Летняя школа «Современная математика»
Дубна, июль 2007

В. Доценко

Арифметика квадратичных форм

Электронное издание

Москва
Издательство МЦНМО

УДК 511
ББК 22.13
Д71

Доценко В.
Арифметика квадратичных форм
Электронное издание
М.: МЦНМО, 2023
29 с.
ISBN 978-5-4439-3428-0

Какие целые числа можно представить в виде суммы двух квадратов? С исследования вопросов такого рода началась современная теория чисел. В брошюре обсуждаются некоторые классические результаты, возникающие на этом пути, от теоремы Ферма—Эйлера до теоремы Минковского—Хассе.

Брошюра написана по материалам цикла лекций на Летней школе «Современная математика» в Дубне в 2007 г. Она доступна студентам младших курсов и школьникам старших классов.

Подготовлено на основе книги: *В. Доценко*. Арифметика квадратичных форм. — 2-е изд., стереотип. — М.: МЦНМО, 2019. — ISBN 978-5-4439-2828-9.

Издательство Московского центра
непрерывного математического образования
119002, Москва, Большой Власьевский пер., 11,
тел. (499) 241–08–04.
http://www.mccme.ru

ISBN 978-5-4439-3428-0

Введение

Текст содержит записки курса лекций, прочитанного в июле 2007 года участникам Летней школы «Современная математика». Мы приводим в точности то, что вошло в основной курс, не пытаясь обмануть читателя и уместить в текст доказательства и формулировки, которые не вошли в курс из-за нехватки времени. Нам представляется, что недостающие доказательства легко восстановить; интересующийся читатель найдет их, а также многие другие замечательные теоремы, в любой из следующих книг:

1. *З. И. Боревич*, *И. Р. Шафаревич*. Теория чисел. М.: Наука, 1985.
2. *Дж. Касселс*. Рациональные квадратичные формы. М.: Мир, 1982.
3. *Ж.-П. Серр*. Курс арифметики. М.: Мир, 1972.

Лекция 1. Суммы двух квадратов

Мы начнем с того, что объясним несколько доказательств следующего замечательного утверждения.

Теорема 1 (Ферма—Эйлера о двух квадратах). *Для того чтобы целое положительное число n можно было представить в виде суммы квадратов двух целых чисел, необходимо и достаточно, чтобы любой простой делитель числа n, дающий остаток 3 при делении на 4, входил в разложение n на простые множители в четной степени.*

Доказательство этой теоремы состоит из трех шагов. Два из них совсем просты, а третий можно производить разными способами, и мы обсудим некоторые из них.

Шаг 1. Непредставимость остальных чисел. Пусть x^2+y^2 делится на простое $p=4k+3$ (x, y — целые числа). Тогда

$$x^{p-1}+y^{p-1}=x^{4k+2}+y^{4k+2}=(x^2)^{2k+1}+(y^2)^{2k+1}$$

делится на x^2+y^2 и потому делится на p.

Согласно малой теореме Ферма, x^{p-1} сравнимо с нулем или единицей по модулю p, и легко видеть, что $x^{p-1}+y^{p-1}$ делится на p, если и только если x и y делятся на p.

Поэтому равенство $n=x^2+y^2$ можно сократить на квадрат любого простого делителя n, который сравним с 3 по модулю 4. Значит, такой простой делитель входит в разложение n в четной степени. □

Шаг 2. Мультипликативность. Легко видеть, что

$$(a^2+b^2)(c^2+d^2)=(ad-bc)^2+(ac+bd)^2,$$

и потому произведение двух чисел, представимых в виде суммы двух квадратов, тоже представимо в виде суммы двух квадратов.

Использованное равенство отражает тот известный факт, что модуль произведения двух комплексных чисел равен произведению модулей. □

Для завершения доказательства теоремы Ферма—Эйлера нам осталось доказать, что любое простое число вида $4k+1$ представимо в виде суммы двух квадратов.

Это можно доказать многими способами. Большинство из них опираются на следующее более слабое утверждение.

Предложение 1. *Для простого числа p вида $4k+1$ найдутся такие x и y, не делящиеся на p, что x^2+y^2 делится на p. Более того, можно взять $y=1$.*

Доказательство. Проще всего воспользоваться теоремой Вильсона: $(p-1)!+1=(4k)!+1$ делится на p, и

$$(4k)!\equiv(-1)^{2k}((2k)!)^2\equiv((2k)!)^2 \pmod p,$$

так что для $r=(2k)!$ получаем, что r^2+1 делится на p. □

Шаг 3 по Лагранжу. Наиболее непосредственно предложение 1 используется в первом нашем доказательстве (не первом хронологически!).

Возьмем такое r, что r^2+1 делится на p. Рассмотрим все пары (a,b) с $0\leqslant a,b\leqslant[\sqrt{p}]$ и построим для каждой из них число $a+br$. Таких пар больше, чем p, поэтому среди отвечающих им чисел найдутся два, сравнимые по модулю p. Покоординатная разность соответствующих пар даст число $A+Br$, которое делится на p. Значит, и $A^2-B^2r^2=(A+Br)(A-Br)$ делится на p. Но $A^2-B^2r^2\equiv A^2+B^2 \pmod p$, так что A^2+B^2 делится на p. При этом $|A|<\sqrt{p}$, $|B|<\sqrt{p}$, поэтому $A^2+B^2<2p$. Значит, $A^2+B^2=p$. □

Шаг 3 по Эйлеру и Ферма. Следующее доказательство принадлежит Эйлеру, который хотел реализовать «принцип спуска» Ферма.

Пусть $x^2+y^2=mp$ для некоторого $m>1$ (x, y не делятся на p). Можно заменить x и y на сравнимые с ними по модулю p числа между $-\frac{p}{2}$ и $\frac{p}{2}$. Тогда имеем $mp=x^2+y^2\leqslant\frac{p^2}{4}+\frac{p^2}{4}=\frac{p^2}{2}$, откуда $m\leqslant\frac{p}{2}<p$. Выберем числа u и v между $-\frac{m}{2}$ и $\frac{m}{2}$, для которых $x\equiv u \pmod m$, $y\equiv v \pmod m$. Тогда $u^2+v^2=mt$ для некоторого t и, как и выше, $t\leqslant\frac{m}{2}<m$. При этом $t\neq0$, иначе x и y кратны m, и из $x^2+y^2=mp$ имеем, что p кратно m, и потому $m=1$ (ибо $m<p$), противоречие. Перемножая наши равенства и используя формулу для произведения сумм квадратов, получаем

$$m^2tp=(x^2+y^2)(u^2+v^2)=(xv-yu)^2+(xu+yv)^2.$$

Заметим, что $xv-yu\equiv0\equiv xu+yv \pmod m$ по определению чисел u и v. Поэтому наше равенство можно переписать в виде

$$tp=a^2+b^2$$

с целыми a и b. Мы получили кратное числа p с меньшим частным, которое представимо в виде суммы квадратов. Индукция завершает доказательство. □

Шаг 3 «по Гауссу». Это доказательство могло бы принадлежать Гауссу. Во всяком случае, оно использует *целые гауссовы числа* (комплексные числа $a+bi$ такие, что числа a и b целые).

Гауссовы числа можно делить с остатком: для любых гауссовых чисел a и b ($b\neq 0$) можно найти такие гауссовы числа q и r, что $a=qb+r$ и $|r|<|b|$. Как и для обычных целых чисел, деление с остатком позволяет построить алгоритм Евклида для отыскания наибольшего общего делителя и доказать основную теорему арифметики.

Пусть x^2+y^2 делится на p (x, y не делятся на p). Найдем наибольший общий делитель $\pi=a+bi$ чисел $x+iy$ и p. Он не может быть равен единице (раз $x^2+y^2=(x-iy)(x+iy)$ делится на p), но и не может быть равен p. При этом в обычных целых числах $|\pi|^2$ является делителем $|p|^2=p^2$. Значит, $p=|\pi|^2=a^2+b^2$, что и требовалось. □

Шаг 3 по Минковскому: геометрия чисел. Это доказательство использует геометрию куда тоньше, чем предыдущее.

Докажем сначала, что если a, b, c — целые числа, для которых $ac-b^2=1$, то существует решение уравнения $ax^2+2bxy+cy^2=1$ с целыми x, y. Найдем наименьшее значение $ax^2+2bxy+cy^2$ при целых x и y. Пусть это значение равно m. Множество решений неравенства $ax^2+2bxy+cy^2\leqslant m$ — внутренность эллипса. Ясно, что если сжать этот эллипс гомотетично с центром в нуле в два раза, после чего параллельно перенести его во все целые точки, то полученные эллипсы не имеют общих внутренних точек. Площадь такого эллипса равна $\dfrac{\pi m}{4(ac-b^2)}=\dfrac{\pi m}{4}$. Если бы эта площадь была больше 1, то мы легко получили бы противоречие (количество целых точек в квадрате размера $N\times N$ примерно равно площади квадрата), так что $m\leqslant\dfrac{4}{\pi}$, и потому $m=1$.

Возьмем такое r, что r^2+1 делится на p. Применим наше утверждение к $a=p$, $b=r$, $c=\dfrac{r^2+1}{p}$. Для целых x и y получим

$$1=px^2+2rxy+\frac{r^2+1}{p}y^2=\frac{p^2x^2+2prxy+r^2y^2+y^2}{p}=\frac{(px+ry)^2+y^2}{p},$$

откуда $p=(px+ry)^2+y^2$, что и требовалось. □

Шаг 3 по Дону Цагиру: инволюции. Это доказательство, пожалуй, наиболее загадочно и необъяснимо.

Рассмотрим уравнение $x^2+4yz=p$. Будем решать его в целых неотрицательных числах x, y, z. Положим[1]

$$J[(x,y,z)]=\begin{cases}(x+2z,\,z,\,y-x-z) & \text{при } x<y-z,\\ (2y-x,\,y,\,x-y+z) & \text{при } y-z\leqslant x\leqslant 2y,\\ (x-2y,\,x-y+z,\,y) & \text{при } 2y<x.\end{cases}$$

[1]Геометрическую интерпретацию этого преобразования можно найти в книге А. В. Спивака «Арифметика-2» (М.: Бюро Квантум, 2008).

Оказывается, если (x, y, z) — решение нашего уравнения, то $J(x, y, z)$ тоже будет решением (т. е. J — преобразование множества решений в себя). Действительно,

- если $x < y - z$, то $(x + 2z)^2 + 4z(y - x - z) = x^2 + 4yz$,
- если $y - z \leqslant x \leqslant 2y$, то $(2y - x)^2 + 4y(x - y + z) = x^2 + 4yz$,
- если $x > 2y$, то $(x - 2y)^2 + 4(x - y + z)y = x^2 + 4yz$.

Замечательным и неожиданным образом оказывается, что двукратное применение преобразования J есть тождественное преобразование (т. е. J — *инволюция*). Действительно,

- если $x < y - z$, то $2z < 2z + x$, и

$$J \circ J[(x, y, z)] = (x + 2z - 2z, x + 2z - z + y - x - z, z) = (x, y, z).$$

- если $y - z \leqslant x \leqslant 2y$, то $y - (x - y + z) \leqslant 2y - x \leqslant 2y$, и

$$J \circ J[(x, y, z)] = (2y - (2y - x), y, (2y - x) - y + (x - y + z)) = (x, y, z).$$

- если $x > 2y$, то $x - 2y < (x - y + z) - y$, и

$$J \circ J[(x, y, z)] = ((x - 2y) + 2y, y, (x - y + z) - (x - 2y) - y) = (x, y, z).$$

У нашей инволюции, как нетрудно видеть, ровно одна неподвижная точка на множестве решений: тройка $(1, 1, k)$ (если $p = 4k + 1$). Все остальные решения действие инволюции разбивает на пары. Множество решений конечно, так что в нем нечетное число элементов.

С другой стороны, на этом множестве есть и другая инволюция: инволюция, переставляющая y и z. Раз число решений нечетно, у этой инволюции должна быть неподвижная точка. Для соответствующего решения $y = z$ и $p = x^2 + (2y)^2$. □

Другие варианты доказательства шага 3 не обсуждаются в нашем курсе. Из наиболее интересных упомянем способ Лежандра, использовавшего разложение числа $\sqrt{p}$ в цепную дробь[1], и способ Якобшталя[2], строившего представление в виде суммы квадратов с использованием символов Лежандра.

---

[1] О нем можно прочитать, например, в статье «Цепные дроби» полутома «Числа и фигуры» в «Новой школьной энциклопедии» (М.: Росмэн, 2005).

[2] Замечательно, что этот способ, в отличие от обсуждавшихся выше, дает явные формулы для чисел x и y. Заинтересованный читатель может найти подробности в книге Дэвенпорта «Высшая арифметика. Введение в теорию чисел» (М.: Наука, 1965).

Задачи

Задача 1. Докажите, что представление простого числа вида $4k+1$ в виде x^2+y^2 единственно с точностью до перестановки слагаемых и замены знаков у x и y.

Задача 2. Найдите число решений по модулю p уравнения $x^2+y^2=1$. (Указание: число решений равно сумме $\sum_{y=0}^{p-1}\left(1+\left(\frac{1-y^2}{p}\right)\right)$, где $\left(\frac{a}{p}\right)$ — символ Лежандра; см., при необходимости, предварительные сведения в конце брошюры.)

Задача 3. (а) Пусть p — простое число. Докажите, что нетривиальное решение сравнения $x^2+3y^2\equiv 0 \pmod p$ существует, если и только если p сравнимо с 1 по модулю 3. (б) Докажите аналогичное утверждение для квадратичной формы x^2+5y^2. (в) Докажите аналогичное утверждение для квадратичной формы x^2+xy+y^2.

Задача 4* (продолжение). Попробуйте доказать утверждения о представимости простых чисел в виде x^2+3y^2, x^2+5y^2, x^2+xy+y^2 аналогично доказательству Дона Цагира. (Автору доказательства неизвестны, но, скорее всего, это должно быть нетрудно.)

Задача 5. Докажите, что уравнение $(x^2-13)(x^2-17)(x^2-221)=0$ разрешимо (а) по любому простому модулю; (б*) вообще по любому модулю.

Задача 6*. Докажите, что уравнение $3x^3+4y^3+5z^3=0$ не имеет нетривиальных целых решений, но имеет нетривиальное решение по любому простому модулю.

Задача 7. (а) Докажите, что линейное уравнение с целыми коэффициентами $a_1x_1+\ldots+a_nx_n=b$ имеет решение в целых числах тогда и только тогда, когда оно имеет решение по любому модулю. (б) Докажите аналогичное утверждение для систем линейных уравнений.

Задача 8. Докажите, что для k, не делящегося на $p-1$,

$$\sum_{x=0}^{p-1} x^k \equiv 0 \pmod p.$$

Задача 9. Найдите число решений по модулю 7 сравнения

$$x^3+y^3+z^3+t^3\equiv 0 \pmod 7.$$

(Указание: для всех четверок, которые не удовлетворяют сравнению, $(x^3+y^3+z^3+t^3)^6\equiv 1 \pmod 7$.)

Задача 10 (теорема Шевалле—Варнинга). Пусть p — простое число. Если $F(x_1,\ldots,x_n)$ — однородный многочлен степени $r<n$ с целыми коэффициентами, то число решений сравнения $F(x_1,\ldots,x_n)\equiv$

$\equiv 0 \pmod{p}$ делится на p. В частности, последнее сравнение имеет нетривиальное решение по модулю p.

Задача 11 (продолжение). Приведите пример однородного многочлена степени 3 от трех переменных, значение которого делится на 5, если и только если все аргументы делятся на 5 (про такой многочлен говорят, что он *не представляет нуль по модулю* 5 *нетривиальным образом*).

Задача 12*. Пусть $f(x_1, \ldots, x_n) = \sum_{i,j} a_{ij} x_i x_j$ — квадратичная форма с целыми коэффициентами. Пусть известно, что $f(x_1, \ldots, x_n) > 0$ при $(x_1, \ldots, x_n) \neq (0, \ldots, 0)$. Далее, пусть для любых рациональных $t_1, \ldots, t_n$ найдутся целые $a_1, \ldots, a_n$ такие, что

$$f(t_1 - a_1, \ldots, t_n - a_n) < 1.$$

Докажите, что если для целого числа k уравнение $f(x_1, \ldots, x_n) = k$ имеет рациональные решения, то оно имеет и целые решения. (В частности, это верно для формы $f(x, y, z) = x^2 + y^2 + z^2$.)

Лекция 2. Суммы четырех квадратов

Удивительным образом, с суммами трех квадратов дело обстоит гораздо сложнее. А именно, верна следующая теорема.

Теорема 2. *Целое положительное число представимо в виде суммы трех квадратов, если и только если оно* не *имеет вида* $4^a(8b+7)$.

Легко видеть, что числа вида $4^a(8b+7)$ действительно не представимы (это делается с помощью вычислений по модулю 8).

Все другие числа представимы, но доказать это непросто. Лежандр исходно доказывал это с помощью гипотезы, которая впоследствии стала известна как теорема Дирихле о простых в арифметических прогрессиях (в период работы Лежандра это утверждение еще не было доказано). Мы выведем это утверждение из «теоремы Минковского—Хассе» в последней лекции.

Одна из причин того, что эту теорему так трудно доказать, состоит в том, что она «не мультипликативна» (и поэтому недостаточно знать, какие простые числа представимы в виде суммы трех квадратов): например, числа 3 и 5 представимы в виде суммы трех квадратов, а их произведение — не представимо.

В случае четырех квадратов ситуация оказывается проще: дело в том, что мультипликативное правило для сумм четырех квадратов есть. Это следует из существования *кватернионов* — далеко идущего обобщения комплексных чисел. Мы вкратце обсудим кватернионный способ доказательства чуть ниже, а для начала сформулируем теорему о четырех квадратах и выведем ее из теоремы о сумме трех квадратов.

Теорема 3. *Любое целое число представимо в виде суммы четырех квадратов.*

Вывод теоремы о четырех квадратах из теоремы о трех квадратах. Если число не имеет вида $4^a(8b+7)$, то оно представимо даже в виде суммы трех квадратов. Если же число имеет вид $4^a(8b+7)$, то мы представим $8b+3$ в виде суммы трех квадратов, добавим квадрат $4=2^2$, чтобы получить $8b+7$, и умножим нашу сумму квадратов на $4^a=(2^a)^2$. □

Приведем для двух из доказательств теоремы о двух квадратах аналогичные им доказательства теоремы о суммах четырех квадратов.

Прежде всего заметим, что в случае этой теоремы шаг 1 не нужен (мы доказываем, что все числа представимы). Шаг 2, как мы указывали, удается произвести аналогично.

Как и в случае двух квадратов, прежде чем доказывать представимость числа p, докажем представимость нуля по модулю p.

Предложение 2. *Для любого простого числа p найдется сумма четырех квадратов (не все из которых делятся на p), которая делится на p.*

Доказательство. Мы даже докажем, что есть сумма трех квадратов, делящаяся на p. В самом деле, рассмотрим два множества остатков по модулю p: все квадратичные вычеты и все остатки вида $-1-y^2$. В каждом из этих множеств $\frac{p+1}{2}$ элементов (если $p \neq 2$, конечно). Значит, эти два множества остатков пересекаются, то есть для некоторых x и y имеем $x^2 \equiv -1-y^2 \pmod{p}$, и x^2+y^2+1 делится на p. □

Шаг 3: метод спуска. Пусть $x^2+y^2+z^2+t^2 = mp$ для некоторого $m>1$. Если m четно, то числа x, y, z, t можно разбить на пары одинаковой четности. Можно считать, что x и y одинаковой четности, а также z и t одинаковой четности. В таком случае мы можем представить в виде суммы квадратов число $\frac{m}{2}p$:

$$\frac{m}{2}p = \left(\frac{x+y}{2}\right)^2 + \left(\frac{x-y}{2}\right)^2 + \left(\frac{z+t}{2}\right)^2 + \left(\frac{z-t}{2}\right)^2,$$

и мы произвели спуск к меньшему кратному.

Пусть теперь m нечетно. Заменяя x, y, z, t на сравнимые с ними по модулю p числа, модули которых меньше $\frac{p}{2}$, мы видим, что можно считать $m<p$. Если все x, y, z, t делятся на m, то mp делится на m^2 и p делится на m, противоречие. Заменим числа x, y, z, t на сравнимые с ними по модулю m числа a, b, c, d, модули которых меньше $\frac{m}{2}$, тогда $a^2+b^2+c^2+d^2<m^2$, и при этом $a^2+b^2+c^2+d^2 \equiv 0 \pmod{m}$. Обозначим частное от деления $a^2+b^2+c^2+d^2$ на m через m_1. Имеем

$$m^2pm_1 = (x^2+y^2+z^2+t^2)(a^2+b^2+c^2+d^2) = \alpha^2+\beta^2+\gamma^2+\delta^2,$$

где $\alpha, \beta, \gamma, \delta$ получаются из следующей формулы произведения:

$$\begin{aligned}(x_0^2+x_1^2+x_2^2+x_3^2)(y_0^2+y_1^2+y_2^2+y_3^2) = \\ = (x_0y_0-x_1y_1-x_2y_2-x_3y_3)^2 + (x_0y_1+x_1y_0+x_2y_3-x_3y_2)^2 + \\ + (x_0y_2-x_1y_3+x_2y_0+x_3y_1)^2 + (x_0y_3+x_1y_2-x_2y_1+x_3y_0)^2. \quad (1)\end{aligned}$$

Из этих формул легко видеть, что числа $\alpha, \beta, \gamma, \delta$ делятся на m. Поэтому pm_1 представимо в виде суммы четырех квадратов, так что мы произвели спуск к меньшему значению m.

Шаг 3: кватернионы. Напомним правило умножения кватернионов, открытое Уильямом Роуэном Гамильтоном одним туманным осенним вечером:

$$(x_0+x_1i+x_2j+x_3k)(y_0+y_1i+y_2j+y_3k)=$$
$$=(x_0y_0-x_1y_1-x_2y_2-x_3y_3)+(x_0y_1+x_1y_0+x_2y_3-x_3y_2)i+$$
$$+(x_0y_2-x_1y_3+x_2y_0+x_3y_1)j+(x_0y_3+x_1y_2-x_2y_1+x_3y_0)k. \quad (2)$$

Как и для комплексных чисел, модуль произведения двух кватернионов равен произведению их модулей. Это объясняет, откуда берутся формулы произведения типа (1).

Кватернионы с целыми коэффициентами («липшицевы кватернионы», в терминологии Дж. Конвея) нельзя делить с остатком: в четырехмерном кубе расстояние от центра до вершины равно ребру куба (из-за этого непонятно, как разделить с остатком, например, $1+i+j+k$ на 2 — все делимое остатком быть не может, так как его модуль как раз равен модулю делителя). Чтобы можно было делить с остатком, надо рассматривать кватернионы, у которых все коэффициенты целые или все одновременно полуцелые («гурвицевы целые кватернионы» по Конвею[1]).

Для таких кватернионов можно говорить про (левый или правый[2]) наибольший общий делитель, и для представления $x^2+y^2+z^2+t^2=mp$ с целыми x, y, z, t, не делящимися одновременно на p, найти наибольший (правый) общий делитель $x+iy+jz+kt$ и p. Этот наибольший общий делитель и даст искомое представление в виде суммы целых или полуцелых квадратов. Дальше нужно при необходимости произвести поправку: умножить этот наибольший общий делитель на одно из чисел $\frac{\pm1\pm i\pm j\pm k}{2}$, которые обратимы в гурвицевых кватернионах и не изменяют по существу наибольший общий делитель, но могут сделать его коэффициенты целыми.

Теорема Лежандра

В этом разделе мы докажем следующую теорему.

Теорема 4 (Лежандр). *Пусть a, b, c — попарно взаимно простые целые положительные числа, свободные от квадратов. Тогда уравнение*

$$ax^2+by^2-cz^2=0$$

[1]Подробности можно найти в книге Дж. Конвея и Д. Смита «О кватернионах и октавах, об их геометрии, арифметике и симметрии» (М.: МЦНМО, 2009).

[2]А можно использовать более научную терминологию и обсуждать левые и правые идеалы в кватернионах; из возможности деления с остатком следует, что любой левый (или правый) идеал главный.

имеет нетривиальное решение в рациональных числах, если и только если разрешимо каждое из сравнений

$$t^2 \equiv bc \pmod{a},$$
$$t^2 \equiv ca \pmod{b},$$
$$t^2 \equiv -ab \pmod{c}.$$

Сам Лежандр доказывал эту теорему индукцией по коэффициентам (точнее, по параметру $I = \min(a,b,c)\max(a,b,c)$). Вы можете попробовать в качестве упражнения реконструировать его доказательство — это не очень сложно.

Доказательство. Пусть уравнение имеет нетривиальное решение. Тогда

$$0 = ax^2 + by^2 - cz^2 \equiv ax^2 + by^2 \equiv a^{-1}((ax)^2 + aby^2) \pmod{c},$$

поэтому $t = \dfrac{ax}{y} \mod c$ дает решение последнего из сравнений. Разрешимость остальных двух сравнений доказывается аналогично.

Доказательство в обратную сторону менее тривиально. Пусть p — какой-нибудь нечетный простой делитель числа c. Тогда имеем

$$ax^2 + by^2 - cz^2 \equiv ax^2 + by^2 \equiv a^{-1}((ax)^2 + aby^2) \pmod{p}.$$

В силу условия теоремы последнее сравнение имеет нетривиальное решение. Следовательно, нашу форму можно представить в виде произведения линейных форм по модулю p:

$$ax^2 + by^2 - cz^2 \equiv L_p(x,y,z)M_p(x,y,z) \pmod{p}.$$

(Хотя формы L_p и M_p можно выбрать вообще не зависящими от z, будем, тем не менее, записывать их как формы от всех трех аргументов.)

Аналогичные сравнения имеют место по модулю любого нечетного простого делителя чисел a, b, а также по модулю 2, поскольку по модулю 2 форма $ax^2 + by^2 - cz^2$ сравнима с $(ax + by - cz)^2$. Воспользуемся теперь китайской теоремой об остатках и найдем линейные формы L и M, для которых

$$L \equiv L_p \pmod{p},$$
$$M \equiv M_p \pmod{p}$$

при всех простых p, делящих одно из чисел a, b, c. Для этих форм имеем

$$ax^2 + by^2 - cz^2 \equiv L(x,y,z)M(x,y,z) \pmod{abc}.$$

Пусть теперь x, y, z пробегают значения $0 \leqslant x < \sqrt{bc}$, $0 \leqslant y < \sqrt{ac}$, $0 \leqslant z < \sqrt{ab}$. Если исключить из рассмотрения тривиальный случай

формы $x^2+y^2-z^2$, то троек чисел, удовлетворяющих таким неравенствам, строго больше, чем $\sqrt{bc}\sqrt{ac}\sqrt{ab}=abc$.

Это значит, что какие-то два из значений формы L в этих тройках чисел сравнимы по модулю abc. Вычитая эти значения, получаем, что для некоторых x, y, z с $|x|<\sqrt{bc}$, $|y|<\sqrt{ac}$, $|x|<\sqrt{ab}$ имеем $L(x,y,z)\equiv 0 \pmod{abc}$, а значит, и $ax^2+by^2-cz^2\equiv 0 \pmod{abc}$.

Из наших неравенств вытекает, что $-abc<ax^2+by^2-cz^2<2abc$, поэтому либо наша форма представляет нуль, либо она представляет abc. Осталось заметить, что если $ax^2+by^2-cz^2=abc$, то

$$a(xz+by)^2+b(yz-ax)^2-c(z^2+ab)^2=0. \qquad \square$$

Теорема Шевалле—Варнинга

Доказательство теоремы Лежандра может навести на мысль, что наличие нетривиальных рациональных решений уравнения

$$ax^2+by^2-cz^2=0$$

тесно связано с наличием решений по модулю простых делителей чисел a, b и c. Вообще говоря, разрешимость по простому модулю является более слабым условием. А именно, по простому модулю любая квадратичная форма от трех и более переменных (нетривиальным образом) представляет нуль, как показывает следующая теорема.

Теорема 5 (Шевалле—Варнинг). *Пусть p — простое число. Если $F(x_1,\ldots,x_n)$ — однородный многочлен степени $r<n$ с целыми коэффициентами, то число решений сравнения $F(x_1,\ldots,x_n)\equiv 0 \pmod{p}$ делится на p. В частности, последнее сравнение имеет нетривиальное решение по модулю p.*

Доказательство. Заметим, что число решений этого сравнения сравнимо с суммой

$$\sum_{x_1,\ldots,x_n=0}^{p-1}(1-F^{p-1}(x_1,\ldots,x_n))$$

(это сразу следует из малой теоремы Ферма). Докажем, что эта сумма делится на p для любого многочлена степени меньше чем $n(p-1)$. Достаточно проверить это для монома $x_1^{k_1}\ldots x_n^{k_n}$. Сумма значений этого монома по всем наборам из n вычетов равна

$$\left(\sum_{x_1=0}^{p-1}x_1^{k_1}\right)\ldots\left(\sum_{x_n=0}^{p-1}x_n^{k_n}\right).$$

Из соотношения на степень и число переменных следует, что хотя бы одно из чисел $k_1, \ldots, k_n$ меньше $p-1$. Если это число равно нулю, соответствующий сомножитель равен p (мы считаем, что $0^0 = 1$), если это число не равно нулю, то соответствующий сомножитель делится на p по задаче 8.

А раз количество решений делится на p и сравнение имеет одно тривиальное решение $x_1 = \ldots = x_n = 0$, оно имеет и нетривиальное решение. □

Задачи

Задача 13*. Придумайте обобщения других доказательств теоремы Ферма—Эйлера на случай четырех квадратов. (Предупреждение: эти обобщения во многих случаях неизвестны.)

Задача 14. Представляют ли нуль в поле рациональных чисел формы $3x^2 + 5y^2 - 7z^2$ и $3x^2 - 5y^2 - 7z^2$?

Задача 15. Опишите все рациональные числа, представимые формой $5x^2 - 7y^2$.

Задача 16. (а) Докажите, что если невырожденная квадратичная форма (для тех, кто не знает, что это такое: считайте, что форма есть сумма квадратов переменных с ненулевыми коэффициентами) над полем рациональных чисел представляет нуль нетривиальным образом, то она представляет вообще любое число.

(б) Докажите, что квадратичная форма $f(x_1, \ldots, x_n)$ представляет число a, если и только если форма $ax_0^2 - f$ представляет нуль.

Задача 17. Докажите, что последние n цифр десятичной записи совпадают (а) у чисел $5^{2^{n+1}}$ и 5^{2^n}; (б) у чисел $2^{16^{n+1}}$ и 2^{16^n}.

Лекция 3. *p*-адические числа и лемма Гензеля

Теорема Лежандра носит весьма глубокий характер и имеет далекие обобщения. Чтобы сформулировать эти обобщения, нам придется расширить область определения наших форм, используя не только рациональные, но и так называемые *p-адические числа*.

Здесь и далее буквой p всегда обозначается простое число. В разных разделах математики используются разные способы говорить о p-адических числах. Опишем два общепринятых способа.

Способ первый: пополнения. Рассмотрим на множестве рациональных чисел *p-адическое расстояние* $d_p(x, y) = \frac{1}{p^n}$, где p^n — максимальная степень p, на которую делится числитель несократимой дроби для $x - y$ (если p входит в знаменатель, то степень отрицательна; если $x = y$, то $d_p(x, y) = 0$).

Легко проверить, что это действительно расстояние, т. е. выполнено неравенство треугольника. Множество p-адических чисел $\mathbb{Q}_p$ — это *пополнение* множества рациональных чисел относительно этого расстояния (мы добавляем пределы всех фундаментальных последовательностей), подобно тому, как множество действительных чисел — пополнение относительно обычного расстояния. Число $d_p(a, 0)$ обычно обозначают $\|a\|_p$ и называют p-адической нормой числа a. Эта норма (на всех p-адических числах) обладает следующими свойствами:

- $\|a+b\|_p \leqslant \max(\|a\|_p, \|b\|_p)$ (усиленное неравенство треугольника),
- $\|ab\|_p = \|a\|_p \cdot \|b\|_p$ (мультипликативность).

Можно доказать (мы этого делать не будем), что никаких других норм, согласованных с арифметическими операциями таким образом, на рациональных числах нет (теорема Островского).

Способ второй: бесконечные влево *p*-ичные записи. Мы рассматриваем числа в p-ичной записи, только в отличие от действительных чисел, где разрешаются бесконечные вправо дроби, мы разрешаем лишь конечное число знаков после запятой, но (возможно) бесконечное число знаков до запятой (знака «минус» не бывает). С такими числами можно производить все стандартные арифметические действия (просто «в столбик»). Например, для 2-адических чисел $\ldots111 + 1 = 0$ (т. е. $-1 = \ldots111$), $\ldots111 \cdot 1{,}1 = \ldots11110{,}1$.

Легко понять, что указанные два способа дают одно и то же: оба они добавляют к рациональным числам все (формальные) суммы ря-

дов вида $\sum_{k=k_0}^{+\infty} a_k p^k$ с целыми a_k. Несомненно достоинство второго способа, который позволяет явно строить p-адические числа — цифру за цифрой. Мы будем использовать этот прием для построения решений уравнений в p-адических числах.

Легко понять, как p-адические норма и расстояние продолжаются с рациональных чисел на p-адические. В первом случае это естественно следует из общих свойств пополнения, во втором — из того, что понятие максимальной степени p, на которую делится p-адическое число, легко определить для бесконечных влево чисел (и далее мы будем много раз использовать сравнения для p-адических чисел).

Множество всех p-адических чисел, у которых нет знаков после запятой, называется множеством *целых p-адических чисел* и обозначается через $\mathbb{Z}_p$.

Замечание. Множество $\mathbb{Z}_p$ с топологией, которую задает p-адическое расстояние, гомеоморфно так называемому *канторову множеству*, которое некоторым из слушателей курса знакомо по лекциям А. А. Кириллова на этой школе[1]. Фрактальная природа $\mathbb{Z}_p$ довольно ясна и без явного описания гомеоморфизма.

Покажем, как можно работать с p-адическими числами — используя описанный выше прием выписывания решения цифра за цифрой.

Пример 1. Докажем, что сравнение $x^2 \equiv 2 \pmod{7^k}$ имеет решение при любом натуральном k. Более того, мы проверим, что для всякого решения такого сравнения есть число y, сравнимое с x по модулю 7^k, для которого $y^2 \equiv 2 \pmod{7^{k+1}}$.

Таким образом, последовательность этих решений будет сходиться к некоторому 7-адическому числу. Разумеется, квадрат этого числа будет равен 2, т. е. мы докажем, что в $\mathbb{Z}_7$ существует $\sqrt{2}$.

Как скорректировать решение (получить y из x)? Будем искать его в виде $y = x + 7^k a$. Заметим, что

$$y^2 = x^2 + 2ax \cdot 7^k + 7^{2k} a^2 \equiv x^2 + 2ax \cdot 7^k \pmod{7^{k+1}}.$$

Таким образом, сравнение $y^2 \equiv 1 \pmod{7^{k+1}}$ эквивалентно сравнению $\frac{x^2-2}{7^k} + 2ax \equiv 0 \pmod 7$. Это сравнение с неизвестным a, очевидно, имеет решение по модулю 7.

Пример 2. Докажем, что целое p-адическое число a, последняя цифра которого не равна нулю, имеет обратное по умножению в $\mathbb{Z}_p$. Для этого проверим, что для решения сравнения $ax \equiv 1 \pmod{p^k}$ най-

[1]По мотивам этого курса опубликована брошюра А. А. Кириллова «Повесть о двух фракталах» (М.: МЦНМО, 2010).

дется такое $y \in \mathbb{Z}_p$, что $y \equiv x \pmod{p^k}$ и $ay \equiv 1 \pmod{p^{k+1}}$. Как и выше, ищем такое y в виде $y = x + cp^k$. Имеем $ay = ax + acp^k$, и для наших целей нужно, чтобы $\dfrac{ax-1}{p^k} + ac \equiv 0 \pmod{p}$. Последнее сравнение в силу наших предположений имеет решение.

Примеры выше обобщает следующий результат, который приводит к эффективным алгоритмам построения решений p-адических уравнений.

Теорема 6 (Лемма Гензеля). *Пусть $f(x)$ — многочлен с целыми p-адическими коэффициентами. Предположим, что $a \in \mathbb{Z}_p$ таково, что $f(a) \equiv 0 \pmod{p^n}$, и $\|f'(a)\|_p = p^{-k}$ для некоторого $k < \dfrac{n}{2}$. Тогда существует $b \in \mathbb{Z}_p$, сравнимое с a по модулю p^{n-k}, для которого $\|f'(b)\|_p = p^{-k}$ и $f(b) \equiv 0 \pmod{p^{n+1}}$.*

Доказательство. Будем искать b в виде $a + p^{n-k}c$, где $c \in \mathbb{Z}_p$. По формуле Тейлора[1]

$$f(b) = f(a) + p^{n-k}f'(a)c + p^{2n-2k}d,$$

где $\|d\|_p \leqslant 1$. По нашему предположению $f(a) = p^n A$, $f'(a) = p^k B$, где A — целое, а B — обратимое целое. Это позволяет выбрать c таким образом, чтобы $A + cB$ делилось на p. Тогда $f(b)$ делится на p^{n+1}, поскольку $2n - 2k \geqslant n + 1$. При этом $f'(b) \equiv p^k B \pmod{p^{n-k}}$, и потому $\|f'(b)\|_p = p^{-k}$ (раз $n - k > k$). □

Следствие 1. *В предположениях леммы Гензеля в $\mathbb{Z}_p$ существует решение уравнения $f(x) = 0$.*

Доказательство. Действительно, начнем с начального приближения и будем повторять шаг леммы Гензеля (это возможно, поскольку делимость производной на p не ухудшается). Мы получим последовательность целых чисел, которая сходится, так как фундаментальна относительно p-адического расстояния. □

Можно заметить, что при доказательстве леммы приближения к решению строятся в точности по *методу Ньютона*: $x_{(n+1)} = x_{(n)} - \dfrac{f(x_{(n)})}{f'(x_{(n)})}$.

Следствие 2. *Пусть $f(x_1, x_2, \ldots, x_m)$ — многочлен с целыми p-адическими коэффициентами. Предположим, что $a_1, \ldots, a_m \in \mathbb{Z}_p$, причем*

[1]Обычно формулу Тейлора пишут с коэффициентами $\dfrac{f^{(l)}(a)}{l!}$, что заставляет беспокоиться о степенях p в знаменателе. Это беспокойство напрасно; коэффициенты являются целыми p-адическими числами: они ведь просто-напросто описывают переразложение многочлена с целыми коэффициентами в точке a.

$\|f(a_1, \ldots, a_m)\|_p \leqslant p^{-n}$, *и*

$$\left\| \frac{\partial f}{\partial x_j}(a_1, \ldots, a_m) \right\|_p = p^{-k}$$

для некоторого j *и некоторого* $k < \frac{n}{2}$. *Тогда существуют* $b_1, \ldots, b_m \in \mathbb{Z}_p$, *сравнимые с* $a_1, \ldots, a_m$ *по модулю* p^{n-k}, *для которых* $f(b_1, \ldots, b_m) = 0$.

Доказательство. Действительно, для $m = 1$ это уже доказано. Для $m > 1$ заморозим все координаты, кроме j-й, и применим результат для $m = 1$. □

Следствие 3. *Любой простой (не обнуляющий хотя бы одну из частных производных) нуль по модулю* p *многочлена с целыми* p*-адическими коэффициентами поднимается до целого* p*-адического нуля этого многочлена.*

Следствие 4. 1) *Пусть* $p \neq 2$. *Для того чтобы* $a \in \mathbb{Z}_p$, *где* $\|a\|_p = k$, *было квадратом другого* p*-адического числа, необходимо и достаточно, чтобы* k *было четно и* $\frac{a}{p^k}$ *было сравнимо с квадратичным вычетом по модулю* p.

2) *Пусть* $p = 2$. *Для того чтобы* $a \in \mathbb{Z}_2$ *с* $\|a\|_2 = k$ *было квадратом, необходимо и достаточно, чтобы* k *было четно и* $\frac{a}{2^k}$ *было сравнимо с* 1 *по модулю* 8.

Замечание. Из последнего следствия вытекает, что с точностью до умножения на квадраты любое p-адическое число равно

• $1, \varepsilon, p, \varepsilon p$ (где ε — произвольный фиксированный квадратичный невычет по модулю p) для нечетного p;

• $\pm 1, \pm 2, \pm 5, \pm 10$ для $p = 2$.

Следствие 5. *Пусть* $\sum_{i,j} a_{ij} x_i x_j$ — *квадратичная форма с целыми* p*-адическими коэффициентами. Предположим, что определитель матрицы этой формы обратим в* $\mathbb{Z}_p$.

1) *При* $p \neq 2$ *всякое примитивное*[1] *решение сравнения*

$$\sum_{i,j} a_{ij} x_i x_j \equiv 0 \pmod{p}$$

можно поднять до целого p*-адического решения.*

2) *При* $p = 2$ *всякое примитивное решение сравнения*

$$\sum_{i,j} a_{ij} x_i x_j \equiv 0 \pmod{8}$$

можно поднять до целого 2*-адического решения.*

[1] Т. е. не имеющее общих делителей.

Доказательство следствия всякий, кто знает линейную алгебру, легко воспроизведет самостоятельно; тем же, кто линейную алгебру не изучал, мы предлагаем в это поверить.

Контрольный вопрос[1]: заметим, что каждое из чисел 1, 3, 5, 7 является квадратным корнем из 1 по модулю 8. Казалось бы, лемма Гензеля позволит поднять эти корни до квадратных корней из 1 в $\mathbb{Z}_2$. С другой стороны, уравнение $x^2 = 1$ над полем $\mathbb{Q}_2$ имеет два решения. Нет ли тут противоречия?

[1]Автор признателен Александру Шамову, который задал этот вопрос на занятии.

Лекция 4. Квадратичные формы над $\mathbb{Q}_p$

Применим полученные результаты, чтобы выяснить, какие квадратичные формы представляют (нетривиальным образом) нуль над p-адическими числами. Для этого мы выберем координаты, в которых форма записывается в виде суммы квадратов (с p-адическими коэффициентами). Это можно сделать стандартным образом («выделение полного квадрата»).

Следствие 4 из предыдущего раздела, описывающее квадраты в $\mathbb{Q}_p$, решает вопрос о представимости нуля формами от двух переменных. Естественный следующий шаг — формы от трех переменных.

Определение. Пусть $a, b \in \mathbb{Q}_p$. Обозначим через $f(x, y, z)$ квадратичную форму $z^2 - ax^2 - by^2$. Положим

$$(a, b)_p = \begin{cases} 1, & \text{если } f \text{ представляет нуль,} \\ -1 & \text{в противном случае.} \end{cases}$$

Число $(a, b)_p$ называется *символом Гильберта* a и b.

Мы вычислим символ Гильберта для любых двух элементов $\mathbb{Q}_p$, но начнем с вывода его простейших свойств.

Предложение 3. *Имеют место равенства*

1) $(a, b)_p = (b, a)_p$, $(a, c^2)_p = 1$, $(a, bc^2)_p = (a, b)_p$;

2) $(a, -a)_p = 1$, $(a, 1-a)_p = 1$;

3) *если* $(a, b)_p = 1$, *то* $(aa', b)_p = (a', b)_p$;

4) $(a, -ab)_p = (a, b)_p = (a, (1-a)b)_p$.

Доказательство. Несколько нетривиально только третье утверждение. Если b — квадрат, то утверждение очевидно. Пусть b не квадрат, и уравнение $z^2 - ax^2 - by^2 = 0$ имеет нетривиальное решение. Тогда для этого решения $x \neq 0$ и имеет решение уравнение $t^2 - bs^2 = a$. Аналогично, наличие решений у уравнения $z^2 - (aa')x^2 - by^2 = 0$ эквивалентно наличию решений уравнения $t^2 - bs^2 = aa'$. Осталось воспользоваться тем, что произведение и частное чисел вида $u^2 - bv^2$ — тоже числа такого вида (упражнение: докажите это). □

Теорема 7. 1) *Пусть* p *нечетно,* $a = p^k u$, $b = p^l v$, *где* $\|u\|_p = \|v\|_p = 1$. *Тогда*

$$(a, b)_p = (-1)^{kl\frac{p-1}{2}} \left(\frac{u}{p}\right)^l \left(\frac{v}{p}\right)^k.$$

2) *Пусть* $p=2$. *Запишем* $a=2^k u$, $b=2^k v$, *где* $\|u\|_2=\|v\|_2=1$. *Тогда*[1]

$$(a,b)_2=(-1)^{\frac{u-1}{2}\frac{v-1}{2}+k\frac{v^2-1}{8}+l\frac{u^2-1}{8}}.$$

Доказательство. Мы докажем все для нечетного простого, оставляя случай $p=2$ в качестве упражнения (указание: если ничего не приходит в голову, надо заняться перебором, ведь мы знаем все 2-адические числа с точностью до умножения на квадраты).

Ясно, что можно заменить k и l их остатками по модулю 2. Рассмотрим возможные случаи.

Случай $k=l=0$ мы обсуждали в лекции 2 в связи с теоремами Лежандра и Шевалле—Варнинга. Соответствующее сравнение по модулю p имеет нетривиальное решение, и следствие леммы Гензеля гарантирует нам существование решения.

Случай $k=1$, $l=0$. Надо проверить, что $(pu,v)_p=\left(\frac{v}{p}\right)$. Поскольку $(u,v)_p=1$, достаточно доказать, что $(p,v)_p=\left(\frac{v}{p}\right)$. Если v — квадрат, то обе части равны 1. В противном случае у уравнения не может быть решения, поскольку его можно было бы выбрать примитивным и получить решение по модулю p.

Случай $k=l=1$. Надо проверить, что

$$(pu,pv)_p=(-1)^{\frac{p-1}{2}}\left(\frac{u}{p}\right)\left(\frac{v}{p}\right),$$

то есть $(pu,pv)_p=\left(\frac{-uv}{p}\right)$. Но $(pu,pv)_p=(pu,-pupv)_p=(pu,-uv)_p$, и осталось использовать только что доказанный результат. □

Следствие 6. $(aa',b)_p=(a,b)_p(a',b)_p$.

Для вещественных чисел a и b положим символ Гильберта $(a,b)_\infty$ равным ±1 в зависимости от того, представляет ли форма $z^2-ax^2-by^2$ нуль над $\mathbb{R}$.

Доказанная во второй лекции теорема Лежандра утверждает фактически, что форма $ax^2+by^2+cz^2$ представляет нуль над рациональными числами тогда и только тогда, когда она представляет нуль над всеми $\mathbb{Q}_p$ (включая $\mathbb{R}:=\mathbb{Q}_\infty$).

В частности, форма $z^2-ax^2-by^2$ представляет нуль над рациональными числами тогда и только тогда, когда все символы Гильберта $(a,b)_p$ равны единице.

[1] Вместо $\frac{u-1}{2}$, $\frac{u^2-1}{8}$, $\left(\frac{u}{p}\right)$ аккуратный читатель должен подставить эти числа по модулю 2.

Предложение 4 (закон взаимности для символа Гильберта). *Для рациональных a, b имеет место формула*[1]

$$\prod_{p \text{ простое или } \infty} (a,b)_p = 1.$$

Доказательство. В силу предыдущего следствия, достаточно доказать это равенство, когда каждое из чисел a и b равно простому числу или -1. Для таких чисел это легко выводится из свойств символа Лежандра. Например, если p и q — нечетные простые, то $(p,q)_r = 1$ при $r \notin \{2, p, q\}$, а

$$(p,q)_p = \left(\frac{q}{p}\right), \quad (p,q)_q = \left(\frac{p}{q}\right), \quad (p,q)_2 = (-1)^{\frac{p-1}{2}\frac{q-1}{2}},$$

и закон взаимности в этом случае оказывается равносилен квадратичному закону взаимности в его обычной формулировке. □

Следствие 7. *Пусть $a, b \in \mathbb{Q}$. Если квадратичная форма*

$$z^2 - ax^2 - by^2$$

представляет нуль над всеми полями $\mathbb{Q}_p$ (включая $\mathbb{R} = \mathbb{Q}_\infty$), кроме $\mathbb{Q}_q$, то она представляет нуль и над $\mathbb{Q}_q$ (а значит, представляет нуль и над $\mathbb{Q}$).

Действительно, недостающий символ Гильберта можно вычислить с помощью закона взаимности.

Определение. Пусть квадратичная форма f над $\mathbb{Q}_p$ записана в виде суммы квадратов

$$f(x_1, \ldots, x_n) = \sum_i a_i x_i^2.$$

Сопоставим этой форме два числа: *дискриминант* $d(f) = a_1 a_2 \ldots a_n$ и *инвариант Хассе* $\varepsilon(f) = \prod_{i<j} (a_i, a_j)_p$

Знакомые с линейной алгеброй легко докажут следующее предложение.

Предложение 5. *Инвариант Хассе — действительно инвариант, то есть не изменяется при переходе к другой системе координат. Дискриминант инвариантен с точностью до умножения на ненулевые квадраты.*

Инвариант Хассе используется для того, чтобы выяснять, представляет ли форма нуль.

[1] В этом бесконечном произведении все сомножители, кроме конечного числа, равны 1, и потому оно имеет смысл.

Теорема 8. *Форма f от n переменных над $\mathbb{Q}_p$ с $d(f)\neq 0$ представляет нуль, если и только если выполнено одно из условий*:

1) $n=2$ *и* $d(f)$ *равно* -1 *с точностью до умножения на квадраты*;

2) $n=3$ *и инвариант Хассе* $\varepsilon(f)$ *равен* $(-1,-d(f))_p$;

3) $n=4$ *и либо* d *не квадрат, либо* d *квадрат и инвариант Хассе* $\varepsilon(f)$ *равен* $(-1,-1)_p$;

4) $n\geqslant 5$.

Эту теорему мы не будем доказывать. На самом деле она доказывается довольно несложно, и читатели, которые считают, что разобрались в том, что уже доказано, могут попробовать доказать ее в качестве упражнения. (Например, при $n\geqslant 5$ и нечетном p надо заметить, что из коэффициентов формы, записанной в диагональном виде $\sum\limits_i a_i x_i^2$, либо не менее трех делятся на p, либо не менее трех не делятся на p, и далее использовать, что форма от трех переменных, коэффициенты которой не делятся на p, представляет нуль.)

Следствие 8. *Форма f от n переменных над $\mathbb{Q}_p$ с $d(f)\neq 0$ представляет $a\in\mathbb{Q}_p$, если и только если выполнено одно из условий*:

1) $n=1$ *и* $d(f)$ *равно* a *с точностью до умножения на квадраты*;

2) $n=2$ *и инвариант Хассе* $\varepsilon(f)$ *равен* $(a,-d(f))_p$;

3) $n=3$ *и либо* $-\dfrac{a}{d}$ *не квадрат, либо* $-\dfrac{a}{d}$ *квадрат и инвариант Хассе* $\varepsilon(f)$ *равен* $(-1,-d(f))_p$;

4) $n\geqslant 4$.

Теорема Минковского—Хассе

Следующая теорема является одним из красивейших и важнейших результатов теории рациональных квадратичных форм.

Теорема 9 (Минковского—Хассе). *Квадратичная форма от n переменных с рациональными коэффициентами представляет нуль над $\mathbb{Q}$, если и только если она представляет нуль над $\mathbb{R}$ и над всеми $\mathbb{Q}_p$.*

Следствие 9. *Квадратичная форма с рациональными коэффициентами представляет рациональное число a, если и только если она представляет его над $\mathbb{R}$ и над всеми $\mathbb{Q}_p$.*

Выведем из теоремы Минковского—Хассе теорему 2 о трех квадратах. Согласно задаче 12*, достаточно выяснить, какие числа представимы над $\mathbb{Q}$. Над $\mathbb{Q}_p$ с нечетным p сумма трех квадратов представляет нуль (разрешимость сравнения плюс лемма Гензеля), и потому представляет любое число. Представимость над $\mathbb{R}$ дает условие положительности. Осталось выяснить, какое условие дает представимость над $\mathbb{Q}_2$. У формы $x^2+y^2+z^2-nt^2$ дискриминант $-n$ и инвариант Хассе -1. Таким образом, n не представимо, если и только если $-n$ является

квадратом в $\mathbb{Z}_2$, то есть $-n = 2^{2a}(8b+1)$, что эквивалентно условию, сформулированному в теореме о трех квадратах.

Перейдем теперь к доказательству теоремы Минковского—Хассе. Необходимость очевидна, будем доказывать достаточность.

Случай $n = 2$ тривиален: можно считать, что форма имеет вид $x^2 - dy^2$, и тогда представимость нуля над $\mathbb{Q}_p$ означает, что p входит в d в четной степени, а представимость над $\mathbb{R}$ — положительность d, что и требовалось.

Случай $n = 3$ следует, как мы уже говорили, из теоремы Лежандра. Мы не будем обсуждать подробности; это совсем не трудно.

Случай $n = 4$ наиболее нетривиальный и красивый. Будем считать, что наша форма имеет вид

$$a_1x_1^2 + a_2x_2^2 + a_3x_3^2 + a_4x_4^2,$$

где a_i — целые и свободные от квадратов, причем $a_1 > 0$, $a_4 < 0$. Мы докажем, что найдется ненулевое целое число, которое представимо и формой $a_1x_1^2 + a_2x_2^2$, и формой $-a_3x_3^2 - a_4x_4^2$. Это немедленно докажет, что наша форма представляет нуль.

Пусть $p_1, \ldots, p_r$ — все простые делители чисел a_i. Для каждого $p = 2, p_1, \ldots, p_r$ выберем представление нуля

$$a_1\xi_1^2 + \ldots + a_4\xi_4^2 = 0$$

в $\mathbb{Z}_p$, в котором все координаты не равны нулю (почему так можно сделать?), и положим

$$b_p = a_1\xi_1^2 + a_2\xi_2^2 = -a_3\xi_3^2 - a_4\xi_4^2.$$

Можно считать, что $b_p \neq 0$ и даже $b_p \neq 0 \pmod{p^2}$ (почему?). Рассмотрим систему сравнений

$$\begin{cases} a \equiv b_2 \pmod{16}, \\ a \equiv b_{p_1} \pmod{p_1^2}, \\ \ldots\ldots\ldots\ldots\ldots \\ a \equiv b_{p_r} \pmod{p_r^2}. \end{cases}$$

Такое число a определено однозначно по модулю $m = 16p_1^2 \ldots p_r^2$. Поскольку b_{p_i} делится на p_i в не более чем первой степени, $\frac{b_{p_i}}{a}$ — обратимое целое p_i-адическое число (оно даже сравнимо с 1 по модулю p). Аналогично, $\frac{b_2}{a}$ обратимо в $\mathbb{Z}_2$ и сравнимо с 1 по модулю 8. Значит, $\frac{b_p}{a}$ является квадратом в $\mathbb{Q}_p$ при всех рассматриваемых p.

Таким образом, представимость b_p и представимость a над $\mathbb{Q}_p$ каждой из двух форм при таких p равносильны. Для p, не делящих a, представимость a над $\mathbb{Q}_p$ получается автоматически. Поэтому для представимости a над $\mathbb{Q}$ достаточно показать представимость над $\mathbb{Q}_p$ при p, делящих a. Если бы существовало ровно одно такое p, то закон взаимности для символа Гильберта показал бы нам, что в этом случае a тоже представимо. Как это гарантировать?

Рассмотрим прогрессию $\frac{a+mn}{\text{НОД}(a,m)}$. По теореме Дирихле в ней найдется простое число q. Значит, $a' = q \cdot \text{НОД}(a,m)$, сравнимое с a по модулю m, имеет кроме простых делителей p_i только один простой делитель, что и требовалось.

Случай $n \geqslant 5$. Достаточно, очевидно, доказать нашу теорему в случае $n = 5$. Рассмотрим форму

$$a_1x_1^2 + a_2x_2^2 + a_3x_3^2 + a_4x_4^2 + a_5x_5^2,$$

где, как и выше, мы считаем, что a_i — целые и свободные от квадратов, причем $a_1 > 0$, $a_5 < 0$. Аналогично доказанному выше, мы с помощью теоремы Дирихле получим, что существует нечетное простое число q, не делящее a_i, и целое не равное нулю число a, которое представимо каждой из форм $a_1x_1^2 + a_2x_2^2$ и $-a_3x_3^2 - a_4x_4^2 - a_5x_5^2$ над всеми $\mathbb{Q}_p$, кроме, возможно, $\mathbb{Q}_q$.

Докажем, что обе эти формы представляют a и над $\mathbb{Q}_q$. Действительно, для первой формы это доказывается так же, как и выше. Вторая же форма представляет нуль (теорема Шевалле—Варнинга плюс подъем решений) и потому представляет вообще все числа. Значит, эти формы представляют a и над $\mathbb{Q}$ (в них меньше переменных, и для таких форм все уже доказано). Отсюда следует, что наша форма представляет нуль. □

Необходимые предварительные сведения

В этом разделе собраны важные факты арифметики, существенные для понимания этого курса. Многие из этих утверждений несложно доказываются и почти наверняка знакомы читателям брошюры.

Основная теорема арифметики. Любое целое положительное число раскладывается в произведение простых сомножителей единственным образом (с точностью до перестановки сомножителей). Эквивалентно (почему?), если произведение двух сомножителей делится на простое число p, то хотя бы один из них делится на p.

Малая теорема Ферма. Для любого целого числа a и простого числа p имеем

$$a^p \equiv a \pmod{p}.$$

Эквивалентно, для целого числа a, не делящегося на p, имеем $a^{p-1} \equiv \equiv 1 \pmod{p}$.

Теорема Вильсона. Для простого числа p имеем

$$(p-1)! \equiv -1 \pmod{p}.$$

Теорема Безу. Многочлен степени n с целыми коэффициентами, не все из которых делятся на простое число p, имеет по модулю p не более n корней.

Китайская теорема об остатках. Пусть $d_1, \ldots, d_n$ — попарно взаимно простые целые числа. Тогда существует решение системы сравнений

$$\begin{cases} x \equiv a_1 \pmod{d_1}, \\ x \equiv a_2 \pmod{d_2}, \\ \ldots\ldots\ldots\ldots \\ x \equiv a_n \pmod{d_n}. \end{cases}$$

Эта система равносильна сравнению по модулю $d_1 \cdot \ldots \cdot d_n$.

Символ Лежандра

Определение. Остаток по модулю p называется *квадратичным вычетом*, если он сравним с квадратом по модулю p, и *квадратичным*

невычетом в противном случае. *Символ Лежандра* определяется так:

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

Свойства символа Лежандра. Следующие свойства символа Лежандра надо воспринимать как обязательное упражнение, если вы их не знали заранее.

- $\sum\limits_{a=0}^{p-1}\left(\frac{a}{p}\right)=0$, или, иначе говоря, квадратичных невычетов по модулю p столько же, сколько и вычетов.
- $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)=\left(\frac{ab}{p}\right)$.
- $\left(\frac{a}{p}\right)\equiv a^{\frac{p-1}{2}} \pmod p$.

Один из наиболее красивых фактов классической теории чисел — квадратичный закон взаимности. Мы будем его использовать в качестве «черного ящика».

Квадратичный закон взаимности. Для нечетных простых p и q

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

для $q=2$ и нечетного простого p

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

Интересующиеся могут попробовать доказать его самостоятельно (Гаусс, например, придумал чуть ли не десяток доказательств!) или прочитать доказательство в какой-либо книжке. Одно из моих любимых доказательств можно узнать из статьи В. В. Прасолова «Доказательство квадратичного закона взаимности по Золотареву», опубликованной в выпуске 4 сборника «Математическое просвещение» (М.: МЦНМО, 2000).

Содержание