АРИФМЕТИКА КВАДРАТИЧНЫХ ФОРМ

ВЛАДИМИР ДОЦЕНКО

Введение

Этот текст содержит записки лекций курса, 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, но интересующийся читатель найдёт их, а также многие другие замечательные теоремы, в любой из следующих книг:

1) З. И. Боревич, И. Р. Шафаревич. Теория чисел.
2) Дж. Касселс. Рациональные квадратичные формы.
3) Ж.–П. Серр. Курс арифметики.

Лекция 1

Суммы двух квадратов

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

Теорема 1 (Теорема 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 каждый простой делитель p числа n, дающий остаток 3 при делении на 4, входил в разложение n на простые множители в нечётной степени.*

Доказательство этой теоремы состоит из нескольких частей. Две из них совсем просты, и доказательства тут стандартны. Доказательство третьей же можно производить разными способами, некоторые из которых мы обсудим.

Шаг 1: почему другие числа не представимы? 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 нулём 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, и потому такой простой делитель не может входить в разложение n в нечётной степени.

Шаг 2: достаточно выяснять для простых чисел. Легко видеть, что

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

и потому произведение представимых чисел представимо. (Использованное равенство отражает тот известный факт, что модуль произведения двух комплексных чисел равен произведению модулей.)

Шаг 3: любое простое число вида $4k+1$ представимо. Доказательство на этом шаге можно проводить многими разными способами. Большинство из них используют следующий промежуточный шаг: для простого числа $p=4k+1$ найдутся такие x и y, не делящиеся на p, что x^2+y^2 *делится на* p. Это доказательство проще всего произвести с использованием теоремы 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.

Наиболее непосредственно следствие теоремы Вильсона используется в первом нашем доказательстве (не первом хронологически!).

Шаг 3 по Лагранжу.Возьмём такое r, что r^2+1 делится на p. Рассмотрим все пары (a,b) с $0\le a,b\le[\sqrt{p}]$, 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, $A^2+B^2=p$.

Следующее доказательство принадлежит Эйлеру, который хотел реализовать идею Ферма с «принципом спуска».

Шаг 3 по Эйлеру [и 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 $mp=x^2+y^2\le\frac{p^2}{4}+\frac{p^2}{4}=\frac{p^2}{2}$, откуда $m\le\frac{p}{2}<p$. 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, $t\le m/2<m$. При этом $t\ne0$, 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 $xv - yu \equiv 0 \equiv xu + yv \pmod{m}$ 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.

Следующее доказательство могло бы принадлежать Гауссу. Во всяком случае, оно использует «целые гауссовы числа» $a+bi$, где $i^2 = -1$.

Шаг 3 «по Гауссу». Мы используем то, что целые гауссовы числа можно делить с остатком, и потому есть алгоритм Евклида для отыскания наибольшего общего делителя. Пусть x^2+y^2 делится на p (x, y не делятся на p). Найдём наибольший общий делитель d 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, поскольку x и y не делятся на p. При этом $|d|^2$ является делителем $|p|^2 = p^2$. Значит, $|d|^2 = p$, что и требовалось.

Следующее доказательство использует геометрию куда тоньше, чем предыдущее.

Шаг 3 по Минковскому: геометрия чисел. 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. Найдём наименьшее значение $ax^2 + 2bxy + cy^2$ при целых x, y. Пусть это значение равно m. Множество решений неравенства $ax^2 + 2bxy + cy^2 \le m$ является эллипсом. 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 $\frac{\pi m}{4(ac-b^2)} = \frac{\pi m}{4}$. Если бы эта площадь была бы больше 1, то мы бы легко получили противоречие (в квадрате $N \times N$ целых точек примерно столько же, какова его площадь...), так что $m \le \frac{4}{\pi}$, и потому $m = 1$.

Вернёмся теперь к следствию теоремы Вильсона. Мы знаем, что для $r = (2k)!$ число r^2+1 делится на p. Применим наше утверждение к $a = p$, $b = r$, $c = \frac{r^2+1}{p}$. Получаем, что для некоторых целых x и y имеем

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

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

Следующее доказательство, пожалуй, является наиболее загадочным и необъяснимым.

Шаг 3 по Дону Цагиру: инволюции. Рассмотрим уравнение $x^2 + 4yz = p$. Будем решать его в целых неотрицательных числах x, y, z. Положим

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

Оказывается, что J — преобразование множества решений нашего уравнения в себя. Действительно,

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

Оказывается (замечательным и неожиданным образом), что

$$J \circ J[(x,y,z)] = (x,y,z)$$

(как говорят, J является инволюцией). 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 $y - z \le x \le 2y$, то $y - (x-y+z) \le 2y - x \le 2y$, и

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

- если $2y < x$, 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 $p = 4k+1$). Множество решений конечно, так что в нём нечётное число элементов. С другой стороны, на этом множестве есть инволюция, переставляющая y и z. Раз число решений нечётно, у этой инволюции должна быть неподвижная точка. Для соответствующего решения $y = z$, и $p = x^2 + (2y)^2$. Доказательство завершено.

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

Задачи

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

2. Найдите число решений по модулю p уравнения $x^2+y^2=1$. (Указание. Это число равно сумме $\sum_{y=0}^{p-1}(1+\left(\dfrac{1-y^2}{p}\right))$.)

3. (**а**) Известно, что 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 какое-нибудь утверждение в том же духе, если заменить x^2+3y^2 на x^2+5y^2. (**в**) Докажите какое-нибудь утверждение в том же духе, если заменить x^2+3y^2 на x^2+xy+y^2.

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 Д. Цагира. (Автору эти доказательства неизвестны, но, скорее всего, это должно быть нетрудно.)

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

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

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.

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

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

9. Найдите число решений сравнения $x^3+y^3+z^3+t^3 \equiv 0 \pmod 7$. (Указание. Для всех четвёрок, которые не удовлетворяют сравнению, $(x^3+y^3+z^3+t^3)^6 \equiv 1 \pmod 7$.)

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 $F(x_1,\ldots,x_n) \equiv 0 \pmod p$ делится на p (и потому это сравнение имеет нетривиальное решение по модулю p).

11. (Продолжение) Придумайте однородный многочлен степени 3 от трёх переменных, который не представляет нуль по модулю 5 нетривиальным образом.

12.* Пусть $f(x_1,\ldots,x_n)=\sum_{i,j} a_{ij}x_ix_j$ — 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

$t_1, \dots, t_n$ найдутся целые $a_1, \dots, a_n$, такие что

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

Докажите, что если для целого числа k уравнение $f(x_1, \dots, x_n) = k$ 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 трёх квадратов

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

Теорема 2. *Целое положительное число представимо в виде суммы трёх квадратов если и только если оно* не *имеет вид* $4^a(8b+7)$ *с целыми неотрицательными* a *и* b.

Легко видеть, что числа $4^a(8b + 7)$ действительно не представимы, это делается с помощью вычислений по модулю 8. Все другие числа представимы, но доказательство этого 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 ещё 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»: недостаточно знать, какие простые числа представимы. Например, 3 и 5 представимы, а 15 — не представимо.

Суммы четырёх квадратов

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

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

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

Приведём для некоторых из доказательств теоремы о суммах двух квадратов аналогичные им доказательства теоремы о суммах четырёх квадратов. Прежде всего, заметим, что в случае этой теоремы Шаг 1 не нужен (мы доказываем, что все числа представимы!). Шаг 2, как мы указывали, удаётся произвести аналогично. В качестве варианта промежуточного шага мы докажем, что найдётся сумма четырёх квадратов, которая делится на p (а сами квадраты, как и раньше, не все делятся на p). На самом деле, мы даже докажем, что есть сумма трёх 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) — проверьте это сами. 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 чётно, то числа x, y, z, t можно разбить на пары одинаковой чётности. Можно считать, что x и y одинаковой чётности, а также z и t одинаковой чётности. В таком случае мы можем представить в виде суммы квадратов $\frac{m}{2}p$:

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

и мы произвели спуск к меньшему кратному.

Пусть теперь m нечётно. 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 $\frac{m}{2}$, мы имеем, что $a^2+b^2+c^2+d^2 < m^2$, 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 α, β, γ, δ получаются из следующей формулы произведения:

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

Из этих формул легко видеть, что числа α, β, γ, δ делятся на m. Поэтому pm_1 представимо в виде суммы четырёх квадратов, и $m_1 < m$, так что мы произвели спуск.

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

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

Кватернионы с целыми коэффициентами («липшицевы кватернионы», в терминологии Дж. Конвея) нельзя делить с остатком: в четырёхмерном кубе расстояние от центра до вершины равно ребру куба. Чтобы можно было делить с остатком, надо рассматривать кватернионы, у которых все коэффициенты целые, или все одновременно полуцелые («гурвицевы целые кватернионы» по Конвею). Для таких кватернионов можно говорить про (левый или правый[1]) 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. Это представление в виде суммы целых или полуцелых квадратов, и 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 целочисленным.

Теорема Лежандра

В этом разделе мы докажем следующую теорему.

Теорема 4 (Лежандр[2])**.** *Пусть a, b, c — попарно взаимно простые целые положительные числа, свободные от квадратов. Тогда уравнение $ax^2+by^2-cz^2=0$ имеет нетривиальное решение в рациональных числах если и только разрешима система сравнений*

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

Пусть p — какой-нибудь нечётный простой делитель числа c. Из предположений теоремы следует, что сравнение $ax^2+by^2-cz^2\equiv 0$

[1] А можно использовать более научную терминологию и обсуждать левые и правые идеалы в кватернионах; деление с остатком учит нас, что любой левый (или правый) идеал главный.

[2] Сам Лежандр доказывал свою теорему индукцией по параметру $I=\min(a,b,c)\max(a,b,c)$, корректируя постепенно квадратичную форму. Вы можете попробовать в качестве упражнения реконструировать его доказательство — это не очень сложно.

$(\mathrm{mod}\ p)$ имеет ненулевое решение, ведь

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

Это значит, что нашу форму можно представить в виде произведения линейных форм по модулю p:

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

Аналогичные сравнения имеют место по модулю любого нечётного 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 найдём линейные формы L и M, для которых

$$\begin{cases} L \equiv L_p & (\mathrm{mod}\ p), \\ M \equiv M_p & (\mathrm{mod}\ p) \end{cases}$$

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 $0 \le x < \sqrt{bc}$, $0 \le y < \sqrt{ac}$, $0 \le z < \sqrt{ab}$. Если исключить из рассмотрения тривиальный случай формы $x^2 + y^2 - z^2$, то троек чисел с этими условиями строго больше, чем $\sqrt{ab}\sqrt{bc}\sqrt{ac} = abc$. 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 $|x| < \sqrt{bc}$, $|y| < \sqrt{ac}$, $|z| < \sqrt{ab}$ имеем $ax^2 + by^2 - cz^2 \equiv 0 \pmod{abc}$. 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

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

Доказанную нами теорему можно переформулировать следующим образом[3].

Теорема 5 (Переформулировка теоремы Лежандра)**.** *Квадратичная форма $ax^2 + by^2 + cz^2$ с целыми попарно взаимно простыми коэффициентами представляет нуль над рациональными числами тогда и только тогда, когда она представляет нуль над вещественными числами и по любому простому модулю.*

Как мы видели, если простой модуль не содержится в множестве делителей a, b, c, то исходная теорема ничего не говорит о наличии решений. В действительности, по такому модулю нетривиальное представление нуля найдётся всегда. Это немедленно следует из теоремы Шевалле–Варнинга.

[3] Здесь и далее слова «представляет нуль» подразумевают наличие нетривиального решения у соответствующего уравнения.

Доказательство теоремы Шевалле–Варнинга. Мы докажем, что общее число решений сравнения делится на p, и потому из наличия тривиального решения сразу следует наличие нетривиальных. Заметим, что число решений этого сравнения сравнимо с суммой

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

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

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

Из соотношения на степень и число переменных следует, что хотя бы одно из чисел $k_1,\dots,k_n$ меньше $p-1$, и из задачи 8 следует, что соответствующий сомножитель делится на p.

Задачи

13.* Придумайте обобщения для случая четырёх квадратов других доказательств теоремы Ферма–Эйлера. (Предупреждение: эти обобщения, как правило, неизвестны.)

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

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

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) представляет нуль (как обычно, нетривиальным образом), то она представляет любое число вообще.

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

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

Лекция 3

Доказанная нами в прошлой лекции переформулировка теоремы Лежандра носит весьма глубокий характер и имеет далёкие обобщения. Для того, чтобы сформулировать это обобщение, нам придётся расширить область определения наших форм, используя не только рациональные, но и так называемые p-адические числа.

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 $d_p(x, y)$, которое определяется так: $d_p(x, y) = \frac{1}{p^n}$, 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* рациональных чисел относительно этого расстояния (мы добавляем пределы всех фундаментальных последовательностей), подобно тому, как множество действительных чисел — это 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:

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

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 числа. 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 действия, например (для 2-адических чисел):

$$\ldots 111 + 1 = 0,$$
$$\ldots 111 \cdot 11 = ..111101.$$

На самом деле, совсем легко понять, что указанные два способа дают одно и то же. Оба из них говорят, что ряды вида $\sum_{k=k_0}^{+\infty} a_k p^k$ с целыми a_k становятся сходящимися, и надо включить в рассмотрение и их тоже. Несомненно достоинство второго способа, который позволяет явно строить p-адические числа — цифру за цифрой. Мы будем использовать этот приём 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 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 $\mathbb{Z}_p$. Множество всех p-адических чисел обозначается через $\mathbb{Q}_p$.

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

Пример 1. Докажем, что сравнение $x^2 \equiv 2 \pmod{7^k}$ имеет решение при любом натуральном k. Более того, мы проверим, что для решения такого сравнения есть число y, сравнимое с x по модулю 7, для которого $y^2 \equiv 2 \pmod{7^{k+1}}$. Это будет означать, что последовательность этих решений сходится к некоторому 7-адическому число. Разумеется, квадрат этого числа будет равен 2, и $\sqrt{2}$ существует в $\mathbb{Z}_7$. 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 $y^2 \equiv 2 \pmod{7^{k+1}}$ 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 $ax \equiv 1 \pmod{p^k}$ найдётся 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 $\frac{ax-1}{p^k} + ac \equiv 0 \pmod p$. Последнее сравнение в силу наших предположений имеет решение.

Лемма Гензеля

В действительности, имеет место 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 $k < \frac{n}{2}$. Тогда существует $b \in \mathbb{Z}_p$, сравнимое с a по модулю p^{n-k}, для которого $\|f'(b)\|_p = p^{-k}$, а $f(b) \equiv 0 \pmod{p^{n+1}}$.*

Будем искать b в виде $a + p^{n-k}c$, где $c \in \mathbb{Z}_p$. По формуле Тейлора[4] имеем

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

где $\|d\|_p \leq 1$. 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 $2n - 2k \geq n + 1$. 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 $f(x) = 0$.*

Действительно, стартуем с начального приближения и будем итерировать шаг леммы Гензеля (это возможно, поскольку делимость производной на p не ухудшается). Мы получим последовательность целых чисел, фундаментальную относительно p-адического расстояния (и потому сходящуюся).

Следствие 2. *Пусть $f(x_1, x_2, \ldots, x_m)$ — многочлен с целыми p-адическими коэффициентами. Предположим, что $a_1, \ldots, a_m \in \mathbb{Z}_p$, причём $\|f(a_1, \ldots, a_m)\|_p \leq p^{-n}$, 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 $f(b_1, \ldots, b_m) = 0$.

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

[4] Обычно формулу Тейлора пишут с коэффициентами $\frac{f^{(l)}(a)}{l!}$, 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.

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, $a \in \mathbb{Z}_p$ с $\|a\|_p = k$, было квадратом другого p-адического числа, необходимо и достаточно, чтобы k было чётно, 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 чётно, $\frac{a}{2^k}$ было сравнимо с 1 по модулю 8.*

Замечание 2. С точностью до умножения на квадраты любое p-адическое число равно

- 1, ε, p, εp (ε — произвольный фиксированный невычет по модулю p) для нечётного p;
- ± 1, ± 2, ± 5, ± 10 для $p = 2$.

Следствие 5. *Пусть $\sum_{i,j} a_{ij}x_ix_j (a_{ij} \in \mathbb{Z}_p)$ — квадратичная форма. Предположим, что определитель матрицы этой формы обратим в $\mathbb{Z}_p$.*

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

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

можно поднять до целого p-адического решения.

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

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

можно поднять до целого 2-адического решения.

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

Контрольный вопрос.[5] 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?

[5]Автор признателен Александру Шамову, который озвучил этот вопрос на занятии.

Лекция 4

Квадратичные формы над $\mathbb{Q}_p$

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

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

Определение 1. 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 начнём с вывода его простейших свойств.

Предложение 1. *Имеют место равенства:*

1) $(a, b)_p = (b, a)_p$, $(a, c^2)_p = 1$;
2) $(a, -a)_p = 1$, $(a, 1 - a)_p = 1$;
3) *если* $(a, b)_p = 1$, *то* $(aa', b)_p = (a', b)_p$;
4) $(a, -ab)_p = (a, b)_p = (a, (1 - a)b)_p$.

Несколько нетривиально только третье утверждение. Если b — квадрат, то утверждение очевидно. Пусть b не квадрат, и $z^2 - ax^2 - by^2 = 0$ 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 $t^2 - bs^2 = aa'$. Теперь осталось использовать тот факт, что произведение и частное чисел вида $u^2 - bv^2$ — тоже числа такого вида (упражнение).

Теорема 7. *1) Пусть p нечётно. Запишем $a = p^k u$, $b = p^l v$, 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 $a = 2^k u$, $b = 2^l v$, где $\|u\|_2 = \|v\|_2 = 1$. Тогда

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

Здесь вместо $\frac{u-1}{2}$, $\frac{u^2-1}{8}$ *(а также и в* $\left(\frac{u}{p}\right)$*) аккуратный читатель должен подставить эти числа по модулю* 2.

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

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

Случай $k = l = 0$**.** Этот случай мы обсуждали в прошлой лекции в связи с теоремой Лагранжа. 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

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

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

Следствие 6. *Для всех* $a, a', b \in \mathbb{Q}_p$ *верно* $(aa', b)_p = (a, b)_p (a', b)_p$.

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

Предложение 2 (Закон взаимности для символа Гильберта)**.** *Для рациональных* a*,* b *имеет место формула*[6]

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

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 — нечётные простые, то $(p, q)_r = 1$ при

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

$r \notin \{2, p, q\}$, 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 $\mathbb{Q}_q$ (и потому представляет нуль над $\mathbb{Q}$).

Это следует из того, что недостающий символ Гильберта можно вычислить с помощью закона взаимности.

Определение 2. 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 3. *Инвариант Хассе действительно является инвариантом, т. е. один и тот же для разных систем координат. Дискриминант является инвариантом с точностью до умножения на ненулевые квадраты.*

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

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 $(-1, -d(f))_p = \varepsilon(f)$;*
3) *$n = 4$ и либо d — не квадрат, либо d — квадрат и $\varepsilon(f) = (-1,-1)_p$;*
4) *$n \geq 5$.*

Эту теорему мы не будем доказывать в данном курсе. На самом деле, она доказывается довольно нетрудно, и слушатели курса, которые считают, что разобрались в том, что уже доказано, могут попробовать доказать её в качестве упражнения. (Например, при $n \geq 5$ и нечётном p надо заметить, что из коэффициентов формы, записанной в диагональном виде $\sum_i a_i x_i^2$, либо не менее трёх делящихся на p, либо не менее трёх не делящихся на p, и далее использовать, что форма от трёх 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 $(a, -d(f))_p = \varepsilon(f)$;
3) $n = 3$ и либо $-\frac{a}{d}$ — не квадрат, либо $-\frac{a}{d}$ — квадрат и $(-1, -d(f))_p = \varepsilon(f)$;
4) $n \geq 4$.

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

Теорема 9 (Теорема 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 о трёх квадратах. Согласно задаче 12, достаточно выяснить, какие числа представимы над $\mathbb{Q}$. Над $\mathbb{Q}_p$ с нечётным p сумма трёх квадратов представляет нуль (разрешимость сравнения плюс лемма Гензеля), и потому представляет любое число. Представимость над $\mathbb{R}$ даёт условие положительности. Осталось выяснить, какое условие даёт 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 $\mathbb{Z}_2$, т. е. $-n = 2^{2a}(8b + 1)$, что эквивалентно условию, сформулированному в теореме о трёх квадратах.

Доказательство теоремы Минковского–Хассе

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

Случай $n = 3$ даётся теоремой Лежандра. Мы не будем обсуждать подробности; это совсем нетрудно.

Случай $n = 4$ наиболее нетривиальный и наиболее 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, причём $a_1 > 0$, $a_4 < 0$. Мы докажем, что найдётся 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 $b_p \not\equiv 0 \pmod{p^2}$ (почему?). Рассмотрим систему сравнений

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

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? На этот вопрос даёт ответ теорема Дирихле о простых в арифметической прогрессии. В самом деле, рассмотрим прогрессию $\frac{a+mn}{\text{НОД}(a,m)}$. В ней найдётся простое число q. Значит, $a' = q\,\text{НОД}(a, m)$, сравнимое с a по модулю m, имеет кроме простых делителей p_i только один простой делитель, что и требовалось.

Случай $n \geq 5$. 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, причём $a_1 > 0$, $a_5 < 0$. Аналогично доказанному выше, мы с помощью теоремы Дирихле получим, что существует нечётное простое число q, не делящее a_i, и целое не равное нулю число a, такое что a 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 подъём решений) и потому представляет вообще все числа. Значит, эти формы представляют a и над $\mathbb{Q}$ (в них меньше переменных, и для таких форм всё 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 слушателям курса.

1. (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.

2. (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 $a^{p-1} \equiv 1 \pmod{p}$.

3. (Теорема Вильсона) Для простого числа p имеем $(p-1)! \equiv -1 \pmod{p}$.

4. (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.

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

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

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

Определение 3. Остаток по модулю p называется *квадратичным вычетом*, если он сравним с квадратом по модулю p, и *квадратичным невычетом* в противном случае. *Символ Лежандра* $\left(\dfrac{a}{p}\right)$ определяется так:

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

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

6.

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

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

7. (Квадратичный закон взаимности) Для нечётных простых p и q имеем

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

8. (Символ Лежандра для $p = 2$) Для нечётного простого p имеем

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

Мы доказываем квадратичный закон взаимности в этом миникурсе. Интересующиеся могут попробовать доказать его самостоятельно (Гаусс, например, придумал несколько десятков доказательств!), или прочитать доказательство в какой-либо книжке. Одно из любимых доказательств автора этого текста можно узнать из статьи В. В. Прасолова «Доказательство квадратичного закона взаимности по Золотарёву», опубликованной в сборнике «Математическое просвещение».