\ldots$, $\dfrac{p-1}{2} \cdot a$, имеющие отрицательные остатки, — это в точности те числа, которые лежат на отрезках с нечетными номерами. Но если число ax лежит на некотором отрезке, номер этого отрезка равен $\left[\dfrac{ax}{p/2}\right]$. Значит, в сумме $\sum\limits_{x=1}^{(p-1)/2} \left[\dfrac{ax}{p/2}\right]$ четные слагаемые соответствуют числам с положительными остатками, а нечетные — числам с отрицательными остатками. Таким образом, четность количества чисел с отрицательными остатками равна четности нашей суммы. Осталось применить лемму Гаусса. □

Применим это предложение для вычисления символов Лежандра $\left(\dfrac{p}{q}\right)$ и $\left(\dfrac{q}{p}\right)$. Тогда для доказательства квадратичного закона взаимности остается доказать, что четности чисел

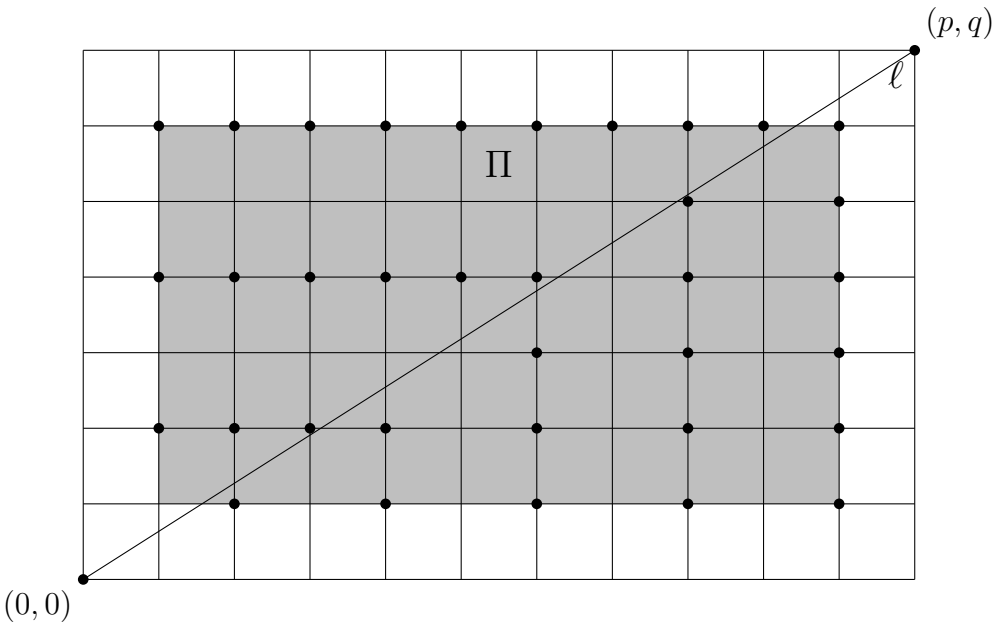
$$\sum_{x=1}^{(p-1)/2} \left[\frac{q}{p} \cdot (2x)\right] + \sum_{y=1}^{(q-1)/2} \left[\frac{p}{q} \cdot (2y)\right] \quad \text{и} \quad \frac{p-1}{2} \cdot \frac{q-1}{2}$$

равны. Именно это утверждение мы и будем доказывать.

Сначала поймем, как можно связать с левым выражением точки на координатной плоскости. Для этого рассмотрим декартову систему координат Oxy и нарисуем на ней прямоугольник высоты q и ширины p с вершиной в начале координат, лежащий в первой четверти. Координаты 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 $y = \dfrac{q}{p} \cdot x$.

Рассмотрим произвольное натуральное число x, где $1 \leq x \leq \dfrac{p-1}{2}$. Выберем все точки в прямоугольнике с абсциссой $2x$ и целой ординатой, лежащие ниже прямой ℓ. Их ордината должна удовлетворять условиям $1 \leq y \leq \dfrac{q}{p} \cdot (2x)$. Таким образом, количество этих точек равно $\left[\dfrac{q}{p} \cdot (2x)\right]$. Суммируя по x, получаем, что сумма $\sum\limits_{x=1}^{(p-1)/2} \left[\dfrac{q}{p} \cdot (2x)\right]$ равна количеству точек в прямоугольнике П, который ограничен прямыми $x = 1$, $y = 1$, $x = p - 1$, $y = q - 1$, которые лежат ниже прямой ℓ и имеют *чётные абсциссы*.

Аналогично, сумма $\sum\limits_{y=1}^{(q-1)/2} \left[\dfrac{p}{q} \cdot (2y)\right]$ равна количеству точек в прямоугольнике П, которые лежат выше прямой ℓ и имеют *чётные ординаты*.



Подчеркнем еще раз, что суммы $\sum\limits_{x=1}^{(p-1)/2}\left[\frac{q}{p}\cdot(2x)\right]$ и $\sum\limits_{y=1}^{(q-1)/2}\left[\frac{p}{q}\cdot(2y)\right]$ сами по себе весьма трудны для изучения. Но если их сложить, то получающееся выражение оказывается гораздо более удобным.

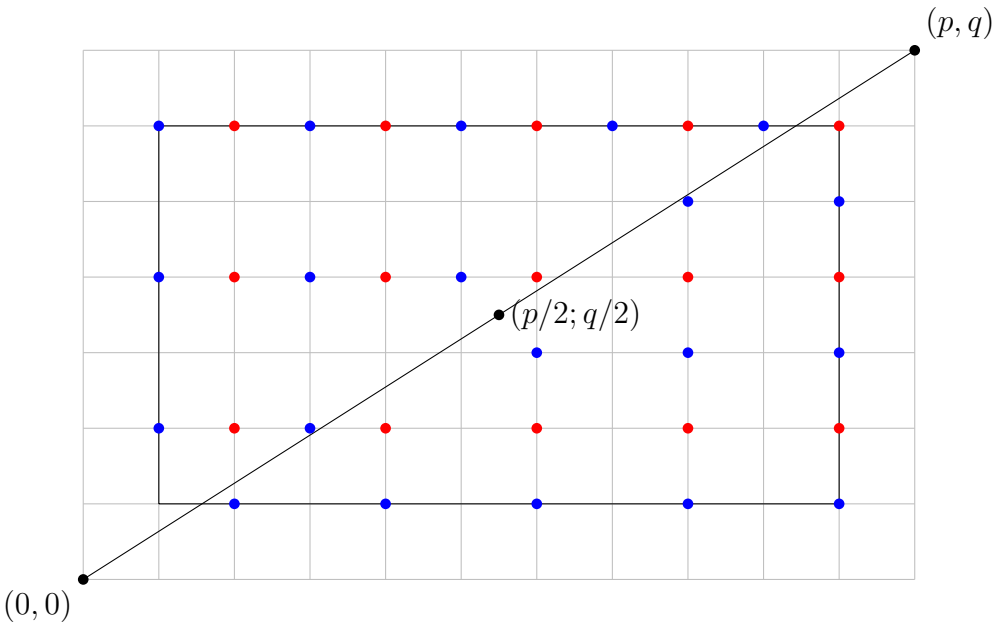
Отметим также, что прямая ℓ *не является* диагональю в прямоугольнике П.

Таким образом, доказательство квадратичного закона взаимности сводится к проверке следующего утверждения:

четности чисел $\sum\limits_{x=1}^{(p-1)/2}\left[\frac{q}{p}\cdot(2x)\right]+\sum\limits_{y=1}^{(q-1)/2}\left[\frac{p}{q}\cdot(2y)\right]$ *и* $\frac{p-1}{2}\cdot\frac{q-1}{2}$ *совпадают.*

Мы дадим четыре разных доказательства этого утверждения. Все они будут использовать те иил иные геометрические и комбинаторные соображения, позволяющие преобразовать первое выражение, не меняя его четность. Посмотрим, как это можно сделать.

Доказательство 2. Покрасим точку (x, y), лежащую в прямоугольнике, в *красный* цвет, если обе координаты x и y у нее четны. Все остальные точки покрасим в *синий* цвет:



Заметим, что красных точек ровно $\frac{p-1}{2} \cdot \frac{q-1}{2}$, поскольку есть $\frac{p-1}{2}$ способов выбрать её x-координату и $\frac{q-1}{2}$ — y-координату. Значит, достаточно доказать, что количество синих точек четно. Это легко сделать, разбив синие точки на пары симметричных относительно центра прямоугольника П: сопоставим каждой синей точке $A(x, y)$ точку $A'(p-x, q-y)$. Несложно видеть, что точка A' также является синей. Кроме того, центр прямоугольника П имеет нецелые координаты, а потому не является ни красным, ни синим.

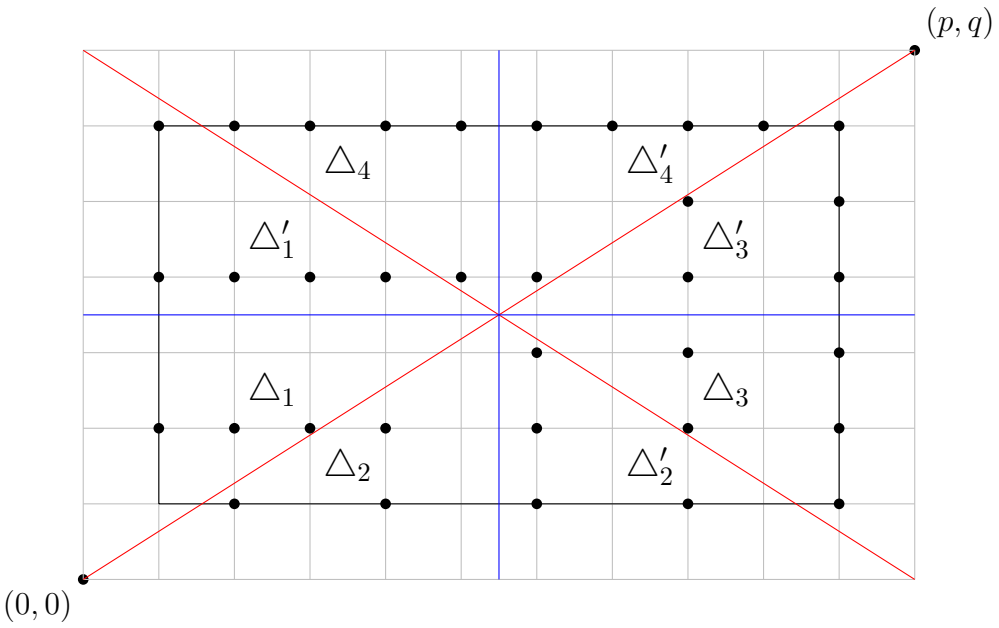
Итак, все точки в прямоугольнике П разбились на два класса — красные и синие. При этом синих точек четное количество, а красных точек ровно $\frac{p-1}{2} \cdot \frac{q-1}{2}$. Отсюда следует, что

$$\sum_{x=1}^{(p-1)/2} \left[\frac{q}{p} \cdot (2x)\right] + \sum_{y=1}^{(q-1)/2} \left[\frac{p}{q} \cdot (2y)\right] \equiv_2 \frac{p-1}{2} \cdot \frac{q-1}{2},$$

что и требовалось доказать. □

В данном доказательстве ключевой идеей являлась перегруппировка точек: мы хотели собрать из них прямоугольник размерами $\frac{p-1}{2} \times \frac{q-1}{2}$, оставив вне него четное количество других точек. Следующие два доказательства также реализуют эту идею, но другими способами.

Доказательство 3. Вновь рассмотрим точки в прямоугольнике П, одна из координат которых четна. С помощью некоторых естественных геометрических преобразований мы сейчас разобьем некоторые точки на пары, что позволит убрать их, не изменив четности общего количества точек, а остальные точки перенесем в прямоугольник размерами $\frac{p-1}{2} \times \frac{q-1}{2}$.

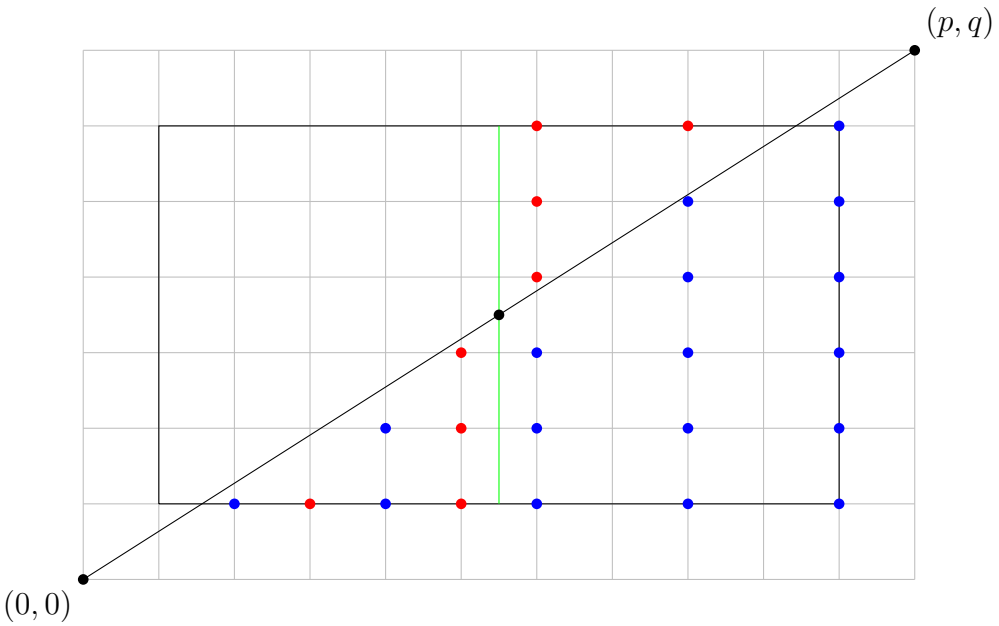


Рассмотрим красные и синие прямые. Они разбивают прямоугольник, ограниченный осями координат и прямыми $x = p$, $y = q$, на восемь треугольников. Заметим, что треугольники $\triangle_3$ и $\triangle'_3$, а также треугольники $\triangle_4$ и $\triangle'_4$ и отмеченные точки в них симметричны относительно одной из синих прямых. Значит, отмеченные точки в этих треугольниках бьются на пары, и мы можем убрать их, не изменив четность общего количества точек.

Далее, отразим треугольники $\triangle'_1$ и $\triangle'_2$ относительно соответственно горизонтальной и вертикальной синих прямых. Ясно, что отразив эти треугольники, мы получим прямоугольник, ограниченный осями координат и прямыми $x = p/2$ и $y = q/2$. Кроме того, при этих симметриях никакие отмеченные точки не склеятся, т.к. если у точки в треугольнике $\triangle'_1$ была четная координата y, то после отражения она станет нечетной. Аналогично, точки треугольника $\triangle'_2$ с четными координатами x перейдут в точки с нечетными координатами x.

Таким образом, мы собрали отмеченные точки в треугольниках $\triangle_1$, $\triangle'_1$, $\triangle_2$, $\triangle'_2$ в один прямоугольник. Ясно, что его размеры равны $\dfrac{p-1}{2} \times \dfrac{q-1}{2}$, а потому общее количество точек в нем равно $\dfrac{p-1}{2} \cdot \dfrac{q-1}{2}$, что и требовалось доказать. □

Доказательство 4. Соберем отмеченные точки прямоугольника П в прямоугольнике размером $\dfrac{p-1}{2} \times \dfrac{q-1}{2}$ еще одним способом. Для этого сначала рассмотрим отмеченные точки, лежащие под прямой ℓ. Покрасим их всех в синий цвет.



Теперь рассмотрим синие точки, лежащие правее зеленой прямой $x = p/2$, и закрасим красным цветом все точки, которые, во-первых, лежат в прямоугольнике П, а во-вторых, находятся в столбах, содержащих синие точки. Заметим, что красные точки лежат выше прямой ℓ и в каждом стоолбце четность количества синих точек и красных точек совпадает (т.к. их сумма равна $p - 1$ и потому четна). Поэтому заметим синие точки на красные, лежащие в тех же столбцах. Это не изменит четности общего количества отмеченных точек.

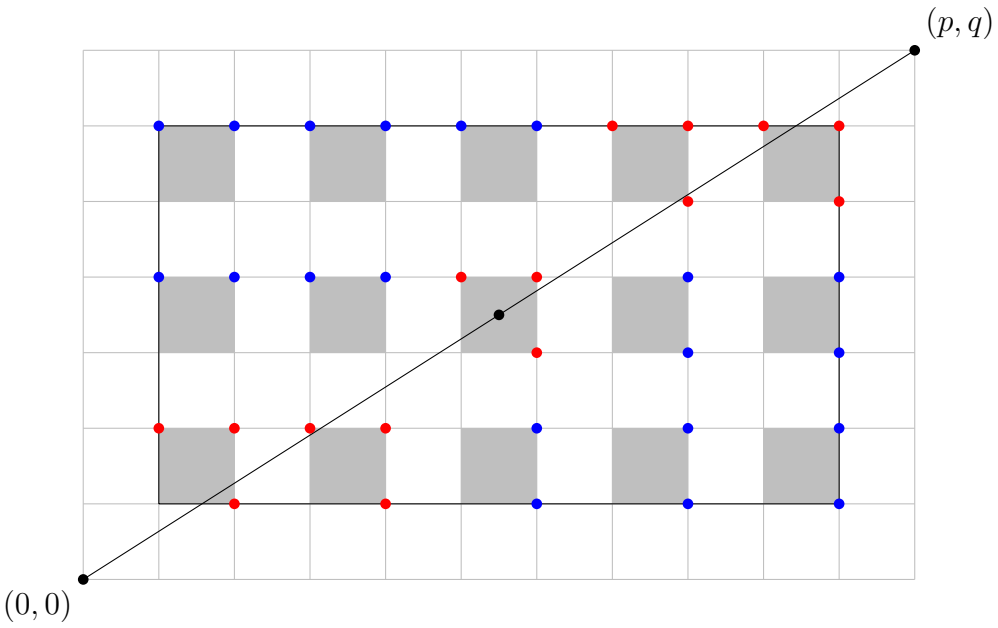
Далее уже привычно отразим красные точки относительно центра прямоугольника П. В результате красные точки перейдут в красные точки, лежащие под прямой ℓ и имеющие нечетные координаты x. В результате мы получим полностью заполненную часть прямоугольника, ограниченного прямыми $x = 1$, $y = 1$, $x = \dfrac{p-1}{2}$, $y = \dfrac{q-1}{2}$, которая лежит ниже прямой ℓ.

Абсолютно аналогично можно заполнить часть этого прямоугольника, лежащую выше прямой ℓ. В итоге мы, не изменив четности количества отмеченных точек, вновь собрали их в прямоугольник размерами $\dfrac{p-1}{2} \times \dfrac{q-1}{2}$, что и требовалось. □

Приведем еще одно рассуждение, которое в чем-то напоминает доказательство 1. Здесь мы будем группировать по парам не симметричные точки, а точки, находящиеся рядом друг с другом.

Доказательство 5. Рассмотрим прямоугольник П и отмеченные клетки в нем. Покрасим клетки прямоугольника П в разреженную шахматную раскраску, закрасив клетки, которые находятся на пересечении строк и столбцов с четными номерами (мы ведем нумерацию строк и столбцов, начиная с 1).

Теперь будем красить отмеченные точки по следующему правилу. Возьмем закрашенную клетку и отмеченные точки, лежащие на ней. Если клетка не пересекается прямой ℓ, покрасим точки на ней в синий цвет, а если пересекается, то в красный. Заметим, что на каждой покрашенной клетке есть либо ровно две синие точки, либо ровно три красные. Поскольку нас интересует четность общего количества отмеченных точек, мы можем убрать все синие точки и рассматривать только красные.



Заметим, что все закрашенные клетки симметричны относительно центра прямоугольника П, поэтому и красные точки разбиваются на пары центрально симметричных. Значит, количество красных точек будет нечетным, если и только если центр одного из квадратиков совпадает с центром прямоугольника П. Это в свою очередь возможно только в случае, когда номера строки и столбца, не пересечении которых находится центр прямоугольника П, четны. Эти номера равны соответственно $\frac{p+1}{2}$ и $\frac{q+1}{2}$. Значит, количество красных точек нечетно тогда и только тогда, когда числа $\frac{p+1}{2}$ и $\frac{q+1}{2}$ четны, а это равносильно условиям $p \equiv_4 q \equiv_4 3$. Поскольку четность числа $\frac{(p-1)(q-1)}{4}$ устроена точно так же, мы вновь получаем доказательство нашего утверждения. □

В заключение приведем последнее геометрическое доказательство, которое выглядит скорее как трюк, но преследует естественную цель — убрать условие четности координат рассматриваемых точек.

Доказательство 6. Ранее мы доказали, что число a, не кратное нечетному простому числу p, является квадратичным вычетом по модулю p тогда и только тогда, когда число $\sum\limits_{x=1}^{(p-1)/2} \left[\frac{qx}{p/2}\right]$ четно. Докажем, что на самом деле четность этой суммы совпадает с четностью суммы $\sum\limits_{x=1}^{(p-1)/2} \left[\frac{qx}{p}\right]$. Заменяя при необходимости число a на число $p-a$, можно считать, что a нечетно.

Рассмотрим следующее преобразование символов Лежандра:

$$\left(\frac{2}{p}\right)\left(\frac{a}{p}\right) = \left(\frac{2a}{p}\right) = \left(\frac{2a+2p}{p}\right) = \left(\frac{(a+p)/2}{p}\right).$$

Знак последнего символа Лежандра зависит от знака следующей суммы: $\sum\limits_{x=1}^{(p-1)/2} \left[\frac{x(a+p)/2}{p/2}\right]$. Преобразуем ее:

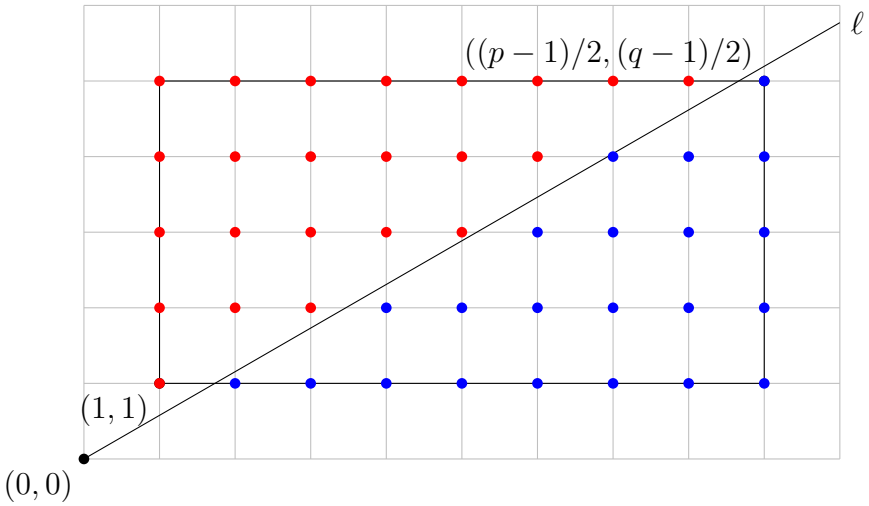
$$\sum_{x=1}^{(p-1)/2} \left[\frac{x(a+p)/2}{p/2}\right] = \sum_{x=1}^{(p-1)/2} \left[\frac{x(a+p)}{p}\right] = \sum_{x=1}^{(p-1)/2} x + \sum_{x=1}^{(p-1)/2} \left[\frac{xa}{p}\right] = \frac{p^2-1}{8} + \sum_{x=1}^{(p-1)/2} \left[\frac{xa}{p}\right].$$

Поскольку $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$, получаем, что $\left(\frac{a}{p}\right) = (-1)^{\sum\limits_{x=1}^{(p-1)/2} \left[\frac{xa}{p}\right]}$, что и требовалось.

Перейдем теперь к доказательству квадратичного закона взаимности. Согласно доказанному выше, нам нужно проверить, что четности чисел

$$\sum_{x=1}^{(p-1)/2} \left[\frac{xq}{p}\right] + \sum_{y=1}^{(q-1)/2} \left[\frac{yp}{q}\right] \quad \text{и} \quad \frac{p-1}{2} \cdot \frac{q-1}{2}$$

совпадают. На самом деле мы сейчас увидим, что эти числа просто равны.



Вновь введем декартову систему координат, рассмотрим прямоугольник, ограниченный прямыми $x = 1$, $y = 1$, $x = \frac{p-1}{2}$, $y = \frac{q-1}{2}$, и проведем прямую (не диагональ!) ℓ, заданную уравнением $y = \frac{q}{p} \cdot x$. Ясно, что первая сумма — это количество точек с натуральными координатами внутри этого прямоугольника, лежащих под прямой ℓ (синие точки), а вторая сумма — количество точек над прямой ℓ (красные точки). Значит, общее количество точек равно $\frac{p-1}{2} \cdot \frac{q-1}{2}$, что и требовалось доказать. □

Мы потратили много сил, разбирая различные доказательства квадратичного закона взаимности. Настало время потренироваться его применять. Стандартная техника использования КЗВ в задачах заключается в том, что мы должны вывести из условия задачи, что некоторое число является вычетом или невычетом по подходящему модулю, а затем, применив КЗВ, прийти к противоречию. Сначала приведены задачи, где искомый вычет или невычет является числом, а затем — задачи, где вычет является переменной величиной.

Задача 5.2. Используя квадратичный закон взаимности и свойство мультипликативности символа Лежандра, разберитесь, является ли 79 квадратичным вычетом по модулю 101.

Задача 5.3. Докажите, что ни при каком натуральном n у числа $2^n + 1$ не может быть простых делителей вида $8k + 7$.

Задача 5.4. (a) Докажите, что -3 — квадратичный вычет по модулю нечетного простого числа p тогда и только тогда, когда $p \equiv_6 1$.

(b) Докажите, что простых чисел вида $6k + 1$ бесконечно много.

Задача 5.5. Целые числа x и y таковы, что x^2+xy+y^2 делится на простое число p вида $3k+2$. Докажите, что сами числа x и y делятся на p.

Задача 5.6. Докажите, что если число $p = 2^n + 1$ — простое и больше 3, то минимальная степень T такая, что $3^T \equiv_p 1$, равна $p-1$.

Задача 5.7. Натуральные числа a и b таковы, что числа $15a+16b$ и $16a-15b$ являются точными квадратами. Каково наименьшее возможное значение меньшего из этих квадратов?

Задача 5.8. Найдите наименьший простой делитель числа $12^{2^{15}} + 1$.

Задача 5.9. Докажите, что дробь $\dfrac{a^2+b^2+c^2}{3(ab+bc+ca)}$ не является натуральным числом ни при каких натуральных a, b, c.

Задача 5.10. Найти все целые числа x и y, для которых число $\dfrac{x^2+x+2}{y^6-2}$ целое.

Задача 5.11. Дано натуральное число $n > 1$. Докажите, что любой нечётный делитель $d > 10$ числа $5n^2+1$ имеет в своей десятичной записи чётную цифру.

Задача 5.12. Пусть $P(x) = x^3 + 14x^2 - 2x + 1$. Докажите, что существует такое натуральное n, что число $\underbrace{P(P(\dots P}_{n}(x))) - x$ делится на 101 при любом натуральном x.

Задача 5.13. Натуральные числа m и n таковы, что число $\frac{(m+3)^n+1}{3m}$ натуральное. Докажите, что тогда это число нечетно.

Задача 5.14. Определим последовательность $\{x_n\}$ следующим образом: $x_1 = a$, $x_{n+1} = 2x_n + 1$. Пусть $y_n = 2^{x_n} - 1$. Какое максимальное количество подряд идущих простых чисел может встретиться в последовательности $\{y_n\}$?

Задача 5.15. Даны натуральные числа: нечётное a, чётное b, простое p. Известно, что $p = a^2 + b^2$. Докажите, что a — квадратичный вычет по модулю p.

Задача 5.16. Докажите гипотезу Эйлера, используя КЗВ. Т.е. докажите, что если $p \equiv_{4a} q$, то $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$.

6. Символ Якоби и обобщение КЗВ

До сих пор мы развивали теорию квадратичных вычетов по *простым* модулям. Настало время поговорить о *составных* модулях. Проблемы, возникающие при переходе от простого модуля к составному, кратко можно сформулировать в одной фразе: *мы переходим от поля $\mathbb{Z}_p$ к кольцу $\mathbb{Z}_m$*. Это означает, что мы теряем одну из арифметических операций — операцию деления. Оказывается, что это очень значимая потеря: если внимательно проследить доказательства стартовых фактов про символы Лежандра, становится понятно, что на возможность деления сравнений опирается подавляющее число рассуждений. Поэтому дословно перенести развитую нами теорию на случай составного модуля, увы, невозможно.

Попробуем поступить так же, как и при решении задач прошлого раздела: при появлении составного числа разложим его на простые сомножители и рассмотрим отдельно каждый сомножитель. Эта естественная идея приводит к следующему важному определению.

Определение 2. *Символ Якоби* целого числа a по модулю нечетного натурального числа m определяется следующим образом: если $m = p_1 \dots p_t$ — разложение m на (возможно, повторя-

ющиеся) простые множители, то

$$\left(\frac{a}{m}\right) = \left(\frac{a}{p_1}\right) \dots \left(\frac{a}{p_t}\right).$$

Обратите внимание на то, что мы рассматриваем лишь *нечетные* модули m. Это требование связано с тем, что четное простое число 2 находится на особом положении в теории чисел. Вспомним, например, что в развитой нами теории символов Лежандра мы всегда рассматривали именно нечетные простые числа. Так что это существенное условие мы перенесем и в определение символа Якоби.

Попробуем понять, как свойство быть квадратичным вычетом или невычетом по простым модулям связано со свойством быть квадратичным вычетом или невычетом по модулю составному. Поначалу кажется, что связь довольно слабая. Например, если $\left(\frac{a}{m}\right) = 1$, то a не обязан быть вычетом в $\mathbb{Z}_m$: так, $\left(\frac{2}{15}\right) = 1$, ибо $\left(\frac{2}{3}\right) = \left(\frac{2}{5}\right) = -1$, но 2 — невычет в $\mathbb{Z}_{15}$. Значит, важно не равенство 1 символа Якоби, а наличие в нем отрицательного символа Лежандра:

> *если в нечетном числе m найдется простой делитель p, для которого $\left(\frac{a}{p}\right) = -1$, то a — невычет в $\mathbb{Z}_m$.*

А когда можно гарантированно найти такой простой делитель? Например, когда сам символ Якоби отрицателен! Ведь символ Якоби равен произведению символов Лежандра, и если это произведение отрицательно, то среди сомножителей тоже должен найтись отрицательный. Таким образом, нами доказано следующее утверждение.

Предложение 8. *Если для некоторого целого числа a и нечетного натурального числа m выполнено равенство $\left(\frac{a}{m}\right) = -1$, то a — квадратичный невычет по модулю m.*

Чтобы применять это предложение, нам нужно научиться вычислять символы Якоби. Конечно, делать это по определению очень неудобно. Тем не менее, удивительно, что многие свойства символа Лежандра, доказанные нами ранее и использующиеся для его вычисления, остаются справедливы и для символа Якоби! Начнем со следующего несложного утверждения.

Предложение 9. *Для символов Якоби справедливы следующие формулы:*

$$\left(\frac{a_1 a_2}{m}\right) = \left(\frac{a_1}{m}\right)\left(\frac{a_2}{m}\right) \quad \text{и} \quad \left(\frac{a}{m_1 m_2}\right) = \left(\frac{a}{m_1}\right)\left(\frac{a}{m_2}\right).$$

Ясно, что первая формула следует из мультипликативности символа Лежандра, а вторая — из определения символа Якоби.

Однако этих свойств недостаточно для эффективного применения символов Якоби. Вспомним, что при работе с символами Лежандра нами наиболее активно использовались символы Лежандра для чисел -1 и 2, а также квадратичный закон взаимности. Число -1 помогало справляться с отрицательными числами, число 2 — с четными, а квадратичный закон взаимности мог менять число и модуль, реализуя некоторый аналог алгоритма Евклида. Невероятно, что все три этих соображения переносятся на символы Якоби, причем дословно! Сформулируем все три аналога этих соображений для символа Якоби в одной теореме, которую будем называть *квадратичным законом взаимности для символов Якоби.*

Теорема 6 (Квадратичный закон взаимности для символов Якоби)**.** *1. Если m — нечетное натуральное число, то* $\left(\frac{-1}{m}\right) = (-1)^{\frac{m-1}{2}}$.

2. Если m — нечетное натуральное число, то $\left(\frac{2}{m}\right) = (-1)^{\frac{m^2-1}{8}}$.

3. Если m и n — нечетные взаимно простые натуральные числа, то $\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{(m-1)(n-1)}{4}}$.

Доказательство. Оказывается, что все три пункта этой теоремы доказываются с помощью фактически одного вспомогательного утверждения. Сформулируем его отдельно.

> *если r и s — нечетные натуральные числа, то справедливы следующие сравнения:*
> $\frac{rs-1}{2} \equiv_2 \frac{r-1}{2} + \frac{s-1}{2}$ *и* $\frac{r^2s^2-1}{8} \equiv_2 \frac{r^2-1}{8} + \frac{s^2-1}{8}$.

Давайте поймем, в чем смысл этого утверждения, доказав с его помощью нашу теорему. Начнем с п.1. Разложим число m на простые множители: $m = p_1 \dots p_t$. Используя теорему о корне из -1 и наше утверждение, запишем следующий цепочку равенств:

$$\left(\frac{-1}{m}\right) = \left(\frac{-1}{p_1}\right) \dots \left(\frac{-1}{p_t}\right) = (-1)^{\frac{p_1-1}{2}+\dots+\frac{p_t-1}{2}} =^{!} (-1)^{\frac{p_1\dots p_t-1}{2}} = (-1)^{\frac{m-1}{2}}.$$

В переходе «$=^{!}$» мы как раз и использовали наше утверждение: сумма $\frac{p_1-1}{2} + \frac{p_2-1}{2}$ и число $\frac{p_1p_2-1}{2}$ имеют одинаковую четность, так что мы можем заменить сумму $\frac{p_1-1}{2} + \dots + \frac{p_t-1}{2}$ на число $\frac{p_1\dots p_t-1}{2}$, не поменяв при этом четность.

На этой идее основаны и доказательства оставшихся пунктов. П.2 доказывается аналогично п.1, а п.3 требует одного небольшого соображения, Пусть $m = p_1 \dots p_t$ и $n = q_1 \dots q_s$ — разложения на простые сомножители. Тогда

$$\begin{aligned}
\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) &= \left[\left(\frac{m}{q_1}\right) \dots \left(\frac{m}{q_s}\right)\right] \cdot \left[\left(\frac{n}{p_1}\right) \dots \left(\frac{n}{p_t}\right)\right] = \\
&= \left[\left\{\left(\frac{p_1}{q_1}\right) \dots \left(\frac{p_t}{q_1}\right)\right\} \dots \left\{\left(\frac{p_1}{q_s}\right) \dots \left(\frac{p_t}{q_s}\right)\right\}\right] \cdot \left[\left\{\left(\frac{q_1}{p_1}\right) \dots \left(\frac{q_s}{p_1}\right)\right\} \dots \left\{\left(\frac{q_1}{p_t}\right) \dots \left(\frac{q_s}{p_t}\right)\right\}\right] = \\
&= \left[\left(\frac{p_1}{q_1}\right)\left(\frac{q_1}{p_1}\right)\right] \cdot \left[\left(\frac{p_2}{q_1}\right)\left(\frac{q_1}{p_2}\right)\right] \cdot \left[\left(\frac{p_1}{q_2}\right)\left(\frac{q_2}{p_1}\right)\right] \cdot \dots \cdot \left[\left(\frac{p_t}{q_s}\right)\left(\frac{q_s}{p_t}\right)\right] = \\
&= \left[(-1)^{\frac{p_1-1}{2}\cdot\frac{q_1-1}{2}}\right] \cdot \left[(-1)^{\frac{p_2-1}{2}\cdot\frac{q_1-1}{2}}\right] \cdot \left[(-1)^{\frac{p_1-1}{2}\cdot\frac{q_2-1}{2}}\right] \cdot \dots \cdot \left[(-1)^{\frac{p_t-1}{2}\cdot\frac{q_s-1}{2}}\right] = \\
&= (-1)^{\frac{p_1-1}{2}\cdot\frac{q_1-1}{2}+\frac{p_1-1}{2}\cdot\frac{q_2-1}{2}+\frac{p_2-1}{2}\cdot\frac{q_1-1}{2}+\dots+\frac{p_t-1}{2}\cdot\frac{q_s-1}{2}}.
\end{aligned}$$

Преобразуем степень в последнем выражении. Для этого сгруппируем все слагаемые, которые содержат множитель $\frac{q_1-1}{2}$, и вынесем этот множитель за скобку. Получаем, что

$$\begin{aligned}
\frac{p_1-1}{2}\cdot\frac{q_1-1}{2} + \frac{p_2-1}{2}\cdot\frac{q_1-1}{2} + \dots + \frac{p_t-1}{2}\cdot\frac{q_1-1}{2} &= \left(\frac{p_1-1}{2} + \frac{p_2-1}{2} + \dots + \frac{p_t-1}{2}\right)\cdot\frac{q_1-1}{2} \equiv_2 \\
&\equiv_2 \frac{p_1p_2\dots p_t-1}{2}\cdot\frac{q_1-1}{2} = \frac{m-1}{2}\cdot\frac{q_1-1}{2}.
\end{aligned}$$

Здесь мы вновь использовали наше утверждение о группировке дробей $\frac{p_1-1}{2}, \ldots, \frac{p_t-1}{2}$.

Аналогично, преобразуем оставшиеся слагаемые, группируя и вынося множители $\frac{q_2-1}{2}, \ldots, \frac{q_s-1}{2}$. В итоге мы получим следующее выражение:

$$\frac{m-1}{2} \cdot \frac{q_1-1}{2} + \frac{m-1}{2} \cdot \frac{q_2-1}{2} + \ldots + \frac{m-1}{2} \cdot \frac{q_s-1}{2}.$$

Остается теперь вынести множитель $\frac{m-1}{2}$ и сгруппировать слагаемые $\frac{q_1-1}{2}, \ldots, \frac{q_s-1}{2}$ в выражение $\frac{q_1 q_2 \ldots q_s - 1}{2} = \frac{n-1}{2}$. Таким образом, окончательно получаем, что

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{p_1-1}{2}\cdot\frac{q_1-1}{2}+\frac{p_1-1}{2}\cdot\frac{q_2-1}{2}+\frac{p_2-1}{2}\cdot\frac{q_1-1}{2}+\ldots+\frac{p_t-1}{2}\cdot\frac{q_s-1}{2}} = (-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}},$$

что и требовалось.

Таким образом, нам остается проверить справедливость нашего утверждения о группировке дробей. Оно совсем легко получается из полезного алгебраического тождества $(r-1)(s-1) = rs-r-s+1$. Ясно, что $(r-1)(s-1) \equiv_4 0$, откуда $rs-1 \equiv_4 (r-1)+(s-1)$. Остается разделить эта сравнение на 2, не забыв при этом поделить на 2 и модуль 4. Так доказывается первая формула. Вторая следует из равенства $(r^2-1)(s^2-1) = r^2s^2 - r^2 - s^2 + 1$ и сравнения этого равенства по модулю 16.

Таким образом, квадратичный закон взаимности для символов Якоби полностью доказан. □

Возможно, приведенное выше доказательство квадратичного закона взаимности для символов Якоби оставило легкое неудовлетворение. Действительно, в отличие от доказательств в случае символов Лежандра, где было явно показано, каков геометрические смысл КЗВ, для символов Якоби итоговый результат (весьма красивый и кратко записанный) получается путем применения кучи арифметических преобразований, что никак не вскрывает истинную причину существования КЗВ.

Безусловно, существуют рассуждения, которые лишены этого недостатка. Однако, увы, ничто не дается просто так: доказательства, проясняющие суть для символов Якоби, зачастую используют весьма трудную технику, которая выходит за рамки этой книги (впрочем, искушенному читателю можно посоветовать обратиться к книге [1]). Тем не менее, в следующем разделе мы покажем еще один подход к доказательству квадратичных законов взаимности для символов Лежандра. Этот подход носит комбинаторный характер и существенно опирается на факты, связанные с *перестановками*. Мы не будем давать подробного описания необходимых теоретических фактов, связанных с перестановками, посоветовав читателю обратиться, например, к книге [3], а сосредоточимся на применении этих фактов для наших теоретико-числовых нужд. Кажется, что эти комбинаторные рассуждения можно обобщить на символы Якоби. Однако, к сожалению, авторам неизвестно такое обобщение. Возможно, его удастся придумать читателям...

Ну а сейчас давайте попробуем научиться применять КЗВ для символов Якоби. В качестве примера докажем следующую весьма непростую теорему.

Теорема 7. *Пусть a — произвольное целое число, не являющееся точным квадратом. Тогда существует бесконечно много простых чисел p, по модулю которых число a — квадратичный невычет.*

Доказательство. Ясно, что можно считать число a свободным от квадратов (т.е. считать, что любое простое число входит в разложение a в степени либо 0, либо 1). Отдельно разберем случай $a = 2$. Наша цель — сначала построить такое, возможно, нечетное составное число m, для которого $\left(\frac{2}{m}\right) = -1$, и тогда, как мы помним, в разложении m на простые сомножители найдется такое простое число p, для которого $\left(\frac{2}{p}\right) = -1$.

Пусть $q_1, \ldots, q_s$ — простые числа, отличные от 3, для которых 2 — невычет. Рассмотрим число $m = 8q_1 \ldots q_s + 3$. Ясно, что число m не делится ни на 3, ни на одно из чисел $q_1, \ldots, q_s$, и кроме того по квадратичному закону взаимности Якоби $\left(\frac{2}{m}\right) = -1$. Значит, в разложении числа m на простые множители найдется такое простое число q_{s+1}, для которого 2 — тоже невычет. Таким образом, мы нашли новое простое число, для которого 2 — невычет. Повторяя этот процесс, получаем бесконечную серию простых.

Рассмотрим теперь случай, когда $a = 2^\varepsilon p_1 \ldots p_t$, где $\varepsilon = 0$ или 1, а $p_1, \ldots, p_t$ — различные простые числа, причем $t \geq 1$. Мы поступим аналогично предыдущему случаю, построим, вообще говоря, составное число m, для которого число a — невычет, а затем выберем в нем подходящий простой множитель. Правда, сделать это будет несколько труднее из-за более сложного вида числа a.

Пусть мы уже построили какой-то набор простых чисел $q_1, \ldots, q_s$, для которых число a — невычет (в начальный момент времени этот набор может быть пустым). Пусть также b — некоторый невычет по простому модулю p_t. Рассмотрим систему сравнений

$$x \equiv_{q_1} 1, \ \ldots, \ x \equiv_{q_s} 1, \quad x \equiv_8 1, \quad x \equiv_{p_1} 1, \ \ldots, \ x \equiv_{p_{t-1}} 1, \quad x \equiv_{p_t} b.$$

Обозначим через m решение этого сравнения (оно существует по китайской теореме об остатках). Т.к. $m \equiv_8 1$, то $\left(\frac{2}{m}\right) = 1$ и $\left(\frac{n}{m}\right) = \left(\frac{m}{n}\right)$ для любого нечетного натурального числа n, взаимно простого с m. Значит,

$$\left(\frac{a}{m}\right) = \left(\frac{2}{m}\right)^\varepsilon \left(\frac{p_1}{m}\right) \ldots \left(\frac{p_{t-1}}{m}\right)\left(\frac{p_t}{m}\right) = \left(\frac{m}{p_1}\right) \ldots \left(\frac{m}{p_{t-1}}\right)\left(\frac{m}{p_t}\right) = \left(\frac{1}{p_1}\right) \ldots \left(\frac{1}{p_{t-1}}\right)\left(\frac{b}{p_t}\right) = -1.$$

Поэтому в числе m найдется простой множитель q_{s+1}, для которого a — невычет. Ясно, что m не делится ни на 3, ни на $q_1, \ldots, q_s$, а потому число q_{s+1} — новое простое число, для которого a — невычет. Продолжая эту процедуру, мы вновь получим бесконечную серию простых, что и требовалось доказать. □

На практике квадратичный закон взаимности Якоби обычно используется для чисел -1 и 2. Более общих применений этого закона в рамках школьных задач обычно не возникает.

Задача 6.1. Докажите, что число $4xyz - x - y$ не может быть точным квадратом при натуральных x, y, z.

Задача 6.2. Докажите, что уравнение $x^2 = y^3 - 5$ не имеет решений в целых числах.

Задача 6.3. Докажите, что число $4kxy - 1$ не может делить число $x^m + y^n$ для всех натуральных x, y, k, m, n.

7. Комбинаторное доказательство КЗВ

В этом разделе мы рассмотрим еще одно (уже седьмое!) доказательство квадратичного закона взаимности для символов Лежандра. Его основу составляет толкование символа Лежандра

в терминах некоторой перестановки. Мы не будем подробно останавливаться на теоретических вопросах, связанных с перестановками (необходимые факты можно найти, например, в [3]), считая, что читатель знаком с понятием перестановки, разложением на циклы и знаком перестановки.

Зафиксируем нечетное простое число p и целое число a, не кратное p. Чтобы понять, каким образом в задачах, связанных с остатками по модулю p, могут возникнуть перестановки, рассмотрим следующее комбинаторное доказательство малой теоремы Ферма.

Комбинаторное доказательство малой теоремы Ферма. Рассмотрим множество остатков $\mathbb{Z}_p$ и отображение $\sigma_{a,p}\colon \mathbb{Z}_p \to \mathbb{Z}_p$, $\sigma_{a,p}(x) = ax \pmod p$. Это не что иное, как уже знакомое нам умножение всех остатков на фиксированное число a. Как мы помним, в результате такого умножения все остатки остаются различными, но меняют свое положение. В результате возникает *перестановка* на множестве ненулевых остатков. Именно эта перестановка будет нам важно при доказательстве и малой теоремы Ферма, и квадратичного закона взаимности.

Разложим перестановку $\sigma_{a,p}$ на циклы. Ясно, что остаток 0 перейдет сам в себя, так что мы получим вырожденный цикл длины 1. Теперь рассмотрим цикл, начинающийся с остатка 1:

$$1 \to a \to a^2 \to a^3 \to \ldots \to a^{T-1} \to a^T \equiv_p 1.$$

Т.е. если T длина этого цикла, то $a^T \equiv_p 1$ и T — это порядок числа a по модулю p.

Поймем, как устроены другие циклы. Возьмем произвольный остаток x_1, которого не было в первом цикле, и начнем сдвигать его перестановкой $\sigma_{a,p}$. Ясно, что цикл, который мы получим, возникает из первого цикла умножением всех его элементов на x_1:

$$x_1 \to x_1 a \to x_1 a^2 \to x_1 a^3 \to \ldots \to x_1 a^{T-1} \to x_1 a^T \equiv_p x_1.$$

Таким образом, все циклы перестановки $\sigma_{a,p}$ имеют фиксированную длину T, равную порядку числа a по модулю p.

Теперь доказательство малой теоремы Ферма уже совсем несложно. Перестановка $\sigma_{a,p}$ переставляет $p-1$ ненулевой элемент и при этом разбивается на циклы одинаковой длины T (мы не рассматриваем здесь остаток 0). Это означает, что число $p-1$ делится на T. Но тогда если $a^T \equiv_p 1$, то и $a^{p-1} \equiv_p 1$, что и требовалось доказать. □

Итак, перестановка $\sigma_{a,p}$ несет в себе существенную информацию о взаимодействии числа a и поля остатков $\mathbb{Z}_p$. Так, структура циклов этой перестановки фактически привела нас к доказательству малой теоремы Ферма. Какие еще характеристики перестановки $\sigma_{a,p}$ можно исследовать? Для нас основную роль будет играть *знак* перестановки $\sigma_{a,p}$, который мы обозначим через $\operatorname{sgn}(\sigma_{a,p})$. Напомним, что *знаком перестановки* называется (-1) в степени, равной количеству *инверсий* перестановки. В свою очередь инверсия — это беспорядок, формируемый перестановкой: если пара элементов $i < j$ переходит в пару элементов $\sigma_{a,p}(i) > \sigma_{a,p}(j)$, то говорят, что пара (i, j) образует инверсию. Четность количества таких инверсий и определяет знак перестановки.

А именно, справедлива следующая теорема. Эта теорема (видимо, как и следующее из нее доказательство квадратичного закона взаимности) была получена Золотаревым.

Теорема 8 (Золотарев)**.** *Для нечетного простого числа p и целого числа a, не кратного p, имеет место равенство* $\left(\dfrac{a}{p}\right) = \operatorname{sgn}(\sigma_{a,p})$.

Доказательство. Есть много разных доказательств теоремы Золотарева, но мы дадим доказательство, которое использует лишь определение знака перестановки в терминах инверсий. Для

этого рассмотрим следующее выражение:

$$A := \prod_{i<j} \frac{\sigma_{a,p}(i) - \sigma_{a,p}(j)}{i-j} = \prod_{i<j} \frac{ai - aj}{i-j}.$$

(Здесь знак $\prod\limits_{i<j}$ обозначает взятие произведения соответствующих дробей, которые получаются, когда числа i и j пробегают все возможные значения от 0 до $p-1$, причем i всегда выбирается меньшим, чем j.) С одной стороны, если рассмотреть каждую дробь $\dfrac{ai-aj}{i-j}$, она равна a, а количество сомножителей равно $C_p^2 = \dfrac{p(p-1)}{2}$, так что $A = a^{\frac{p(p-1)}{2}} \equiv_p a^{\frac{p-1}{2}} \equiv_p \left(\dfrac{a}{p}\right)$. С другой стороны, в числителе и знаменателе выражения A возникают одни и те же разности остатков (поскольку умножение на a переставляет остатки), но некоторые разности возникают с другим знаком. Например, если $p = 5$ и $a = 2$, выражение A имеет следующий вид:

$$A = \frac{(0-2)(0-4)(0-1)(0-3)(2-4)(2-1)(2-3)(4-1)(4-3)(1-3)}{(0-1)(0-2)(0-3)(0-4)(1-2)(1-3)(1-4)(2-3)(2-4)(3-4)}.$$

Ясно, что количество скобок с «неправильным» знаком — это в точности количество инверсий перестановки $\sigma_{a,p}$. А поскольку скобки в числителе и знаменателе совпадают по модулю, выражение A в точности равно знаку $\operatorname{sgn}(\sigma_{a,p})$ перестановки $\sigma_{a,p}$, что и требовалось доказать. □

Ясно, что теперь квадратичный закон взаимности $\left(\dfrac{p}{q}\right)\left(\dfrac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$ можно переписать следующим образом:

$$\operatorname{sgn}(\sigma_{p,q})\operatorname{sgn}(\sigma_{q,p}) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

Именно это равенство мы и будем доказывать. Прежде чем переходить к доказательству, нам потребуется так называемая *китайская теорема об остатках* (КТО), сформулированная в несколько необычном виде. В стандартной формулировке, примененной для случая двух различных простых модулей p и q, она выглядит так:

> *система сравнений* $x \equiv_p u$, $x \equiv_q v$ *имеет единственное решение на отрезке* $[0, uv-1]$.

Сейчас мы дадим эквивалентную формулировку этой теореме. Однако осознать эту эквивалентность может быть не так просто.

Теорема 9 (Китайская теорема об остатках)**.** *Кольцо остатков* $\mathbb{Z}_{pq}$ *является прямой суммой колец остатков* $\mathbb{Z}_p$ *и* $\mathbb{Z}_q$*:* $\mathbb{Z}_{pq} = \mathbb{Z}_p \oplus \mathbb{Z}_q$.

Поясним, что скрывается за формулировкой этой теоремы. Начнем со следующего замечания. Классическая формулировка КТО по сути означает, что *пара остатков* (u, v) по модулям p и q однозначно задает *остаток* x по модулю pq. Иначе говоря, существует *биекция* (взаимнооднозначное соответствие) между множеством пар остатков, которое обозначается через $\mathbb{Z}_p \times \mathbb{Z}_q$, и множеством остатков $\mathbb{Z}_{pq}$. Действительно, если взять пару остатков (u, v), то им соответствует единственный остаток x, и наоборот, если взять произвольный остаток $x \in \mathbb{Z}_{pq}$, то ему соответствуют остатки $u \equiv_p x$ и $v \equiv_q x$. Таким образом, мы поняли, что китайская теорема об остатках на самом деле позволяет сделать следующее: она позволяет заменить рассмотрение пар остатков по простым (даже по взаимно простым) модулям p и q на рассмотрение остатков по одному модулю, равному произведению pq.

Осталось пояснить слова «прямая сумма». Они означают, что соответствие между парами остатков из $\mathbb{Z}_p \times \mathbb{Z}_q$ и $\mathbb{Z}_{pq}$ *согласовано с операциями сложения и вычитания остатков*: если паре (u_1, v_1) соответствует остаток x_1, а паре (u_2, v_2) — остаток x_2, то паре $(u_1 + u_2, v_1 + v_2)$ соответствует остаток $x_1 + x_2$ (аналогично, паре $(u_1 - u_2, v_1 - v_2)$ соответствует остаток $x_1 - x_2$). Это очевидно следует из свойств сравнений, но на математическом языке записывается красиво и витиевато: $\mathbb{Z}_p \oplus \mathbb{Z}_q = \mathbb{Z}_{pq}$.

Итак, мы поняли, что китайская теорема об остатках позволяет установить соответствие между парами остатков из $\mathbb{Z}_p \times \mathbb{Z}_q$ и остатками из $\mathbb{Z}_{pq}$, и это соответствие согласовано с операциями сложения и вычитания остатков.

Геометрически равенство $\mathbb{Z}_p \oplus \mathbb{Z}_q = \mathbb{Z}_{pq}$ можно увидеть следующим образом: мы берем прямоугольную таблицу $p \times q$ и записываем в ячейках остатки по модулю pq. При этом каждая строка должна содержать все остатки по модулю p, а каждый столбец должен содержать все остатки по модулю q. Проще всего заполнить таблицу, двигаясь или по строкам (снизу вверх), или по столбцам (слева направо). Соответствующие приверы для случая $p = 7$ и $q = 5$ приведены ниже.

28	29	30	31	32	33	34
21	22	23	24	25	26	27
14	15	16	17	18	19	20
7	8	9	10	11	12	13
0	1	2	3	4	5	6

4	9	14	19	24	29	34
3	8	13	18	23	28	33
2	7	12	17	22	27	32
1	6	11	16	21	26	31
0	5	10	15	20	25	30

Теперь мы готовы переходить к комбинаторному доказательству квадратичного закона взаимности.

Доказательство 7. Чтобы доказать равенство $\operatorname{sgn}(\sigma_{p,q}) \operatorname{sgn}(\sigma_{q,p}) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$, мы зададим три перестановки на множестве $\mathbb{Z}_{pq}$. Для этого положим

$$\mu(a, b) = (a, a + pb), \quad \nu(a, b) = (qa + b, b), \quad \pi\colon (a, a + pb) \mapsto (qa + b, b).$$

Поясним смысл перестановок μ, ν и π. Перестановка μ действует по столбцам, переставляя элементы каждого столбца внутри себя и не меняя элементы из разных столбцов. Аналогично, перестановка ν действует по строкам, переставляя элементы строки внутри себя и не меняя элементы разных строк. Поскольку каждый столбец — это экземпляр множества $\mathbb{Z}_q$, а каждая строка — экземпляр множества $\mathbb{Z}_p$, можно сказать, что перестановки μ и ν заданы на множествах $\mathbb{Z}_q$ и $\mathbb{Z}_p$ соответственно.

Что же касается перестановки π, то можно сказать, что перестановка π получается из перестановок μ и ν следующим образом: $\pi = \nu \circ \mu^{-1}$. С точки зрения элементов это так:

$$(a, a + pb) \xrightarrow{\mu^{-1}} (a, b) \xrightarrow{\nu} (qa + b, b).$$

Иначе говоря, перестановка π переводит левую таблицу из приведенного выше примера в правую.

Сейчас мы вычислим знаки этих трех перестановок. Учитывая свойство мультипликативности знака, $\operatorname{sgn}(\mu) \operatorname{sgn}(\nu) = \operatorname{sgn}(\pi)$. Когда мы подставим сюда явные формулы для знаков, это равенство превратится в формулу $\operatorname{sgn}(\sigma_{p,q}) \operatorname{sgn}(\sigma_{q,p}) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$.

Начнем с перестановки ν. Как мы поняли, эта перестановка действует на каждой отдельной строке, т.е. на множестве $\mathbb{Z}_p$. Поскольку общее количество строк нечетно, то знак перестановки ν, определенной на всем множестве $\mathbb{Z}_{pq}$, равен знаку перестановки ν на множестве $\mathbb{Z}_p$. По сути мы спроектировали картинку на горизонтальную ось и теперь можем использовать лишь одну

координату «по оси абсцисс». В таким случае мы получаем следующую перестановку множества $\mathbb{Z}_p$ (для удобства будем обозначать ее также через ν): $\nu(a) = qa + b \pmod p$.

Как вычислить знак такой перестановки? Заметим, что перестановка ν получается из уже известной нам перестановки $\sigma_{q,p}$ путем прибавления фиксированного остатка b. Поймем, что такое прибавление не изменит знака перестановки $\sigma_{q,p}$. Для этого рассмотрим вспомогательную перестановку $\tau\colon a \mapsto a+1$. Т.к. перестановка τ определена на множестве $\mathbb{Z}_p$, состоящем из нечетного числа элементов, $\operatorname{sgn}(\tau) = 1$: инверсии образуют лишь пары $(0,1)$, $(0,2)$, $\ldots$, $(0,p-1)$. С другой стороны, перестановка ν получается из перестановки $\sigma_{q,p}$ путем b-кратного применения перестановки τ. Тогда

$$\operatorname{sgn}(\nu) = \operatorname{sgn}(\sigma_{q,p}) \operatorname{sgn}(\tau)^b = \operatorname{sgn}(\sigma_{q,p}).$$

Абсолютно аналогично доказывается, что $\operatorname{sgn}(\mu) = \operatorname{sgn}(\sigma_{p,q})$.

Теперь наступает самый главый момент: вычисление знака перестановки π. Вычислим этот знак, явно описав инверсии этой перестановки. Для этого рассмотрим два элемента $x_1 < x_2$ в левой таблице, изображающей множество $\mathbb{Z}_{pq}$, которые переходят в элементы $y_1 > y_2$ в правой таблице, также изображающей множество $\mathbb{Z}_{pq}$. Тогда $x_1 = a_1 + b_1 p$, $x_2 = a_2 + b_2 p$, $y_1 = qa_1 + b_1$, $y_2 = qa_2 + b_2$. Ясно, что $x_1 < x_2$, если и только если $b_1 < b_2$ или $b_1 = b_2$ и $a_1 < a_2$. С другой стороны, $y_1 > y_2$, если и только если $a_1 > a_2$ или $a_1 = a_2$ и $b_1 > b_2$. Сравнивая эти условия, заключаем, что неравенства $x_1 < x_2$, $y_1 > y_2$ равносильны неравенствам $a_1 > a_2$ и $b_1 < b_2$. Геометрически это можно увидеть следующим образом. Рассмотрим прямоугольник, образованный пересечениями строк и столбцов, в которых стоят элементы x_1 и x_2. Тогда эти элементы образуют инверсию тогда и только тогда, когда их расположение такое: $\begin{smallmatrix} x_2 & * \\ * & x_1 \end{smallmatrix}$.

Отсюда легко посчитать количество пар элементов, образующих инверсию. Для этого заметим, что так расположенные элементы задают пару столбцов и пару строк в таблице $\mathbb{Z}_{pq}$. Пара столбцов может быть выбрана C_p^2 вариантами, а пара строк — C_q^2 вариантами. Таким образом, окончательно получаем:

$$\operatorname{sgn}(\pi) = (-1)^{C_p^2 C_q^2} = (-1)^{\frac{p(p-1)}{2} \cdot \frac{q(q-1)}{2}} = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$$

(в последнем переходе мы использовали нечетность чисел p и q).

Остается подставить найденные нами знаки перестановок ν, μ и π в формулу $\operatorname{sgn}(\mu)\operatorname{sgn}(\nu) = \operatorname{sgn}(\pi)$. В итоге мы получаем равенство $\operatorname{sgn}(\sigma_{p,q})\operatorname{sgn}(\sigma_{q,p}) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$. Вспоминая, что $\operatorname{sgn}(\sigma_{p,q}) = \left(\frac{p}{q}\right)$ и $\operatorname{sgn}(\sigma_{q,p}) = \left(\frac{q}{p}\right)$, мы окончательно получаем квадратичный закон взаимности:

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

Наше доказательство, а вместе с ним и повествование о квадратичных вычетах, закончено. □

8. Решения задач

Задача 3.3. (a) Докажите, что если простое число p является делителем числа $x^2 - 6x + 3$, где x — целое, то оно также является делителем числа $y^2 - 2y - 53$ для некоторого целого y.

(b) Докажите, что если простое число p является делителем числа $x^2 - x + 3$, где x — целое, то оно также является делителем числа $y^2 - y + 25$ для некоторого целого y.

Решение. (a) Выделим полные квадраты в указанных трехчленах: $(x-3)^2 \equiv_p 6$ и $(y-1)^2 \equiv_p 54$. Чтобы найти требуемый y, умножим первое сравнение на 9 (это число является вычетом по

любому простому модулю). Тогда $(3x-9)^2 \equiv_p 54$. Значит, полагая $y-1 = 3x-9$, или $y = 3x-8$, мы получаем требуемое.

(b) В этом пункте, чтобы выделить полный квадрат, полезно домножить каждое из сравнений на 4:

$$4x^2 - 4x + 12 \equiv_p 0, \quad 4y^2 - 4y + 100 \equiv_p 0 \quad \Longrightarrow \quad (2x-1)^2 \equiv_p -11, \quad (2y-1)^2 \equiv_p -99.$$

Вновь домножим первое сравнение на 9: $(6x-3)^2 \equiv_p -99$. Тогда, полагая $2y-1 = 6x-3$, или $y = 3x-1$, мы получаем требуемое.

Задача 3.4. Числа a^2+5a+1 и $2a^2-a+2$ не делятся на простое число p ни при каких целых a. Докажите, что для некоторого натурального n число $n^2+3n+11$ делится на p.

Решение. Вновь выделим в трехчленах полные квадраты, домножив первый и третий на 4, а второй на 8:

$$4a^2 + 20a + 4 \not\equiv_p 0, \quad 16a^2 - 8a + 16 \not\equiv_p 0 \quad \Longrightarrow \quad (2a+5)^2 \not\equiv_p 21, \quad (4a-1)^2 \not\equiv_p -15$$

и $4n^2 + 12n + 44 \equiv_p 0 \Longrightarrow (2n+3)^2 \equiv_p -35$. Получаем, что

$$\left(\frac{21}{p}\right) = \left(\frac{-15}{p}\right) = -1 \quad \Longrightarrow \quad 1 = \left(\frac{21}{p}\right)\cdot\left(\frac{-15}{p}\right) = \left(\frac{-35\cdot 3^2}{p}\right) = \left(\frac{-35}{p}\right),$$

откуда следует, что -35 — квадратичный вычет по модулю p. Значит, существует такой остаток x, что $x^2 \equiv_p -35$. Полагая $n \equiv_p (x-3)/2$, получаем требуемое (деление на 2 законно, т.к. $p \neq 2$, иначе при $a = 0$ трехчлен $2a^2 - a + 2$ делится на 2).

Задача 3.5. Пусть a и b — целые числа и p — нечетное простое число, такое, что a не делится на p. Докажите, что $\sum\limits_{x=0}^{p-1}\left(\frac{ax+b}{p}\right) = 0$.

Решение. Заметим, что при $a \not\equiv_p 0$ множество остатков $\{ax+b\}$ образует полную систему вычетов по модулю p. Это означает, что в сумме $\sum\limits_{x=0}^{p-1}\left(\frac{ax+b}{p}\right)$ есть один нуль, и половина из оставшихся слагаемых равна 1, а вторая половина равна -1. Значит, сумма всех символов Лежандра равна 0.

Задача 3.6. Пусть p — нечетное простое число. Докажите, что наименьший квадратичный невычет по модулю p меньше $\sqrt{p}+1$.

Решение. Предположим противное: пусть все остатки от 1 до $\sqrt{p}+1$ являются вычетами. Докажем, что тогда все ненулевые остатки по модулю p также являются вычетами. В самом деле, если x — наименьший невычет, то $x \geq \sqrt{p}+1$. Рассмотрим всевозможные произведения чисел $1\cdot x$, $2\cdot x$, …, $(x-1)x$. Т.к. $(x-1)x > (x-1)^2 > (\sqrt{p})^2 = p$, то найдется такое произведение, которое будет больше p. Выберем наименьшее такое произведение. Оно будет лежать в промежутке от p до $p+x$ (поскольку расстояния между двумя соседними произведениями равно x). Значит, это произведение сравними с остатком из промежутка от 0 до x и потому является вычетом. Получается, что мы умножили некоторый вычет на невычет x и получили вычет — противоречие.

Задача 3.7. Докажите, что многочлен x^4+1 приводим над $\mathbb{Z}_p$ для любого простого p (т.е. он представим в виде произведения двух многочленов положительной степени с коэффициентами в $\mathbb{Z}_p$).

Решение. Пусть $\left(\frac{-1}{p}\right) = 1$. Тогда $x^4+1 \equiv_p x^4 - a^2 = (x^2-a)(x^2+a)$, где $a^2 \equiv_p -1$.

Пусть $\left(\frac{2}{p}\right) = 1$. Тогда $x^4+1 = (x^4+2x^2+1)-2x^2 \equiv_p (x^2+1)^2-(bx)^2 = (x^2-bx+1)(x^2+bx+1)$, где $b^2 \equiv_p 2$.

Если же $\left(\frac{-1}{p}\right) = \left(\frac{2}{p}\right) = -1$, то $\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\cdot\left(\frac{2}{p}\right) = 1$ и

$$x^4+1 = (x^4-2x^2+1)-(-2x^2) \equiv_p (x^2+1)^2-(cx)^2 = (x^2-cx+1)(x^2+cx+1),$$

где $c^2 \equiv_p -2$.

Задача 3.8. Пусть A — это множество ненулевых остатков $a \in \mathbb{Z}_p$, таких, что остатки a и $4-a$ являются невычетами по модулю p. Найдите остаток произведения всех элементов множества A по модулю p.

Решение. Рассмотрим вместе с множеством A множество B, состоящее из таких остатков $b \in \mathbb{Z}_p$, что b и $4-b$ являются вычетами. Докажем, что при $a \not\equiv_p 2$ отображение $(a, 4-a) \mapsto a(4-a)$ отображает множество $A \setminus \{2\}$ во множество B. В самом деле, пусть $b = a(4-a)$. Тогда b есть произведение двух невычетов и потому является вычетом, а также $4-b = 4-a(4-a) = (a-2)^2$ — вычет. Аналогично, при $b \not\equiv_p 2$ отображение $(b, 4-b) \mapsto b(4-b)$ отображает множество $B\setminus\{2\}$ во множество B.

Далее, докажем, что образы этих отображений не пересекаются, и их объединение есть все множество B. Действительно если $a(4-a) \equiv_p b(4-b)$ для некоторых $a \in A$ и $b \in B$, то $(a-b)(a+b-4) \equiv_p 0$, откуда $b \equiv_p a$ или $b \equiv_p 4-a$, что невозможно. С другой стороны, для каждого остатка $b \in B$ рассмотрим уравнение $x(4-x) \equiv_p b$. Перепишем его в виде $(x-2)^2 \equiv_p 4-b$. Т.к. $4-b \equiv_p c^2$ — вычет, то $x_{1,2} \equiv_p 2 \pm c$. Т.к. $x_1x_2 \equiv_p b$ и $x_1+x_2 \equiv_p 4$, то либо x_1 и $x_2 \equiv_p 4-x_1$ оба являются невычетами и потому лежат в A, либо оба являются вычетами и потому лежат в B.

Таким образом, произведение всех элементов множеств A и B, за исключением остатка 2, сравнимо по модулю p с произведением всех элементов множества B:

$$\prod_{a\in A\setminus\{2\}} a \cdot \prod_{b\in B\setminus\{2\}} b \equiv_p \prod_{b\in B} b.$$

Тогда если $2 \in A$, можно сократить наше сравнение на $\prod_{b\in B\setminus\{2\}} b \equiv_p \prod_{b\in B} b$ и домножить оставшееся сравнение на 2, откуда $\prod_{a\in A} a \equiv_p 2$. Если же $2 \in B$, то, сокращая наше сравнение на $\prod_{b\in B\setminus\{2\}} b$, сразу получаем, что $\prod_{a\in A} a \equiv_p 2$.

Ответ. $\prod_{a\in A} a \equiv_p 2$.

Задача 4.1. Пусть $p = 4k-1$ — простое число. Докажите, что если сравнение $x^2 \equiv_p a$ имеет решение, то $x \equiv_p \pm a^k$.

Решение. Если $a \equiv_p 0$, то утверждение задачи очевидно, в противном случае по критерию Эйлера получаем, что $1 = \left(\frac{a}{p}\right) \equiv_p a^{(p-1)/2} = a^{2k-1}$. Домножив на a левую и правую части этого сравнения, получаем, что $a^{2k} \equiv_p a$, т.е. $x \equiv_p \pm a^k$ удовлетворяет сравнению $x^2 \equiv_p a$, что и требовалось.

Задача 4.2. Существуют ли 18 последовательных натуральных чисел, которые можно разбить на две группы с одинаковыми произведениями?

Решение. Предположим, что такие числа нашлись. Заметим, что среди этих чисел не более одного делятся на 19. Если такое число есть, то произведение, содержащее это число, делится на 19, а оставшееся произведение — нет, что невозможно. Значит, среди наших чисел нет числа, кратного 19, и остатки этих чисел равны 1, 2, …, 18.

Если эти остатки удалось разбить на два равных произведения Π_1 и Π_2, то $\Pi_1 \equiv_{19} \Pi_2$. Домножим это сравнение на Π_1 и воспользуемся теоремой Вильсона: $\Pi_1^2 \equiv_{19} \Pi_1\Pi_2 \equiv_{19} 18! \equiv_{19} -1$. Получается, что -1 — вычет по модулю 19, что невозможно, т.к. $19 \equiv_4 -1$.

Задача 4.3. (a) Докажите, что простых чисел вида $4k+1$ бесконечно много. (*Указание*: рассмотрите многочлен $f(x) = x^2 + 1$.)

(b) Докажите, что существует бесконечно много натуральных чисел n, для которых число $n^2 + 1$ имеет не менее 2022 различных простых делителей.

Решение. (a) Рассмотрим многочлен $f(x) = x^2 + 1$. Заметим, что у чисел вида $f(n)$, где $n \in \mathbb{N}$, бесконечно много различных нечетных простых делителей. В самом деле, если $p_1, \ldots, p_m$ — все нечетные простые делители чисел вида $f(n)$, то число $f(2p_1 \ldots p_m)$ нечетно, не делится ни на одно из чисел $p_1, \ldots, p_m$ и больше 1, а потому у него должен быть нечетный простой делитель, отличный от $p_1, \ldots, p_m$. С другой стороны, каждый нечетный простой делитель числа вида $f(n)$ имеет вид $4k+1$. Отсюда следует требуемое.

(b) Рассмотрим простые числа $p_1, \ldots, p_{2022}$ вида $4k+1$, и для каждого из этих чисел найдем соответствующие числа $n_1, \ldots, n_{2022}$, для которых $f(n_i) \vdots p_i$. По китайской теореме об остатках найдется бесконечно много чисел n, что $n \equiv_{p_i} n_i$ для всех $i = 1, \ldots, 2022$. Эти числа и будут искомыми.

Задача 4.4. Докажите, что число $4mn - m - n$ не является точным квадратом ни при каких натуральных числах m и n.

Решение. Предположим, что $4mn - m - n = x^2$ для некоторого натурального x домножим это равенство на 4, прибавим к обеим частям 1 и разложим левую часть на множители, В итоге наше навенство примет вид $(4m-1)(4n-1) = (2x)^2 + 1$. Рассмотрим число $4m-1$ и выберем у него простой делитель $p \equiv_4 -1$. Тогда $(2x)^2 \equiv_p -1$, что невозможно — противоречие.

Задача 4.5. Докажите, что число $\dfrac{x^2+1}{y^2-5}$ никогда не является целым при натуральных $x, y > 2$.

Решение. Предположим противное. Если $y \equiv_2 1$, то $y^2 - 5 \equiv_4 0$, а $x^2 + 1 \equiv_4 2$, что невозможно. Значит, $y \equiv_2 0$ и $y^2 - 5 \equiv_4 -1$. Выберем у числа $y^2 - 5$ простой делитель $p \equiv_4 -1$ и получим, что $x^2 \equiv_p -1$, что невозможно — противоречие.

Задача 4.6. Докажите, что уравнение $x^2 = y^3 + 7$ не имеет решений в целых числах.

Решение. Прибавим к обеим частям уравнения 1 и разложим правую часть по формуле суммы кубов: $x^2 + 1 = (y+2)(y^2 - 2y + 4)$. Заметим, что левая часть имеет простые делители вида $4k+1$, поэтому оба множителя в правой части таке имеют вид $4k+1$. Но тогда $y \equiv_4 -1$ и $y^2 - 2y + 4 \equiv_4 3$ — противоречие. С другой стороны, левая и правая части не могут быть степенями двойки, выше первой, поскольку $x^2 + 1 \not\equiv_4 0$. Наконец, при $x = 1$ получаем, что $y^3 = 6$, что невозможно.

Задача 4.7. Пусть p — нечетное простое число. Сколько существует пар соседних друг с другом квадратичных вычетов? Иначе говоря, какова мощность множества

$$\{x^2 + 1 : x \in \mathbb{Z}_p\} \cap \{y^2 : y \in \mathbb{Z}_p\}?$$

Решение. Пусть $x^2 + 1 \equiv_p y^2$. Запишем это сравнение в виде $(y-x)(y+x) \equiv_p 1$. Пусть $t := y + x$. Тогда $y - x = t^{-1}$ и $y = \dfrac{1}{2}\big(t + t^{-1}\big)$, $x = \dfrac{1}{2}\big(t - t^{-1}\big)$. Далее, $y^2 = \dfrac{1}{4}\big(t^2 + t^{-2} + 2\big)$, и нас интересует, сколько различных зачений может принимать величина $t^2 + t^{-2}$, если t пробегает все ненулевые остатки по модулю p.

Посмотрим, при каких условиях две величины $t^2 + t^{-2}$ и $s^2 + s^{-2}$ совпадают по модулю p. Для этого домножим сравнение $t^2 + t^{-2} \equiv_p s^2 + s^{-2}$ на $(ts)^2$, перенесем все слагаемые в левую

часть и разложим получившееся выражение на множители. Мы получим следующее сравнение: $(t-s)(t+s)(ts-1)(ts+1) \equiv_p 0$. Таким образом, $t^2+t^{-2} \equiv_p s^2+s^{-2}$ тогда и только тогда, когда $s \equiv_p \pm t, \pm t^{-1}$.

Разобьем все ненулевые остатки по модулю p на четверки вида $(t, t^{-1}, -t, -t^{-1})$. Количество таких четверок и будет ответом в нашей задаче. Заметим, однако, что при некоторых t такая четверка вырождается в пару остатков. Это происходит в одном из следующих двух случаев: если $t \equiv_p t^{-1}$ или если $t \equiv_p -t^{-1}$. В первом случае получаем отдельную пару $t \equiv_p \pm 1$, а во втором — отдельную пару $t \equiv_p \pm a$, где $a^2 \equiv_p -1$. Но вторая пара может существовать, если и только если $p = 4k+1$.

Таким образом, в случае, когда $p = 4k+1$, получается $\dfrac{(p-1)-2-2}{4}+1+1 = k+1$ различных значений для величины t^2+t^{-2} (и, как следствие, столько же значений для величины y^2, такой, что $x^2+1 \equiv_p y^2$), а в случае, когда $p = 4k+3$, получается $\dfrac{(p-1)-2}{4}+1 = k+1$ различных значений для величины t^2+t^{-2}. Оба этих ответа можно кратко записать одним способом: $\left\lceil \dfrac{p}{4} \right\rceil$.

Ответ. $\left\lceil \dfrac{p}{4} \right\rceil$.

Задача 4.8. Даны нечетное простое число p и натуральное число d. Выразите через p и d количество пар решений сравнения $dx^2 + y^2 \equiv_p 1$.

Решение. Если d делится на p, то очевидно, что решений будет $2p$: это все пары вида $(x, \pm 1)$. Рассмотрим теперь случай, когда d не делится на p. В этом случае перепишем сравнение в виде $y^2 \equiv_p 1 - dx^2$ и запишем количество решений с помощью суммы символов Лежандра: $\sum\limits_{x=0}^{p-1} \left(1 + \left(\dfrac{1-dx^2}{p}\right)\right)$. Согласно теореме 4, эта сумма равна $p - \left(\dfrac{-d}{p}\right)$.

Ответ. Количество пар решений равно $2p$, если d делится на p, и равно $p - \left(\dfrac{-d}{p}\right)$, если d не делится на p.

Задача 4.9. Для нечетного простого числа p вычислите количество неупорядоченных пар квадратичных вычетов с суммой 1.

Решение. Для начала используем результат задачи **4.8.** Получаем, что количество пар решений сравнения $x^2 + y^2 \equiv_p 1$ равно $p - \left(\dfrac{-1}{p}\right) = p - (-1)^{\frac{p-1}{2}}$. Далее, заметим, что все решения этого сравнения, за исключением некоторых, бьются на группы $\{(\pm x, \pm y), (\pm y, \pm x)\}$ из восьми элементов. Исключениями являются следующие случаи:

- случай $(0, \pm 1)$;
- случай $(\pm 1, 0)$;
- случай $(\pm a, \pm a)$, где $a^2 \equiv_p 2$ (только если $\left(\dfrac{2}{p}\right) = 1$).

Таким образом, возникают два варианта.

Если $\left(\dfrac{2}{p}\right) = -1$, то получается $\dfrac{p-(-1)^{\frac{p-1}{2}}-2-2}{8}+1$ пара вычетов.

Если $\left(\dfrac{2}{p}\right) = 1$, то получается $\dfrac{p-(-1)^{\frac{p-1}{2}}-2-2-4}{8}+1+1$ пара вычетов.

Ответ. Если $\left(\frac{2}{p}\right) = -1$, то получается $\frac{p-(-1)^{\frac{p-1}{2}}-4}{8}+1$ пара вычетов. Если $\left(\frac{2}{p}\right) = 1$, то получается $\frac{p-(-1)^{\frac{p-1}{2}}}{8}+1$ пара вычетов.

Задача 4.10. Используя результат предыдущей задачи, вычислите символ Лежандра $\left(\frac{2}{p}\right)$. (В следующем разделе мы вычислим этот символ дрнугим способом.)

Решение. Дроби из ответа к задаче **4.9.** должны быть целыми. Посмотрим, при каких p будет целой дробь $\frac{p-(-1)^{\frac{p-1}{2}}}{8}$ (для таких p число 2 будет вычетом). Рассмотрим остатки числа p по модулю 8.

Если $p = 8k+1$, то дробь равна k — целое число.

Если $p = 8k+3$, то дробь равна $\frac{2k+1}{2}$ — нецелое число.

Если $p = 8k+5$, то дробь равна $\frac{2k+1}{2}$ — нецелое число.

Если $p = 8k+7$, то дробь равна $k+1$ — целое число.

Таким образом, нам подходят случаи $p = 8k+1$ и $p = 8k+7$. Кратко эти случаи удобно записать в виде $p \equiv_8 \pm 1$, а соответствующая формула для символа Лежандра выглядит так: $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

Ответ. $\left(\frac{2}{p}\right) = 1$ тогда и только тогда, когда $p \equiv_8 \pm 1$.

Задача 5.1. Считая, что гипотеза Эйлера справедлива, выведите из нее квадратичный закон взаимности.

Решение. Если $p = q$, то гипотеза Эйлера очевидна. Теперь рассмотрим два случая.

Случай 1: $p - q = 4a$ для некоторого натурального числа a. А таком случае имеем:

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

и

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

В силу гипотезы Эйлера $\left(\frac{a}{q}\right) = \left(\frac{a}{p}\right)$, откуда

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

т.е. $\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}}$. Остается заметить, что $(-1)^{\frac{p-1}{2}} = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$, т.к.

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

Случай 2: $p + q = 4a$ для некоторого натурального числа a. Вычисления в этом случае даже проще:

$$\left(\frac{p}{q}\right) = \left(\frac{4a-q}{q}\right) = \left(\frac{4a}{q}\right) = \left(\frac{a}{q}\right)$$

и

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

В силу гипотезы Эйлера $\left(\frac{a}{q}\right) = \left(\frac{a}{p}\right)$, откуда

$$\left(\frac{p}{q}\right) = \left(\frac{a}{q}\right) = \left(\frac{a}{p}\right) = \left(\frac{q}{p}\right),$$

т.е. $\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = 1$. Остается заметить, что $(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} = 1$, т.к. у одного из чисел p или q будет остаток 1 при делении на 4, и тогда соответствующая дробь является четным числом.

Задача 5.2. Используя квадратичный закон взаимности и свойство мультипликативности символа Лежандра, разберитесь, является ли 79 квадратичным вычетом по модулю 101.

Решение. Применим квадратичный закон взаимности и предложение 6:

$$\left(\frac{79}{101}\right) = \left(\frac{101}{79}\right)(-1)^{\frac{(79-1)(101-1)}{4}} = \left(\frac{101}{79}\right) = \left(\frac{2}{79}\right)\left(\frac{11}{79}\right) = (-1)^{\frac{79^2-1}{8}}\left(\frac{79}{11}\right)(-1)^{\frac{(79-1)(11-1)}{4}} =$$
$$= -\left(\frac{79}{11}\right) = -\left(\frac{2}{11}\right) = -(-1)^{\frac{11^2-1}{8}} = 1.$$

Значит, 79 — это вычет по модулю 101.

Ответ. Число 79 является квадратичным вычетом по модулю 101.

Задача 5.3. Докажите, что ни при каком натуральном n у числа 2^n+1 не может быть простых делителей вида $8k+7$.

Решение. Предположим противное: пусть $2^n \equiv_p -1$ для некоторого простого числа $p = 8k+7$. Если n четно, то -1 — вычет по модулю p, что невозможно, т.к. $p \equiv_4 -1$. Если же n нечетно, то -2 — вычет по модулю p, что опять же невозможно, т.к. -1 — невычет, а 2 — вычет.

Задача 5.4. (a) Докажите, что -3 — квадратичный вычет по модулю нечетного простого числа p тогда и только тогда, когда $p \equiv_6 1$.

(b) Докажите, что простых чисел вида $6k+1$ бесконечно много.

Решение. (a) Применим квадратичный закон взаимности:

$$1 = \left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}} \cdot (-1)^{\frac{(p-1)(3-1)}{4}} \cdot \left(\frac{p}{3}\right) = \left(\frac{p}{3}\right),$$

откуда $p \equiv_3 1$. Поскольку p нечетно, получаем, что $p \equiv_6 1$, что и требовалось.

(b) Рассмотрим многочлен $f(x) = 3x^2+1$. Заметим, что если p — нечетный простой делитель числа $f(n)$, то $(3n)^2 \equiv_p -3$, т.е. $p \equiv_6 1$ по п. (a). Значит, достаточно доказать, что количество нечетных простых делителей чисел вида $f(n)$ бесконечно. Предположим, что $p_1, \ldots, p_m$ — все нечетные простые делители чисел вида $f(n)$. Тогда число $f(2p_1 \ldots p_m)$ нечетно, не делится ни на одно из чисел $p_1, \ldots, p_m$ и больше 1, а потому у него должен быть нечетный простой делитель, отличный от $p_1, \ldots, p_m$. Полученное противоречие завершает решение.

Задача 5.5. Целые числа x и y таковы, что x^2+xy+y^2 делится на простое число p вида $3k+2$. Докажите, что сами числа x и y делятся на p.

Решение. Предположим, что x и y не делятся на p. Домножим сравнение $x^2+xy+y^2 \equiv_p 0$ на 4 и выделив полный квадрат, получаем, что $(2x+y)^2 \equiv_p -3y^2$, т.е. -3 — вычет по модулю p. С другой стороны, из задачи **5.4.** мы знаем, что -3 является вычетом по модулю p только в случае, когда $p \equiv_3 1$ — противоречие.

Задача 5.6. Докажите, что если число $p = 2^n + 1$ — простое и больше 3, то минимальная степень T такая, что $3^T \equiv_p 1$, равна $p - 1$.

Решение. Заметим, что по малой теореме Ферма $3^{p-1} \equiv_p 1$. Кроме того, $3^T \equiv_p 1$. Значит, число $p-1$ делится на T, ведь в противном случае $p-1 = Tq+r$, где $0 < r < T$, и $3^r = 3^{(p-1)-Tq} \equiv_p 1$, что противоречит минимальности числа T. Далее, заметим, что n должно быть четно, ведь в противном случае число 2^n+1 делится на $2+1=3$ и больше 3, а потому никак не может быть простым. Значит, $2^n \equiv_3 2$ и по критерию Эйлера имеем:

$$3^{\frac{p-1}{2}} \equiv_p \left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right) = \left(\frac{2}{3}\right) = -1.$$

Получается, что число T делит число $p-1 = 2^n$, но не делит число $\dfrac{p-1}{2} = 2^{n-1}$. Это возможно, только если $T = 2^n = p-1$, что и требовалось доказать.

Задача 5.7. Натуральные числа a и b таковы, что числа $15a + 16b$ и $16a - 15b$ являются точными квадратами. Каково наименьшее возможное значение меньшего из этих квадратов?

Решение. Пусть $15a + 16b = x^2$ и $16a - 15b = y^2$ для некоторых натуральных чисел x и y. Выразим из этих равенств величину b: $b = \dfrac{16x^2 - 15y^2}{13 \cdot 37}$.

Докажем, что число b натурально, если и только если числа x и y делятся на 13 и 37. Предположим противное: пусть, например, число x не делится на 13. Тогда и число y не делится на 13. Значит, если $16x^2 \equiv_{13} 15y^2 \equiv_{13} 2y^2$, то $2 \equiv_{13} (y/2x)^2$ — вычет. Но $\left(\dfrac{2}{13}\right) = -1$ по предложению 6, т.к. $13 \equiv_8 5$ — противоречие. Значит, числа x и y делятся на 13.

Аналогично, если число x не делится на 37, то и число y не делится на 37. Домножим сравнение $16x^2 \equiv_{37} 15y^2$ на 3. Получаем, что $48x^2 \equiv_{37} 45y^2 \equiv_{37} 8y^2$. Сокращая на $8x^2$, получаем, что $6 \equiv_{37} (y/x)^2$ — вычет. Но по КЗВ

$$\left(\frac{6}{37}\right) = \left(\frac{2}{37}\right)\left(\frac{3}{37}\right) = (-1)\left(\frac{37}{3}\right) = -1$$

— противоречие.

Итак, числа x, y делятся на $13 \cdot 37 = 481$. Значит, x, $y \geq 481$. При этом значения $x = y = 481$ достигаются для $a = 31 \cdot 481$ и $b = 481$.

Ответ. 481^2.

Задача 5.8. Найдите наименьший простой делитель числа $12^{2^{15}} + 1$.

Решение. Пусть p — наименьший простой делитель $12^{2^{15}} + 1$. Возводя в квадрат сравнение $12^{2^{15}} \equiv_p -1$, получаем, что $12^{2^{16}} \equiv_p 1$. Рассмотрим наименьшее натуральное число T, такое, что $2^T \equiv_p 1$ (число T еще называется *порядком числа 2 по модулю p*). Тогда, как мы доказывали в задаче **5.6.**, число $p-1$ делится на T. С другой стороны, 2^{16} тоже делится на T по тем же причинам. Тогда $T = 2^t$, Если $t \leq 15$, то $-1 \equiv_p 2^{2^{15}} \equiv_p 1$, что невозможно. Значит, $t = 16$, $T = 2^{16}$ и $p - 1 \geq T = 2^{16}$, т.е. $p \geq 2^{16} + 1 = 65537$. Число 65537 простое (это так называемое простое число Ферма). Докажем, что $p = 65537$ действительно делит число $2^{2^{15}}+1$. По критерию Эйлера и квадратичному закону взаимности имеем:

$$12^{2^{15}} \equiv_p \left(\frac{12}{p}\right) = \left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right) = -1,$$

что и требовалось.

Ответ. 65537.

Задача 5.9. Докажите, что дробь $\dfrac{a^2+b^2+c^2}{3(ab+bc+ca)}$ не является натуральным числом ни при каких натуральных a, b, c.

Решение. Предположим противное: пусть $\dfrac{a^2+b^2+c^2}{3(ab+bc+ca)} = n$. Без ограничения общности можно считать, что числа a, b и c взаимно просты в совокупности. Домножив на знаменатель и выделяя полный квадрат, перепишем это равенство в виде $(a+b+c)^2 = (3n+2)(ab+bc+ca)$. Заметим, что число $3n+2$ не является точным квадратом и дает остаток -1 по модулю 3. Значит, существует простое число $p \equiv_3 -1$, входящее в разложение числа $3n+2$ на простые в нечетной степени. Ясно, что тогда $a+b+c$ и $ab+bc+ca$ делятся на p. Отсюда следует, что $c \equiv_p -a-b$ и $ab+bc+ca \equiv_p -(a^2+ab+b^2) \equiv_p 0$. Согласно задаче **5.5.** отсюда следует, что числа a и b (а значит, и c) сами делятся на p — противоречие с взаимной простотой чисел a, b и c.

Задача 5.10. Найти все целые числа x и y, для которых число $\dfrac{x^2+x+2}{y^6-2}$ целое.

Решение. Ясно, что при $y = \pm 1$, 0 число x может быть любым. Во всех остальных случаях $y^6-2 > 0$. Заметим, что по малой теореме Ферма $y^6-2 \equiv_7 -1$ или -2, причем оба этих остатка являются невычетами по модулю 7. Значит, найдется простой делитель p числа y^6-2, который также является невычетом по модулю 7 (в частности, $p \neq 2$).

Докажем, что число x^2+x+2 не может делиться на p. В самом деле, в противном случае выполнено сравнение $(2x+1)^2 \equiv_p -7$, т.е. $\left(\dfrac{-7}{p}\right) = 1$. С другой стороны, по квадратичному закону взаимности имеем

$$\left(\frac{-7}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{7}{p}\right) = (-1)^{(p-1)/2} \cdot \left(\frac{p}{7}\right) \cdot (-1)^{(p-1)(7-1)/4} = \left(\frac{p}{7}\right) = -1.$$

Получаем противоречие.

Задача 5.11. Дано натуральное число $n > 1$. Докажите, что любой нечётный делитель $d > 10$ числа $5n^2+1$ имеет в своей десятичной записи чётную цифру.

Решение. Докажем, что вторая цифра числа d будет четной. Для этого достаточно доказать, что $d \equiv_{20} 1, 3, 5, 7, 9$. Заметим, что случай $d \equiv_{20} 5$ невозможен, т.е. нужно проверить, что остатки делителя d по модулю 20 могут быть равны лишь 1, 3, 7 или 9. Далее, заметим, что если числа d_1 и d_2 имеют такие остатки, то остаток произведения $d_1 d_2$ также будет равен 1, 3, 7 или 9: это следует из таблицы уможения по модулю 20:

$\times$	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

Таким образом, достаточно доказать, что любой простой делитель $p > 10$ числа $5n^2+1$ имеет остаток 1, 3, 7 или 9 по модулю 20. Для этого вычислим остатки числа p по модулям 4 и 5. Если $5n^2 \equiv_p -1$, то $(5n)^2 \equiv_p -5$, т.е. -5 — вычет по модулю p. Применим квадратичный закон взаимности:

$$\left(\frac{-5}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{5}{p}\right) = (-1)^{\frac{p-1}{2}} \cdot \left(\frac{p}{5}\right) \cdot (-1)^{\frac{(p-1)(5-1)}{4}} = (-1)^{\frac{p-1}{2}} \cdot \left(\frac{p}{5}\right).$$

Значит, либо $p \equiv_4 1$ и $p \equiv_5 \pm 1$, либо $p \equiv_4 -1$ и $p \equiv_5 \pm 2$. Несложно проверить, что все четыре варианта дают в точности остатки 1, 3, 7 и 9 по модулю 20. Таким образом, наша задача решена.

Задача 5.12. Пусть $P(x) = x^3 + 14x^2 - 2x + 1$. Докажите, что существует такое натуральное n, что число $\underbrace{P(P(\ldots P}_{n}(x))) - x$ делится на 101 при любом натуральном x.

Решение. Очевидно, что если $x \equiv_{101} y$, то $P(x) \equiv_{101} P(y)$. Докажем, что если $x \not\equiv_{101} y$, то и $P(x) \not\equiv_{101} P(y)$. Действительно,

$$\frac{4(P(x) - P(y))}{x - y} = 4(x^2 + xy + y^2 + 14x + 14y - 2) \equiv_{101} (2x + y + 14)^2 + 3(y - 29)^2.$$

Если $P(x) \equiv_{101} P(y)$, то либо $2x + y + 14 \equiv_{101} y - 29 \equiv_{101} 0$, откуда $x \equiv_{101} y \equiv_{101} 29$, либо -3 — вычет по модулю 101, что неверно, т.к. по квадратичному закону взаимности

$$\left(\frac{-3}{101}\right) = \left(\frac{-1}{101}\right)\left(\frac{3}{101}\right) = \left(\frac{3}{101}\right) = \left(\frac{101}{3}\right) = -1.$$

Получаем противоречие.

Итак, отображение $x \mapsto P(x)$ задает перестановку на множестве $\mathbb{Z}_{101}$. Значит, для любого $x \in \mathbb{Z}_{101}$ существует такое натуральное число n_x, что $\underbrace{P(P(\ldots P}_{n_x}(x))) \equiv_{101} x$. Взяв n равным произведению всех чисел n_x, получаем, что $\underbrace{P(P(\ldots P}_{n}(x))) \equiv_{101} x$ для любого $x \in \mathbb{Z}_{101}$, что и требовалось.

Задача 5.13. Натуральные числа m и n таковы, что число $\frac{(m+3)^n+1}{3m}$ натуральное. Докажите, что тогда это число нечетно.

Решение. Сразу ясно, что $m^n + 1 \equiv_3 0$ и $3^n + 1 \equiv_m 0$. Из первого сравнения следует, что $m \equiv_3 2$ и n нечетно. Докажем, что число m делится на 2 и не делится на 4. Заметим, что если нам это удастся, то задача будет решена, т.к. тогда $(m + 3)^n + 1 \equiv_4 1 + 1 = 2$, т.е. степень вхождения числа 2 в числитель и в знаменатель одинакова и равна 1, а потому частное будет нечетным.

Итак, изучим степень вхождения числа 2 в m. Поскольку $3^n + 1 \equiv_8 4$ и $3^n + 1 \equiv_m 0$, то в число m двойка входит в степени не выше 2.

Теперь докажем, что степень вхождения двойки в число m нечетна (вместе с предыдущим рассуждением отсюда будет следовать требуемое). Рассмотрим произвольный нечетный простой делитель p числа m. Тогда $(-3)^n \equiv_p 1$ (т.к. n нечетно) и $(-3)^{p-1} \equiv_p 1$ по малой теореме Ферма. Следовательно, -3 — вычет по модулю p, откуда по критерию Эйлера $(-3)^{\frac{p-1}{2}} \equiv_p 1$. Далее, по квадратичному закону взаимности

$$\left(\frac{p}{3}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = \left(\frac{-3}{p}\right) = 1,$$

т.е. $p \equiv_3 1$. Наконец, получаем, что если $m = 2^t m_1$, где m_1 нечетно, то $m_1 \equiv_3 1$ и $2 \equiv_3 m \equiv_3 2^t$, откуда t нечетно.

Таким образом, $t \leq 2$ и t нечетно. Значит, $t = 1$, и наша задача решена.

Задача 5.14. Определим последовательность $\{x_n\}$ следующим образом: $x_1 = a$, $x_{n+1} = 2x_n + 1$. Пусть $y_n = 2^{x_n} - 1$. Какое максимальное количество подряд идущих простых чисел может встретиться в последовательности $\{y_n\}$?

Решение. Сделаем вначале несколько очевидных наблюдений. Прежде всего без ограничения общности можно считать, что числа y_1, y_2, …, y_k являются простыми (это достигается нужным выбором стартового значения числа x_1). Далее, все числа x_1, x_2, …, x_k также является простыми, поскольку если $x_i = 1$, то и $y_i = 1$, а если $x_i = mn$, где m, $n > 1$ то $2^{x_i} - 1$ делится на $2^m - 1$. В частности, число $a = x_1$ также является простым.

Теперь докажем, что если a — нечетное простое, то среди чисел y_1, y_2, y_3 обязано найтись составное число. Предположим противное. Тогда, как было сказано, числа x_1, x_2 и x_3 также являются простыми. Число x_1 нечетно, а потому $x_2 > 3$ и $x_2 \equiv_4 3$. Аналогично, $x_3 > 7$ и $x_3 \equiv_8 7$. Значит, число 2 является квадратичным вычетом по модулю x_3, и потому найдется какое натуральное число s, что $s^2 \equiv_{x_3} 2$. Но тогда $2^{x_2} \equiv_{x_3} 2^{\frac{x_2-1}{2}} \equiv_{x_3} 1$ по критерию Эйлера. Получаем, что простое число $y_2 = 2^{x_2} - 1$ делится на простое число $x_3 = 2x_2 + 1$. Это возможно, только если эти числа равны, т.е. $2^{x_2} - 1 = 2x_2 + 1$. Однако легко доказать, что $2^t - 1 > 2t + 1$ при всех $t > 3$. Таким образом, мы получаем противоречие. Значит, в случае, когда a — нечетное простое число, может быть не более двух подряд идущих простых чисел в последовательности $\{y_n\}$.

Наконец, если $a = 2$, то $y_1 = 3$ и $y_2 = 31$ — простые, а $y_3 = 2^{11} - 1$ делится на 23 (это прямо следует из нашего решения, ведь 2 является квадратичным вычетом по модулю $x_4 = 23$, потому по критерию Эйлера $2^{\frac{23-1}{2}} \equiv_{23} 1$).

Значит, в любом случае есть не более двух подряд идущих простых чисел в последовательности $\{y_n\}$.

Ответ. Два простых числа.

Задача 5.15. Даны натуральные числа: нечётное a, чётное b, простое p. Известно, что $p = a^2 + b^2$. Докажите, что a — квадратичный вычет по модулю p.

Решение. Прежде всего заметим, что $p \equiv_4 1$. Пусть $a = q_1 \dots q_n$ — разложение числа a на (возможно, совпадающие) простые множители. Тогда $3 \leq q_i \leq p - 1$, поэтому, применяя квадратичный закон взаимности для простых чисел p и $q := q_i$, получаем

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

(т.к. $p = a^2 + b^2 \equiv_q b^2$). Значит, q_i является вычетом по модулю p для любого i. Тогда a является произведением вычетов по модулю p и потому само вычет, что и требовалось доказать.

Задача 5.16. Докажите гипотезу Эйлера, используя КЗВ. Т.е. докажите, что если $p \equiv_{4a} q$, то $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$.

Решение. Если $p = q$, то равенство очевидно. В противном случае $(4a, p) = (4a, q) = 1$. Это позволяет применить следующую стандартную конструкцию. Заметим, что $\left(\frac{-1}{p}\right) = \left(\frac{-1}{q}\right)$, т.к. $p \equiv_4 q$, поэтому, при необходимости вынося из каждого символа Лежандра $\left(\frac{a}{p}\right)$ и $\left(\frac{a}{q}\right)$ величины $\left(\frac{-1}{p}\right)$ и $\left(\frac{-1}{q}\right)$ соответственно, можно считать, что $a > 0$. Далее, если a четно, то $p \equiv_8 q$, поэтому $\left(\frac{2}{p}\right) = \left(\frac{2}{q}\right)$ в силу предложения 6. Значит, вынося каждого символа Лежандра $\left(\frac{a}{p}\right)$ и $\left(\frac{a}{q}\right)$ величины $\left(\frac{2}{p}\right)$ и $\left(\frac{2}{q}\right)$ соответственно, можно добиться, что a — нечетное натуральное число.

Разложим число a в произведение нечетных простых сомножителей (возможно, повторяющихся): $a = r_1 \cdot r_2 \cdot \ldots \cdot r_t$. Теперь докажем равенство $\left(\frac{r}{p}\right) = \left(\frac{r}{q}\right)$ для каждого фиксированного нечетного простого делителя r числа a. Заметим, что $p \equiv_r q$ и $p \equiv_4 q$, поэтому по квадратичному закону взаимности имеем:

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

(равенство $\left(\frac{p}{r}\right) = \left(\frac{q}{r}\right)$ следует из сравнения $p \equiv_r q$, а равенство $(-1)^{\frac{p-1}{2}} = (-1)^{\frac{q-1}{2}}$ — из сравнения $p \equiv_4 q$).

Таким образом, для каждого нечетного простого делителя r числа a справедливо равенство $\left(\frac{r}{p}\right) = \left(\frac{r}{q}\right)$. Осталось перемножить эти равенства и получить требуемое.

Задача 6.1. Докажите, что число $4xyz - x - y$ не может быть точным квадратом при натуральных x, y, z.

Решение. Предположим противное: пусть $4xyz - x - y = a^2$ для некоторого целого a. Домножим это равенство на $4z$, прибавим к обеим частям 1 и разложим левую часть на множители. В результате наше равенство примет следующий вид:

$$(4zx - 1)(4zy - 1) = z(2a)^2 + 1.$$

Получается, что $\left(\frac{-z}{4zx-1}\right) = 1$. С другой стороны, $(z, 4zx - 1) = 1$, поэтому можно посчитать этот символ Якоби с помощью закона взаимности. Для этого разберем два случая.

Случай 1: z нечетно. В таком случае имеем:

$$\left(\frac{-z}{4zx-1}\right) = \left(\frac{-1}{4zx-1}\right) \cdot \left(\frac{z}{4zx-1}\right) = (-1)^{\frac{(4zx-1)-1}{2}} \cdot \left(\frac{4zx-1}{z}\right) \cdot (-1)^{\frac{z-1}{2} \cdot \frac{(4zx-1)-1}{2}} =$$
$$= (-1)^{2zx-1} \cdot \left(\frac{-1}{z}\right) \cdot (-1)^{\frac{z-1}{2} \cdot \frac{(4zx-1)-1}{2}} = (-1) \cdot (-1)^{\frac{z-1}{2}} \cdot (-1)^{\frac{z-1}{2}} = -1$$

— противоречие.

Случай 2: $z = 2^k t$, где t нечетно. В таком случае

$$\left(\frac{-z}{4yz-1}\right) = \left(\frac{-1}{4yz-1}\right) \cdot \left(\frac{z}{4yz-1}\right) = (-1)^{\frac{(4yz-1)-1}{2}} \cdot \left(\frac{2^k t}{2^{k+2}ty-1}\right) = -\left(\frac{2^k t}{2^{k+2}ty-1}\right).$$

Если k четно, то $\left(\frac{2^k t}{2^{k+2}ty-1}\right) = \left(\frac{t}{2^{k+2}ty-1}\right)$, и дальнейшие рассуждения повторяют выкладки из случая 1, из которых мы получаем, что $\left(\frac{t}{2^{k+2}ty-1}\right) = 1$. Если же k нечетно, то

$$\left(\frac{2^k t}{2^{k+2}ty-1}\right) = \left(\frac{2t}{2^{k+2}ty-1}\right) = \left(\frac{2}{2^{k+2}ty-1}\right) \cdot \left(\frac{t}{2^{k+2}ty-1}\right) = 1 \cdot 1 = 1.$$

В итоге получаем, что $1 = \left(\frac{-z}{4yz-1}\right) = -\left(\frac{2^k t}{2^{k+2}ty-1}\right) = -1$ — противоречие.

Таким образом, оба случая оказываются невозможны.

Задача 6.2. Докажите, что уравнение $x^2 = y^3 - 5$ не имеет решений в целых числах.

Решение. Если y четно, то $x^2 = y^3 - 5 \equiv_4 -1$, что невозможно. Поэтому y нечетно.

Если $y \equiv_4 3$, то $x^2 = y^3 - 5 \equiv_4 3^3 - 5 \equiv_4 2$, что вновь невозможно. Таким образом, $y = 4k + 1$ для некоторого целого k.

Перепишем наше уравнение в виде $x^2 + 4 = y^3 - 1$ и подставим в него $y = 4k + 1$. Получим следующее уравнение: $x^2 + 4 = 4k(16k^2 + 12k + 3)$. Поэтому -4, а значит, и -1 — вычет по модулю $16k^2 + 12k + 3$. С другой стороны, $16k^2 + 12k + 3 \equiv_4 3$, а значит, по квадратичному закону взаимности Якоби -1 — невычет по модулю $16k^2 + 12k + 3$. Получаем противоречие и в этом случае.

Задача 6.3. Докажите, что число $4kxy-1$ не может делить число x^m+y^n для всех натуральных x, y, k, m, n.

Решение. Заметим, что числа x^m, y^n и $4kxy-1$ попарно взаимно просты. Теперь нам нужно разобрать три случая.

Случай 1: $m=2m_1$ *и* $n=2n_1$. Тогда число $4kxy$ делит сумму двух квадратов $(x^{m_1})^2+(y^{n_1})^2$. Но тогда -1 — вычет по модулю $4kxy-1$, что невозможно, т.к. $4kxy-1\equiv_4 3$.

Случай 2: $m=2m_1$ *и* $n=2n_1+1$. Здесь рассуждения несколько сложнее. Из условия следует, что число $4kxy-1$ делит число $(x^{m_1})^2+y(y^{n_1})^2$, откуда число $-y$ является вычетом по модулю $4kxy-1$. Докажем, что это не так. Если y нечетно, то сразу применим квадратичный закон взаимности Якоби:

$$\left(\frac{-y}{4kxy-1}\right)=\left(\frac{-1}{4kxy-1}\right)\left(\frac{y}{4kxy-1}\right)=(-1)\left(\frac{4kxy-1}{y}\right)(-1)^{\frac{y-1}{2}\frac{(4kxy-1)-1}{2}}=(-1)\left(\frac{-1}{y}\right)^2=-1$$

— противоречие.

Если же $y=2^ty_1$, где y_1 нечетно, то $\left(\frac{2}{4kxy-1}\right)=1$, а потому

$$\left(\frac{-y}{4kxy-1}\right)=\left(\frac{2}{4kxy-1}\right)^t\left(\frac{-y_1}{4kxy-1}\right)=-1$$

— снова противоречие (последнее равенство следует из вычислений, проведенных для случая нечетного y).

Случай 3: $m=2m_1+1$ *и* $n=2n_1+1$. Этот случай сводится к предыдущему. Действительно, возьмем число $x(x^{m_1})^2+y(y^{n_1})^2$, умножим его на y и получим, что число $-xy$ должно быть вычетом по модулю $4kxy-1$. Противоречие здесь получается точно так же, как и в предыдущем случае. Для удобства положим $z=xy$ и докажем, что $\left(\frac{-z}{4kz-1}\right)=-1$. Если z нечетно, то, применяя квадратичный закон взаимности Якоби, получаем:

$$\left(\frac{-z}{4kz-1}\right)=\left(\frac{-1}{4kz-1}\right)\left(\frac{z}{4kz-1}\right)=(-1)\left(\frac{4kz-1}{z}\right)(-1)^{\frac{z-1}{2}\frac{(4kz-1)-1}{2}}=(-1)\left(\frac{-1}{z}\right)^2=-1.$$

Если же $z=2^tz_1$, где z_1 нечетно, то вновь $\left(\frac{2}{4kz-1}\right)=1$, а потому

$$\left(\frac{-z}{4kz-1}\right)=\left(\frac{2}{4kz-1}\right)^t\left(\frac{-z_1}{4kz-1}\right)=-1$$

— снова противоречие.

9. Приложение: листки со сборов

9.1. Квадратичные вычет – 1

Пусть p — нечетное простое число, a — произвольное целое число, не кратное p. Число a называется *квадратичным вычетом* (или просто *вычетом*) по модулю p, если существует такое целое число x, что $x^2 \equiv_p a$. В противном случае число a называется *квадратичным невычетом* (или просто *невычетом*).

Определение. *Символ Лежандра* $\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{если } a \equiv_p 0, \\ 1, & \text{если } a \text{ — вычет в } \mathbb{Z}_p, \\ -1, & \text{если } a \text{ — невычет в } \mathbb{Z}_p. \end{cases}$

Задача 1. Докажите, что квадратичных вычетов ровно $\frac{p-1}{2}$.

Задача 2. (a) Докажите, что произведение двух вычетов — тоже вычет.
(b) Докажите, что произведение вычета и невычета — невычет.
(c) Докажите, что произведение двух невычетов — вычет.
Замечание. Кратко все три пункта этой задачи означают *мультипликативность символа Лежандра*: $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

Задача 3. (*Критерий Эйлера*) В этой задаче мы докажем следующую формулу: $\left(\frac{a}{p}\right) \equiv_p a^{(p-1)/2}$.
(a) Докажите, что если a — вычет, то $a^{(p-1)/2} \equiv_p 1$.
(b) Докажите, что если a — невычет, то $a^{(p-1)/2} \equiv_p -1$.
(*Указание*: попробуйте модифицировать доказательство малой теоремы Ферма.)
(c) Докажите, что -1 является квадратичным вычетом по простому модулю p тогда и только тогда, когда p имеет вид $4k+1$.

Задача 4. Целые числа x и y таковы, что $x^2 + y^2$ делится на простое число p вида $4k+3$. Докажите, что сами числа x и y делятся на p.

Задача 5. Докажите, что при любых натуральных x, $y > 2$ число $\frac{x^2+1}{y^2-5}$ не является целым.

Задача 6. Докажите, что если простое число p является делителем числа $x^2 - 6x + 3$, где x — целое, то оно также является делителем числа $y^2 - 2y - 53$ для некоторого целого y.

Задача 7. Существуют ли 18 последовательных натуральных чисел, которые можно разбить на две группы с одинаковыми произведениями?

Задача 8. Пусть p — нечетное простое число. Какова мощность множества

$$\{x^2 : x \in \mathbb{Z}_p\} \cap \{y^2 + 1 : y \in \mathbb{Z}_p\}?$$

Задача 9. Пусть p — нечетное простое число. Докажите, что наименьший квадратичный невычет по модулю p меньше $\sqrt{p} + 1$.

9.2. Квадратичные вычеты – 1: добавка

Задача 10. Докажите, что существует бесконечно много натуральных чисел n, для которых число n^2+1 имеет не менее 2022 различных простых делителей.

Задача 11. Докажите, что число $4mn-m-n$ не является точным квадратом ни при каких натуральных числах m и n.

Задача 12. Докажите, что многочлен x^4+1 приводим над $\mathbb{Z}_p$ для любого простого p (т.е. он представим в виде произведения двух многочленов положительной степени с коэффициентами в $\mathbb{Z}_p$).

Задача 13. Пусть A — это множество ненулевых остатков $a \in \mathbb{Z}_p$, таких, что остатки a и $4-a$ являются невычетами по модулю p. Найдите остаток произведения всех элементов множества A по модулю p.

9.3. Квадратичные вычеты – 2

Для нечётного простого p запишем все ненулевые остатки по модулю p в виде

$$1, 2, 3, \ldots, \frac{p-3}{2}, \frac{p-1}{2}, -\frac{p-1}{2}, -\frac{p-3}{2}, \ldots -3, -2, -1.$$

Назовём остатки $1, 2, 3, \ldots, \dfrac{p-3}{2}, \dfrac{p-1}{2}$ *положительными*, а остальные — *отрицательными*.

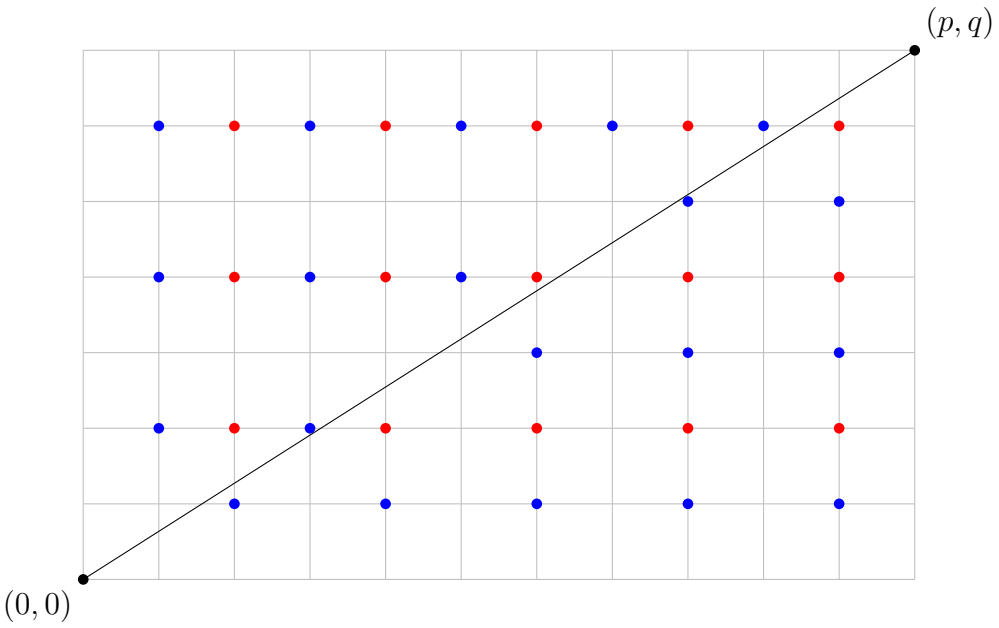
Задача 1. Докажите, что ненулевой остаток a является квадратичным вычетом по модулю нечётного простого p тогда и только тогда, когда среди остатков $a, 2a, 3a, \ldots, \dfrac{p-1}{2}a$ чётное число отрицательных.

Задача 2. Докажите, для нечётного простого p что остаток 2 является квадратичным вычетом тогда и только тогда, когда p имеет вид $8k \pm 1$. *Иными словами,* $\left(\dfrac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

Задача 3. (**Квадратичный закон взаимности**)
(a) Докажите, что натуральное число a, не кратное нечётному простому p, является квадратичным вычетом по модулю p тогда и только тогда, когда $\sum\limits_{i=1}^{(p-1)/2} \left[\dfrac{a \cdot i}{p/2}\right] \equiv_2 0$.
(b) Докажите, что для любых различных нечётных простых чисел p и q выполнено

$$\sum_{i=1}^{(p-1)/2} \left[\frac{q}{p} \cdot (2i)\right] + \sum_{j=1}^{(q-1)/2} \left[\frac{p}{q} \cdot (2j)\right] \equiv_2 \frac{p-1}{2} \cdot \frac{q-1}{2}.$$

(*Кстати, это доказательство КЗВ называют геометрическим.*)



(с) Докажите КЗВ: для любых различных нечётных простых p и q выполнено

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

Задача 4. Используя квадратичный закон взаимности и свойство мультипликативности символа Лежандра, разберитесь, является ли 79 квадратичным вычетом по модулю 101.

Задача 5. Докажите, что ни при каком натуральном n у числа $2^n + 1$ не может быть простых делителей вида $8k + 7$.

Задача 6. Целые числа x и y таковы, что $x^2 + xy + y^2$ делится на простое число p вида $3k + 2$. Докажите, что сами x и y делятся на p.

Задача 7. Докажите, что если число $p = 2^n + 1$ — простое ($n > 1$), то минимальная степень T такая, что $3^T \equiv_p 1$, равна $p - 1$.

Задача 8. Дано натуральное число $n > 1$. Докажите, что любой нечётный делитель $d > 10$ числа $5n^2 + 1$ имеет в своей десятичной записи чётную цифру.

Задача 9. Даны натуральные числа: нечётное a, чётное b, простое p. Известно, что $p = a^2 + b^2$. Докажите, что a — квадратичный вычет по модулю p.

9.4. КЗВ: бонусное доказательство

Для всякого ненулевого остатка a по нечётному простому модулю p определим перестановку $\sigma_{a,p} \colon \mathbb{Z}_p \to \mathbb{Z}_p$ с помощью формулы $\sigma_{a,p}(x) = ax$ для всех $x \in \mathbb{Z}_p$.

Задача 1. Докажите, что ненулевой остаток a по нечётному простому модулю p является квадратичным вычетом тогда и только тогда, когда перестановка $\sigma_{a,p}$ — чётная.

Иными словами, $\left(\frac{a}{p}\right) = \operatorname{sgn}(\sigma_{a,p})$.

Задача 2. Даны различные нечётные простые числа p и q.
Определим на множестве $\mathbb{Z}_p \times \mathbb{Z}_q$ перестановки μ и ν по следующим формулам:

$$\forall a \in \mathbb{Z}_p, \forall b \in \mathbb{Z}_q \quad \mu(a, b) = (a, a + pb), \quad \nu(a, b) = (qa + b, b).$$

Определим также перестановку

$$\pi\colon \mathbb{Z}_{pq} \to \mathbb{Z}_{pq}, \quad \forall a \in \mathbb{Z}_p, \forall b \in \mathbb{Z}_q \quad \pi\colon a + pb \mapsto qa + b.$$

(a) Докажите, что $\operatorname{sgn}(\mu) = \left(\frac{p}{q}\right)$ и $\operatorname{sgn}(\nu) = \left(\frac{q}{p}\right)$.

(b) Докажите, что $\operatorname{sgn}(\pi) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$.

28	29	30	31	32	33	34
21	22	23	24	25	26	27
14	15	16	17	18	19	20
7	8	9	10	11	12	13
0	1	2	3	4	5	6

$\xrightarrow{\pi}$

4	9	14	19	24	29	34
3	8	13	18	23	28	33
2	7	12	17	22	27	32
1	6	11	16	21	26	31
0	5	10	15	20	25	30

(c) Соотнесите знаки перестановок π и $\nu \circ \mu^{-1}$ и завершите доказательство КЗВ:

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

Список литературы

[1] К. Айэрленд, М. Роузен. *Классическое введение в современную теорию чисел*. М.: Мир, 1987.

[2] Е. А. Горин, *Перестановки и квадратичный закон взаимности по Золотареву-Фробениусу-Руссо*, Чебышевский сб., **14**:4 (2013), 80-94.

[3] А. Шень. *Перестановки*. М.: МЦНМО, 2020.

[4] В. И. Арнольд, *Топология алгебры: комбинаторика операции возведения в квадрат*, Функц. анализ и его прил., **37**:3 (2003), 20-35.

[5] В. Доценко. *Арифметика квадратичных форм*. М.: МЦНМО, 2015.

[6] П. В. Бибиков, К. В. Козеренко, А. И. Малахов. *Теория чисел во Второй школе*. М.: МЦНМО, 2021.