Вводные задачи

Задача 1. Докажите, что уравнения a) $2x^2 + 2xy - y^2 = 1$, b) $x^2 - xy + y^2 = 2$ не имеют решений в целых числах.

Доказательство. a) Анализ остатков при делении на три показывает, что уравнение

$$2x^2 + 2xy - y^2 = 3x^2 - (y - x)^2 = 1$$

не имеет решений в целых числах.

b) Легко видеть, что если $|x| \geq 3$ или $|y| \geqslant 3$ уравнение $x^2 - xy + y^2 = \frac{1}{2}(x^2 + y^2 + (x - y)^2) = 2$ не имеет решений в целых числах. Перебор оставшихся 25 вариантов показывает, что решений в целых числах у этого уравнения нет.

b) Заметим, что $x^2 - xy + y^2 = (x - y/2)^2 + 3/4y^2 = 2$, то есть $y^2 \leqslant 8/3$, $|y| \leqslant 1$, аналогично для x. Однако хотя бы одно из x и y должно быть чётное, то есть нулевое, пусть $x = 0$, тогда $y^2 = 2$, противоречие. □

Задача 2. Докажите, что уравнения a) $x^2 - 2y^2 = 1$, b) $x^2 - 3y^2 = 1$, c) $x^2 - 6y^2 = 1$ имеют бесконечно много решений в целых числах.

Доказательство. a) Для всякого целого n наборы

$$x = \frac{(3 + 2\sqrt{2})^n + (3 - 2\sqrt{2})^n}{2}, \quad y = \frac{(3 + 2\sqrt{2})^n - (3 - 2\sqrt{2})^n}{2\sqrt{2}}$$

являются решениями уравнения.

b) Для всякого целого n наборы

$$x = \frac{(2 + \sqrt{3})^n + (2 - \sqrt{3})^n}{2}, \quad y = \frac{(2 + \sqrt{3})^n - (2 - \sqrt{3})^n}{2\sqrt{3}}$$

являются решениями уравнения.

c) Для всякого целого n наборы

$$x = \frac{(5 + 2\sqrt{6})^n + (5 - 2\sqrt{6})^n}{2}, \quad y = \frac{(5 + 2\sqrt{6})^n - (5 - 2\sqrt{6})^n}{2\sqrt{6}}$$

являются решениями уравнения. □

Задача 3. Докажите, что уравнение $x^2 + 1000xy + 1000y^2 = 2001$ имеет бесконечно много решений в целых числах.

Доказательство. Дискриминант $1000^2 - 4 \cdot 1000$ уравнения $x^2 + 1000xy + 1000y^2 = 2001$ больше 0 и не является полным квадратом. Следовательно, форма $x^2 + 1000xy + 1000y^2 = 2001$ неопределена, не представляет 0 и представляет 2001 при $x = y = 1$. По задаче 46 отсюда следует, что у уравнения

$$x^2 + 1000xy + 1000y^2 = 2001$$

бесконечно много решений. □

Задача 4. Фиксируем нечётное простое число p. Докажите, что уравнение $x^2 - py^2 = -1$ имеет решение в целых числах, если и только если p имеет остаток 1 при делении на 4.

Доказательство. Пусть уравнение $x^2 - py^2 = -1$ имеет целое решение. Докажем, что p имеет остаток 1 при делении на 4. Действительно, в этом случае -1 является квадратичным вычетом по модулю p, т.е. $p \equiv 1 \pmod 4$.

Наоборот, пусть $p \equiv 1 \pmod 4$. По суперзадаче 46 существует нетривиальное решение уравнения $x^2 - py^2 = 1$.

Пусть S_+ — множество решений (x_0, y_0) уравнения $x^2 - py^2 = 1$ таких, что $x_0, y_0 > 0$. Пусть (x_0, y_0) — это решение из S_+ с наименьшим значением y_0. Тогда

$$(x_0 - 1)(x_0 + 1) = py_0^2. \tag{1}$$

Из (1) следует, что или $2(x_0+1)$, или $2(x_0-1)$ является полным квадратом. Рассмотрим оба варианта.

Пусть $2(x_0+1) = d^2$ для какого-то целого положительного числа d. Тогда d является чётным числом и $d \mid y_0$. Положим $d = 2d_0$. Положим

$$x_1 = (x_0+1)/d = d_0,\ y_1 = y_0/d.$$

Тогда

$$x_1^2 - py_1^2 = \frac{1}{d^2}((x_0+1)^2 - py_0^2) = \frac{2(x_0+1)}{d^2} = 1.$$

Таким образом, (x_1, y_1) также принадлежит S_+. Очевидно, что $y_1 < y_0$, что противоречит предположению о минимальности пары (x_0, y_0).

Пусть $2(x_0-1) = d^2$ для какого-то целого положительного числа d. Тогда d является чётным числом и $d \mid y_0$. Положим $d = 2d_0$. Положим

$$x_1 = (x_0-1)/d = d_0,\ y_1 = y_0/d.$$

Тогда

$$x_1^2 - py_1^2 = \frac{1}{d^2}((x_0-1)^2 - py_0^2) = \frac{2(1-x_0)}{d^2} = -1.$$

Таким образом, (x_1, y_1) является решением уравнения $x^2 - py^2 = -1$. Его и требовалось найти. □

Задача 5. Докажите, что для всякого m количества решений в целых числах уравнений

$$x^2 - xy + y^2 = m \quad \text{и} \quad 3x^2 + 9xy + 7y^2 = m$$

одинаковы.

Доказательство. Мы покажем, что всякому целочисленному решению уравнения $x^2 - xy + y^2 = m$ соответствует целочисленное решение уравнения $3x^2 + 9xy + 7y^2 = m$. И наоборот.

Пусть $v = x + y$, $u = -x - 2y$, очевидно, эти выражения целые. Подставим в $x^2 - xy + y^2$ вместо x выражение $u + 2v$, вместо y выражение $-u - v$. Получим $3u^2 + 9uv + 7v^2$. Таким образом, всякому решению уравнения $3x^2 + 9xy + 7y^2 = m$ соответствует решение уравнения $x^2 - xy + y^2 = m$.

Обратно, подставим в $3x^2 + 9xy + 7y^2$ вместо x выражение $u + 2v$, вместо y выражение $-u - v$. Получим $u^2 - uv + v^2$. Таким образом, всякому решению уравнения $x^2 - xy + y^2 = m$ соответствует решение уравнения $3x^2 + 9xy + 7y^2 = m$. □

Задача 6. Докажите, что для всякого целого числа n уравнение $x^2 + y^2 = n$ имеет решение в целых числах, если и только если оно имеет решения в рациональных числах.

Доказательство. Пусть рациональные числа x, y таковы, что $x^2 + y^2 = n$. Знаменатель чисел x и y в приведённой форме один и тот же. Мы обозначим его d и допустим, что мы выбрали x и y так, чтобы d было наименьшим возможным. Предположим, что $d > 1$ (т.е. что x, y нецелы и у уравнения $x^2+y^2 = n$ нет целых решений). Пусть r_x, r_y – это ближайшие к x, y целые числа соответственно, $s_x := x - r_x$, $s_y := y - r_y$. Тогда

$$|s_x|,\ |s_y| \leqslant \frac{1}{2}, \quad s_x^2 + s_y^2 = n - (r_x^2 + r_y^2) - 2(s_x r_x + s_y r_y). \tag{2}$$

Положим

$$x' = r_x - \frac{s_x(n - r_x^2 - r_y^2)}{s_x^2 + s_y^2}, \qquad y' = r_y - \frac{s_y(n - r_x^2 - r_y^2)}{s_x^2 + s_y^2}.$$

Из (2) следует, что $s_x^2 + s_y^2 = d'/d$, причём $0 < d' < d$. Отсюда следует, что в приведённой форме знаменатель d' дробей x', y' делит d, в частности, меньше d. Имеем $x'^2 + y'^2 = n$. Следовательно, знаменатель дробей x', y' меньше знаменателя дробей x, y. Противоречие. Следовательно, $d = 1$, т.е. уравнение $x^2 + y^2 = n$ имеет решения в целых числах. □

Задача 7. Приведите пример квадратичного уравнения с целыми коэффициентами, имеющего решения в рациональных числах, но не имеющего решений в целых числах.

Доказательство. Рассмотрим уравнение $4x^2 = 1$. Значение $\frac{1}{2}$ даёт рациональное решение этого уравнения, а вот целых решений у этого уравнения нет. $\square$

Задача 8. Докажите, что для любых целых положительных чисел a и b существует бесконечно много натуральных чисел m, для которых уравнение $ax^2 + by^2 = m$ не имеет решений в целых числах.

Доказательство. Пусть N — какое-то целое число. Если для какого-то $n \leqslant N$ уравнение $ax^2 + by^2 = n$ имеет решение, то

$$|x| \leqslant \sqrt{\frac{N}{a}}, \quad |y| \leqslant \sqrt{\frac{N}{b}}.$$

Таким образом, если для всякого $n \leqslant N$ уравнение $ax^2 + by^2 = n$ имеет решение, то существует N пар чисел (x, y) таких, что $0 \leqslant x \leqslant \sqrt{\frac{N}{a}}$, $0 \leqslant y \leqslant \sqrt{\frac{N}{b}}$. Тогда

$$N \leqslant \frac{N}{\sqrt{ab}}.$$

Очевидно, что это неравенство не выполнено для достаточно больших N, если $ab > 1$. С учётом этого осталось рассмотреть случай $a = b = 1$. Ни одно число, имеющее остаток 3 при делении на 4, не представляется в виде $x^2 + y^2$, что завершает доказательство. $\square$

Задача 9. Докажите, что для всякого целого числа m уравнение $x^2 + 2y^2 - 3z^2 = m$ имеет решение в целых числах.

Доказательство. Достаточно показать, что $x^2 + 2y^2 - 3z^2$ представляет 0, все нечётные числа и все числа, имеющие остаток 2 при делении на 4.

Подставим $x = y = z = 1$ в $x^2 + 2y^2 - 3z^2$. Получим 0. Следовательно, $x^2 + 2y^2 - 3z^2$ представляет 0.

Подставим $x = u + 1$, $y = u$, $z = u$ в $x^2 + 2y^2 - 3z^2$. Получим $2u + 1$. Следовательно, $x^2 + 2y^2 - 3z^2$ представляет все нечётные числа.

Подставим $x = u$, $y = u + 1$, $z = u$ в $x^2 + 2y^2 - 3z^2$. Получим $4u + 2$. Следовательно, $x^2 + 2y^2 - 3z^2$ представляет все числа, имеющие остаток 2 при делении на 4.

Если m делится на 4, то поделим все переменные на 2 и сведём задачу к одному из разобранных случаев. $\square$

Квадратичные формы

Задача 10. Опишите все целые числа, которые представляются формами a) $x^2 + y^2$; b) $x^2 - y^2$; c) $x^2 + xy + y^2$.

Доказательство. a) $n = x^2 + y^2$ если и только если в разложении n на простые множители все простые делители, входящие в n в нечётной степени, имеют остаток 1 при делении на 4.

b) $(u+1)^2 - u^2 = 2u + 1$. Следовательно, все нечётные числа представляются формой $x^2 - y^2$. Также $(u + 1)^2 - (u - 1)^2 = 4u$.

Как итог, все целые числа, имеющие остатки 0, 1, 3 при делении на 4 представляются формой $x^2 - y^2$. Анализ остатков при делнии на 4 показывает, что числа с остатками 2 при делении на 4 не представимы в виде $x^2 - y^2$.

c) Фиксируем число n. Рассуждение, аналогичное рассуждению, приведённому в задаче 6, показывает, что $x^2 + xy + y^2 = n$ имеет решение в рациональных числах если и только если оно имеет решение в числах целых. В рациональных числах форма $x^2 + xy + y^2$ эквивалентна форме $x^2 + 3y^2$ ($x^2 + xy + y^2 = (x + \frac{y}{2})^2 + 3(\frac{y}{2})^2$). Покажем, что форма $x^2 + 3y^2$ представляет число n в рациональных числах (см. часть про символ Гильберта), если и только если в разложении числа n на простые множители все простые делители, входящие в нечётной степени, имеют остаток 1 или 0 при делении на 3.

Действительно, $x^2 + 3y^2 = n$ имеет решение в $\mathbb{Q}$ тогда и только тогда, когда $x_1^2 + 3y_1^2 - nz^2 = 0$ имеет решение в $\mathbb{Z}$ с ненулевым z. Это уравнение (по теореме Минковского-Хассе) имеет решение тогда и только тогда, когда символ Гильберта $(n, -3)_p$ равен 1 для всех простых p. Вычислим его непосредственно.

Пусть $p > 3$. Запишем $n = p^\alpha \cdot u$, $3 = p^0 \cdot (-3)$. При помощи явной формулы для символа Гильберта и квадратичного закона взаимности Гаусса (Серр, Глава 1, § 3 Теорема 6) получаем, что

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

то есть данное выражение равно 1 всегда, если α чётно, а при нечётном α оно равно $\left(\frac{p}{3}\right)$, то есть равно 1 тогда и только тогда, когда p имеет остаток 1 при делении на 3. Получили, что если уравнение

$$x_1^2 + 3y_1^2 - nz^2 = 0$$

имеет решения по модулю p, при этом p имеет вид $3k + 2$, то в разложение числа n сомножитель p входит в чётной степени.

Случай $p = 2$ оставим читателю в качестве упражнения.

Случай $p = 3$. Предположим, что $n = 3^\alpha \cdot u$, при этом $\beta = 1$, $v = -1$. Имеем:

$$(n, -3)_3 = (-1)^\alpha \left(\frac{u}{3}\right) \left(\frac{-1}{3}\right)^\alpha = \left(\frac{u}{3}\right).$$

Это выражение равно 1 тогда и только тогда, когда u имеет остаток 1 при делении на 3. Но если мы уже знаем, что все простые делители вида $3k + 2$ входят в чётной степени, то это условие не даёт ничего нового. □

Определение 1. Назовём две формы *эквивалентными*, если они представляют один и тот же набор целых чисел.

Задача 11. Докажите, что квадратичные формы

$$f(x, y), \quad f(x - y, y), \quad f(x, y - x), \quad f(-x, y) \quad \text{и} \quad f(x, -y) \tag{3}$$

попарно эквивалентны.

Доказательство. Если число m представляется формой $f(x, y)$ при $x = x_0$, $y = y_0$, то m представляется формой $f(x-y, y)$ при $x = x_0+y_0$, $y = y_0$, формой $f(x, y-x)$ при $x = x_0$, $y = y_0+x_0$, формой $f(-x, y)$ при $x = -x_0$, $y = y_0$, формой $f(x, -y)$ при $x = x_0$, $y = -y_0$. Таким образом, все числа представляемые формой $f(x, y)$ представляются и другими формами списка (3). Аналогично доказывается и то, что все числа, представляемые любой другой формой списка (3), представляются и всеми остальными формами списка (3). Таким образом, все формы списка (3) эквивалентны. □

Задача 12. a) Докажите, что формы $x^2 + y^2$ и $x^2 + xy + y^2$ не эквивалентны.

b) Докажите, что форма $4x^2 - 6xy + 5y^2$ не эквивалентна форме $ax^2 + by^2$ ни для каких целых чисел a и b.

Доказательство. a) Форма $x^2 + y^2$ представляет 2, а $x^2 + xy + y^2$ — нет. Следовательно, они не эквивалентны.

b) Значения вокруг единственного колодца формы $4x^2 - 6xy + 5y^2$ равны 3, 4, 5. Следовательно, числа 3, 4, 5 являются тремя наименьшими значениями формы $4x^2 - 6xy + 5y^2$.

Пусть $a, b \geqslant 0$. Тогда тремя наименьшими значениями формы $ax^2 + by^2$ могут быть наборы чисел

$$\{a,\ b,\ a + b\}, \quad \{a,\ 2a,\ b\}, \quad \{a,\ b,\ 2b\}, \quad \{a,\ 2a,\ 4a\}, \quad \{b,\ 2b,\ 4b\}. \tag{4}$$

Очевидно, что набор 3, 4, 5 не является ни одним из (4) ни для каких a и b.

Следовательно, формы $4x^2 - 6xy + 5y^2$ и $ax^2 + by^2$ не эквивалентны ни при каких неотрицательных числах a, b. □

Задача 13. Приведите пример неотрицательно определённой формы, которая не является положительно определённой.

Доказательство. Пример: $f(x, y) = x^2$. □

Расширенная арифметика

Задача 14. Пусть m и n – целые числа, свободные от квадратов. Если уравнение

$$z^2 - mx^2 - ny^2 = 0 \tag{5}$$

имеет ненулевое решение в рациональных числах, то выполнены следующие условия

a) хотя бы одно из чисел m, n положительно,

b) m является квадратичным вычетом при делении на n,

c) n является квадратичным вычетом при делении на m.

Доказательство. Фиксируем ненулевое рациональное решение (x_0, y_0, z_0) уравнения (5). Мы можем считать (и считаем), что числа x_0, y_0, z_0 взаимно просты в совокупности.

a) Если $m, n \leqslant 0$, то $x_0^2 - my_0^2 - nz_0^2 \geqslant 0$, и равенство достигается только при $x_0 = y_0 = z_0 = 0$. Противоречие.

b) Достаточно доказать, что для всякого простого делителя p числа m число n является полным квадратом в остатках при делении на p.

Пусть p — это какой-то простой делитель m. Если $n \vdots p$, то утверждение задачи, очевидно, выполнено. Пусть $n \not\vdots p$. Рассмотрим два случая: $y_0 \vdots p$ и $y_0 \not\vdots p$.

Допустим, что $y_0 \vdots p$. Тогда x_0, z_0 также делятся на p, что противоречит тому, что

$$\text{НОД}(x_0, y_0, z_0) = 1.$$

Следовательно, $y_0 \not\vdots p$. Тогда в остатках при делении на p выполнено равенство

$$n \equiv (z/y)^2 \pmod p,$$

что завершает доказательство пункта b).

Пункт c) доказывается аналогично пункту b). □

Задача 15. Сведите метатеорему для двух переменных к решению уравнений вида (5).

Доказательство. Всякое квадратное уравнение имеет вид

$$f(X_1, X_2) = f_2(X_1, X_2) + f_1(X_1, X_2) + f_0 = 0,$$

где f_2 — это однородный многочлен степени 2, f_1 — степени 1, f_0 — степени 0 (т.е. константа).

Начнём с некоторого общего утверждения: уравнения

$$f(X_1, X_2) = 0 \text{ и } f(X_1 + cX_2 + t, X_2) = 0$$

либо одновременно имеют решения, либо одновременно не имеют решений в рациональных числах для всяких рациональных чисел c, t. Мы оставляем это утверждение в качестве простого упражнения.

Очевидно, что замены вида

$$f(X_1, X_2) \to f(X_1 + cX_2, X_2) \tag{6}$$

действуют независимо на компоненты f_1, f_2 и сохраняют f_0.

Представим f_2 в виде

$$c_1X_1^2 + c_{12}X_1X_2 + c_2X_2^2,$$

где c_1, c_2, c_{12} — это параметры.

Если $f_2 \neq 0$, то, сделав несколько замен вида (6), мы можем считать, что $c_1 \neq 0$.

Рассмотрим функцию

$$f(X_1 - \frac{c_{12}}{2c_1}X_2, X_2). \tag{7}$$

Легко видеть, что (7) имеет вид

$$c_1X_1^2 + c_2'X_2^2$$

для некоторого рационального числа c_2'. Итак, мы можем считать

$$f_2(X_1, X_2) = c_1 X_1^2 + c_2 X_2^2$$

для каких-то рациональных чисел c_1, c_2. Если $c_2 = 0$, а $c_1 \neq 0$, то уравнение $f = 0$ принимает вид

$$c_1 X_1^2 = -rX_2 - f_0$$

и решается элементарно. Таким образом, далее мы считаем, что $c_1 \neq 0$. По аналогичным соображениям мы считаем, что $c_2 \neq 0$.

Линейная функция $f_1(X_1, X_2)$ представима в виде $r_1 X_1 + r_2 X_2$. Рассмотрим замену

$$f(X_1, X_2) \to f\left(X_1 - \frac{r_1}{2c_1}, X_2 - \frac{r_2}{2c_2}\right).$$

У функции $f(X_1 - \frac{r_1}{2c_1}, X_2 - \frac{r_2}{2c_2})$ часть f_1 равна 0. В этом случае уравнение $f = 0$ принимает вид

$$c_1 X_1^2 + c_2 X_2^2 + f_0 = 0.$$

Это уравнение эквивалентно однородному уравнению

$$z^2 + \frac{c_2}{c_1} y^2 + \frac{f_0}{c_1} z^2 = 0.$$

Что и требовалось доказать. □

Задача 16. Уравнение с целыми коэффициентами $f = 0$ имеет решение в $\mathbb{Z}_p$, если и только если оно имеет решение в остатках при делении на p^n для всякого $n \in \mathbb{Z}_{\geqslant 0}$.

Доказательство. Пусть $x_1, \ldots, x_n$ — это решение в $\mathbb{Z}_p$ уравнения $f = 0$. Тогда классы $x_1, \ldots, x_n$ в остатках при делении на p^n являются решениями в остатках при делении на p^n. В частности, $f \equiv 0$ имеет решение в остатках при делении на p^n для всякого целого положительного числа n.

Наоборот, положим, что уравнение $f \equiv 0$ имеет решение в остатках при делении на p^m для любого целого положительного числа m. Обозначим через S_m для каждого m множество решений в остатках при делении на p^m уравнения $f \equiv 0$. По предположению это множество остатков не пусто для всякого $m \geqslant 0$.

Так как любой остаток при делении на p^{m+1} можно рассмотреть по модулю p^m, то имеется отображение $S_{m+1} \to S_m$. Обозначим через S_m^∞ пересечение образов S_{m+k} для всех $k \geqslant 0$. Так как $S_{m+k} \neq 0$, то $S_m^\infty \neq 0$. Для каждого $s_m \in S_m^\infty$ существует $s_{m+1} \in S_{m+1}^\infty$ такой, что s_m есть образ s_{m+1}. Таким образом, можно построить бесконечную цепочку

$$s_1, \ldots, s_m, \ldots, \tag{8}$$

где s_m есть набор из n остатков при делении на p^m и s_m есть проекция s_{m+1} в остатки при делении на p^m. Последовательность (8) задаёт единственный набор из n целых p-адических чисел $x_1, \ldots, x_n$, обладающих заданными наборами остатков $s_1, \ldots, s_m, \ldots$ при делении на $p, \ldots, p^m, \ldots$.

Числа $x_1, \ldots, x_n$ являются решениями уравнения $f = 0$. □

Задача 17. Когда p-адическое число в форме (2) равно 0?

Доказательство. Ответ, следующий из определения: «Когда $a_{-k} + \ldots + a_{-k+i} p^i \equiv 0 (\mathrm{mod}\ p^{i+1}) \quad \forall i$». □

Задача 18. Докажите, что произведение двух ненулевых p-адических чисел не равно 0.

Доказательство. Рассмотрим два ненулевых p-адических числа a, b. Без ограничения общности мы считаем, что $a, b \in \mathbb{Z}_p$ и $a, b \not\equiv 0 (\mathrm{mod}\ p)$. Тогда $ab \not\equiv 0 (\mathrm{mod}\ p)$ и, следовательно, $ab \neq 0$. □

Задача 19. Докажите, что $\mathbb{Q} \subset \mathbb{Q}_p$ для всякого простого числа p (докажите, что для всякой пары ненулевых целых чисел m, n существует p-адическое число x такое, что $nx = m$).

Доказательство. Без ограничения общности считаем, что m, n взаимно просты с p. В этом предположении задача 16 следует из задачи 20. □

Задача 20. Докажите, что -1 является полным квадратом в p-адических числах тогда и только тогда, когда p имеет остаток 1 при делении на 4.

Доказательство. Следует из задачи 21. □

Задача 21. Придумайте описание для p-адических чисел, являющихся полными квадратами.

Доказательство. Мы рассмотрим два случая: $p = 2$ и $p \neq 2$.

Пусть $p = 2$. Всякое 2-адическое число x представимо в виде $2^n(2m+1)$, где n — это целое число, а m — это целое 2-адическое число. Имеем $x^2 = 2^{2n}(1 + 8\frac{m(m+1)}{2})$. Положим $m' = \frac{m(m+1)}{2}$. Тогда

$$x^2 = 2^{2n}(1 + 8m'), \tag{9}$$

где m' — это целое 2-адическое число.

Докажем, что всякое 2-адическое число вида (9) является полным квадратом в 2-адических числах. Для этого достаточно показать, что всякое целое 2-адическое число m' представимо в виде $\frac{m(m+1)}{2}$.

Благодаря задаче 16, достаточно доказать, что сравнение $x(x+1) \equiv 2m'$ имеет решения в $\mathbb{Z}$ для всякого $i \in \mathbb{Z}_{\geqslant 0}$. Мы докажем это утверждение по индукции.

База: $i = 1$, очевидно, выполнена.

Переход: $i \to i+1$. Пусть $m_i \in \mathbb{Z}$ — это решение уравнения $x(x+1) \equiv 2m' (\mathrm{mod}\ 2^i)$. Выполнено одно из двух условий

1) $m_i(m_i+1) \equiv 2m' \pmod{2^{i+1}}$,

2) $m_i(m_i+1) \equiv 2m' + 2^i \pmod{2^{i+1}}$.

В случае 1) m_i является решением сравнения $x(x+1) \equiv 2m' \pmod{2^{i+1}}$. В случае 2) $m_i + 2^i$ является решением сравнения $x(x+1) \equiv 2m' \pmod{2^{i+1}}$.

Пусть $p \neq 2$, т.е. p — нечётное простое число. Всякое p-адическое число x представимо в виде $p^n m$, где n — это целое число, а m — это целое p-адическое число, не делящееся на p. Имеем $x^2 = p^{2n}m^2$. Положим $m' = m^2$. Тогда

$$x^2 = p^{2n}m', \tag{10}$$

где m' — это целое p-адическое число, остаток при делении на p которого является квадратичным вычетом и не равен 0.

Докажем, что всякое p-адическое число вида (9) является полным квадратом в p-адических числах. Для этого достаточно показать, что всякое целое p-адическое число m' такое, что

3) m' не делится на p,

4) остаток при делении m' на p является квадратичным вычетом и не равен 0,

представимо в виде m^2.

Благодаря задаче 16 достаточно доказать, что уравнение $x^2 \equiv m' \pmod{p^i}$ имеет решения в $\mathbb{Z}$ для всякого $i \in \mathbb{Z}_{\geqslant 0}$. Мы докажем это утверждение по индукции.

База: $i = 1$ выполнена, так как остаток при делении на p числа m' является квадратичным вычетом.

Переход: $i \to i+1$. Пусть $m_i \in \mathbb{Z}$ — это решение уравнения $x^2 \equiv m' \pmod{p^i}$. Тогда

$$m_{i+1}^2 \equiv m' + rp^i \pmod{p^{i+1}},$$

где $r \in \mathbb{Z}$ — это какое-то число. Так как m' не делится на p и $p \neq 2$, то существует $r' \in \mathbb{Z}$ такое, что $2m_i r' \equiv r \pmod{p^{i+1}}$. Положим $m_{i+1} := m_i - r'p^i$. Тогда $m_{i+1}^2 \equiv m' \pmod{p^{i+1}}$. Что завершает переход. □

Задача 22. Докажите, что любое ненулевое 3-адическое число m есть или x^2, или $2x^2$, или $3x^2$, или $6x^2$ для какого-то 3-адического числа x.

Доказательство. Заметим, что для любого p произвольное p-адическое число представляется в виде $p^i \cdot a \cdot y$, где a — целое число от 1 до $p-1$, p^i — степень p, а y — целое p-адическое число, сравнимое с единицей по модулю p (по задаче 21 оно автоматически является полным квадратом). Тогда, подставляя $p = 3$, получаем, что в зависимости от чётности числа i число p^i — или квадрат, или утроенный квадрат, $a \in \{1,\ 2\}$, y — точный квадрат. Поэтому их произведение является одним из предложенных вариантов. □

Задача 23. Пусть p — нечётное простое число, а $x_1, \ldots, x_5$ — ненулевые p-адические числа. Докажите, что x_i/x_j есть полный квадрат в p-адических числах для каких-то i, j $(1 \leqslant i < j \leqslant 5)$.

Доказательство. Аналогично решению предыдущей задачи любое число представляется в виде $p^i \cdot a \cdot y$. Разобьём числа на 2 группы. В первой группе i четно, во второй — нечетно. После чего разобьём каждую на 2 подгруппы: в первой подгруппе a является квадратичным вычетом, а во второй — нет. Заметим, что по принципу Дирихле хотя бы 2 из взятых нами чисел попадет в одну группу. Их отношение имеет вид:

$$p^j \cdot a_{new} \cdot \frac{y_1}{y_2},$$

где j делится на 2, a_{new} является квадратичным вычетом (как отношение двух вычетов либо двух невычетов), а $\frac{y_1}{y_2}$ является p-адическим числом, начинающимся с единицы. Теперь очевидно, что это число является квадратом, как произведение трех квадратов. □

Задача 24. Докажите, что для всякого нечётного простого числа p существуют ненулевые p-адические числа $x_1, \ldots, x_{p-1}$ такие, что $x_1^2 + \ldots + x_{p-1}^2 + 1 = 0$.

Доказательство. Заметим, что по задаче 21 число $1 - p$ является полным квадратом в p-адических чисел. Следовательно, $-1 = 1 + 1 \ldots + 1$ ($p - 2$ единицы)$+1 - p$ есть сумма $(p - 1)$-го квадрата в p-адических числах. Что и требовалось доказать. □

Задача 25. Докажите, что уравнение $x^2 + x + 1 = 0$ имеет ровно два решения в целых 7-адических числах.

Доказательство. Решения уравнения $x^2 + x + 1 = 0$ выражается формулой $x_{1,2} = \frac{-1 \pm \sqrt{-3}}{2}$. Так как $\sqrt{-3} \in \mathbb{Z}_7$ (см. задачу 21), то $x^2 + x + 1 = 0$ имеет два различных решения в $\mathbb{Z}_7$. □

Задача 26. Докажите, что уравнение $x^2 + y^2 = -1$ имеет решения в p-адических числах для всякого нечётного простого числа p.

Доказательство. Достаточно доказать, что это уравнение имеет решение по модулю p. Проверим это. Выражение x^2 может принимать $(p + 1)/2$ различных значений: ноль и все квадратичные вычеты. Перечислим все значения выражения $-x^2 - 1$. Если хотя бы одно из них может быть представлено в виде y^2, то задач решена. Если же ни одно из них не имеет вид y^2, то для возможных значений y^2 (в остатках по модулю p) имеется максимум $(p - 1)/2$ возможных значений. Противоречие.

Второе решение. Достаточно доказать, что уравнение $x^2 + y^2 = -1$ имеет ненулевое решение в $\mathbb{Z}/p$. Всякий квадратичный вычет представим в виде $x^2 + y^2$. Если в виде $x^2 + y^2$ представимы только квадратичные вычеты, то в виде $x_1^2 + \ldots + x_{p-1}^2$ представимы только квадратичные вычеты. Но в виде $x_1^2 + \ldots + x_{p-1}^2$ представимы все остатки при делении на p. Следовательно, $x^2 + y^2$ представляет квадратичные невычеты. Следовательно, $x^2 + y^2$ представляет все элементы $\mathbb{Z}/p$. В том числе, -1. □

Задача 27. Докажите принцип Минковского-Хассе для уравнений от одной и двух переменных.

Доказательство. А) Уравнения от одной переменной. Уравнение имеет вид $ax^2 = b$. Достаточно доказать что, если уравнение не имеет решений в $\mathbb{Q}$, то оно не имеет решений или в $\mathbb{R}$ или в $\mathbb{Q}_p$ для какого-то p. Если $ax^2 = b$ не имеет решений в $\mathbb{Q}$, то b/a не является полным квадратом в $\mathbb{Q}$, т.е. или $b/a < 0$, или какой-то простой делитель p входит в b/a нечётное число раз. В первом случае $ax^2 = b$ не имеет решений в $\mathbb{R}$, а во втором — в $\mathbb{Q}_p$.

В) Уравнения от двух переменных. По задаче 15 всякое уравнение в рациональных числах от двух переменных эквивалентно уравнению $ax^2 + by^2 = 1$. При этом можно считать, что

1) числа a, b целые и свободны от квадратов,

2) $|a| \leqslant |b|$.

Достаточно доказать, что если уравнение $ax^2 + by^2 = 1$ имеет решение в $\mathbb{Q}_p$ для всякого p и в $\mathbb{R}$, то оно имеет решение в $\mathbb{Q}$. Положим $m(a, b) := |a| + |b|$. Будем доказывать наше утверждение индукцией по $m(a, b)$.

База: $m(a, b) = 2$ проверяется непосредственно.

Переход: $m \to m + 1$. Пусть a, b — это какие-то числа, удовлетворяющие условиям 1), 2) и такие, что

• $m(a, b) = m + 1$

• уравнение $ax^2 + by^2 = 1$ имеет решения в p-адических числах для всякого p и имеет решение в $\mathbb{R}$.

Рассмотрим два случая: $|a| = |b|$ и $|a| < |b|$. Если $|a| = |b|$, то уравнение $ax^2 + by^2 = 1$ эквивалентно уравнению

$$-(b/a)y^2 + az^2 = 1. \tag{11}$$

Более того, уравнение (11) имеет решения в $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{Q}_p$, если и только если уравнение $ax^2+by^2 = 1$ имеет решение в том же множестве чисел. Так как $m(-\frac{b}{a}, a) < m(a, b) = m + 1$, то $-(b/a)y^2 + az^2 = 1$ имеет решения в $\mathbb{Q}$ по предположению индукции. Следовательно, и исходное уравнение имеет решение в $\mathbb{Q}$.

Пусть теперь $|a| < |b|$. Из условия • следует, что a является полным квадратом в остатках при делении на b, т.е.

$$a + bb' = t^2,$$

где b', t — это какие-то целые числа и $b' \geqslant 0$. Без ограничения общности считаем, что

$$|t| \leqslant \frac{|b|}{2}.$$

Уравнение $ax^2 + by^2 = 1$ имеет решения в $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{Q}_p$, если и только если в тех же множествах чисел имеет решение уравнение

$$ax^2 + b'y^2 = 1, \qquad b' = \frac{t^2 - a}{b}.$$

Имеем $|b'| \leqslant \frac{|b|}{4}$ и, следовательно $m(a, b') < m(a, b) = m + 1$. Так $m(a, b') \leqslant m$, то $ax^2 + b'y^2 = 1$ имеет решения в $\mathbb{Q}$ по предположению индукции. Следовательно, и исходное уравнение имеет решение в $\mathbb{Q}$. Доказательство завершено. □

Задача 28. Докажите, что для символа Гильберта выполнены следующие соотношения

1) $(a, b)_p = (b, a)_p$,
2) $(a, c^2)_p = 1$,
3) $(a, -a)_p = 1, \quad (a, 1 - a)_p = 1$,
4) $(a, b)_p = (a, -ab)_p = (a, (1 - a)b)_p$.

Доказательство. 1) очевидно из определения.

2) Уравнение $z^2 - ax^2 - c^2y^2 = 0$ имеет ненулевое решение $z = c, x = 0, y = 1$.

3) Уравнение $z^2 - ax^2 + ay^2 = 0$ имеет ненулевое решение $z = 0, x = y = 1$.

Уравнение $z^2 - ax^2 - (1 - a)y^2 = 0$ имеет ненулевое решение $x = y = z = 1$.

4) Следует из пункта 3) и задачи 29. □

Задача 29. Пусть $(a, b)_p = 1$. Тогда $(a', b)_p = (aa', b)_p$ для любого a'.

Доказательство. Пусть b является полным квадратом. Тогда $(a, b)_p = (aa', b)_p = 1$.

Пусть теперь b не является полным квадратом. Мы воспользуемся следующей леммой.

Лемма 1. Если

• b не является полным квадратом,

• $(a, b)_p = 1$ и $(a', b)_p = 1$,

то $(aa', b) = 1$.

Завершим, используя лемму 1, решение задачи 29. Если $(a', b)_p = 1$, то $(aa', b)_p = 1$по лемме 1. Если $(aa', b)_p = 1$, то $(a', b)_p = (a^2a', b)_p = 1$ по лемме 1. Таким образом, если одно из чисел $(aa', b)_p, (a', b)_p$ равно 1, то и второе равно 1. Следовательно, эти числа равны.

Доказательство леммы 1. Пусть x_0, y_0, z_0 — это ненулевое решение уравнения $z_0^2 - ax_0^2 - by_0^2 = 0$. Так как b не является полным квадратом в $\mathbb{Q}_p$, то $x_0 \neq 0$. Тогда мы можем считать, что $x_0 = 1$ и $a = z_0^2 - by_0^2$. По аналогичным соображениям существуют z_1, y_1 такие, что $a' = z_1^2 - by_1^2$. Тогда

$$aa' = (z_0z_1 - by_0y_1)^2 - b(z_0y_1 + z_1y_0)^2.$$

Следовательно, $(aa', b) = 1$. □

□

Чтобы компактно записать явную формулу для символа Гильберта, нам потребуется *символ Лежандра* $\left(\dfrac{x}{p}\right)$, определённый для любых целого x и простого p. Он равен 1, -1 или 0 в зависимости от того, является x ненулевым квадратичным вычетом, невычетом или нулём по модулю p.

Задача 30. Пусть p – нечётное простое число, $a = p^\alpha u$, $b = p^\beta v$, где α, β, u, v – это целые числа такие, что u и v взаимно просты с p. Докажите, что

$$(a,b)_p = (-1)^{\alpha\beta\varepsilon(p)} \left(\frac{u}{p}\right)^\beta \left(\frac{v}{p}\right)^\alpha,$$

где $\varepsilon(p) := \frac{p-1}{2}$.

Доказательство. Доказательство этого факта можно прочитать в книжке Ж.-П. Серра “A course in arithmetic”, Глава 3, § 1, Теорема 1. □

Задача 31. Найдите явную формулу для $(a,b)_2$ при всех целых числах a, b.

Доказательство. Пусть $a = 2^\alpha u$, $b = 2^\beta v$, где α, β, u, v — это целые числа такие, что u и v нечетны. Символ Гильберта $(a,b)_2$ задаётся формулой

$$(-1)^{\varepsilon(u)\varepsilon(v)+\alpha\omega(v)+\beta\omega(u)},$$

где $\varepsilon(u) = \frac{u-1}{2}$, а $\omega(u) = \frac{u^2-1}{8}$. Доказательство этого факта можно прочитать в книжке Ж.-П. Серра “A course in arithmetic”, Глава 3, § 1, Теорема 1. □

Задача 32. Докажите, что $(a,b)_p(a,b')_p = (a,bb')_p$ для любых целых чисел a, b, b'.

Доказательство. Доказательство этого факта можно прочитать в книжке Ж.-П. Серра “A course in arithmetic”, Глава 3, § 1, Теорема 2. □

Задача 33. Докажите, что уравнение $ax^2 + by^2 = c$ (a, b, c – это параметры; x, y – это переменные) имеет решение в p-адических числах, если и только если $(c, -ab)_p = (a,b)_p$.

Доказательство. Если уравнение $ax^2 + by^2 = c$ имеет решение, то уравнение

$$z^2 - \frac{a}{c}x^2 - \frac{b}{c}y^2 = 0$$

также имеет решение. Что по определению значит, что $(a/c, b/c)_p = 1$. Преобразуя, имеем

$$1 = (a/c, b/c)_p = (a,b)_p(a,c)_p(b,c)_p(c,c)_p = (a,b)_p(ab,c)_p(c,-1)_p. \tag{12}$$

Откуда $(a,b)_p = (c,-ab)_p$.

Теперь положим, что $(a,b)_p = (c,-ab)_p$, и докажем, что уравнение $ax^2 + by^2 = c$ имеет ненулевое решение. Тогда из выкладок (12) следует, что $(a/c, b/c)_p = 1$. Тогда уравнение $z^2 - \frac{a}{c}x^2 - \frac{a}{b}y^2 = 0$ имеет решения. Обозначим одно такое решение (x_0, y_0, z_0). Если $z_0 \neq 0$, то $(\frac{x_0}{z_0}, \frac{y_0}{z_0})$ — это решение уравнения $ax^2 + by^2 = c$.

Таким образом, если $z_0 \neq 0$, то задача решена. Далее мы считаем, что $z_0 = 0$. Для всяких r_x, r_y рассмотрим уравнение

$$a(tx_0 + r_x)^2 + b(ty_0 + r_y)^2 = c.$$

Оно эквивалентно уравнению

$$(ar_x^2 + br_y^2) + 2t(ax_0r_y + by_0r_x) = c. \tag{13}$$

Для общей пары рациональных чисел (r_x, r_y) имеем $(ax_0r_y + by_0r_x) \neq 0$ и $t_0 = \frac{c-(ar_x^2+br_y^2)}{2(ax_0r_y+by_0r_x)}$ является решением уравнения (13). Соответственно, уравнение $ax^2 + by^2 = c$ имеет бесконечно много рациональных решений. □

Используя свойства символа Гильберта, решите следующую задачу.

Задача 34. Фиксируем однородный многочлен $f = a_1x_1^2 + a_2x_2^2 + \ldots + a_nx_n^2 (n \geqslant 2)$, где $a_1, \ldots, a_n \neq 0$. Положим

$$d = a_1a_2\ldots.a_n \quad \text{и} \quad \varepsilon = \prod_{i<j}(a_i, a_j)_p. \tag{14}$$

Докажите, что уравнение $f = 0$ имеет ненулевое решение в p-адических числах тогда и только тогда, когда выполнено одно из следующих условий

1) $n = 2$, а число $-d$ является полным квадратом в $\mathbb{Q}_p$;

2) $n = 3$ и $(-1, d)_p = \varepsilon$;

3) $n = 4$ и $d \neq \alpha^2$, или же $d = \alpha^2$ и $\varepsilon = (-1, -1)_p$;

4) $n \geqslant 5$. (т.е., если f зависит от 5 и более переменных, то уравнение $f = 0$ имеет ненулевое решение в $\mathbb{Q}_p$ для любого p.)

Доказательство. Доказательство этого факта можно прочитать в книжке Ж.-П. Серра “A course in arithmetic”, Глава 4, § 2, Теорема 6. □

Выведите из задачи 34 следующее утверждение.

Задача 35. Фиксируем однородный многочлен $f = a_1x_1^2 + a_2x_2^2 + \ldots + a_nx_n^2$ $(n \geqslant 2)$, где $a_1, \ldots, a_n \neq 0$, а также целое число $a \neq 0$. Определим d и ε формулой (14). Докажите, что уравнение $f = a$ имеет решение в p-адических числах тогда и только тогда, когда выполнено одно из следующих условий:

1) $n = 1$, а число a/d является полным квадратом в $\mathbb{Q}_p$;

2) $n = 2$ и $(a, -d)_p = \varepsilon$;

3) $n = 3$ и: ad не является точным квадратом в $\mathbb{Q}_p$ или ad является точным квадратом и $\varepsilon = (-1, -d)_p$;

4) $n \geqslant 4$. (Т.е., если f зависит от 4 и более переменных, то уравнение $f = a$ имеет ненулевое решение в $\mathbb{Q}_p$ для любого p).

Доказательство. 1) $a_1x_1^2 = a \Leftrightarrow x_1^2 = \frac{a}{a_1}$. Очевидно, у него есть решения в p-адических числах тогда и только тогда, когда $\frac{a}{a_1}$ является точным квадратом в $\mathbb{Q}_p$.

2) $a_1x_1^2 + a_2x_2^2 = a$. Условие $(a, -d)_p = \varepsilon$ эквивалентно $(a, -a_1a_2)_p = (a_1, a_2)$, что совпадает с задачей 33 для $a = a_1$, $b = a_2$, $c = a$.

3) Требуется решить уравнение $a_1x_1^2 + a_2x_2^2 + a_3x_3^2 - a = 0$. Очевидно, оно эквивалентно уравнению $a_1x_1^2 + a_2x_2^2 + a_3x_3^2 - ax_4^2 = 0$, поскольку получается заменой

$$(x_1, x_2, x_3, x_4) \leftrightsquigarrow (\frac{x_1}{x_4}\frac{x_2}{x_4}\frac{x_3}{x_4}, 1),$$

а это уравнение имеет решения в p-адических числах.

Теперь докажем, что если есть нетривиальное решение с $x_4 = 0$, то существует и нетривиальное решение с $x_4 \neq 0$. Без ограничения общности $x_1 \neq 0$. Пусть (C, D) — решение уравнения $C^2 - D^2 = -\frac{a}{a_1}$ (например, $C = \frac{1-a/a_1}{2}$, $D = \frac{-1-a/a_1}{2}$)).

Очевидно, можно умножить наше решение на $\frac{C}{x1}$, получится $(C,\ x_2,\ x_3,\ 0)$. Легко проверить, что

$$f(C, x_2, x_3, 0) = f(D, x_2, x_3, 1),$$

и мы свели задачу к задаче 34c.

Первый случай: $ad \neq -m^2$ в $\mathbb{Q}_p$. Это эквивалентно $d \neq m^2$.

Второй случай: $ad = -m^2$.

Требуется: $(a_1, a_2)_p(a_1, a_3)_p(a_2, a_3)_p = (-1, -a_1a_2a_3)_p \Leftrightarrow (a_1, a_2)_p(a_1, a_3)_p(a_2, a_3)_p(-a, d) = (-1, -1)_p$.

Очевидно, для решения задачи вида $a = b \Leftrightarrow c = d$, где (a, b, c, d) из множества $\{1, -1\}$, достаточно проверить $ac = bd$, то есть

$$(-a, d)_p = (-1, -d)_p(-1, -1)_p \quad \Leftrightarrow \quad (-a, d)_p = (-1, -1)_p(-1, -1)_p(-1, d)_p \quad \Leftrightarrow$$
$$\Leftrightarrow \quad (-a, d)_p = (-1, d)_p \quad \Leftrightarrow \quad (-1, d)_p(-a, d)_p = 1 \quad \Leftrightarrow \quad (a, d)_p = 1 \quad \Leftrightarrow$$
$$\Leftrightarrow \quad (a, a)_p(a, \frac{d}{a})_p = 1 \quad \Leftrightarrow \quad 1 \cdot 1 = 1,$$

поскольку $\frac{d}{a}$ является точным квадратом в $\mathbb{Q}_p$.

4) Как и в 3), требуется решить уравнение

$$a_1x_1^2 + a_2x_2^2 + a_3x_3^2 + a_4x_4^2 - ax_5^2 = 0.$$

Но у него всегда есть решения по задаче 34d.

Также доказательство этого факта можно прочитать в книжке Ж.-П. Серра “A course in arithmetic”, Глава 4, § 2, Следствие Теоремы 6 □

Задача 36. Докажите принцип Минковского-Хассе.

Доказательство. Доказательство этого факта можно прочитать в книжке Ж.-П. Серра “A course in arithmetic”, Глава 4, § 3, Теорема 8. □

Задача 37. Используя задачу 35 и принцип Минковского-Хассе, докажите, что целое число n представимо в виде суммы трёх квадратов рациональных чисел, если и только если оно не представимо в виде $4^a(8b-1)$, т.е. если $-n$ не является полным квадратом в $\mathbb{Q}_2$.

Доказательство. По теореме Минковского-Хассе достаточно проверить, есть ли у уравнения $x^2+y^2+z^2 = n$ p-адические решения или нет. Сохраняем обозначения решения задачи 35. $a_1 = a_2 = a_3 = 1$, $d = 1$, $\varepsilon = (1,1)_p^3 = (1,1)_p$, $a = n$. Сначала докажем, что для $p > 2$ уравнение решается в p-адических числах.

Если n не имеет вид $-m^2$, то всё доказано. Если $n = -m^2$, то $\varepsilon = (1,1)_p = [Problem30] = 1 = [Problem30] = (-1,-1)_p$, то есть у него есть решения.

Осталось рассмотреть случай $p = 2$. Если $n \neq -m^2$, то задача решена. Теперь пусть $n = -m^2$.

Если у уравнения есть решение, то

$$\varepsilon = (1,1)_2 = (-1,-1)_2,$$

что противоречит задаче 31. □

Задача 38. Фиксируем целое число n. Докажите, что если существуют рациональные числа x, y, z такие, что $x^2 + y^2 + z^2 = n$, то существуют и целые числа x', y', z' такие, что

$$(x')^2 + (y')^2 + (z')^2 = n.$$

Выведите из этого утверждения теорему Гаусса.

Доказательство. Пусть рациональные числа x, y, z таковы, что $x^2+y^2+z^2 = n$. Пусть d — это общий знаменатель чисел x, y, z. Выберем x, y, z так, чтобы d было наименьшим возможным. Допустим, что $d > 1$ (т.е. что одно из чисел x, y или z нецело и целых решений у уравнения $x^2 + y^2 + z^2 = n$ нет). Пусть r_x, r_y, r_z — это ближайшие к x, y, z числа соответственно, $s_x := x - r_x, s_y := y - r_y, s_z := z - r_z$. Тогда

$$|s_x|, |s_y|, |s_z| \leqslant \frac{1}{2}, \qquad s_x^2 + s_y^2 + s_z^2 = n - (r_x^2 + r_y^2 + r_z^2) - 2(s_xr_x + s_yr_y + s_zr_z). \tag{15}$$

Положим

$$x' = r_x - \frac{s_x(n - r_x^2 - r_y^2 - r_z^2)}{s_x^2 + s_y^2 + s_z^2}, \qquad y' = r_y - \frac{s_y(n - r_x^2 - r_y^2 - r_z^2)}{s_x^2 + s_y^2 + s_z^2}, \qquad z' = r_z - \frac{s_z(n - r_x^2 - r_y^2 - r_z^2)}{s_x^2 + s_y^2 + s_z^2}.$$

Из (15) следует, что $s_x^2 + s_y^2 + s_z^2 = d'/d$, причём $0 < d' < d$. Откуда следует, что общий знаменатель x', y', z' делит d', то есть меньше d. Заметим, что $x'^2 + y'^2 + z'^2 = n$. Противоречие. Следовательно, $d = 1$ и уравнение $x^2 + y^2 + z^2 = n$ имеет решение в целых числах.

По задаче 37 любое целое положительное число N, не представимое в виде $4^n(8m-1)$ является суммой трёх квадратов рациональных чисел. Благодаря текущей задаче, такое число N есть и сумма трёх квадратов целых чисел. □

Задача 39. Выведите из теоремы Гаусса теорему Лежандра.

Доказательство. Из теоремы Гаусса следует, что всякое положительное целое число, имеющее остатки 1, 2, 3, 5, 6 при делении на 8 представимо в виде суммы трёх квадратов (а, значит, и виде суммы четырёх квадратов). Таким образом, достаточно доказать, что любое положительное целое число, имеющее остатки 0, 4, 7 при делении на 8 представимо в виде суммы 4 квадратов.

Если число n представимо в виде суммы четырёх квадратов, то $4n$ тоже представимо. Отсюда следует, что достаточно доказать, что любое число, имеющее остаток 7 при делении на 8 представимо в виде суммы четырёх квадратов.

Фиксируем положительное целое число n, имеющее остаток 7 при делении на 8. Так как $n-1$ имеет остаток 6 при делении на 8, то $n-1$ представимо по теореме Гаусса в виде суммы трёх квадратов. Следовательно, n представимо в виде суммы четырёх квадратов. $\square$

Важные свойства символа Гильберта

Цель этого раздела — доказать, что для фиксированной пары ненулевых целых чисел (a, b) символ Гильберта $(a, b)_p$ равен 1 для почти всех (=всех, кроме конечного числа) простых чисел p. Как водится, это утверждение является частным случаем более общего утверждения.

Задача 40. a) Пусть f – это однородный многочлен степени n от k переменных, где $k > n$. Тогда число решений f (включая нулевое) в остатках при делении на p делится на p (Подсказка: примените малую теорему Ферма и рассмотрите случай $p = 2$).

b) Пусть f – это многочлен степени не более n от k переменных, где $k > n$. Тогда число решений уравнения $f = 0$ в остатках при делении на p делится на p.

Доказательство. Из пункта b) пункт a) очевидно следует. Мы докажем пункт b). Рассмотрим многочлен $f(x_1, \ldots, x_k)$ степени n. Рассмотрим сумму

$$\sum_{x_1,\ldots,x_n} f(x_1, \ldots, x_n)^{p-1}, \tag{16}$$

где $x_1, \ldots, x_n$ пробегают все остатки при делении на p. Заметим, что все элементы суммы (16) равны 0 или 1 в остатках при делении на p. Соответственно, значение суммы (16) определяет остаток при делении на p числа решений уравнения $f(x_1, \ldots, x_k)$ в остатках при делении на p. Заметим что степень многочлена $f(x_1, \ldots, x_k)^{p-1}$ равна $(p-1)n$. Следовательно, в каждый моном $f(x_1, \ldots, x_k)^{p-1}$ хотя бы одна из $k > n$ переменных входит в степени меньшей $p - 1$. Заметим, что в для такого монома суммирование (16) даёт ноль, т.к.

$$\sum_{x_i} x_i^l \equiv 0 \pmod p,$$

если $l < p - 1$. Следовательно, (16)$\equiv 0 \pmod p$ и число решений уравнения $f(x_1, \ldots, x_n) = 0$ сравнимо с 0 по модулю p. □

Задача 41. Выведите из предыдущей задачи, что уравнение $ax^2 + by^2 + cz^2 = 0$ от переменных x, y, z имеет ненулевое решение в остатках при делении на p.

Доказательство. Многочлен $ax^2 + by^2 + cz^2$ имеет степень 2 и зависит от трёх переменных. Следовательно, число решений уравнения $ax^2 + by^2 + cz^2 \equiv 0$ сравнимо с 0 по модулю p. В частности, это значит, что у уравнения $ax^2 + by^2 + cz^2 \equiv 0$ есть ненулевое решение. □

Задача 42. Выведите из предыдущей задачи, что для пары ненулевых целых чисел (a, b) символ Гильберта $(a, b)_p$ равен единице, если $a, b \not\vdots\, p$. Объясните, почему символ Гильберта $(a, b)_p$ равен 1 для почти всех p.

Доказательство. Фиксируем $p \neq 2$ и такое, что a, b не делится на p. Докажем, что $(a, b)_p = 1$.

Пусть (x_0, y_0, z_0) — какое-то решение уравнения $z^2 - ax^2 - by^2 \equiv 0 \pmod p$ такое, что

$$(x_0, y_0, z_0) \not\equiv (0, 0, 0) \pmod p$$

(такое решение существует по задаче 41). Без ограничения общности считаем, что $z_0 \not\equiv 0 (\mathrm{mod}\, p)$. Тогда в силу задачи 21 число $ax_0^2 + by_0^2$ является полным квадратом в p-адических числах и, следовательно, уравнение $z^2 - ax^2 - by^2 = 0$ имеет ненулевое решение в p-адических числах, т.е. $(a, b)_p = 1$. □

Задача 43. Выведите из задачи 41, что уравнение $ax^2 + by^2 + cz^2 + dv^2 + ew^2 = 0$ от переменных x, y, z, v, w (a, b, c, d, e – это целые параметры) имеет ненулевое решение в $\mathbb{Q}_p$ для всех простых чисел p.

Доказательство. Без ограничения общности считаем, что числа a, b, c, d, e целые и свободны от квадратов. Докажем, что мы можем считать, что никакие три из чисел a, b, c, d, e не имеют общего делителя. Действительно, пусть p — это общий простой делитель трёх или более чисел. Тогда, умножая уравнение $ax^2 + by^2 + cz^2 + dv^2 + ew^2 = 0$ на p и сокращая полные квадраты, приходим к уравнению, в

котором p делит не более 2 из чисел a, b, c, d, e. Очевидно, что эта процедура «сокращения простого делителя» применима независимо ко всем простым делителям чисел a, b, c, d, e. Таким образом, для каждого простого числа p по крайней мере 3 из чисел a, b, c, d, e не делятся на p.

Фиксируем простое число p. Без ограничения общности считаем, что a, b, c не делятся на p.

Если p — нечётное простое число, то, используя задачу 42, получаем, что уравнение

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

(а, следовательно, и уравнение $ax^2 + by^2 + cz^2 + dv^2 + ew^2 = 0$) имеет ненулевое решение в $\mathbb{Q}_p$.

Если $p = 2$, то задачу можно решать перебором остатков чисел a, b, c, d, e по модулю 8. □

Задача 44. Докажите, что для всякой пары ненулевых целых чисел (a, b) имеет место равенство

$$\prod_p (a, b)_p = (a, b)_{-1}, \tag{17}$$

где произведение берётся по всем простым числам p, а

$$(a, b)_{-1} = \begin{cases} 1, & \text{если уравнение } z^2 - ax^2 - by^2 = 0 \text{ имеет решение в } \mathbb{R}, \\ -1 & \text{иначе.} \end{cases}$$

Доказательство. В силу мультипликативности символа Гильберта (задача 32), достаточно проверить (17) для случая, когда a, b — это простые числа или -1.

Начнём со случая, в котором $a = b = -1$. Тогда $(a, b)_p = (-1, -1)_p$ может быть не равно 1, только если $p = 2$. В этом случае непосредственно проверяется, что $(-1, -1)_2 = (-1, -1)_{-1} = -1$.

Следующий случай: $a = -1$, b — это простое число. Тогда $(a, b)_p = (-1, b)_p$ может быть не равно 1, только если $p = b$ или $p = 2$. В этом случае непосредственно проверяется, что $(-1, p)_p = (-1, p)_2$ для $p \neq 2$ и $(-1, 2)_2 = 1$. Откуда следует, что левая часть (17) равна правой части (17) и равна 1. □

Имеет место следующий «далёкий аналог китайской теоремы об остатках»: оказывается, что по значениям символа Гильберта может быть построен элемент с данными значениями.

Задача 45. Зафиксируем конечный набор ненулевых целых чисел a_i и для каждого простого p зададим значения $\varepsilon_{i,p} = \pm 1$. Тогда система уравнений

$$(a_i, x)_p = \varepsilon_{i,p} \quad \forall i,\ \forall p,$$

имеет решение, если и только если

a) почти все (=все кроме конечного числа) $\varepsilon_{i,p} = 1$,

b) для каждого простого числа p существует ненулевое p-адическое число x_p такое, что

$$(a_i, x_p) = \varepsilon_{i,p}.$$

Доказательство. Доказательство этого факта можно прочитать в книжке Ж.-П. Серра “A course in arithmetic”, Глава 3, § 2, Теорема 4. □

Уравнения от двух переменных и карты (ДУ-3)

Рассматривается уравнение

$$E_m: \quad ax^2 + bxy + cy^2 = m \tag{18}$$

от целых переменных x, y, где a, b, c, m — какие-то целые числа (параметры).

Задача 46 (Суперзадача)**.** Докажите, что если уравнение E_m имеет решения при каком-то положительном числе m, при каком-то отрицательном числе m и не имеет решений при $m = 0$, то для всякого m или E_m не имеет решений, или же E_m имеет бесконечно много решений.

Доказательство. Из условия задачи следует, что $f(x, y) = ax^2 + bxy + cy^2$ является знакопеременной квадратичной формой и не представляет 0. Следовательно, карта f разделяется на положительную и отрицательную часть периодической рекой. Следовательно, карта f периодична и, следовательно, любое значение, выписанное на карте, повторяется на ней бесконечно много раз. Откуда и следует утверждение суперзадачи. □

Задача 47 (Суперзадача)**.** Верно ли, что если уравнение E_m имеет решения в целых числах при

$$m = \pm 1,\ \pm 2,\ \pm 3,$$

то E_m имеет решения при всяком целом числе m?

Доказательство. Имеется контрпример: $f(x, y) = x^2 + xy - 18y^2$. □

Задача 48 (Суперзадача)**.** Докажите, что если уравнения E_1, E_2, E_3, E_5 имеют решения в целых числах, то уравнение E_m имеет решения при каком-то $m < 0$.

Доказательство. Допустим обратное, то есть допустим, что f положительно определена или неотрицательно определена. Мы рассмотрим эти два случая отдельно.

Пусть f неотрицательно определена. Тогда $f(x, y) = r(px + qy)^2$ для каких-то целых чисел r, p, q. Так как f представляет 1, то $r = 1$. Но тогда f не представляет 5.

Пусть теперь f положительно определена. Без ограничения общности считаем, что

$$f = px^2 + qy^2 + r(x - y)^2$$

для каких-то неотрицательных чисел p, q, r (см. задачу 60). Числа p, q, r или одновременно целые или одновременно полуцелые. Без ограничения общности считаем, что $p \geq q \geqslant r$.

Наименьшее ненулевое значение f равно $q + r$. Так как f представляет 1, $q + r = 1$. Следовательно, или $q = 1$, $r = 0$, или $q = r = \frac{1}{2}$. Мы рассмотрим оба этих случая.

Положим, что $q = 1$, $r = 0$. Так как f представляет 2, то $p = 1$ или $p = 2$. В первом случае f не представляет 3, а втором случае f не представляет 5.

Положим теперь, что $q = r = \frac{1}{2}$. Тогда для всех положительных p имеем

$$f(x, y) \geqslant x^2 - xy + y^2.$$

Так как f представляет 2, то $f(x, y) = 2$ для каких-то целых чисел x, y. В частности, $x^2 - xy + y^2 \leq 2$. Это неравенство выполнено для следующих пар (x, y):

$$(0, 1), \qquad (1, 0), \qquad (1, 1).$$

Так как $f(0, 1) = 1$, остаётся два варианта: $f(1, 0) = 2$, $f(1, 1) = 2$. Мы рассмотрим оба этих варианта.

Положим $f(1, 0) = 2$. Тогда $p = \frac{3}{2}$, $f = y^2 - xy + 2y^2$. В этом случае f не представляет 3.

Положим $f(1, 1) = 2$. Тогда $p = \frac{3}{2}$, $f = y^2 - xy + 2y^2$. В этом случае f не представляет 3. □

Рисуем картинки

Задача 49. Покажите, что если $\{w_1, w_2\}$ — это базис $\mathbb{Z}^2$, то пары

$$\{w_2, w_1\},\ \{w_1 - w_2, w_2\},\ \{w_1 + w_2, w_2\},\ \{-w_1, w_2\} \tag{19}$$

также являются базисами $\mathbb{Z}^2$.

Доказательство. По аналогии с решением задачи 11. □

Задача 50. Покажите, что преобразованиями (19) можно из любого базиса получить любой другой.

Доказательство. Пусть $\{u, v\} := \{(a, b), (c, d)\}$ — какой-то базис $\mathbb{Z}^2$. Мы докажем, что преобразованиями (19) можно получить из любого базиса $\{u, v\}$ базис $\{(1, 0), (0, 1)\}$. Рассмотрим квадратичную форму $f(x, y) := x^2 - xy + y^2$. В соответствии с задачей 60 в каком-то базисе $\{u', v'\}$, получаемом из $\{u, v\}$ преобразованиями (19) форма f будет эквивалентна форме вида

$$\begin{gathered} px^2 + qy^2 + r(x + y)^2, \\ 2p = f(v') + f(u' + v') - f(u') \geqslant 0, \\ 2q = f(u') + f(u' + v') - f(v') \geqslant 0, \\ 2r = f(u' + v') - f(u') - f(v') \geqslant 0. \end{gathered} \tag{20}$$

Наименьшие значения формы (20) достигаются на парах (x, y) равных

$$(0, 1), \qquad (1, 0), \qquad (1, 1), \tag{21}$$

и значение на любой другой паре (x, y) больше хотя бы одного из этих значений. Так как $x^2 - xy + y^2$ положительно определена, значение (20) на всех парах, кроме пар списка (21), больше 1. Следовательно, значение (20) на парах (21) равно 1. Что влечёт одно утверждение из трёх идущих ниже

$$\{u', v'\} = \{(0, 1), (1, 0)\}, \qquad \{u', v'\} = \{(0, 1), (1, 1)\}, \qquad \{u', v'\} = \{(1, 0), (1, 1)\}. \tag{22}$$

Следовательно, базис $\{u, v\}$ эквивалентен одному из базисов (22). Что и требовалось доказать. □

Задача 51. Покажите, что квадратичная форма может записываться одинаково в нескольких разных базисах.

Доказательство. Форма $x^2 - 2y^2$ имеет один и тот же вид в базисах $\{(3, 2), (4, 3)\}$ и $\{(1, 0), (0, 1)\}$. □

Задача 52. Укажите квадратичную форму, для которой любым двум разным базисам $\mathbb{Z}^2$ соответствуют различные квадратичные формы.

Доказательство. Положим $f(x, y) := 2x^2 - xy + 3y^2$. Покажем, что разным базисам соответствуют разные формы. Допустим обратное, т.е. что существуют два разных базиса, в которых форма имеет один и тот же вид. Будем последовательно и синхронно восстанавливать по этим базисам всю карту квадратичной формы. Рассмотрим первое пересечение областей восстановления. Это пересечение есть или ребро или вершина. Рассмотрим эти случаи отдельно.

Пусть это пересечение — вершина. Тогда карта квадратичной формы, симметрична относительно одного из рёбер, выходящих из этой точки. Как следствие, единственный колодец формы $2x^2 - xy + 3y^2$ также симметричен относительно одного из рёбер, выходящих из него. Что неверно, так как значения вокруг колодца равны 2, 3, 4.

Пусть это пересечение — ребро. Тогда карта квадратичной формы, сохраняется при перемене местами вершин ребра. Как следствие, вершинами ребра являются колодцы, в частности, форма $2x^2 - xy + 3y^2$ имеет два колодца. Противоречие.

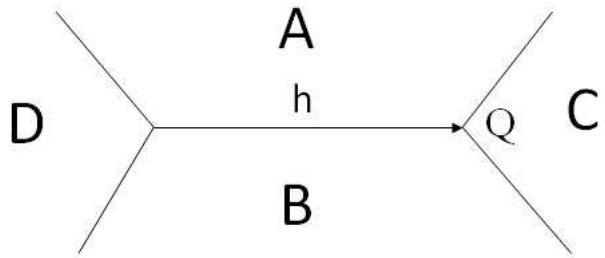
Следовательно, форма $2x^2 - xy + 3y^2$ имеет разный вид в разных базисах. □

Упражнение 1. Выпишите все расширения данного базиса $\{w_1, w_2\}$. Выпишите все специализации данного супербазиса $\{\pm w_1,\ \pm w_2,\ \pm(w_1 + w_2)\}$.

Упражнение 2. Нарисуйте (ориентированные) карты для квадратичных форм

$$f_1 = 3x^2 + 9xy + 7y^2, \quad f_2 = x^2 - 2y^2, \quad f_3 = x^2 - 3y^2.$$

В следующих двух задачах числа A, B, C, D, h относятся к картинке



Задача 53. Покажите, что для чисел A, B, C, D, h выполнены соотношения:

$$C = A + B + h, \quad D = A + B - h.$$

Доказательство. Утверждение задачи эквивалентно следующему тождеству для квадратичных форм.

$$f(x + y) + f(x - y) = 2(f(x) + f(y)).$$

□

Задача 54. Пусть A, B, C положительны, а ребро h направлено от C к D. Покажите, что тогда число D также положительно, а стрелки на двух остальных рёбрах, инцидентных вершине Q, направлены прочь от Q.

Доказательство. Так как $D, h > 0$, $C = D + 2h > 0$. Числа в областях, инцидентных рёбрам, инцидентным вершине D равны

$$4A + 2h + B, 4B + 2h + A \ (> A, B). \tag{23}$$

Следовательно, оставшиеся две стрелки направлены от вершины D. □

Задача 55. Докажите, что граф, задаваемый точками-супербазисами и рёбрами-базисами, является деревом, т.е. не содержит циклов.

Доказательство. Рассмотрим квадратичную форму $f(x, y) = x^2 + xy + y^2$. Её карта обладает единственным колодцем Q и по задаче 54 все стрелки этой карты направлены прочь от Q. Если бы на карте существовал цикл, то все стрелки не могли бы быть направлены прочь от Q. Следовательно, карта формы f не содержит циклов. Но сам граф карты не зависит от формы, поэтому для любой f он будет деревом. □

Задача 56. Пусть Q — единственный колодец положительно определённой квадратичной формы f, а p, q, r — это числа, записанные в областях, примыкающих к Q. Покажите, что в любой другой области карты f написано число, большее, чем любое из чисел p, q, r.

Доказательство. Фиксируем область A такую, что

a) A не граничит с колодцем,

b) значение f на A наименьшее среди всех областей, удовлетворяющих a).

Мы докажем, что $f(A) > p, q, r$. Это завершит решение задачи. Выделим наименьший по длине путь W от A до колодца Q. Так как W кратчайший, то он упирается в A. По определению колодца все стрелки с ним граничащие направлены от него. Из этого и задачи 54 следует, что все стрелки W направлены от Q. Следовательно, последняя стрелка в пути W указывает на A. В силу условий a), b), это возможно только если W состоит из одного ребра. Для областей, соединённых ребром с колодцем, утверждение задачи проверяется непосредственно (см. формулу (23)). □

Задача 57. Докажите, что всякая положительно определённая квадратичная форма обладает колодцем.

Доказательство. Выберем вершину карты Q, для которой сумма значений в соседних областях наименьшая. Она и будет колодцем (см. также задачу 53). □

Задача 58. a) Докажите, что положительно определённая квадратичная форма имеет не более двух колодцев.

b) Укажите квадратичную форму, обладающую двумя колодцами.

Доказательство. b) Форма $x^2 + y^2$ положительно определена и обладает двумя колодцами.

a) Пусть Q — это какой-то колодец, а $p \geqslant q \geqslant r$ — это значения в областях вокруг него. Есть два случая $q + r > p$ или $q + r = p$. Мы рассмотрим эти случаи отдельно.

Положим, что $q + r > p$. Тогда все три стрелки, выходящие из Q, направлены прочь от Q. Фиксируем вершину Q' и предположим, что она является колодцем. Пусть W — это кратчайший путь, соединяющий Q и Q'. По задаче 54, все стрелки W направлены от Q к Q'. Следовательно Q' — не колодец.

Положим, что $q+r = p$. Тогда второй конец ребра E, отделяющего значение q от значения r, также является колодцем, и мы обозначим его Q'. Наборы чисел вокруг Q и Q' одинаковы. Пусть существует ещё один колодец Q'' и пусть W — это кратчайший из путей, соединяющих Q'' либо с Q, либо с Q'. Тогда W не проходит через второй колодец. Без ограничения общности мы считаем, что W соединяет Q с Q''. Тогда все рёбра на W направлены от Q, и, следовательно, Q'' не является колодцем. □

Задача 59. Объясните, как решить уравнение $ax^2 + bxy + cy^2 = m$ (a, b, c, m — параметры, x, y, z — переменные) в предположении, что форма $ax^2 + bxy + cz^2$ положительно определена.

Доказательство. После замены переменных, мы можем считать, что $f = px^2 + q(x - y)^2 + ry^2$ для положительных чисел p, q, r (см. задачу 60). Если $f(x, y) = n$ имеет решение в целых числах, то

$$px^2 \leqslant n, ry^2 \leqslant n. \tag{24}$$

Число пар целых чисел (x, y), для которых x, y удовлетворяют неравенствам (24), конечно. Проверив их все, мы определим, имеет ли уравнение $f(x, y) = n$ решение или нет. □

Задача 60 (Классификация положительно определённых квадратичных форм)**.**

a) Покажите, что каждая положительно определённая квадратичная форма эквивалентна квадратичной форме вида

$$(p + q)x^2 + 2qxy + (q + r)y^2 \tag{25}$$

для какого-то набора положительных чисел p, q, r.

b) Покажите, что две квадратичные формы, соответствующие наборам

$$(p_1, q_1, r_1) \text{ и } (p_2, q_2, r_2),$$

эквивалентны тогда и только тогда, когда эти наборы совпадают как множества.

c) Определите какие наборы (p, q, r) задают целую квадратичную форму.

d) Определите какие наборы (p, q, r) задают положительно определённую квадратичную форму.

Доказательство. Пусть Q — это какой-то колодец f, а m, n, k — это числа вокруг колодца. Положим

$$p = \frac{m + n - k}{2}, q = \frac{m + k - n}{2}, r = \frac{k + n - m}{2}.$$

Тогда f эквивалентна форме

$$px^2 + qy^2 + r(x - y)^2 = (25).$$

Пункт b) в наших обозначениях неверен. Контрпример: $x^2 + 3y^2$ и $x^2 + xy + y^2$. В условии требуется исправить «эквивалентны» на «линейно эквивалентны».

Ответ пункта c): когда числа p, q, r целы, или когда числа $p - \frac{1}{2}$, $q - \frac{1}{2}$, $r - \frac{1}{2}$ целы.

Ответ пункта d): форма f положительно определена, если $p, q, r \geqslant 0$ и хотя бы два из чисел p, q, r отличны от 0. □