

Экспоненциальные диофантовы уравнения

Проект подготовили и представляют:
И. Климанова, П. Козлов, А. Мирошников.

Аннотация

В этом проекте мы познакомим вас с некоторыми экспоненциальными диофантовыми уравнениями и методами их решения. Он состоит из нескольких разделов, и мы рекомендуем решать задачи в том порядке, в котором они представлены.

В разделе 1 мы исследуем экспоненциальные диофантовы уравнения вида $a^x - b^y = c$.

Раздел 2 посвящен нахождению пар последовательных чисел, все простые делители которых лежат в заданном множестве. Мы покажем, что таких пар конечное число, и все они могут быть получены из решения конечного количества уравнений Пелля.

В разделе 3 приведены несколько классических и олимпиадных задач, которые сводятся к обобщённому уравнению Пелля и решаются изучением простых делителей одной из компонент его решений.

При помощи раздела 4 вы научитесь решать некоторые уравнения в факториальных кольцах, а задачи раздела 6 помогут вам доказывать факториальность колец определённого вида.

Наконец, в разделе 5 собраны несколько классических уравнений Лебега-Нагеля, которые вы можете решить, применив методы, описанные в проекте.

Содержание

1	Об уравнении $a^x - b^y = c$	2
2	О задаче Стёрмера	9
3	По следам Стёрмера	22
4	Об уравнениях в факториальных кольцах	29
5	Об уравнениях Лебега-Нагеля	36
6	К доказательству факториальности	43

Благодарности.

Авторы проекта благодарят О. Никитенко, М. Суркова и Ю. Хромина за неоценимую помощь в проверке решений участников конференции.

1 Об уравнении $a^x - b^y = c$

Этот раздел посвящён следующей теореме:

Теорема. Для любых натуральных чисел $a, b \geq 2$ и натурального c уравнение

$$a^x - b^y = c \quad (*)$$

имеет не более двух решений (x, y) в натуральных числах.

Доказательство этой трудной теоремы не является частью этого проекта. Вместо этого мы займемся *поиском* и *подсчетом количества* всех решений уравнения $(*)$ для конкретных значений a, b, c .

Предполагается, что все уравнения ниже необходимо решить в натуральных числах, если явно не указано обратное.

Задача 1.1. Решите уравнения (а) $2^x - 3^y = 1$; (б) $3^x - 2^y = 1$

Решение. (а) Так как $3^y \not\equiv -1 \pmod{8}$, то $x \leq 2$. Остаётся проверить $x = 1, 2$.

Ответ: $(2, 1)$.

(б) Если $y \geq 3$, то $3^y \equiv 1 \pmod{8}$. Это сравнение выполняется тогда и только тогда, когда y делится на 2. Пусть $y = 2t$, тогда $(3^t - 1)(3^t + 1) = 2^y$, и $3^t - 1, 3^t + 1$ являются степенями 2. Это возможно только если $t = 1, y = 3$.

Ответ: $(1, 1), (2, 3)$. ■

Иногда много информации о структуре решений уравнения $(*)$ можно получить, исследуя его по разным модулям. Предлагаем убедиться в этом на примере следующих двух задач.

Задача 1.2. Предположим, с некоторыми натуральными c, x, y выполняется равенство $2^x - 3^y = c$. Докажите, что

(а) если $x \geq 3$, то $c \equiv 5, 7 \pmod{8}$;

(б) если $c = 2^k + 3^l$ при целых $k \geq 3, l \geq 1$, то решений нет.

Решение. Оба пункта решаются рассмотрением по модулю 8. ■

Задача 1.3. Найдите все натуральные $c \leq 100$ такие, что уравнение $2^x - 3^y = c$ имеет два решения.

Решение. *Шаг 1: сужение c .* Если $2 \mid c$ или $3 \mid c$, то $2^x - 3^y = c$ невозможно. При $x = 1$ уравнение даёт $3^y < 0$, а при $x = 2$ получаем лишь $c \in \{1\}$ (при $y = 1$). Значит, для двух решений необходимо $x \geq 3$, откуда по Задаче 1.2а

$$c \equiv 5 \text{ или } 7 \pmod{8}.$$

Шаг 2: малые x . Прямая проверка при $3 \leq x \leq 9$ (то есть $2^x \leq 512$) среди чисел $c \leq 100$, удовлетворяющих условиям шага 1, показывает: два решения имеют только $c = 5$ и $c = 13$.

Шаг 3: отсекание больших x . Покажем, что при $x \geq 10$ новых решений нет ни для одного из оставшихся c . Работаем по модулям $2^{10} = 1024$ и 257 (простое, порядок 2 по модулю 257 равен 16, а порядок 3 равен 256).

Для каждого c решаем сравнение $3^y \equiv -c \pmod{1024}$: так как порядок 3 по модулю 1024 равен 256, получаем конечный набор допустимых вычетов $y \pmod{256}$. Для каждого такого y значение $3^y + c \pmod{257}$ фиксировано (порядок 3 mod 257 тоже 256).

Остаётся проверить, что ни одно из полученных значений $3^y + c \pmod{257}$ не совпадает ни с одним из 16 вычетов $\{2^x \pmod{257}\}$. Это конечная проверка, которая для всех допустимых $c \leq 100$ даёт отрицательный ответ.

Следовательно, при $x \geq 10$ уравнение $2^x - 3^y = c$ решений не имеет, и ответ исчерпывается $c \in \{5, 13\}$.

Ответ: $c = 5, 13$. ■

Ниже рассмотрим некоторые исключительные случаи уравнения (*).

Задача 1.4. Предположим, что числа a, b, c не являются взаимно простыми. Докажите, что уравнение (*) имеет конечное количество решений.

Решение. Если какие-то два числа имеют общий простой делитель p , то из уравнения следует, что на p делятся все три числа. Если $x, y > m = v_p(c)$, то левая часть уравнения делится на p^{m+1} , в то время как правая не делится. Значит, одна из переменных x, y ограничена сверху, а, значит, ограничена и вторая. ■

Задача 1.5. Предположим, что каждый простой делитель числа a также делит b . Докажите, что уравнение (*) имеет не более одного решения.

Решение. Предположим, существуют два решения (x_1, y_1) и (x_2, y_2) , причём $x_1 < x_2$ и, как следствие, $y_1 < y_2$. Тогда

$$a^{x_1}(a^{x_2-x_1} - 1) = b^{y_1}(b^{y_2-y_1} - 1).$$

Любой простой делитель p числа a также делит b , поэтому $v_p(a^{x_1}) = v_p(b^{y_1})$. Следовательно, a^{x_1} делит b^{y_1} , поэтому $c = a^{x_1} - b^{y_1} < 0$, но $c > 0$. Противоречие. ■

Сконцентрируемся теперь на случае взаимно простых a, b, c . Для начала обратим внимание на случай $c = 1$.

Задача 1.6. Докажите, что для любого натурального $b > 1$ уравнение $2^x - b^y = 1$ не имеет решений при $y > 1$.

Решение. Пусть y четное. Поскольку b нечётно, имеем $b^y + 1 \equiv_4 2 \equiv 2^x$, откуда $x = 1$ и решений нет.

Пусть y нечетно. Тогда

$$2^x = b^y + 1 = (b + 1)(b^{y-1} - b^{y-2} + \dots - b + 1),$$

откуда $(b^{y-1} - b^{y-2} + \dots - b + 1) = 2^k$ для некоторого k . Но число $b^{y-1} - b^{y-2} + \dots - b + 1$ нечётно, как сумма нечётного числа нечётных чисел, следовательно, $b + 1 = 2^x$ и $y = 1$. ■

Определение. Рассмотрим взаимно простые натуральные числа z и M . Порядком числа z по модулю M , обозначаем $\text{ord}_z(M)$, назовём наименьшее натуральное число h такое, что $z^h \equiv 1 \pmod{M}$.

Из теоремы Эйлера следует, что число $\text{ord}_z(M)$ существует и делит $\varphi(M)$. Легко также заметить, что если (x, y) — решение уравнения $(*)$ с $c = 1$, то $x = \text{ord}_a(b^y)$.

Задача 1.7. Пусть $b = p$ — нечётное простое число.

(а) Докажите, что существует такое целое v такое, что

$$\text{ord}_a(p^{n+1}) = \begin{cases} \text{ord}_a(p^n), & \text{если } n < v \\ p \cdot \text{ord}_a(p^n), & \text{если } n \geq v. \end{cases}$$

(б) Докажите, что уравнение $a^x - p^y = 1$ имеет не более одного решения.

Решение. (а) Возьмем в качестве $v > 0$ максимальную степень числа p , на которую делится число $a^{\text{ord}_a(p)} - 1$. Тогда $\text{ord}_a(p) = \dots = \text{ord}_a(p^v)$ по определению. Осталось доказать равенство $\text{ord}_a(p^{n+1}) = p \cdot \text{ord}_a(p^n)$ для всех $n > v$. Зафиксируем произвольное n . Покажем, что число $a^{p \cdot \text{ord}_a(p^n)} - 1$ делится на p^{n+1} , но не делится на p^{n+2} . Действительно,

$$a^{p \cdot \text{ord}_a(p^n)} - 1 = \left(a^{\text{ord}_a(p^n)}\right)^p - 1 = (1 + p^n q)^p - 1 \stackrel{(1)}{=} \sum_{i=1}^p C_p^i p^{in} q^n = p^{n+1} Q.$$

Равенство (1) верно по биному Ньютона, а $Q \equiv q \not\equiv 0 \pmod{p}$ по определению $\text{ord}_a(p^n)$ и поскольку все слагаемые вида $C_p^k p^{kn} q^n$ делятся на p^{n+2} при $k > 1$.

Осталось доказать, что ни для какого m в пределах $\text{ord}_a(p^n) < m < p \cdot \text{ord}_a(p^n)$ число $a^m - 1$ не делится на p^{n+1} . Предположим, такое m нашлось. Тогда $p \cdot \text{ord}_a(p^n)$ делится на m и m делится на $\text{ord}_a(p^n)$. Но p простое, а, значит, это невозможно.

(б) Пусть нашлось два решения $(\text{ord}_a(p^n), n)$ и $(\text{ord}_a(p^{n+m}), n+m)$, где $m > 0$. Тогда по пункту (а) имеем $\text{ord}_a(p^{n+m}) = p^m \text{ord}_a(p^n)$. Таким образом,

$$a^{\text{ord}_a(p^{n+m})} - 1 = \left(a^{\text{ord}_a(p^n)}\right)^{p^m} - 1 = (1 + p^n)^{p^m} - 1 = p^{n+m} + Q > p^{n+m},$$

где Q есть оставшиеся ненулевые слагаемые при раскрытии бинома Ньютона. ■

Задача 1.8. Докажите, что уравнение $a^x - b^y = 1$ имеет не более одного решения за исключением случая $a = 3, b = 2$.

Решение. Предположим, что нашлись два различных решения. Запишем их так, чтобы $x < s$:

$$a^x - 1 = b^y, \quad a^s - 1 = b^{y+n}$$

для некоторых $n > 0$. Тогда

$$a^s - 1 = (a^x - 1)b^n,$$

то есть $a^x - 1 \mid a^s - 1$. Покажем, что отсюда $x \mid s$. Пусть $s = qx + r$, где $0 \leq r < x$. Тогда

$$a^s - 1 = (a^x)^q a^r - 1 = (a^x - 1)((a^x)^{q-1} + (a^x)^{q-2} + \dots + 1) + (a^r - 1).$$

Так как $a^x - 1$ делит левую часть и первое слагаемое, оно делит и $a^r - 1$. Но $0 \leq a^r - 1 < a^x - 1$, значит $a^r - 1 = 0$, то есть $r = 0$. Следовательно, $s = kx$ для некоторого целого $k > 1$.

Пусть p — нечетный простой делитель b . Так как $a^x - 1 = b^y$, имеем $p \mid a^x - 1$. По LTE,

$$v_p(a^{kx} - 1) = v_p(a^x - 1) + v_p(k) = v_p(b^y) + v_p(k).$$

С другой стороны, $a^{kx} - 1 = a^s - 1 = b^{y+n}$, поэтому

$$v_p(a^{kx} - 1) = v_p(b^{y+n}) = v_p(b^y) + v_p(b^n).$$

Следовательно, $v_p(k) = v_p(b^n)$ для каждого нечетного $p \mid b$. Обозначим через b_0 нечетную часть числа b . Тогда

$$b_0^n \mid k.$$

Случай 1: b имеет нечетный простой делитель. Тогда $b_0 \geq 3$. Из $a^x = 1 + b^y$ получаем

$$b^{y+n} = a^{kx} - 1 = (1 + b^y)^k - 1 \geq b^{yk} \geq b^{yb_0^n}.$$

Для $b_0 \geq 3$ и $n \geq 1$ выполнено $b_0^n > n + 1$. Значит,

$$b^{y+n} \geq b^{yb_0^n} > b^{y(n+1)}.$$

Сравнивая показатели, получаем $y + n > y(n + 1)$, то есть $n(y - 1) < 0$. Противоречие. Следовательно, при $b_0 > 1$ двух решений быть не может.

Случай 2: $b = 2^e$, где $e \geq 1$. Тогда a нечетно и

$$a^x - 1 = 2^{ey}. \tag{1}$$

Если $x = 1$, то $a = 2^{ey} + 1$; для фиксированных a и $b = 2^e$ это дает не более одного решения.

Пусть теперь $x > 1$. Разложим

$$a^x - 1 = (a - 1)(a^{x-1} + a^{x-2} + \dots + 1) = 2^{ey}.$$

Оба множителя положительны и их произведение — степень двойки, поэтому каждый из них является степенью двойки. Сумма $S = a^{x-1} + \dots + 1$ имеет ту же четность, что и x , так как a нечетно. Поскольку $S > 1$ и S — степень двойки, S четно, а значит x четно.

Пусть $x = 2t$. Тогда

$$a^{2t} - 1 = (a^t - 1)(a^t + 1) = 2^{ey}.$$

Числа $a^t - 1$ и $a^t + 1$ — две последовательные четные степени двойки. Единственная такая пара — это 2 и 4: если 2^r и 2^s ($s > r$) отличаются на 2, то $2^r(2^{s-r} - 1) = 2$, откуда $r = 1$ и $s - r = 1$. Следовательно,

$$a^t - 1 = 2, \quad a^t + 1 = 4,$$

то есть $a^t = 3$. Значит, $t = 1$, $a = 3$, $x = 2$, и из (1) получаем

$$3^2 - 1 = 8 = 2^{ey},$$

откуда $ey = 3$.

Итак, единственное возможное решение с $x > 1$ имеет вид $a = 3$, $x = 2$, $ey = 3$. Для $b = 2^e$ это дает $e = 1$ или $e = 3$. При $e = 3$ есть только это решение ($y = 1$). При $e = 1$ получаем $b = 2$, $a = 3$, и, кроме решения $x = 2$, $y = 3$, существует еще решение $x = 1$, $y = 1$, так как $3^1 - 2^1 = 1$. Это и есть исключительный случай.

Таким образом, для всех a, b уравнение $a^x - b^y = 1$ имеет не более одного решения, за исключением пары $a = 3$, $b = 2$, для которой есть два решения:

$$3^1 - 2^1 = 1, \quad 3^2 - 2^3 = 1.$$

■

Нам неизвестен элементарный алгоритм, который по уравнению (*) при $s > 1$ находит все его решения или утверждает, что решений нет. Следующие две идеи могут быть использованы для доказательства того, что это уравнение при фиксированных параметрах a, b, c не имеет решений при достаточно больших x и y :

(1) Для любых x_0, y_0 , если пара (x, y) , где $x \geq x_0$ и $y \geq y_0$, является решением уравнения (*), то остатки чисел x и y по модулям $\text{ord}_a(b^{y_0})$ и $\text{ord}_b(a^{x_0})$ соответственно фиксированы.

(2) Если существует такой *магический модуль* P , что множества остатков, которые дают две последовательности a_n и b_m при делении на N , не пересекаются, то равенство $a_n = b_m$ невозможно ни при каких n, m .

Поиск такого модуля (если он вообще существует) может оказаться трудной задачей. Мы предлагаем искать его среди простых вида $dn + 1$, где d равно $\text{ord}_a(b^{y_0})$ или $\text{ord}_b(a^{x_0})$.

В качестве примера мы найдем все решения уравнения

$$2^x - 11^y = 5.$$

1. Легко найти решение $(x, y) = (4, 1)$. Докажем, что решения, для которого $x \geq 5$, не существует.
2. Вычислим $\text{ord}_{11}(2^5) = 8$. Из сравнения $11^y \equiv -5 \pmod{2^5}$ имеем $y \equiv 5 \pmod{8}$.
3. Поищем магический модуль среди простых вида $8n+1$. Проверим сначала $P = 17$. Пусть $a_n = 11^{5+8n} + 5$ и $b_m = 2^m$. Последовательность $\{a_n\}$ даёт остатки $-2, -5$ по модулю 17, а последовательность $\{b_m\}$ — остатки $\pm 1, \pm 2, \pm 4, \pm 8$. Делаем вывод, что $a_k \equiv b_m \equiv -2 \pmod{17}$ — в этом случае противоречия не получено.
4. Далее мы встаём перед выбором: либо рассматривать сравнение по другой степени 2 или 11, либо проверять следующее простое вида $8n+1$. Проверим, что при $x = 5$ решений нет, продолжим смотреть по модулю 2^6 , следующей степени двойки, и сделаем аналогичные шаги.
5. Из сравнения $11^y \equiv -5 \pmod{2^6}$ имеем $y \equiv 13 \pmod{16}$. Поищем магический модуль среди простых вида $16n+1$ и снова проверим $P = 17$. Пусть $a_n = 11^{13+16n} + 5$ и $b_m = 2^m$. Последовательность $\{a_n\}$ всегда даёт остаток -5 по модулю 17, а последовательность $\{b_m\}$ — остатки $\pm 1, \pm 2, \pm 4, \pm 8$. Эти множества остатков не пересекаются, поэтому уравнение $2^x - 11^y = 5$ не имеет решений при $x \geq 6$.

Ниже мы предлагаем вам решить несколько уравнений, для которых применимы одна или несколько идей, описанных выше.

Задача 1.9. Решите уравнение $10^x - 7^y = 3$.

Решение. При $x \geq 3$ решений нет, поскольку $7^y \equiv \pm 1 \not\equiv 3 \pmod{8}$. Тогда $x \leq 2$ и единственное решение $(1, 1)$ находится перебором.

Ответ: $(1, 1)$. ■

Задача 1.10. Решите уравнение $2^x - 5^y = 3$.

Решение. Проверив маленькие решения в натуральных числах, найдём, что $(3, 1)$ и $(7, 3)$ являются решениями данного уравнения. Чтобы доказать, что других решений не существует, предположим, что существует решение (x, y) , удовлетворяющее условию $x \geq 8$. Рассмотрим уравнение по модулю $2^8 = 256$. При $x \geq 8$ выполняется сравнение $2^x \equiv 0 \pmod{256}$. Исходное уравнение принимает вид

$$5^y + 3 \equiv 0 \pmod{256} \implies 5^y \equiv 253 \pmod{256}.$$

Решая это сравнение, получаем $y \equiv 35 \pmod{64}$. Проверим остатки при делении числа $5^y + 3$ при делении на магическое простое $257 = 4 \cdot 64 + 1$. Получим, что

$$5^y + 3 \equiv 17, 36, 227, \text{ или } 246 \pmod{257},$$

но ни один из этих остатков не лежит во множестве $\{2^k \pmod{257} \mid k \in \mathbb{N}^*\}$. Получено противоречие. Следовательно, предположение $x \geq 8$ неверно. Перебирая значения $x \in \{1, 2, \dots, 7\}$, мы можем убедиться в отсутствии других решений.

Ответ: $(3, 1), (7, 3)$. ■

Задача 1.11. Решите уравнение $3^x - 7^y = 2$.

Решение. Если $y = 1$, то $x = 2$. Предположим, что существует решение при $y \geq 2$, тогда $x \geq 4$, и $3^x - 9 = 7^y - 7$. Пусть $a = x - 2 \geq 2$, $b = y - 1 \geq 1$, тогда перепишем уравнение в виде

$$9(3^a - 1) = 7(7^b - 1).$$

Так как $7|3^a - 1$, мы имеем $\text{ord}_3(7) = 6|a$, поэтому $3^a - 1$ делится на $3^6 - 1$, которое делится на 13. Следовательно, $13|7^b - 1$, откуда $\text{ord}_7(13) = 12|b$. Из этого следует, что $7^b - 1$ делится на $7^{12} - 1$, которое делится на 43. Это значит, что $43|3^a - 1$, поэтому $\text{ord}_3(43) = 42|a$, и $3^a - 1$ делится на $3^{42} - 1$, которое делится на 49. Это невозможно, поскольку $7(7^b - 1)$ не делится на 49.

Ответ: $(2, 1)$. ■

Задача 1.12. (а) Найдите хотя бы одно целое $c > 4$, при котором уравнение

$$(c + 2)^x - 2^y = c$$

имеет больше одного решения.

(б) Решите это уравнение для найденного c .

Решение. Докажем, что уравнение

$$91^x - 2^y = 89$$

имеет два решения. Проверив маленькие значения x , найдём, что $(1, 1)$ и $(2, 13)$ являются решениями этого уравнения. Предположим, что найдётся решение с $x \geq 3$. Рассмотрим уравнение по модулю $7^3 = 343$, получим $2^y \equiv 254 \pmod{343}$. Отсюда следует, что $y \equiv 76 \pmod{147}$.

Проверим остатки при делении числа $2^y + 89$ при делении на магическое простое $2647 = 18 \cdot 147 + 1$. Получим, что

$$2^y + 89 \equiv 2083, 941, 1900, 1046, 1536, 1602, 2432, 437, 2059 \pmod{2647},$$

но множество эти остатков не пересекается с множеством остатков степеней 91 при делении на 2647, противоречие.

Ответ: $(1, 1), (2, 13)$. ■

В дополнение к теореме, упомянутой в начале раздела, мы верим, что верна следующая гипотеза:

Гипотеза. Количество троек натуральных чисел a, b, c , при которых уравнение $(*)$ имеет ровно два решения, конечно.

Жюри известно 15 таких троек. А сколько сможете найти вы?

Задача 1.13. Найдите как минимум 8 троек натуральных чисел a, b, c таких, что уравнение $(*)$ имеет ровно два решения.

Решение. Полный список известных жюри на данный момент троек следующий:

$$(2, 3, 5), (2, 3, 13), (4, 3, 13), (16, 3, 13), (2, 5, 3), (3, 2, 1), (13, 3, 10), (91, 2, 89), \\ (6, 2, 4), (6, 3, 1215), (6, 9, 1215), (6, 81, 1215), (15, 6, 9), (280, 5, 275), (4930, 30, 4900).$$



2 О задаче Стёрмера

Конечность решений диофантового уравнения (*) можно иначе переформулировать следующим образом: возьмем все степени числа a и все степени числа b , упорядочим их по возрастанию. Вот пример для $a = 2$, $b = 3$:

$$2^1, 3^1, 2^2, 2^3, 3^2, 2^4, 3^3, 2^5, 2^6, 3^4, 2^7, \dots$$

Тогда расстояние между соседними членами последовательности стремится к бесконечности. Иными словами, для любого целого числа найдется такой номер в последовательности, начиная с которого все последующие расстояния будут больше этого числа.

Следующее утверждение обобщает предыдущее наблюдение. Зафиксируем некоторое конечное множество Q простых чисел. Возьмем те и только те числа, простые делители которых принадлежат множеству Q , и упорядочим их по возрастанию. Ниже приведён пример для набора $Q = \{2, 3, 5\}$:

$$2^1, 3^1, 2^2, 5^1, 2^1 \cdot 3^1, 2^3, 3^2, 2^1 \cdot 5^1, 2^2 \cdot 3^1, 3 \cdot 5, \dots$$

Тогда расстояние между соседними членами последовательности стремится к бесконечности.

Доказательство этого трудного утверждения не является частью этого проекта. Вместо этого мы докажем оценку сверху на количество пар подряд идущих чисел в указанной последовательности, зависящую только от размера набора Q . Ниже будем считать, что множество Q состоит из t простых чисел

$$q_1 < q_2 < \dots < q_t.$$

Определение. Определим множество Q -гладких чисел как множество чисел вида

$$\{q_1^{e_1} q_2^{e_2} \cdots q_t^{e_t} \mid e_i \geq 0\}.$$

Согласно определению, Q -гладкими числами являются те и только те числа, любой простой делитель которых лежит в Q .

Задача 2.1. Найдите все последовательные пары $\{2, 3\}$ -гладких чисел. Другими словами, решите уравнение $2^x 3^y - 2^z 3^t = 1$ в неотрицательных целых x, y, z, t .

Решение. Поскольку $(2^x 3^y, 2^z 3^t) = 1$, то возможны лишь следующие 4 случая:

- 1) $x = 0, y = 0$. Тогда $1 - 2^z 3^t = 1$ и решений нет;
- 2) $z = 0, t = 0$. Тогда сразу находим пару $(1, 2)$;
- 3) $y = 0, z = 0$. Тогда $2^x - 3^t = 1$. По задаче 1.1.а находим пару $(3, 4)$;
- 4) $x = 0, t = 0$. Тогда $3^y - 2^z = 1$. По задаче 1.1.б находим пары $(2, 3)$ и $(8, 9)$.

Ответ: Существует всего 4 пары последовательных $\{2, 3\}$ -гладких чисел:

$$(1, 2), (2, 3), (3, 4), (8, 9).$$

■

Далее везде считаем, что D — натуральное число, не являющееся точным квадратом. Обозначим за (x_1, y_1) *фундаментальное* (минимальное положительное) решение уравнения Пелля

$$x^2 - Dy^2 = 1.$$

Все положительные решения (x_n, y_n) этого уравнения задаются равенством

$$x_n + y_n \sqrt{D} = (x_1 + y_1 \sqrt{D})^n.$$

Задача 2.2. (а) Докажите, что y_n делится на y_1 для любого натурального n .

(б) Докажите, что если n делится на k , то y_n делится на y_k .

Решение. (а) Следует из пункта (б) при $k = 1$.

(б) Поскольку n делится на k , то $n = km$ для некоторого m . Тогда утверждение следует из задачи 2.5.ж после замены $y_i = y_1 U_i$ для $i = k, n$:

$$y_n = y_{km} = y_k \sum_{i \geq 0} C_m^{2i+1} D^i x_k^{m-1-2i}.$$

■

В некоторых случаях полезно изучить простые делители y_n . Например, уравнение $a^{2k} - b^{2m+1} = 1$, частный случай уравнения (*), сводится к уравнению Пелля посредством следующей замены: $D = b, x = a^k, y = b^m$. Оказывается, в условиях этого примера проверить существование решения нетрудно по следующей задаче.

Задача 2.3. Докажите, что уравнение Пелля имеет не более одного решения (x, y) такого, что любой простой делитель y делит D .

Решение. Заметим сразу, что если (x, y) — решение уравнения Пелля, то $(x, D) = 1$ и $(x, y) = 1$. В противном случае левая часть уравнения $x^2 - Dy^2 = 1$ делится на их наибольший общий делитель, а правая — нет, что невозможно.

Теперь предположим, что утверждение задачи неверно, то есть такие два решения найдутся. Среди них хотя бы одно отлично от фундаментального решения (x_1, y_1) . Обозначим такое решение за (x_n, y_n) . Заметим, что поскольку $y_1 \mid y_n$ (по задаче 2.2.а), то любой простой делитель y_1 также делит D .

Поэтому теперь мы, на самом деле, докажем, что не существует такого решения (x, y) , отличного от фундаментального, что любой простой делитель y делит D . Далее для любого простого $p \mid n$ имеем $y_p \mid y_n$ (по задаче 2.2.б), а, значит, для решения (x_p, y_p) также выполнено, что любой простой делитель y_p делит D .

Рассмотрим U_p и его простой делитель q . По определению $y_p = U_p y_1$, поэтому $U_p \mid y_p$, откуда $q \mid y_p \Rightarrow q \mid D$.

По задаче 2.5.е:

$$U_n = \sum_{i \geq 0} C_n^{2i+1} D^i y_1^{2i} x_1^{n-1-2i}$$

Рассмотрим это выражение по модулю q . Поскольку $q \mid D$, все слагаемые при $i \geq 1$ обнуляются:

$$0 \equiv p x_1^{p-1}$$

Поскольку $(x_1, D) = 1$ и $q \mid D$, то $q \nmid x_1$. Следовательно, $q \mid p$, что для простых чисел означает $q = p$. Таким образом, единственным простым делителем U_p может быть только само число p . Значит, $U_p = p^k$ для некоторого натурального k . Также заметим, что $x_1 > 1$, поскольку $D y_1^2 \neq 0$. Поэтому $U_p \geq p x_1^{p-1} > p$. Значит, $k \geq 2$, и $p^2 \mid U_p$.

- Рассмотрим случай $p > 3$. Заметим, что все слагаемые

$$C_p^{2i+1} D^i y_1^{2i} x_1^{p-1-2i}$$

при $i \geq 2$ делятся на D^2 , то есть делятся на p^2 . Значит,

$$p x_1^{p-1} + C_p^3 D y_1^2 x_1^{p-3} \equiv 0 \pmod{p^2}.$$

Имеем $C_p^3 = \frac{p(p-1)(p-2)}{2}$, то есть $p \mid C_p^3$ при $p > 3$. А поскольку $p \mid D$, то $p^2 \mid C_p^3 D y_1^2 x_1^{p-3}$, и тогда $p^2 \mid p x_1^{p-1}$. Откуда $p \mid x_1^{p-1}$, чего быть не может, как мы уже доказывали ранее. Противоречие. Значит, наше предположение оказалось неверным, и задача доказана.

- Теперь рассмотрим случай $p = 3$. Тогда $U_3 = 3x_1^2 + D y_1^2 = 3^k$.

Положим $D = 3d$, тогда $x_1^2 + d y_1^2 = 3^{k-1}$.

Также известно, что $x_1^2 - D y_1^2 = 1$, то есть $x_1^2 - 3(3^{k-1} - x_1^2) = 1$, откуда $(2x_1 - 1)(2x_1 + 1) = 3^k$.

Значит, каждая из скобок — это некоторая степень тройки. Заметим, что разность между скобками равна 2, то есть одновременно они делиться на 3 не могут. Поэтому получаем $2x_1 - 1 = 1, 2x_1 + 1 = 3^k$. Но тогда $x_1 = 1$, противоречие.

- Осталось разобрать случай $p = 2$.

По задаче 2.5 б: $U_2 = 2x_1 U_1 = 2x_1$. Значит, $x_1 = 2^{k-1}$, где $k \geq 2$, то есть $2 \mid x_1$. А поскольку $2 \mid U_p$, то $2 \mid D$, и получаем противоречие с тем, что $(x_1, D) = 1$. ■

Эта идея позволила Стёрмеру в 1897 году доказать обещанную нами оценку сверху.

Задача 2.4. (а) Докажите, что количество пар последовательных Q -гладких чисел не превосходит количества Q -гладких чисел вида $n^2 - 1$.

(б) Докажите, что существует не более 3^t пар последовательных Q -гладких чисел.

Решение. (а) Обозначим два последовательных Q -гладких числа за S и $S + 1$. Тогда заметим, что поскольку одно из них четное, то 2 лежит в множестве Q как делитель Q -гладкого числа.

Тогда докажем, что число $4S(S + 1)$ также Q -гладкое. Действительно, любой его простой делитель p делит одно из чисел $4, S, (S + 1)$. Поскольку все три числа Q -гладкие, их простые делители принадлежат Q .

Заметим, что $4S(S + 1) = (2S + 1)^2 - 1$. Положим $n = 2S + 1$. Тогда выражение принимает вид $n^2 - 1$. Число n однозначно восстанавливается по S , следовательно, разным парам последовательных Q -гладких чисел соответствуют различные Q -гладкие числа вида $n^2 - 1$. Тогда количество таких пар не превосходит количества Q -гладких чисел вида $n^2 - 1$.

(б) Согласно пункту (а) достаточно оценить количество Q -гладких чисел вида $n^2 - 1$. Мы докажем, что их не более, чем 3^t , где $t = |Q|$.

Рассмотрим Q -гладкое число вида $n^2 - 1$. Будем строить по нему уравнение Пелля. Пусть $n^2 - 1 = p_1^{a_1} \dots p_k^{a_k}$, где все $p_i \in Q$, а все $a_i > 0$. Тогда положим $D = p_1^{b_1} \dots p_k^{b_k}$, где $b_i = 1$, если a_i нечетно, и $b_i = 2$, если четно. Такое D является Q -гладким по построению..

При этом отношение $\frac{n}{D} = p_1^{a_1-b_1} \dots p_k^{a_k-b_k}$ является полным квадратом, поскольку степени всех простых в разложении четны и неотрицательны.

Обозначим $y_n = \sqrt{\frac{n}{D}}$. Тогда пара (n, y_n) является решением уравнения $x^2 - Dy^2 = 1$. Причем, это решение обладает следующим свойством – любой простой делитель y_n делит D . Действительно, если $p \mid y_n$, то p входит в разложение $n^2 - 1$, а, значит, по определению, $p \mid D$.

Теперь докажем, что разным числам $n^2 - 1$ соответствуют разные D . Пусть не так, и для некоторых $n^2 - 1$ и $m^2 - 1$ ($n^2 - 1 \neq m^2 - 1$, т.е. $n \neq m$) было получено одно и то же значение D . Тогда у уравнения $x^2 - Dy^2 = 1$ есть два различных решения (n, y_n) и (m, y_m) (т.к. $n \neq m$), у которых все простые делители y -компоненты делят D . По задаче 2.3 получаем противоречие.

Мы получили, что разные Q -гладкие числа вида $n^2 - 1$ дают разные D . Теперь оценим количество таких D . Это Q -гладкие числа, у которых степени вхождения всех простых не превосходят 2. Это значит, что для каждого простого p_i из Q есть три возможных степени вхождения – 0, 1, 2. А все остальные простые не входят в разложение. Поэтому всего возможных D не более, чем 3^t . ■

Полученная оценка сверху обусловлена количеством уравнений Пелля, которые необходимо проверить на наличие особенного решения. Рассмотрим альтернативный подход, который требует решения только $2^t - 1$ уравнений Пелля. Он потребует до-

полнительных технических подробностей, но даст лучшую оценку на количество пар последовательных Q -гладких чисел.

По Задаче 2.2а числа $U_n := y_n/y_1$ являются натуральными. В дальнейшем нам будет удобно выделить «нетривиальные» делители y_n и исследовать свойства последовательности $\{U_n\}$.

Задача 2.5. Докажите следующие равенства

- (а) $x_{2n} = 2x_n^2 - 1$, (б) $U_{2n} = 2x_n U_n$,
 (в) $x_{m \pm n} = x_m x_n \pm D y_m y_n$, (г) $U_{m \pm n} = x_n U_m \pm x_m U_n$,
 д) $x_n = \sum_{i \geq 0} C_n^{2i} D^i y_1^{2i} x_1^{n-2i}$, (е) $U_n = \sum_{i \geq 0} C_n^{2i+1} D^i y_1^{2i} x_1^{n-1-2i}$,
 (ж) $U_{mn} = \sum_{i \geq 0} C_n^{2i+1} D^i U_m^{2i+1} y_1^{2i} x_m^{n-1-2i}$.

Решение. (а) $x_{2n} = 2x_n^2 - 1$

Рассмотрим разложение для $x_{2n} + y_{2n}\sqrt{D}$:

$$x_{2n} + y_{2n}\sqrt{D} = (x_1 + y_1\sqrt{D})^{2n} = ((x_1 + y_1\sqrt{D})^n)^2 = (x_n + y_n\sqrt{D})^2 = x_n^2 + D y_n^2 + 2x_n y_n \sqrt{D}$$

Отсюда $x_{2n} = x_n^2 + D y_n^2$. Учитывая, что (x_n, y_n) — решение уравнения Пелля ($x_n^2 - D y_n^2 = 1$), имеем $D y_n^2 = x_n^2 - 1$. Подставляя, получаем:

$$x_{2n} = x_n^2 + (x_n^2 - 1) = 2x_n^2 - 1.$$

(б) $U_{2n} = 2x_n U_n$

Из того же разложения в пункте (а) следует, что $y_{2n} = 2x_n y_n$. Разделив обе части на y_1 , получаем:

$$\frac{y_{2n}}{y_1} = 2x_n \frac{y_n}{y_1} \implies U_{2n} = 2x_n U_n.$$

(в) $x_{m \pm n} = x_m x_n \pm D y_m y_n$

Воспользуемся представлением через фундаментальное решение:

$$x_{m \pm n} + y_{m \pm n}\sqrt{D} = (x_1 + y_1\sqrt{D})^m \cdot (x_1 + y_1\sqrt{D})^{\pm n} = (x_m + y_m\sqrt{D}) \cdot (x_n + y_n\sqrt{D})^{\pm 1}$$

Причем, поскольку $(x_n + y_n\sqrt{D}) \cdot (x_n - y_n\sqrt{D}) = x_n^2 - D y_n^2 = 1$, то

$$(x_n + y_n\sqrt{D})^{-1} = (x_n - y_n\sqrt{D}).$$

Поэтому

$$x_{m \pm n} + y_{m \pm n}\sqrt{D} = (x_m + y_m\sqrt{D})(x_n \pm y_n\sqrt{D}) = (x_m x_n \pm D y_m y_n) + (x_m y_n \pm x_n y_m)\sqrt{D}.$$

Сравнивая рациональные части: $x_{m \pm n} = x_m x_n \pm D y_m y_n$.

(г) $U_{m \pm n} = x_n U_m \pm x_m U_n$

Сравнивая иррациональные части из разложения в пункте (в):

$$y_{m \pm n} = x_m y_n \pm x_n y_m.$$

Разделим на y_1 :

$$\frac{y_{m \pm n}}{y_1} = x_m \frac{y_n}{y_1} \pm x_n \frac{y_m}{y_1} \implies U_{m \pm n} = x_m U_n \pm x_n U_m.$$

$$(д) \quad x_n = \sum_{i \geq 0} C_n^{2i} D^i y_1^{2i} x_1^{n-2i}$$

Раскроем по биному Ньютона выражение $x_n + y_n \sqrt{D} = (x_1 + y_1 \sqrt{D})^n$:

$$x_n + y_n \sqrt{D} = \sum_{k=0}^n C_n^k x_1^{n-k} (y_1 \sqrt{D})^k.$$

Рациональная часть x_n соответствует четным индексам $k = 2i$:

$$x_n = \sum_{2i \leq n} C_n^{2i} x_1^{n-2i} (y_1 \sqrt{D})^{2i} = \sum_{i \geq 0} C_n^{2i} D^i y_1^{2i} x_1^{n-2i}.$$

$$(е) \quad U_n = \sum_{i \geq 0} C_n^{2i+1} D^i y_1^{2i} x_1^{n-1-2i}$$

Иррациональная часть из разложения выше соответствует нечетным индексам $k = 2i+1$:

$$y_n \sqrt{D} = \sum_{2i+1 \leq n} C_n^{2i+1} x_1^{n-(2i+1)} (y_1 \sqrt{D})^{2i+1} = \sum_{i \geq 0} C_n^{2i+1} x_1^{n-2i-1} y_1^{2i+1} D^i \sqrt{D}.$$

Разделим на $y_1 \sqrt{D}$:

$$U_n = \frac{y_n}{y_1} = \sum_{i \geq 0} C_n^{2i+1} D^i y_1^{2i} x_1^{n-1-2i}.$$

$$(ж) \quad U_{mn} = \sum_{i \geq 0} C_n^{2i+1} D^i U_m^{2i+1} y_1^{2i} x_m^{n-1-2i}$$

Заметим, что $x_{mn} + y_{mn} \sqrt{D} = (x_m + y_m \sqrt{D})^n$. Применяя формулу из пункта (е) для пары (x_m, y_m) , получаем:

$$y_{mn} = \sum_{i \geq 0} C_n^{2i+1} y_m^{2i+1} D^i x_m^{n-2i-1}.$$

Разделим на y_1 :

$$U_{mn} = \frac{y_{mn}}{y_1} = \sum_{i \geq 0} C_n^{2i+1} \frac{y_m^{2i+1}}{y_1} D^i x_m^{n-1-2i}.$$

Так как $y_m = U_m y_1$, то $\frac{y_m^{2i+1}}{y_1} = \frac{(U_m y_1)^{2i+1}}{y_1} = U_m^{2i+1} y_1^{2i}$. Подставляя это, получаем искомое равенство. ■

Определение. Для простого числа p определим *индекс появления* его в последовательности $\{U_n\}$ как наименьшее натуральное j , при котором U_j делится на p . Обозначим этот индекс за $w(p)$

Задача 2.6. Докажите, что U_n делится на простое p тогда и только тогда, когда n делится на $w(p)$.

Решение. ($\Leftarrow$): Пусть n делится на $w(p)$, то есть $n = k w(p)$ для некоторого натурального k . Согласно формуле для U_{mn} (задача 2.5ж), число $U_{k w(p)}$ делится на $U_{w(p)}$. А так как по определению $w(p)$ число $U_{w(p)}$ делится на p , то и U_n делится на p .

($\Rightarrow$): Пусть U_n делится на p . Предположим противное, то есть n не делится на $w(p)$. Тогда рассмотрим: $n = t w(p) + r$, где $1 \leq r < w(p)$. По задаче 2.5г:

$$U_n = U_{t w(p) + r} = x_r U_{t w(p)} + x_{t w(p)} U_r$$

Поскольку $p \mid U_n$, а также $p \mid U_{t\omega(p)}$, p должно делить оставшееся слагаемое: $p \mid x_{t\omega(p)}U_r$. Заметим, что $(x_k, U_k) = 1$, так как $x_k^2 - Dy_1^2U_k^2 = 1$. Поскольку $p \mid U_{t\omega(p)}$, то p не может делить $x_{t\omega(p)}$. Значит, из $p \mid x_{t\omega(p)}U_r$ следует, что $p \mid U_r$. Однако поскольку $\omega(p)$ — это наименьший положительный индекс, для которого U делится на p , приходим к противоречию. ■

Легко видеть, что $w(2) = 2$. Следующая задача показывает, что индекс появления $w(p)$ существует для каждого простого p .

Задача 2.7. (Закон появления). Пусть p — нечётное простое число. Докажите, что

(а) $w(p) = p$, если Dy_1 делится на p ,

(б) $w(p)$ делит $(p - \varepsilon)/2$, если Dy_1 не делится на p , где

$$\varepsilon := \left(\frac{D}{p} \right) \equiv D^{(p-1)/2} \pmod{p}.$$

Решение. (а) Если $p \mid Dy_1$, то согласно Задаче 2.5д имеем: $U_n = \sum_{i \geq 0} C_n^{2i+1} D^i y_1^{2i} x_1^{n-1-2i}$. Рассмотрим это выражение по модулю p . Все члены для $i \geq 1$ делятся на Dy_1 , а следовательно, делятся на p . Таким образом:

$$U_n \equiv nx_1^{n-1} \pmod{p}.$$

Поскольку $(x_1, p) = 1$, то $U_n \equiv 0 \pmod{p} \iff n \equiv 0 \pmod{p}$. Минимальное такое n — это число p , следовательно, $w(p) = p$.

(б) Используя разложения из задачи 2.5 и учитывая, что $C_p^k \equiv 0 \pmod{p}$ для $0 < k < p$, получаем:

$$x_p \equiv x_1^p \pmod{p}, \quad U_p \equiv D^{\frac{p-1}{2}} y_1^{p-1} \pmod{p}.$$

Заметим, что $x_1^p \equiv x_1 \pmod{p}$, поскольку либо $p \mid x_1$, в этом случае обе стороны $\equiv 0 \pmod{p}$, либо $p \nmid x_1$, и по малой теореме Ферма $x_1^{p-1} \equiv 1 \pmod{p}$. Также, поскольку $p \nmid Dy_1$, отсюда следует, что $y_1^{p-1} \equiv 1 \pmod{p}$. Тогда $x_p \equiv x_1 \pmod{p}$ и $U_p \equiv \varepsilon \pmod{p}$.

Теперь применим формулу из задачи 2.5ж для $y_{p-\varepsilon}$:

$$y_{p-\varepsilon} = y_p x_1 - \varepsilon x_p y_1 \equiv (\varepsilon y_1) x_1 - \varepsilon x_1 y_1 = 0 \pmod{p}.$$

При записи этой формулы мы использовали тот факт, что $\varepsilon = \pm 1$.

Теперь у нас есть сравнение $U_{p-\varepsilon} = y_{p-\varepsilon}/y_1 \equiv 0 \pmod{p}$. Согласно задаче 2.6, это подразумевает $\omega(p) \mid (p - \varepsilon)$.

Используя формулы из Задачи 2.5аб, получаем

$$U_{p-\varepsilon} = 2x_{\frac{p-\varepsilon}{2}} U_{\frac{p-\varepsilon}{2}} \equiv 0 \pmod{p}, \quad x_{p-\varepsilon} = 2x_{\frac{p-\varepsilon}{2}}^2 - 1.$$

Поскольку $x_{p-\varepsilon} = x_p x_1 - \varepsilon Dy_p y_1 \equiv x_1^2 - Dy_1^2 = 1 \pmod{p}$, мы имеем:

$$2x_{\frac{p-\varepsilon}{2}}^2 - 1 \equiv 1 \pmod{p} \implies x_{\frac{p-\varepsilon}{2}}^2 \equiv 1 \pmod{p}.$$

Таким образом, $x_{\frac{p-\varepsilon}{2}} \not\equiv 0 \pmod{p}$. Из равенства $2x_{\frac{p-\varepsilon}{2}} U_{\frac{p-\varepsilon}{2}} \equiv 0$ следует, что $U_{\frac{p-\varepsilon}{2}} \equiv 0 \pmod{p}$. Согласно задаче 2.6, условие $p \mid U_{\frac{p-\varepsilon}{2}}$ эквивалентно тому факту, что $\omega(p) \mid \frac{p-\varepsilon}{2}$.

Задача 2.8. Пусть $p > 3$ простое число, делящее Dy_1 . Докажите, что $U_p \equiv p \pmod{p^2}$.

Решение. По задаче 2.5е:

$$U_p = \sum_{i=0}^{\frac{p-1}{2}} C_p^{2i+1} D^i y_1^{2i} x_1^{p-1-2i}.$$

Распишем первые два слагаемых этой суммы:

$$U_p = C_p^1 x_1^{p-1} + C_p^3 D y_1^2 x_1^{p-3} + \sum_{i=2}^{\frac{p-1}{2}} C_p^{2i+1} D^i y_1^{2i} x_1^{p-1-2i}.$$

Рассмотрим это выражение по модулю p^2 .

Все слагаемые при $i \geq 2$ делятся на $(Dy_1)^2$, а в силу того, что $p \mid Dy_1$, то они делятся и на p^2 . При $i = 1$ слагаемое также делится на p^2 , поскольку Dy_1 делится на p , а также $C_p^3 = \frac{p(p-1)(p-2)}{6}$ делится на p (при $p > 3$).

Поэтому $U_p \equiv p x_1^{p-1} \pmod{p^2}$. А т.к. $(x_1, D) = 1$, $(x_1, y_1) = 1$ и $p \mid Dy_1$, то $p \nmid x_1$, и $x_1^{p-1} \equiv 1 \pmod{p}$. Тогда $p x_1^{p-1} \equiv p \pmod{p^2}$. ■

Задача 2.9. (Закон повторения). Докажите, что для каждого простого делителя p числа U_n , натурального k взаимно простого с p и $\lambda \geq 0$ выполняется следующее равенство

$$\nu_p(U_{kn p^\lambda}) = \nu_p(U_n) + \lambda.$$

Решение. Заметим, что поскольку $\nu_p(U_n) = v \geq 1$, то из $x_n^2 - Dy_1^2 U_n^2 = 1$ следует $p \nmid x_n$.

- Докажем, что $\nu_p(U_{kn}) = \nu_p(U_n)$, если $(k, p) = 1$. По задаче 2.5.ж:

$$U_{nk} = \sum_{i \geq 0} C_k^{2i+1} D^i U_n^{2i+1} y_1^{2i} x_n^{k-1-2i}.$$

При $i \geq 1$ все слагаемые делятся на U_n^3 , то есть делятся на p^{3v} . Т.к. $v \geq 1$, получаем, что по модулю p^{v+1} :

$$U_{nk} \equiv k U_n x_n^{k-1} \equiv k U_n \pmod{p^{v+1}}$$

Тогда т.к. $(k, p) = 1$, то $\nu_p(k U_n) = v$. А, значит, $\nu_p(U_{nk}) = v$.

- Докажем теперь, что $\nu_p(U_{pn}) = \nu_p(U_n) + 1$.

Снова распишем по задаче 2.5.ж:

$$U_{np} = \sum_{i \geq 0} C_p^{2i+1} D^i U_n^{2i+1} y_1^{2i} x_n^{p-1-2i}.$$

При $i \geq 1$ все слагаемые делятся на U_n^3 , то есть делятся на p^{3v} . Т.к. $v \geq 1$, получаем, что по модулю p^{v+2} :

$$U_{np} \equiv pU_n x_n^{k-1} \equiv pU_n \pmod{p^{v+2}}$$

Имеем $\nu_p(pU_n) = v + 1$. А, значит, $\nu_p(U_{np}) = v + 1$.

Применяя λ раз рассуждения второго случая, получим $\nu_p(U_{np^\lambda}) = \nu_p(U_n) + \lambda$. Комбинируя с шагом 1, получаем $\nu_p(U_{knp^\lambda}) = \nu_p(U_n) + \lambda$. ■

Для краткости запишем

$$\alpha = x_1 + y_1 \sqrt{D}, \quad \beta = x_1 - y_1 \sqrt{D}.$$

Введём ещё одно обозначение:

$$G_n := \prod_{\substack{h < n \\ (h,n)=1}} \left(\alpha - \beta e^{2\pi i h/n} \right).$$

К примеру,

$$G_1 = 1, \quad G_2 = \alpha + \beta = 2x_1 = U_2, \quad G_3 = \alpha^2 + \alpha\beta + \beta^2 = U_3.$$

Задача 2.10. Докажите, что G_n целое, а также представляется в виде симметрического многочлена от α и β .

Решение. Заметим, что если $(h, n) = 1$, то $(n - h, n) = 1$. Введем обозначения $e_h = e^{2\pi i h/n}$. Тогда заметим, что $e_h \cdot e_{n-h} = 1$.

Сначала будем доказывать, что $G_n(\alpha, \beta) = G_n(\beta, \alpha)$. Для этого рассмотрим произведение:

$$\prod_{\substack{h < n \\ (h,n)=1}} e^{2\pi i h/n}.$$

Заметим, что оно равно $(-1)^{\varphi(n)}$. Действительно, все e_h разбиваются на пары (e_h, e_{n-h}) , где в каждой паре произведение равно 1. Без пары может оказаться только $e_{n/2}$. Однако при $n > 2$ неверно, что $(n/2, n) = 1$, а потому оно не войдет в произведение. При $n = 2$ имеем $\varphi(n) = 1$, а в произведении будет только $e_1 = -1$.

Теперь домножим $G_n(\alpha, \beta)$ на это произведение, получим:

$$G_n(\alpha, \beta) \cdot \prod_{\substack{h < n \\ (h,n)=1}} e^{2\pi i h/n} = \prod_{\substack{h < n \\ (h,n)=1}} \left(\alpha - \beta e^{2\pi i h/n} \right) e^{2\pi i (n-h)/n}$$

$$G_n(\alpha, \beta) \cdot (-1)^{\varphi(n)} = \prod_{\substack{h < n \\ (h,n)=1}} \left(\alpha e^{2\pi i (n-h)/n} - \beta \right)$$

$$G_n(\alpha, \beta) \cdot (-1)^{\varphi(n)} = \prod_{\substack{h < n \\ (h,n)=1}} \left(\alpha e^{2\pi i h/n} - \beta \right)$$

Последний переход верен в силу того, что в произведении если есть скобка с e_h , то есть такая же скобка с e_{n-h} , и наоборот.

Далее осталось домножить обе части на $(-1)^{\varphi(n)}$:

$$G_n(\alpha, \beta) = \prod_{\substack{h < n \\ (h, n) = 1}} (\beta - \alpha e^{2\pi i h/n})$$

Заметим, что справа получили в точности $G_n(\beta, \alpha)$.

Теперь докажем, что $G_n(\alpha, \beta)$ – многочлен с целыми коэффициентами. Для этого рассмотрим многочлен $P_n(x) = \prod_{(h, n) = 1} (x - e^{2\pi i h/n})$. Докажем, что у этого многочлена целые коэффициенты.

Заметим, что его старший коэффициент равен единице. Также заметим, что верно следующее

$$x^n - 1 = \prod_{d|n} P_d(x)$$

Действительно, левая часть раскладывается как

$$x^n - 1 = \prod_{1 \leq k \leq n} (x - e^{2\pi i k/n})$$

При этом если обозначить $d = (n, k)$, $h = \frac{k}{d}$, то $(h, n) = 1$. И такое разложение единственно, поэтому скобке $(x - e^{2\pi i k/n})$ будет соответствовать ровно одна скобка $(x - e^{2\pi i h/d})$ в произведении $\prod_{d|n} P_d(x)$. И также по любой скобке произведения $\prod_{d|n} P_d(x)$ однозначно определяется соответствующая ей скобка в левой части.

Будем доказывать по индукции, что коэффициенты у $P_n(x)$ целочисленные.

База: $P_1(x) = 1$.

Переход: обозначим за $Q_n(x) = \prod_{d < n, d|n} P_d(x)$, тогда $x^n - 1 = P_n(x)Q_n(x)$.

Заметим, что у многочлена $Q_n(x)$ целочисленные коэффициенты, поскольку он является произведением многочленов с целочисленными коэффициентами. Тогда если выполнить деление многочлена $x^n - 1$ на многочлен $Q_n(x)$, то у полученного многочлена коэффициенты будут рациональны. А в силу того, что старший коэффициент многочлена $Q_n(x)$ равен единице (как произведение единичных старших коэффициентов у $P_d(x)$), то в итоге коэффициенты будут целыми.

При $n > 1$: $G_n(\alpha, \beta) = P_n(\frac{\alpha}{\beta}) \cdot \beta^{\varphi(n)}$, поэтому у него коэффициенты также целые. Заметим также, что $\alpha\beta = x_1^2 - Dy_1^2 = 1$.

В силу того, что G_n симметрический, имеем, что коэффициенты при $\alpha^m \beta^{\varphi(n)-m}$ и $\beta^m \alpha^{\varphi(n)-m}$ одинаковые.

При $n = 2$ утверждение задачи очевидно из явного вида G_n , поэтому рассмотрим $n > 2$. Для него $\varphi(n)$ чётно, а потому в G_n после раскрытия скобок все слагаемые разобьются на пары: $c \cdot \alpha^m \beta^{\varphi(n)-m} + c \cdot \beta^m \alpha^{\varphi(n)-m} = c(\alpha^m \beta^{\varphi(n)-m} + \beta^m \alpha^{\varphi(n)-m})$. Без ограничения общности положим $\varphi(n) - m = m + t, t \geq 0$. Тогда сумма принимает вид $c \cdot \alpha^m \beta^m (\alpha^t + \beta^t) = c(x_t + y_t \sqrt{D} + x_t - y_t \sqrt{D}) = 2cx_t$. Мы получили целое число. Поэтому G_n целое как сумма нескольких целых чисел.

Задача 2.11. Докажите, что

$$U_n = \prod_{\delta|n} G_\delta.$$

Решение. Заметим, что члены последовательности U_n выражаются формулой:

$$U_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}.$$

Воспользуемся разложением, полученным в прошлой задаче, предварительно домножив его на $\beta^{\varphi(n)}$:

$$\alpha^n - \beta^n = \beta^{\varphi(n)} \prod_{\delta|n} P_\delta\left(\frac{\alpha}{\beta}\right).$$

Так как $P_1\left(\frac{\alpha}{\beta}\right)\beta = \alpha - \beta$, то:

$$U_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} = \prod_{\delta|n, \delta>1} P_\delta\left(\frac{\alpha}{\beta}\right)\beta^{\varphi(\delta)}.$$

Определив $G_1 = 1$ и $G_\delta = P_\delta\left(\frac{\alpha}{\beta}\right)\beta^{\varphi(\delta)}$ для $\delta > 1$, мы получаем искомое представление:

$$U_n = \prod_{\delta|n} G_\delta.$$

Из предыдущей задачи следует, что G_n является делителем U_n .

Выделим два вида простых делителей числа G_n . Простой делитель G_n , который делит n , назовём *внутренним*; все остальные простые делители G_n назовём *внешними*.

Задача 2.12. Пусть p — внутренний делитель G_n .

(а) Докажите, что p — наибольший простой делитель n .

(б) Докажите, что G_n не делится на p^2 при $n > 3$.

Решение. (М. Акимова) Пусть p наибольший простой делитель числа n и $v = v_p(n)$. Обозначим $m = n/p^v$.

(а) Возьмем произвольный простой делитель q числа m . По задаче 2.11 имеем

$$U_n = U_m \cdot \prod_{p|d|n} G_d, \quad \text{откуда} \quad v_q(U_n) = v_q(U_m) + \sum_{p|d|n} v_q(G_d).$$

Но поскольку $q \neq p$ по задаче 2.9 имеем $v_q(U_n) = v_q(U_m)$. Значит, для любого d , делящего n и делимого на p , верно $v_q(G_d) = 0$. В частности, $v_q(G_n) = 0$.

(б) По задаче 2.11 запишем

$$U_n = U_{mp^v} = U_{mp^{v-1}} \cdot \prod_{p^v|d|n} G_d, \quad \text{откуда} \quad v_p(U_{mp^v}) = v_p(U_{mp^{v-1}}) + \sum_{p^v|d|n} v_p(G_d).$$

По задаче 2.9 имеем $v_p(U_{mp^v}) = v_q(U_{mp^{v-1}}) + 1$, откуда $\sum_{p^v|d|n} v_p(G_d) = 1$. В частности, $v_p(G_n) \leq 1$. ■

Задача 2.13. Рассмотрим целое $n > 3$.

(а) Докажите, что у G_n есть внешний простой делитель q .

(б) Докажите, что $q \geq 2n - 1$.

Решение. Пусть

$$n = \prod_{i=1}^t p_i^{\alpha_i}$$

— разложение n на простые множители, из которых простое число p_t является наибольшим. Тогда

$$\varphi(n) = \prod_{i=1}^t p_i^{\alpha_i-1} (p_i - 1) \geq p_t - 1.$$

Отсюда

$$\begin{aligned} |G_n| &= \prod_h |\alpha - \beta \exp(2\pi i h/n)| > (\alpha - \beta)^{\varphi(n)} \\ &= (2y_1 \sqrt{D})^{\varphi(n)} > 2^{p_t-1} \geq p_t. \end{aligned}$$

Здесь оценку на модуль произведения можно было сделать, разбив скобки на пары, и каждую оценив через $(\alpha - \beta)^2$.

В итоге мы получили $G_n > p_t$. Пусть у G_n нет внешнего простого делителя. Тогда по задаче 2.12а любой его простой делитель является наибольшим (как внутренний). То есть $G_n = p_t^k$. А поскольку $n > 3$, то по задаче 2.12б $p_t^2 \nmid G_n$, поэтому $k \leq 1$, и $G_n \leq p_t$. Что противоречит только что полученному соотношению.

Следовательно, G_n имеет внешний простой делитель p^* . Пусть $w = w(p^*)$ — ранг появления p^* . Поскольку p^* делит G_n и, следовательно, U_n , то w делит n . Предположим, что $w < n$, так что G_n делит целое число

$$U_n/U_w = \prod_{\delta|n, \delta \nmid w} G_\delta.$$

Тогда p^* делит это отношение. Но p^* , будучи внешним, не делит ни n , ни w , и поэтому, по задаче 2.9, U_n/U_w не делится на p^* . Это противоречие доказывает, что $w = n$. Но тогда $p^* \neq w$, так как p^* не делит n . Следовательно, по задаче 2.7б, w , а значит и n , делит $\frac{1}{2}(p^* \pm 1)$. Таким образом, $p^* \geq 2n - 1$. ■

Определим число $M(Q)$ следующим образом:

$$M(Q) = \max(3, (q_t + 1)/2).$$

Задача 2.14. Пусть Q' — множество из $2^t - 1$ бесквадратных Q -гладких чисел, за исключением 2, а S — целое число такое, что оба числа S и $S+1$ являются Q -гладкими. Докажите, что $S = (x_n - 1)/2$, где (x_n, y_n) решение уравнения Пелля

$$x^2 - 2dy^2 = 1,$$

такое, что

$$d \in Q', \quad 1 \leq n \leq M(Q).$$

Решение. Предположим сначала, что (x_n, y_n) — решение уравнения Пелля

$$x^2 - 2dy^2 = 1, d \in Q', 1 \leq n \leq M(Q).$$

Тогда, поскольку x_n нечетно, а y_n четно,

$$S(S+1) = \frac{(x_n^2 - 1)}{4} = 2d\left(\frac{y_n}{2}\right)^2 \in Q$$

.

Теперь предположим, что $S(S+1) \in Q$, то есть

$$S(S+1) = 2q_1^{\alpha_1} q_2^{\alpha_2} \dots q_t^{\alpha_t},$$

где $\alpha_i = \varepsilon_i + 2\beta_i$, $\varepsilon_i \in \{0, 1\}$.

Кроме того, $x = 2S + 1$, $y = 2q_1^{\beta_1} q_2^{\beta_2} \dots q_t^{\beta_t} \in Q$, $d = q_1^{\varepsilon_1} q_2^{\varepsilon_2} \dots q_t^{\varepsilon_t} \in Q'$.

Умножая выражение $S(S+1)$ на 4, мы видим, что

$$4S^2 + 4S = x^2 - 1 = 2dy^2.$$

Следовательно, каждое такое S приводит к некоторому решению (x, y) уравнения $x^2 - 2dy^2 = 1$, в котором y и d принадлежат Q и Q' соответственно. Как хорошо известно, (x, y) должно быть (x_n, y_n) для некоторого $n \geq 1$. Остаётся показать, что $n \leq M$.

Предположим вместо этого, что $n > M$. Применяя задачу 2.13 и пользуясь тем, что $G_n \mid U_n \mid y_n$, заключаем, что y_n делится на простое число p такое, что

$$p \geq 2n - 1 > 2M - 1 \geq q_t.$$

Следовательно, y_n не принадлежит Q , противоречие. Таким образом, $n \leq M$. ■

Следующая теорема является прямым следствием предыдущей задачи:

Теорема. Существует не более $(2^t - 1) \cdot M(Q)$ пар последовательных Q -гладких чисел.

Задача 2.15. Найдите все пары последовательных $\{2, 3, 5\}$ -гладких чисел.

Решение. Воспользуемся предыдущей задачей. $Q' = \{1, 3, 5, 6, 10, 15, 30\}$, $M(Q) = 3$.

Тогда нам достаточно рассмотреть 7 вариантов параметра d для уравнения Пелля. И для каждого такого уравнения рассмотреть решения с $n \leq 3$.

- $x^2 - 2y^2 = 1$

В данном случае $(x_1, y_1) = (3, 2)$, $(x_2, y_2) = (17, 12)$, $(x_3, y_3) = (99, 70)$.

Из них получим следующие пары: $(1, 2)$, $(8, 9)$.

- $x^2 - 6y^2 = 1$

В данном случае $(x_1, y_1) = (5, 2)$, $(x_2, y_2) = (49, 20)$, $(x_3, y_3) = (485, 198)$.

Из них получим следующие пары: $(2, 3)$, $(24, 25)$.

- $x^2 - 10y^2 = 1$

В этом случае аналогично получаем пару $(9, 10)$.

- $x^2 - 12y^2 = 1$

В этом случае получаем пару $(3, 4)$.

- $x^2 - 20y^2 = 1$

Получаем пары $(4, 5)$, $(80, 81)$.

- $x^2 - 30y^2 = 1$

Получаем пару $(5, 6)$.

- $x^2 - 60y^2 = 1$

Получаем пару $(15, 16)$.

■

3 По следам Стёрмера

Во втором разделе мы упомянули о том, как факт, сформулированный в Задаче 2.3, помог Стёрмеру доказать оценку сверху на количество пар последовательных Q -гладких чисел. Подобное изучение структуры простых делителей одной из компонент решения уравнения Пелля и подобных ему может быть полезно для решения многих теоретико-числовых задач. Мы предлагаем вам решить некоторые из них.

Задача 3.1. Пусть (x, y) — решение уравнения $x^2 - 1 = y^q$ для некоторого простого $q \geq 5$.

(а) Докажите, что x не может быть чётным.

(б) Докажите, что либо $\left(\frac{x+3}{2}\right)^2$, либо $\left(\frac{x-3}{2}\right)^2$ представляется в виде разности двух точных q -ых степеней.

(в) Докажите, что x не делится на q .

(г) Докажите, что $y + 1$ является точным квадратом.

(д) Докажите, что уравнение

$$x^2 - 1 = y^q$$

не имеет решений для простого $q \geq 5$ в натуральных числах.

Решение. (а) Предположим, что x — четное число, тогда y — нечетное, а $x - 1$ и $x + 1$ взаимно просты. Отсюда следует, что $x - 1$ и $x + 1$ являются точными q -ми степенями. Пусть $x - 1 = s^q$ и $x + 1 = t^q$. Мы имеем $t^q - s^q = 2$ для некоторых $s, t \in \mathbb{Z}$. Это возможно только если $t = 1, s = -1$. Отсюда следует, что $x = 0$, это противоречит натуральности x .

(б) Согласно пункту (а) x — нечетное число, и $(x + 1, x - 1) = 2$. Пусть $\varepsilon = \pm 1$ таково, что $x \equiv \varepsilon \pmod{4}$. Тогда

$$x + \varepsilon = 2w^q, \quad x - \varepsilon = 2^{q-1}z^q, \quad y = 2wz$$

для $w, z \in \mathbb{Z}$ таких, что $\text{НОД}(w, 2z) = 1$. Следовательно,

$$\left(\frac{x - 3\varepsilon}{2}\right)^2 = \left(\frac{x - \varepsilon}{2} - \varepsilon\right)^2 = \left(\frac{x - \varepsilon}{2} + \varepsilon\right)^2 - 4\varepsilon \frac{x - \varepsilon}{2} = (w^2)^q - (2\varepsilon z)^q.$$

(в) **Лемма.** Если $a, b \in \mathbb{Z}$, $(a, b) = 1$ и p — простое число, то

$$\left(\frac{a^p - b^p}{a - b}, a - b\right) = 1 \text{ или } p.$$

Доказательство: Заметим, что

$$\frac{a^p - b^p}{a - b} = \sum_{i=0}^{p-1} a^i b^{p-1-i} \equiv pb^{p-1} \equiv pa^{p-1} \pmod{a - b}.$$

Отсюда следует, что $\left(\frac{a^p - b^p}{a - b}, a - b\right)$ делит как pb^{p-1} , так и pa^{p-1} . Поскольку a и b взаимно просты, мы получаем, что $\left(\frac{a^p - b^p}{a - b}, a - b\right) \mid p$, $\left(\frac{a^p - b^p}{a - b}, a - b\right) = 1$, или p . $\square$
По лемме имеем:

$$\left(\frac{(w^2)^q - (2\varepsilon z)^q}{w^2 - 2\varepsilon z}, w^2 - 2\varepsilon z \right) = 1 \text{ или } q.$$

Если $\frac{(w^2)^q - (2\varepsilon z)^q}{w^2 - 2\varepsilon z}$ и $w^2 - 2\varepsilon z$ взаимно просты, то из пункта (б) следует, что $w^2 - 2\varepsilon z$ является полным квадратом, поэтому $w \leq z$. Но это невозможно для $x > 1$, поскольку

$$\left(\frac{w}{z} \right)^q = 2^{q-2} \frac{x + \varepsilon}{x - \varepsilon} > 1.$$

Следовательно, $x = 1$ и $y = 0$, что приводит к противоречию.

В противном случае, оба числа $\frac{(w^2)^q - (2\varepsilon z)^q}{w^2 - 2\varepsilon z}$ и $w^2 - 2\varepsilon z$ делятся на q , поэтому

$$\left(\frac{x - 3\varepsilon}{2} \right)^2 = (w^2)^q - (2\varepsilon z)^q$$

также делится на q . Следовательно, x не делится на q , так как $q \geq 5$.

(г) По лемме имеем:

$$\left(\frac{y^q + 1}{y + 1}, y + 1 \right) = 1 \text{ или } q.$$

Если $\frac{y^q + 1}{y + 1}$ и $y + 1$ оба делятся на q , то $x^2 = y^q + 1$ также делится на q , что противоречит пункту (в). Если $\frac{y^q + 1}{y + 1}$ и $y + 1$ взаимно просты, то $y + 1$ является полным квадратом.

(д) Если (x, y) является положительным решением уравнения $x^2 - 1 = y^q$, то $y + 1 = s^2$ согласно пункту (г). Отсюда следует, что уравнение Пелля

$$z^2 - y \cdot t^2 = 1$$

имеет по крайней мере два решения: $(z, t) = (s, 1)$ и $(z, t) = (x, y^{\frac{q-1}{2}})$, для которых все простые делители t делят y . Это противоречит результату задачи 2.3. ■

Задача 3.2. (а) Докажите, что все решения уравнения

$$ax^2 - (a - 1)y^2 = 1$$

для заданного целого $a > 1$ описываются следующим образом:

$$x_t \sqrt{a} + y_t \sqrt{a - 1} = (\sqrt{a} + \sqrt{a - 1})^{2t+1},$$

где t — неотрицательное целое.

(б) Решите уравнение

$$\frac{x^{2k+1} - 1}{x - 1} = y^2$$

для натурального k .

Решение. (а) Заметим, что число $\sqrt{\frac{a-1}{a}}$ иррационально, поэтому представление числа в виде $x\sqrt{a} + y\sqrt{a-1}$ не более чем единственно.

Рассмотрим числа $z = x\sqrt{a} + y\sqrt{a-1}$ и $\tilde{z} = x\sqrt{a} - y\sqrt{a-1}$; тогда $z\tilde{z} = 1$. Выберем t такое, что $(\sqrt{a} + \sqrt{a-1})^{2t-1} < x\sqrt{a} + y\sqrt{a-1} \leq (\sqrt{a} + \sqrt{a-1})^{2t+1}$. Положим

$$w = k\sqrt{a} + \ell\sqrt{a-1} = (x\sqrt{a} + y\sqrt{a-1})(\sqrt{a} - \sqrt{a-1})^{2t};$$

тогда $w\tilde{w} = 1$ (в частности, $k\ell \neq 0$) и $\sqrt{a} - \sqrt{a-1} < w \leq \sqrt{a} + \sqrt{a-1}$. Одно из чисел w и $\tilde{w}$ (у которого коэффициенты одного знака) не меньше $\sqrt{a} + \sqrt{a-1}$, а тогда другое (из равенства $w\tilde{w} = 1$) не больше $\sqrt{a} - \sqrt{a-1}$. С учётом неравенств на w , получаем $w = \sqrt{a} + \sqrt{a-1}$, откуда и следует требуемая формула.

(б) Пусть (a, s) — натуральное решение уравнения

$$\frac{x^{2k+1} - 1}{x - 1} = y^2.$$

Заметим, что $a > 1$ по определению.

Тогда

$$a \cdot b^2 - (a - 1) \cdot s^2 = 1.$$

при $b = a^k$.

Из пункта (а) получаем, что

$$(b =) a^k = a^t + \binom{2t+1}{2} a^{t-1} (a-1) + \binom{2t+1}{4} a^{t-2} (a-1)^2 + \dots + \binom{2t+1}{2t} (a-1)^t. \quad (*)$$

Так как $a > 1$, то из $(*)$ получаем $k > t$. Далее обозначим через L и R левую и правую части в $(*)$ и разберём несколько случаев.

Случай 1. Пусть $2 \mid a$. Тогда L чётна, а в R чётны все слагаемые, кроме последнего. Это невозможно.

Случай 2. Пусть в разложение a на простые сомножители входит $p^\alpha > 3$ при нечётном простом p . Тогда L делится на $p^{k\alpha}$. Покажем, что R делится на меньшую степень p , придя к противоречию.

Положим $\beta = v_p(2t+1) \leq t < k$. Покажем, что все слагаемые в R , кроме последнего, делятся на $p^{\beta+1}$, откуда будет следовать, что $v_p(R) = \beta < k \leq k\alpha$.

Для этого достаточно показать, что

$$v_p \left(\binom{2t+1}{2(t-i)} \right) > \beta - i\alpha$$

при всех $1 \leq i \leq \beta/\alpha$. Напомним, что либо $p > 3$, либо $p = 3$ и $\alpha > 1$; тогда при наших ограничениях на i имеем $2i+1 < p^\beta$, а тогда левая часть равна $v_p(2t+1) - v_p(2i+1) = \beta - v_p(2i+1)$, Осталось заметить, что при $p^\alpha > 3$ верно неравенство $v_p(2i+1) < i\alpha$, поскольку $2i+1 < (p^\alpha)^i$.

Случай 3. Остался лишь случай $a = 3$. Снова обозначим $\beta = v_3(2t+1)$; при $\beta = 0$ в сумме R лишь последнее слагаемое не делится на 3, то есть R не делится на a , что

невозможно. Значит, $\beta > 0$, а тогда $t = 3l + 1$. При $l = 0$ получаем, что $k = 2$ и пара $(3, 11)$ является решением. Пусть $l \geq 1$. Тогда сумма последних двух слагаемых в R равна

$$R' = 2^t(2t + 1) + 2^{t-2}(2t + 1)2t(2t - 1) = 2^{t-1}(2t + 1)(18l^2 + 9l + 3),$$

и $v_3(R') = \beta + 1$. Но в каждый из остальных членов 3 входит в большей степени (это доказывается так же, как выше при использовании неравенства $v_3(2i + 1) < i - 1$ при $i > 1$). Значит, R не может являться степенью тройки, и поэтому других решений нет. ■

Задача 3.3. (а) Решите уравнение

$$\frac{x^{4k+2} - 1}{x - 1} = 2y^2$$

для натурального k .

(б) Решите уравнение

$$\frac{x^{4k} - 1}{x - 1} = 2y^2$$

для натурального k .

Решение. (а) Предположим, существует положительное целое число k такое, что данное уравнение имеет положительное целое решение. Заметим, что x — нечетное число. Перепишем уравнение следующим образом:

$$\frac{x^{2k+1} - 1}{x - 1} \cdot \frac{x^{2k+1} + 1}{2} = y^2.$$

Легко видеть, что числа $\frac{x^{2k+1}-1}{x-1}$ и $\frac{x^{2k+1}+1}{2}$ взаимно просты, следовательно, оба являются полными квадратами. Из задачи 3.2б следует, что $x = 3$ и $k = 2$. Но тогда $\frac{x^{2k+1}+1}{2} = \frac{3^5+1}{2} = 122$, что не является полным квадратом. квадрат, противоречие.

(б) (**А. Штурман**) Предположим, что существует положительное целое число $n > 1$ такое, что уравнение

$$\frac{x^{2n} - 1}{x - 1} = 2y^2$$

имеет положительное целое решение. Выберем минимальное $n = n_0$, обладающее этим свойством. Снова заметим, что x нечетное. По пункту (а) n_0 четное, поэтому $n_0 = 2l$. Перепишем уравнение как

$$\frac{x^{2l} - 1}{x - 1} \cdot \frac{x^{2l} + 1}{2} = y^2.$$

Легко видеть, что числа $\frac{x^{2l}-1}{x-1}$ и $\frac{x^{2l}+1}{2}$ взаимно просты, следовательно, они оба являются полными квадратами, соответственно z^2 и t^2 . Обратите внимание, что

$$z^2 = \frac{x^{2l} - 1}{x - 1} = \frac{x^l - 1}{x - 1}(x^l + 1). \quad (*)$$

Если l нечётное, то $\frac{x^l-1}{x-1}$ тоже нечётное и взаимно простое с $x^l + 1$. Следовательно, $\frac{x^l-1}{x-1}$ и $x^l + 1$ являются полными квадратами. Из задачи 3.2б следует, что либо $l = 1$, либо $x = 3, l = 5$. Второй случай невозможен, поскольку $3^5 + 1 = 244$ не является полным квадратом. Следовательно, $l = 1$, и числа $x + 1, \frac{x^2+1}{2}$ являются полными квадратами.

Число $x + 1$ четное, поэтому существуют положительные целые числа a, b такие, что $x + 1 = 4a^2, x^2 + 1 = 2b^2$. Отсюда следует, что

$$8a^4 - 4a^2 + 1 = b^2.$$

Это уравнение в a, b не имеет натуральных решений, но жюри неизвестно элементарное доказательство. Мы принимали решения по модулю доказательства этого факта.

Если l чётно, то

$$\left(\frac{x^l - 1}{x - 1}, x^l + 1 \right) = 2,$$

и $\frac{x^l-1}{x-1}$ является удвоенным квадратом в силу (*). Отсюда следует, что $l = 2$, иначе получаем противоречие с выбором n_0 , так как $l < 2n_0 = 4l$. Следовательно, $\frac{x^2+1}{2}$ и $\frac{x^4+1}{2}$ являются полными квадратами. Это невозможно, поскольку

$$\frac{x^4 + 1}{2} < \frac{x^2(x^2 + 1)}{2} < \left(\sqrt{\frac{x^4 + 1}{2}} + 1 \right)^2.$$

■

Задача 3.4. Докажите, что уравнение

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

не имеет решений в натуральных числах.

Решение. Предположим обратное, пусть (n, m) — положительное целое число. Если n нечётное, то $v_2((2^n - 1)(3^n - 1)) = 1$, что приводит к противоречию. Следовательно, n чётное. Поскольку $(2^n - 1)(3^n - 1) = m^2$, мы можем предположить, что $2^n - 1 = da^2$ и $3^n - 1 = db^2$ с положительными целыми числами a, b и d без квадратов.

Легко видеть, что $d > 1$. Тогда $(2^{\frac{n}{2}}, a)$ и $(3^{\frac{n}{2}}, b)$ являются решениями уравнения Пелля

$$x^2 - dy^2 = 1.$$

Первые компоненты решений этого уравнения Пелля описываются рекуррентным соотношением:

$$x_0 = 1, x_1 = t, x_{k+2} = 2tx_{k+1} - x_k$$

для некоторого целого числа t . Значит, числа $2^{\frac{n}{2}}$ и $3^{\frac{n}{2}}$ являются членами последовательности x_k .

Если t нечётное, то каждый член x_k всегда нечётно, поэтому не может быть натуральной степенью двойки. Следовательно, t чётное. Из рекуррентного соотношения следует, что x_k является чётным тогда и только тогда, когда k является нечётным.

Если $t \equiv 1 \pmod{3}$, то $x_k \equiv 1 \pmod{3}$ для любого k , поэтому x_k не может быть степенью тройки. Если $t \equiv 2 \pmod{3}$, то $x_k \equiv 1 \pmod{3}$, когда k является чётным, и $x_k \equiv 2 \pmod{3}$, когда k является нечётным. поэтому x_k также не может быть степенью тройки.

Следовательно, t делится на 3. Из рекуррентного соотношения следует, что x_k делится на 3 тогда и только тогда, когда k является нечётным. Но мы уже знаем, что k нечётное тогда и только тогда, когда x_k чётное, поэтому x_k не может быть степенью 3, что приводит к противоречию. ■

Задача 3.5. Докажите, что уравнение

$$(2^x - 1)(5^x - 1) = y^n$$

не имеет решений в натуральных числах при $n > 3$.

Решение.

Если $n \mid x$, то левая часть уравнения зажата строго между $(10^{\frac{x}{n}} - 1)^n$ и $(10^{\frac{x}{n}})^n$, что приводит к противоречию.

Не умаляя общности, можем считать, что n — простое число или 4, 6, 9. Сначала рассмотрим второй случай. Поскольку $4 \mid 5^x - 1$, получаем, что $\nu_2(5^x - 1) \geq 4$, следовательно, $4 \mid x$. Поэтому $3 \mid 2^x - 1$, следовательно, $\nu_3((2^x - 1)(5^x - 1)) \geq 4$, откуда следует, что $9 \mid x$. Таким образом, $36 \mid x$, что невозможно при $n = 4, 6, 9$.

Пусть теперь p — простое число. Индукцией по p покажем, что если $n \geq \max(p, 4)$, то каждое простое число $q \leq p$ должно делить y и $p \mid x$. Случаи $p = 2, 3$ уже были разобраны. Для индуктивного шага мы уже знаем, что каждое простое число $q < p$ должно делить y . Тогда, поскольку

$$\nu_q((2^x - 1)(5^x - 1)) \geq n \geq p$$

и

$$\nu_q((2^{q-1} - 1)(5^{q-1} - 1)) \leq \max(2, q - 1) \leq q$$

по лемме об уточнении показателя получаем, что $q^{\lceil \frac{n-q}{2} \rceil} \mid x$. Так как $q^{\frac{n-q}{2}} > n - 2$, это означает, что наибольшая степень q , делящая x , не меньше $n - 1 \geq p - 1$, следовательно, $p - 1 \mid x$. Отсюда следует $p \mid y$. Кроме того, показатель степени p в $(2^x - 1)(5^x - 1)$ не превышает $p - 1 < n$, так как $p \geq 5$, следовательно, $p \mid x$.

Следовательно, при $n \geq 4$ положительных решений не существует. ■

4 Об уравнениях в факториальных кольцах

Подмножество R множества действительных или множества комплексных чисел называется **кольцом**, если $1 \in R$ и если R замкнуто относительно сложения, вычитания и умножения, т.е. для любых $x, y \in R$ верно $x + y, x - y, x \cdot y \in R$. Тривиальные примеры колец: $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$. Для комплексного числа α обозначим через $\mathbb{Z}[\alpha]$ минимальное кольцо, содержащее α . Кольцо $\mathbb{Z}[i]$ называется *гауссовым* и имеет короткое описание:

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}.$$

Задача 4.1. Докажите это и аналогичным образом опишите кольца $\mathbb{Z}[\sqrt{2}]$, $\mathbb{Z}[\sqrt{2}, \sqrt{3}]$, $\mathbb{Z}[\sqrt[3]{2}]$, $\mathbb{Z}[\omega]$, $\mathbb{Z}[\pi]$, где $\omega := e^{2\pi i/3} = (-1 + i\sqrt{3})/2$. (Можно использовать без доказательства трансцендентность числа π .)

Решение. Ответы:

$$\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}, \quad \mathbb{Z}[\sqrt{2}, \sqrt{3}] = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mid a, b, c, d \in \mathbb{Z}\},$$

$$\mathbb{Z}[\sqrt[3]{2}] = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Z}\}, \quad \mathbb{Z}[\omega] = \{a + b\omega \mid a, b \in \mathbb{Z}\},$$

$$\mathbb{Z}[\pi] = \{P(\pi) \mid P \in \mathbb{Z}[x]\}.$$

Набросок доказательства: В каждом равенстве множество справа от равенства вложено в левое по свойству замкнутости кольца. При этом в каждом равенстве левое множество вложено в правое, поскольку правое является кольцом. ■

Определение. Скажем, что число $a \in R$ *делится* на ненулевое число $b \in R$ в *кольце* R , если найдется такое число $q \in R$, что $a = bq$.

Так, например, действительное число $1 + \sqrt{2}$ делится на действительное число $3 + 2\sqrt{2}$ в кольце $\mathbb{Z}[\sqrt{2}]$, поскольку $1 + \sqrt{2} = (3 + 2\sqrt{2})(\sqrt{2} - 1)$.

Оказывается, для некоторых колец верен **аналог основной теоремы арифметики**. Для того чтобы сформулировать это утверждение, нам потребуется определить аналоги «единицы» и «простых» чисел в произвольном кольце.

Определение. *Единицей* или *обратимым числом* в кольце R называется такое число, которое делит в R любое число кольца R .

В кольце $\mathbb{Z}$ единицами являются числа ± 1 . Однако в других кольцах список единиц может быть больше. Например, число $3 + 2\sqrt{2}$ является единицей в $\mathbb{Z}[\sqrt{2}]$.

Задача 4.2. Опишите все единицы в кольцах $\mathbb{Z}[i]$ и $\mathbb{Z}[\sqrt{D}]$, где D натуральное и не является точным квадратом.

Решение. Ответ: для $\mathbb{Z}[i]$ — $\pm 1, \pm i$, для $\mathbb{Z}[\sqrt{D}]$ — решения уравнения $a^2 - Db^2 = \pm 1$.

Набросок доказательства для $\mathbb{Z}[i]$: Число $z = a + bi$ — единица кольца $\mathbb{Z}[i]$ тогда и только тогда, когда $1/z \in \mathbb{Z}[i]$. По равенству

$$\frac{1}{z} = \frac{1}{a + bi} = \frac{a - bi}{(a + bi)(a - bi)} = \frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2}i$$

получаем, равносильность тому, что a и b делятся на $a^2 + b^2$. Это равносильно $a^2 + b^2 = 1$, откуда $z = \pm 1, \pm i$.

Набросок доказательства для $\mathbb{Z}[\sqrt{D}]$: Число $z = a + b\sqrt{D}$ — единица кольца $\mathbb{Z}[\sqrt{D}]$ тогда и только тогда, когда $1/z \in \mathbb{Z}[\sqrt{D}]$. По равенству

$$\frac{1}{z} = \frac{1}{a + b\sqrt{D}} = \frac{a - b\sqrt{D}}{(a + b\sqrt{D})(a - b\sqrt{D})} = \frac{a}{a^2 - Db^2} - \frac{b}{a^2 - Db^2}\sqrt{D}$$

получаем, равносильность тому, что a и b делятся на $a^2 - Db^2$. В следующем абзаце докажем, что это равносильно $a^2 - Db^2 = \pm 1$.

Поскольку a и b делятся на $n = a^2 - Db^2$, то a^2 и b^2 делятся на n^2 , откуда n делится на n^2 , что возможно только при $n = \pm 1$. ■

Определение. Необратимое число называется *неприводимым* в кольце R , если в любом представлении этого числа в виде произведения двух чисел из R присутствует единица этого кольца.

Задача 4.3. Выясните, являются ли следующие гауссовы числа неприводимыми. Если нет, разложите их в произведение неприводимых чисел:

(а) 2, 3, 5, 7, 11, 13; (б) $1 + i$, $3 + 2i$, $2 + 3i$; (в) $1 + 3i$, $3 + 4i$, $5 + 7i$.

Решение. Ответ: $2 = (1 + i)(1 - i)$, $5 = (2 + i)(2 - i)$, $13 = (2 + 3i)(2 - 3i)$, $1 + 3i = (1 + i)(2 + i)$, $3 + 4i = (2 + i)^2$, $5 + 7i = (1 + i)(6 + i)$, остальные — неприводимы.

Лемма 1: если норма $N(a + bi) = a^2 + b^2$ гауссова числа $z = a + bi$ равна простому числу p , то z неприводимо.

Доказательство: возьмем произвольное разложение $z = xy$. По мультипликативности нормы $p = N(z) = N(xy) = N(x)N(y)$. Поскольку p простое, то б.о.о. $N(x) = 1$. Следовательно, x обратимо. □

Лемма 2: пусть p простое вида $4k + 3$, тогда оно неразложимо в $\mathbb{Z}[i]$.

Набросок доказательства: возьмем произвольное разложение $p = xy$. По мультипликативности нормы $p^2 = N(p) = N(xy) = N(x)N(y)$. Предположим, что ни x , ни y необратимы. Тогда $N(x) = N(y) = p$. Тогда p представим в виде суммы двух квадратов. Но любой квадрат дает остаток 0 или 1 при делении на 4, поэтому сумма лишь двух квадратов может быть равна трем. Противоречие. □

Доказательство неприводимости: По лемме 1 числа из пункта б, а также числа $1 - i$, $2 + i$, $2 - i$, $2 - 3i$, $6 + i$, неприводимы. По лемме 2 числа 3, 7, 11 неприводимы. ■

Задача 4.4. Найдите все неприводимые гауссовы числа.

Решение. Докажем, что гауссово число z неприводимо тогда и только тогда, когда его норма равна простому числу, либо оно само равно простому вида $4k + 3$.

Справа налево это утверждение доказывается в решении задачи 4.3. Докажем слева направо.

Пусть норма $a^2 + b^2$ неприводимого числа $z = a + bi$ делится на простое p вида $4k + 3$. Тогда $a^2 + b^2 \equiv 0 \pmod{p}$. Если $b = 0$, то a делится на p и само простое. Иначе $b \neq 0$, откуда b обратим по модулю p и $(ab^{-1})^2 \equiv -1 \pmod{p}$. Значит, -1 является квадратичным вычетом по модулю p , чего не бывает для простых указанного вида.

Пусть норма числа z составная и делится на простое p , представимое в виде суммы двух квадратов: $p = x^2 + y^2$. По рождественской теореме Ферма такое представление имеет двойка и любое простое вида $4k + 1$. Имеем $a^2 \equiv -b^2 \pmod{p}$ и $x^2 \equiv -y^2 \pmod{p}$, откуда $a^2 x^2 \equiv b^2 y^2 \pmod{p}$ и $(ax + by)(ax - by) \equiv 0 \pmod{p}$. Рассмотрим случаи.

Первый: если $ax + by$ делится на p , то

$$0 \equiv ax + by \equiv ax^2 + byx \equiv a(-y^2) + byx \equiv bx - ay \pmod{p}$$

и

$$a + bi = (x + yi) \left(\frac{ax + by}{p} + \frac{bx - ay}{p} i \right),$$

где оба сомножителя необратимы. Противоречие.

Второй: если $ax - by$ делится на p , то

$$0 \equiv ax - by \equiv axy + b(-y^2) \equiv axy + bx^2 \equiv ay + bx \pmod{p}$$

и

$$a + bi = (x - yi) \left(\frac{ax - by}{p} + \frac{bx + ay}{p} i \right),$$

где оба сомножителя необратимы. Противоречие. ■

Определение. Назовём два ненулевых числа в кольце **ассоциированными**, если их отношение равно некоторой единице этого кольца. *Полным разложением* на множители ненулевого необратимого числа $x \in R$ называется представление вида

$$x = p_1 \cdot \dots \cdot p_m,$$

где $p_1, \dots, p_m$ — неприводимые числа в R . Два полных разложения

$$x = p_1 \cdot \dots \cdot p_m = q_1 \cdot \dots \cdot q_k$$

называются *эквивалентными*, если $m = k$ и существует биекция

$$\pi : \{1, \dots, m\} \rightarrow \{1, \dots, k\}$$

такая, что p_i и $q_{\pi(i)}$ ассоциированы для каждого $i = 1, \dots, m$.

Наконец, кольцо называется **факториальным**, если у любого ненулевого необратимого числа из этого кольца существует полное разложение, и любые два его полных

разложения эквивалентны. К примеру, кольцо $\mathbb{Z}$ является факториальным — это и есть основная теорема арифметики.

Теорема. Гауссово кольцо $\mathbb{Z}[i]$, а также кольца $\mathbb{Z}[i\sqrt{2}]$ и $\mathbb{Z}[\omega]$ факториальны.

Доказательству этой теоремы посвящён раздел 6. В следующих задачах этого раздела, а также в задачах раздела 5 вы можете использовать эту теорему без доказательства.

Задача 4.5. Придумайте такое кольцо, в котором для некоторого числа

- (а) нет полного разложения;
- (б) существует два полных неэквивалентных разложения.

Решение. (а) Обозначим $\pi_n = \sqrt[2^n]{\pi}$ и рассмотрим

$$R = \mathbb{Z}[\pi, \sqrt{\pi}, \sqrt[4]{\pi}, \sqrt[8]{\pi}, \sqrt[16]{\pi}, \dots] = \bigcup_{n=1}^{\infty} \mathbb{Z}[\pi_n].$$

Лемма 1. Если x трансцендентно, то $\sqrt{x}$ тоже трансцендентно.

Поскольку π трансцендентно, то многократным применением леммы 1 получаем трансцендентность чисел π_n для каждого n .

Лемма 2. Число π необратимо в R .

Доказательство леммы 2. От противного, пусть $1/\pi \in R$. Тогда найдется такое n , что $1/\pi \in \mathbb{Z}[\pi_n]$ и $\pi = \pi_n^{2^n}$. Возьмем такой $P \in \mathbb{Z}[t]$, что $1/\pi = P(\pi_n)$. Тогда $\pi_n^{2^n} P(\pi_n) - 1 = 0$, что противоречит трансцендентности π_n . $\square$

Предположим, что у необратимого π есть полное разложение в R , т.е.

$$\pi = p_1 \cdot \dots \cdot p_m$$

для некоторых неразложимых $p_1, \dots, p_m \in R$. Найдется такое n , что $p_1, \dots, p_m \in \mathbb{Z}[\pi_n]$.

Лемма 3. Пусть x трансцендентно, $k \geq 0$ целое и

$$x^k = P(x)Q(x),$$

где $P, Q \in \mathbb{Z}[t]$ — многочлены с целыми коэффициентами. Тогда найдутся такие $a, b \geq 0$, $a + b = k$, и $\varepsilon = \pm 1$, т.ч. $P(x) = \varepsilon x^a$ и $Q(x) = \varepsilon x^b$.

Применив лемму 3 для $x = \pi_n$ и $k = 2^n$, получаем, что $p_i = \varepsilon_i \pi_n^{k_i}$, где $\varepsilon_i = \pm 1$ и $k_i \geq 0$ для каждого $i = 1, \dots, m$. Но для любого k число π_n^k не неприводимо в R , поскольку $\pi_n = \pi_{n+1}^2$.

Доказательство леммы 1. От противного, пусть $\sqrt{x}$ алгебраично. Тогда найдется $P \in \mathbb{Z}[t]$, т.ч. $P(\sqrt{x}) = 0$. Рассмотрим $Q(t) = P(t)P(-t) \in \mathbb{Z}[t]$. Многочлен Q четный, поэтому существует $R \in \mathbb{Z}[t]$, т.ч. $Q(t) = R(t^2)$. Тогда $R(x) = Q(\sqrt{x}) = 0$. Противоречие. $\square$

Доказательство леммы 3. Поскольку x трансцендентно, то для числа вида $P(x)$, где $P \in \mathbb{Z}[t]$, корректно определена максимальная и минимальная степени монома многочлена P , обозначаемые $\deg(P)$ и $\mindeg(P)$, соответственно. Применим тривиальное неравенство $\deg(P) \geq \mindeg(P)$ к равенству из условия леммы 3:

$$k = \deg(PQ) = \deg(P) + \deg(Q) \geq \mindeg(P) + \mindeg(Q) = \mindeg(PQ) = k.$$

Следовательно, $\deg(P) = \mindeg(P)$ и $\deg(Q) = \mindeg(Q)$. Значит, P и Q — мономы. $\square$

(б) В кольце $\mathbb{Z}[i\sqrt{5}]$ имеем $6 = 2 \cdot 3 = (1 + i\sqrt{5})(1 - i\sqrt{5})$. Покажем, что эти сомножители попарно неассоциированы и неприводимы.

Аналогично решению задачи 4.2 $\mathbb{Z}[i\sqrt{5}]$ обратимы лишь ± 1 . Следовательно, сомножители попарно неассоциированы.

Если бы указанные сомножители имели нетривиальный делитель, то норма этого делителя была бы нетривиальным делителем норм этих сомножителей. Нормы указанных сомножителей принадлежит множеству $\{2^2, 2 \cdot 3, 3^2\}$, т.е. норма нетривиального делителя равна либо 2, либо 3. Но уравнения $a^2 + 5b^2 = 2$ и $a^2 + 5b^2 = 3$ не имеют решений в целых числах. Поэтому указанные сомножители неприводимы в $\mathbb{Z}[i\sqrt{5}]$. $\blacksquare$

Наибольшим общим делителем НОД(a, b) элементов a и b , одновременно не равных нулю, в кольце R называется любое число $d \in R$, такое что:

- (i) d является общим делителем a и b , и
- (ii) если c — общий делитель a и b , то c также является делителем d .

Существование НОД(a, b) в произвольном кольце не гарантируется, но он существует для факториальных колец (подумайте почему). Числа a и b называются *взаимно простыми*, если любой их НОД(a, b) является единицей в R .

Задача 4.6. (а) Найдите какой-нибудь наибольший общий делитель чисел $4 + i$ и $3 + 4i$.
(б) При каких целых z, t гауссовы числа 2 и $z + ti$ взаимно просты?

Решение. (а) Числа $4 + i$ и $3 + 4i$ взаимно просты, поскольку их нормы взаимно просты.

(б) Пусть r_z и r_t — остатки чисел z и t при делении на 2 соответственно. Тогда $d = (2, z + ti) = (2, r_z + r_t i)$. Поскольку $r_z, r_t \in \{0, 1\}$, то коротким разбором случаев получаем, что d обратимо только при $r_z \not\equiv r_t \pmod{2}$. $\blacksquare$

Задача 4.7. Пусть x и y — взаимно простые числа факториального кольца R , причем $xy = z^n$ для некоторого $z \in R$ и целого $n \geq 2$. Докажите, что $x = u_1 v_1^n$ и $y = u_2 v_2^n$ для некоторых $v_1, v_2 \in R$ и некоторых обратимых чисел $u_1, u_2 \in R$.

Решение. Для неприводимого $p \in R$ введем $v_p(r)$ как максимальную степень числа p , на которую делится $r \in R$. Эта функция корректно определена ввиду факториальности кольца R . Тогда для произвольного неприводимого p , делящего x , имеем

$$v_p(x) \stackrel{(1)}{=} v_p(xy) = v_p(z^n) = n v_p(z),$$

где равенство (1) верно, поскольку x, y взаимно просты. Следовательно, любое неприводимое число входит в x в степени, кратной n , то есть $x = u_1 v_1^n$. Аналогично, $y = u_2 v_2^n$. $\blacksquare$

Разработанная теория позволяет нам решать уравнения с переменными в произвольном факториальном кольце. В частности, теперь вы можете доказать следующий факт.

Задача 4.8. Докажите через теорему, что все пифагоровы тройки $x^2 + y^2 = z^2$ описываются с точностью до перестановки x, y формулами

$$x = k(m^2 - n^2), \quad y = 2kmn, \quad z = k(m^2 + n^2),$$

где k, m и n целые.

Решение. Не умаляя общности, можем считать, что x, y, z попарно взаимно просты в $\mathbb{Z}$. Смотря на уравнение по модулю 4, получаем, что x и y должны быть разной чётности. Легко проверить, что в таком случае числа $x + yi$ и $x - yi$ взаимно просты в $\mathbb{Z}[i]$. Перепишем уравнение в виде

$$(x + yi)(x - yi) = z^2.$$

По Задаче 4.7 существует единица $\varepsilon \in \mathbb{Z}[i]$ и целые m, n такие, что

$$x + yi = \varepsilon(m + ni)^2,$$

откуда с точностью до знака и перестановки переменных получается указанная в условии параметризация. ■

Задача ниже полезна при решении уравнений как в кольце целых чисел, так и в произвольном кольце.

Задача 4.9. Пусть кольцо R факториально и $x, y, z, t \in R$. Докажите, что все решения уравнения $xy = zt$ в R описываются формулами

$$x = uv, \quad y = wr, \quad z = uw, \quad t = vr,$$

где $u, v, w, r \in R$.

Решение. Если $(x, y, z, t) = (uv, wr, uw, vr)$, то $xy = uvwr = zt$. Обратно, предположим, что $xy = zt$. Если $x = 0$, то $zt = 0$, откуда следует, что либо $z = 0$, либо $t = 0$. В первом случае положим $u = 0, v = t, w = y, r = 1$, тогда как во втором случае положим $u = z, v = 0, w = 1, r = y$. Теперь предположим, что $x \neq 0$, и пусть $u = (x, z)$. Тогда $x = uv$ и $z = uw$, где $v, w \in R$ взаимно просты и $v \neq 0$. Подставляя это в уравнение $xy = zt$, получаем $uvy = uwt$, или $vy = wt$. Поскольку v и w взаимно просты, и v является делителем wt , из теоремы следует, что v является делителем t , поэтому мы можем записать $t = vr$ для некоторого $r \in R$. Тогда $vy = w(vr)$, откуда $y = wr$. ■

Задача 4.10. Опишите все решения уравнения

$$x^2 + y^2 = zt$$

в целых числах.

Решение. Сначала опишем решения для взаимно простых и положительных x, y, z, t . Тогда

$$(x + yi)(x - yi) = zt,$$

и по Задаче 4.9

$$x + yi = mn, \quad x - yi = pq, \quad z = np, \quad t = mq.$$

Поскольку np и mq — положительные целые числа, отсюда следует, что $n = k\bar{p}$ и $q = l\bar{m}$ для некоторых положительных рациональных чисел k и l . С другой стороны, из $N(mn) = N(pq)$ вытекает $N(km\bar{p}) = N(lp\bar{m})$, откуда $k = l$. Пусть u и v — взаимно простые натуральные числа, такие что $k = \frac{u}{v}$. Тогда

$$x + yi = \frac{u}{v}m\bar{p}, \quad x - yi = \frac{u}{v}p\bar{m}, \quad z = \frac{u}{v}p\bar{p}, \quad t = \frac{u}{v}m\bar{m}.$$

Это означает, что $u \mid x, y, z, t$, и, следовательно, $u = 1$. Мы также имеем

$$x + yi = \frac{v}{u}n\bar{q}, \quad x - yi = \frac{v}{u}q\bar{n}, \quad z = \frac{v}{u}n\bar{n}, \quad t = \frac{v}{u}q\bar{q},$$

из чего следует, что $v \mid x, y, z, t$, и, значит, $v = 1$. Пусть $n = u + vi$ и $m = w + ri$, где $u, v, w, r \in \mathbb{Z}$. Тогда из (1) получаем

$$x = uw + vr, \quad y = ur - vw, \quad z = u^2 + v^2, \quad t = w^2 + r^2.$$

Легко проверить, что для не обязательно положительных и взаимно простых u, v, w, r справедлива следующая параметризация:

$$x = s(uw + vr), \quad y = s(ur - vw), \quad z = s(u^2 + v^2), \quad t = s(w^2 + r^2).$$

с целыми s, u, v, w, r . ■

Задача 4.11. Докажите, что все решения уравнения

$$x^2 + x + 1 = yz$$

в целых числах описываются формулами

$$x = ab + bc + cd, \quad y = \varepsilon(a^2 + ac + c^2), \quad z = \varepsilon(b^2 + bd + d^2),$$

где $\varepsilon = \pm 1$, а a, b, c, d — целые числа, удовлетворяющие условию $ad - bc = 1$.

Решение. Перепишем уравнение в виде

$$(x - \omega)(x - \omega^2) = yz.$$

По Задаче 4.9 выполняются равенства

$$x - \omega = uv, \quad x - \omega^2 = wr, \quad y = uw, \quad z = vr$$

с некоторыми $u, v, w, r \in \mathbb{Z}[\omega]$. Пусть $u = a - c\omega^2$, $v = b - d\omega$, тогда

$$x - \omega = ab + bc + cd - (ad - bc)\omega,$$

а, значит, $ad - bc = 1$ и $x = ab + bc + cd$.

Заметим, что $u/\bar{w} = uw/(w\bar{w}) = y/(w\bar{w}) \in \mathbb{Q}$. Следовательно $qu = p\bar{w}$ для некоторых взаимно простых в $\mathbb{Z}$ чисел p, q . Легко заметить, что числа p, q также взаимно просты в $\mathbb{Z}[\omega]$. Значит, qu делится на p , и по Теореме $u = pu'$ для некоторого $u' \in \mathbb{Z}[\omega]$. Но тогда $(x - \omega)/p = u'v \in \mathbb{Z}[\omega]$, следовательно $|p| = 1$ и $u = \varepsilon_1\bar{w}$, или $w = \varepsilon_1\bar{u}$, где $\varepsilon_1 = \pm 1$. Аналогично $r = \varepsilon_2\bar{v}$, где $\varepsilon_2 = \pm 1$.

Далее,

$$y = uw = \varepsilon_1 u\bar{u} = \varepsilon_1(a - c\omega^2)(a - c\omega) = \varepsilon_1(a^2 + ac + c^2).$$

Аналогично $z = \varepsilon_2(b^2 + bd + d^2)$. Осталось заметить, что $yz = x^2 + x + 1 > 0$, поэтому $\varepsilon_1\varepsilon_2 = 1$ и $\varepsilon_1 = \varepsilon_2$. ■

5 Об уравнениях Лебега-Нагеля

История экспоненциальных уравнений Лебега-Нагеля $x^2 + C = Ay^n$ началась в 1850 году, когда французский математик В. Лебег решил первое уравнение такого вида (с коэффициентами $A = C = 1$) для произвольного натурального n . В первой половине XX века норвежский исследователь Т. Нагель существенно развил методы решения для ряда аналогичных уравнений, включая знаменитое уравнение Рамануджана-Нагеля $x^2 + 7 = 2^n$. Важнейший теоретический прорыв произошел в 1970–1980-х годах, когда математики Т. Шори и Р. Тейдеман доказали, что при фиксированных коэффициентах уравнение имеет лишь конечное число решений для степеней $n \geq 3$. Значимым результатом стала работа учёных Я. Бюжо, М. Миньотта и С. Сиксека, опубликованная в 2006 году. Авторы полностью решили уравнение $x^2 + C = y^n$ при $1 \leq C \leq 100$.

В настоящий момент уравнения Лебега-Нагеля всё ещё не решены в общем виде. Основной сложностью является то, что при разных параметрах возникают структуры, обладающие непохожими свойствами. Все уравнения, предложенные вам ниже, решаются, однако элементарными средствами.

Задача 5.1. (Теорема Лебега). Решите уравнение

$$x^2 + 1 = y^n$$

для целых $n \geq 2$.

Решение. Легко видеть, что случай четного n невозможен, поскольку два положительных полных квадрата не могут отличаться на 1. Поэтому мы можем решать задачу для нечётного простого $n = p$. Предположим, существует положительное целочисленное решение уравнения $x^2 + 1 = y^p$. Если y четное, то $y^2 \equiv 3 \pmod{4}$, что, конечно, приводит к противоречию. Следовательно, y нечётное, и отсюда сразу следует, что x должно быть четным.

В кольце $\mathbb{Z}[i]$ мы имеем $y^p = x^2 + 1 = (x - i)(x + i)$. Докажем, что не существует простого числа $\pi \in \mathbb{Z}[i]$ такого, что $\pi | x - i$ и $\pi | x + i$. Предположим, что такое простое число существует, тогда оно должно делить $x + i - (x - i) = 2i$, следовательно, π делит 2, поскольку i является единицей. Отсюда следует, что 2 делит y , что, как мы доказали, невозможно. Из задачи 4.7 следует, что с точностью до единиц, $x + i$ и $x - i$ являются p -ми степенями в $\mathbb{Z}[i]$. Поскольку p нечетное, все единицы в $\mathbb{Z}[i]$ являются p -ми степенями, поэтому существуют $a, b \in \mathbb{Z}$ такие, что $x - i = (a + bi)^p$ и $x + i = \overline{x - i} = (a - bi)^p$.

Используя биномиальную теорему Ньютона, мы можем записать:

$$x - i = (a + bi)^p = \sum_{j=0}^p \binom{p}{j} a^j (bi)^{p-j}.$$

Взяв мнимую часть с обеих сторон, получаем:

$$-1 = \sum_{j=0}^{\frac{p-1}{2}} \binom{p}{2j} a^{2j} b^{p-2j} i^{p-2j-1} = b \sum_{j=0}^{\frac{p-1}{2}} \binom{p}{2j} a^{2j} b^{p-2j-1} i^{p-2j-1}. \quad (1)$$

Таким образом, b делит -1 , что дает $b = \pm 1$.

Теперь мы знаем, что $y^p = (a + bi)^p (a - bi)^p = (a + i)^p (a - i)^p = (a^2 + 1)^p$, следовательно, $y = a^2 + 1$ и a — четное число. Очевидно, что a — ненулевое целое число, иначе $y = 0$.

Возвращаясь к (1), мы имеем

$$-1 = b \sum_{j=0}^{\frac{p-1}{2}} \binom{p}{2j} a^{2j} (-1)^{\frac{p-1}{2}-j} = b(-1)^{\frac{p-1}{2}} \sum_{j=0}^{\frac{p-1}{2}} \binom{p}{2j} (-a^2)^j.$$

Отсюда получаем:

$$\sum_{j=0}^{\frac{p-1}{2}} \binom{p}{2j} (-a^2)^j = \pm 1.$$

Рассмотрим это равенство по модулю 4: все члены с $j > 0$ сравнимы с нулём, поскольку a — четное число, поэтому вся сумма по модулю 4 даёт остаток 1. Отсюда следует, что в правой части мы также имеем 1. Следовательно, $\sum_{j=1}^{\frac{p-1}{2}} \binom{p}{2j} (-a^2)^j = 0$. Мы получаем, что

$$a^2 \binom{p}{2} = \sum_{j=2}^{\frac{p-1}{2}} \binom{p}{2j} (-a^2)^j. \quad (2)$$

Заметим, что при $p = 3$ равенство становится следующим: $a^2 \binom{p}{2} = 0$, что подразумевает исключенный случай $a = 0$.

Поскольку

$$\binom{p}{2k} = \frac{p(p-1)}{2k(2k-1)} \binom{p-2}{2k-2},$$

мы получаем для $j > 1$

$$v_2 \left(a^{2j} \binom{p}{2j} \right) \geq 2jv_2(a) + v_2 \left(\binom{p}{2} \right) - v_2(j) > 2v_2(a) + v_2 \left(\binom{p}{2} \right) = v_2 \left(a^2 \binom{p}{2} \right).$$

Мы доказали неравенство

$$v_2 \left(a^2 \binom{p}{2} \right) < v_2 \left(\sum_{j=2}^{\frac{p-1}{2}} \binom{p}{2j} (-a^2)^j \right),$$

что противоречит (2). ■

Задача 5.2. (а) Докажите, что уравнение

$$x^2 + 9 = y^q$$

не имеет решений для простого $q \equiv 3 \pmod{4}$.

(б) Докажите, что уравнение

$$x^2 + 9 = y^q$$

не имеет решений для простого $q \equiv 1 \pmod{4}$.

Решение. Как и в предыдущей задаче, мы получаем, что y нечетное число, x — четное, а числа $3 + ix$ и $3 - ix$ взаимно просты в $\mathbb{Z}[i]$. Таким образом, существуют целые числа a, b такие, что $3 + ix = (a + bi)^p$, $y = a^2 + b^2$.

Приравнивая действительные части, получаем:

$$3 = a^q - \binom{q}{2} a^{q-2} b^2 + \dots - \binom{q}{q-1} (-1)^{\frac{q-1}{2}} a b^{q-1}.$$

Следовательно, $a|3$, и поскольку $\binom{q}{k}$ делится на q для $1 \leq k < q$, мы получаем сравнение $a^q \equiv a \equiv 3 \pmod{q}$. Итак, у нас есть либо $a = -3, q = 3$, либо $a = 3$. В первом случае мы получаем равенство $x^2 + 1 = (y - 2)(y^2 + 2y + 4)$. Это невозможно, потому что правая сторона делится на некоторое простое число $p \equiv 3 \pmod{4}$, в то время как простые делители левой стороны имеют вид $4n + 1$.

Таким образом, $a = 3$, и, следовательно, транспонируя члены, получаем:

$$3^{q-1} - 1 = \binom{q}{2} 3^{q-3} b^2 - \dots - \binom{q}{q-1} (-1)^{\frac{q-1}{2}} b^{q-1}.$$

Поскольку $y = 9 + b^2$ нечетное, b должно быть четным. Теперь запишем:

$$3^{q-1} - 1 = b^2 \left(\binom{q}{2} 3^{q-3} - \dots - \binom{q}{q-1} (-1)^{\frac{q-1}{2}} b^{q-3} \right) = b^2 R.$$

(а) Если $q \equiv 3 \pmod{4}$, то $v_2(3^{q-1} - 1) = 3$. Но

$$\frac{R}{b^2} \equiv \binom{q}{2} 3^{q-3} \equiv 1 \pmod{2}.$$

Следовательно, $v_2(R) = v_2(b^2) = 2v_2(b)$, что является четным числом, противоречие.
 (б) Если $q \equiv 1 \pmod{4}$, пусть $c = v_2(q - 1)$, $d = v_2(b)$. Тогда $v_2(3^{q-1} - 1) = c + 2$. Из тождества

$$\binom{q}{2k} b^{2k-2} = \binom{q}{2} \cdot \binom{q-2}{2k-2} \cdot \frac{2b^{2k-2}}{(2k-1)(2k)}$$

мы делаем вывод, что $v_2\left(\binom{q}{2}\right) < v_2\left(\binom{q}{2k} b^{2k-2}\right)$ для $k > 1$. Следовательно,

$$v_2(\text{RHS}) = v_2(b^2) + v_2\left(\binom{q}{2}\right) = 2d + c - 1,$$

четность которого отличается от $c + 2$, что приводит к противоречию. ■

На примере следующей задачи можно убедиться, какой сильный эффект даёт сочетание метода Стёрмера и теории из раздела 4.

Задача 5.3. (а) Опишите все решения обобщённого уравнения Пелля

$$x^2 - (a^2 + 2)y^2 = -2$$

для натурального a .

(б) Докажите, что при нечётном a это уравнение имеет не более двух решений (x, y) таких, что любой простой делитель y делит $a^2 + 2$.

(в) Решите уравнение

$$x^2 + 2 = y^n$$

для целого $n \geq 2$.

Решение. (а) Из решения задачи 1.13 прошлогодного проекта «Диофантовы уравнения» (<https://t-o-t.org/lktg/2025/1/1-1-diophantine-rus.pdf>) следует, что уравнение $x^2 - (a^2 + 2)y^2 = -2$ имеет не более одного класса решений. Легко установить, что $(a, 1)$ является решением. Поскольку $(a^2 + 1, a)$ является фундаментальным решением уравнения Пелля $x^2 - (a^2 + 2)y^2 = 1$, мы получаем, что все положительные решения уравнения

$$x^2 - (a^2 + 2)y^2 = -2$$

описываются формулой:

$$x_t + y_t \sqrt{a^2 + 2} = \left(a + \sqrt{a^2 + 2}\right) \left(a^2 + 1 + a\sqrt{a^2 + 2}\right)^t = \frac{\left(a + \sqrt{a^2 + 2}\right)^{2t+1}}{2^t}$$

с неотрицательным целым числом t .

(б) Сначала отметим, что $y_1 = 1$. Предположим, что существует $t > 0$ такое, что все простые делители y_t делят $a^2 + 2$. Из равенства

$$2^t \left(x_t + y_t \sqrt{a^2 + 2}\right) = \left(a + \sqrt{a^2 + 2}\right)^{2t+1}$$

следует, что если простое число $p = 2u + 1$ делит $2t + 1$, то y_u делит y_t . Используя равенство

$$2^{\frac{p-1}{2}} y_u = (a^2 + 2)^{\frac{p-1}{2}} + \dots + \binom{p}{p-3} (a^2 + 2) a^{p-3} + p a^{p-1},$$

мы получаем, что y_u имеет единственный простой множитель p . Если $p > 3$, то правая сторона последнего неравенства больше, чем $2^{\frac{p-1}{2}} p$, и она дает остаток p по модулю p^2 , поэтому y_t не может быть степенью p .

Теперь у нас остался случай $p = 3$, поэтому $2t + 1$ и y_t являются степенями 3. Из равенства

$$y_4 = 16a^8 + 56a^6 + 60a^4 + 20a^2 + 1 = (2a^2 + 1)((8a^6 + 24a^4 + 18a^2 + 1)$$

следует, что единственный индекс $t > 0$, удовлетворяющий описанным выше условиям, — это $t = 1$.

(в) Легко видеть, что случай четного n невозможен, поскольку два положительных полных квадрата не могут отличаться на 2. Перепишем уравнение для нечетного n :

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

Из пункта (б) следует, что $n = 3$ и $\left((a^2 + 2)^{\frac{n-1}{2}} \right) = 2a^2 + 1$. Следовательно, $a = 1$ и $(5, 2)$ является единственным решением. ■

Задача 5.4. (а) Решите уравнение

$$x^2 + 4 = y^3.$$

(б) Докажите, что уравнение

$$x^2 + 4 = y^q$$

не имеет решений для простого $q \equiv 1 \pmod{4}$.

Решение. (а) Пусть x — нечетное число. Уравнение можно записать в виде

$$(2 + ix)(2 - ix) = y^3.$$

Покажем, что $2 + ix$ и $2 - ix$ взаимно просты в кольце $\mathbb{Z}[i]$. Действительно, пусть $z = (2 + ix, 2 - ix)$, $z = c + di$. Тогда z делит $(2 + ix) + (2 - ix) = 4$, следовательно; $\bar{z} \mid 4$. Отсюда следует, что $z \cdot \bar{z} = c^2 + d^2$ делит 16. С другой стороны, $z \mid 2 + ix$ подразумевает $\bar{z} \mid 2 - ix$; следовательно, $c^2 + d^2 \mid 4 + x^2$. Но x — нечётное число, поэтому $c^2 + d^2 = 1$, что означает, что z является единицей в $\mathbb{Z}[i]$.

Поскольку $2 + ix$ и $2 - ix$ взаимно просты, из $(2 + ix)(2 - ix) = y^3$ следует, что $2 + ix = (a + bi)^3$ для некоторых целых чисел a и b . Отождествляя действительную и мнимую части, получаем $a(a^2 - 3b^2) = 2$ и $3a^2b - b^3 = x$. Первое уравнение даёт $a = \pm 1$ или $a = \pm 2$, что даёт положительное решение $(11, 5)$.

Если x — чётное число, то y — чётное число. Пусть $x = 2u$ и $y = 2v$. Уравнение принимает вид $u^2 + 1 = 2v^3$, то есть $(u + i)(u - i) = 2v^3$. Поскольку u — нечетное число, мы имеем $i \pm 1 | u \pm 1$.

Так как $(u + i, u - i) = 1$ и $2 = (1 + i)(1 - i)$, получаем:

$$\frac{u + i}{i + 1} \cdot \frac{u - i}{i - 1} = v^3.$$

Поскольку $\frac{u+i}{i+1}$ и $\frac{u-i}{i-1}$ взаимно просты, из задачи 4.7 следует, что:

$$u + i = (1 + i)(a + bi)^3$$

для некоторых целых чисел a и b .

Выделив действительную и мнимую части, получаем:

$$a^3 - 3a^2b - 3ab^2 + b^3 = u \quad \text{и} \quad a^3 + 3a^2b - 3ab^2 - b^3 = 1.$$

Последнее соотношение можно записать как:

$$(a - b)(a^2 + 4ab + b^2) = 1,$$

что приводит к системам:

$$\begin{cases} a - b = 1, \\ a^2 + 4ab + b^2 = 1, \end{cases} \quad \text{и} \quad \begin{cases} a - b = -1, \\ a^2 + 4ab + b^2 = -1. \end{cases}$$

Вторая система не имеет решений. Действительно, можно заметить, что

$$a^2 + 4ab + b^2 = (a + 2b)^2 - 3b^2 \equiv 0, 1 \pmod{3}.$$

Первая система имеет целочисленные решения $(a, b) = (1, 0)$ и $(a, b) = (0, -1)$, что дает положительное решение $(2, 2)$ исходного уравнения.

Ответ: $(2, 2), (11, 5)$.

(б) Если x четное, скажем, $x = 2u$, то y четное, $y = 2v$. Уравнение принимает вид $u^2 + 1 = 2^{q-2}v^2$. Оно не имеет решений, так как $q - 2 > 2$ и 4 не делит $u^2 + 1$.

Если x нечетное, то числа $x + 2i$ и $x - 2i$ взаимно просты в $\mathbb{Z}[i]$. Согласно задаче 4.7, $x + 2i = (a + bi)^q$, для некоторых целых чисел a и b , имеющих разную четность. Определив действительную и мнимую части, получаем:

$$2 = \sum_{r=0}^{(q-1)/2} \binom{q}{2r+1} (a^2)^{(q-1)/2-r} b^{2r+1} (-1)^r. \quad (1)$$

Рассматривая это уравнение по модулю q , получаем:

$$2 \equiv b^q (-1)^{(q-1)/2} \equiv b (-1)^{(q-1)/2} \pmod{q},$$

следовательно

$$b = 2(-1)^{(q-1)/2},$$

так как $b|2$.

Подставляя это выражение для b в (1), получим

$$(-1)^{(q-1)/2} = \sum_{r=0}^{(q-1)/2} \binom{q}{2r+1} (a^2)^{(q-1)/2-r} (-4)^r. \quad (2)$$

Дано, что $q \equiv 1 \pmod{4}$, предположим, что $\nu_2(q-1) = s \geq 2$. Теперь уравнение (2) можно записать в виде

$$1 - q + q(1 - (a^2)^{(q-1)/2}) = \sum_{r=1}^{(q-1)/2} \binom{q}{2r+1} (a^2)^{(q-1)/2-r} (-4)^r. \quad (3)$$

Каждый общий член в правой части этого уравнения имеет следующую форму:

$$\frac{q(q-1)}{2r(2r+1)} \binom{q-2}{2r-1} (a^2)^{(q-1)/2-r} (-4)^r.$$

Так как $2^{2r} > 2r$ для любого положительного целого числа r , мы заключаем, что каждый такой член делится на 2^{s+1} . Поскольку

$$\nu_2((1 - (a^2)^{(q-1)/2})) = \nu_2(1 - a^2) + \nu_2(q-1) - 1 \leq s + 1,$$

согласно лемме об уточнении показателя, левая часть делится на 2^s , но не делится на 2^{s+1} , противоречие. ■

Задача 5.5. Пусть (x, y) — решение уравнения $x^2 + 4 = y^q$ для некоторого простого $q > 3$, такого что $q \equiv 3 \pmod{4}$. Докажите, что

- (а) $q \equiv 3 \pmod{8}$; (б) $y^{\frac{q-1}{2}} + 1$ делится на $y - 8$;
- (в) уравнение $x^2 + 4 = 5^q$ не имеет решений;
- (г) уравнение $x^2 + 4 = y^q$ не имеет решений.

Решение. (а) Как и в решении задачи 5.4b, получаем:

$$(-1)^{(q-1)/2} = \sum_{r=0}^{(q-1)/2} \binom{q}{2r+1} (a^2)^{(q-1)/2-r} (-4)^r. \quad (1)$$

Рассматривая (1) по модулю 8, получаем

$$-1 \equiv q + 4 \pmod{8},$$

так что $q \equiv 3 \pmod{8}$.

(б) Полагая $u = a + 2i, v = a - 2i$, из $x + 2i = (a + bi)^q$ с

$$b = 2(-1)^{(q-1)/2} = -2$$

следует, что

$$\frac{u^q - v^q}{u - v} = -1.$$

Следующее тождество легко проверяется:

$$\frac{u^{(q-1)/2} - v^{(q-1)/2}}{u - v} \cdot (u^{(q+1)/2} + v^{(q+1)/2}) = -(uv)^{(q-1)/2} + \frac{u^q - v^q}{u - v}.$$

Поскольку $q = 8t + 3$, можно записать:

$$\frac{u^{4t+1} - v^{4t+1}}{u - v} \cdot (u^{4t+2} + v^{4t+2}) = -y^{4t+1} - 1. \quad (2)$$

Второй множитель в левой части (2) делится на $(u^2 + v^2)/2 = y - 8$, что и требовалось доказать.

(в) В этом случае $a = 1$. Предположим, что $\nu_2(q - 3) = t \geq 3$. Тогда из (1) следует, что

$$-1 \equiv q - 4 \binom{q}{q-3} \pmod{2^{t+2}},$$

следовательно $q \equiv 3 \pmod{2^{t+1}}$, противоречие.

(г) Предположим теперь, что $a > 1$, тогда $a^2 - 4 > 0$. Поскольку $y - 8 = a^2 - 4 \equiv 5 \pmod{8}$, это число содержит по крайней мере один простой множитель $p \equiv 7 \pmod{8}$ или $p \equiv 5 \pmod{8}$.

Из пункта (б) следует, что $(-y)^{4t+1} \equiv 1 \pmod{p}$, поэтому

$$1 = \left(\frac{-y}{p} \right) = \left(\frac{-8 - (y - 8)}{p} \right) = \left(\frac{-8}{p} \right) = \left(\frac{-2}{p} \right),$$

то есть $p \equiv 1 \pmod{8}$ или $p \equiv 3 \pmod{8}$, что противоречит выбору p . ■

6 К доказательству факториальности

Кольцо R называется **евклидовым**, если существует функция $f : R \setminus \{0\} \rightarrow \mathbb{Z}_{\geq 0}$ такая, что

- (i) $f(a) \leq f(ab)$ для любых ненулевых $a, b \in R$, и
- (ii) если $a, b \in R$ и $b \neq 0$, то существуют такие q и r в R , что $a = bq + r$ и либо $r = 0$, либо $f(r) < f(b)$.

Функция f в данном случае называется *евклидовой нормой*.

Например, множество целых чисел является евклидовым кольцом с евклидовой нормой $f(a) = |a|$, где r — остаток от деления a на b . Интуитивно, евклидово кольцо — это то кольцо, в котором можно выполнять «деление с остатком».

Задача 6.1. Рассмотрим отображение $N(a + bi) = a^2 + b^2$. Докажите, что оно

- (а) мультипликативно, то есть $N(zw) = N(z)N(w)$ для любых комплексных z, w ;
- (б) является евклидовой нормой в гауссовом кольце, то есть кольцо $\mathbb{Z}[i]$ евклидово.

Решение. (а) Пусть $z = a + bi$ и $w = c + di$. Мультипликативность нормы доказывается непосредственной проверкой:

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + cb)^2.$$

(б) Возьмем ненулевые гауссовы числа a, b . Докажем свойство (i): поскольку $b \neq 0$, то $N(b) \geq 1$, и, значит, $N(ab) = N(a)N(b) \geq N(a)$, где равенство верно по пункту (а).

Для доказательства (ii) запишем комплексное число a/b в виде $u + iv$ для некоторых рациональных чисел u, v . Выберем целые числа x и y , ближайшие к u и v соответственно, то есть $|u - x| \leq 1/2$ и $|v - y| \leq 1/2$. Тогда $q = x + iy$ и $r = a - bq$ являются гауссовыми. Кроме того,

$$\begin{aligned} N(r) &= N(a - bq) = N(b)N(a/b - q) = N(b)N((u - x) + (v - y)i) \\ &= N(b)((u - x)^2 + (v - y)^2) \leq N(b)((1/2)^2 + (1/2)^2) \\ &= N(b)/2 < N(b). \end{aligned}$$

■

Далее мы покажем, что многие свойства целых чисел, которые мы использовали для решения уравнений, естественным образом переносятся на евклидовы кольца с практически тем же доказательством.

Задача 6.2. Пусть R — евклидово кольцо, и $a, b \in R$ не равны нулю одновременно. Докажите, что существуют такие $x, y \in R$, что $ax + by$ является наибольшим общим делителем a и b .

Решение. Обозначим

$$S = \{ax + by \mid x, y \in R\}.$$

Выберем произвольные евклидову норму f и ненулевое $d \in S$ с наименьшим значением $f(d)$. Тогда $d = ax_0 + by_0$. Поделим a на d с остатком: возьмем такие $q, r \in R$, что $a = qd + r$ и либо $r = 0$, либо $f(r) < f(d)$. Однако

$$r = a - qd = a - q(ax_0 + by_0) = a(1 - qx_0) + b(-qy_0) \in S.$$

Если $r \neq 0$, то $f(r) < f(d)$, что противоречит выбору d . Следовательно, $r = 0$, и d делит a . Аналогично d делит b . Следовательно, d является общим делителем a и b . Теперь, если c — любой другой общий делитель a и b , то c делит $ax_0 + by_0 = d$. Таким образом, d — наибольший общий делитель a и b . ■

Как следствие из предыдущей задачи, a и b взаимно просты тогда и только тогда, когда существуют такие $x, y \in R$, что

$$ax + by = 1.$$

Задача 6.3. Пусть R — евклидово кольцо, и $a, b, c \in R$. Докажите, что:

- (а) если $a \neq 0$ и b взаимно просты, bc делится на a , то c делится на a ;
- (б) если a и c взаимно просты, а также b и c взаимно просты, то ab и c взаимно просты.

Решение. (а) По задаче 6.2 существуют такие $x_0, y_0 \in R$, что $ax_0 + by_0 = 1$. Тогда

$$c = c(ax_0 + by_0) = (a)cx_0 + (bc)y_0 \equiv 0 + 0 = 0 \pmod{a}.$$

(б) По задаче 6.2 существуют такие $x_1, y_1, x_2, y_2 \in R$, что $ax_1 + cy_1 = 1$ и $bx_2 + cy_2 = 1$. Тогда

$$1 = (ax_1 + cy_1)(bx_2 + cy_2) = ab(x_1x_2) + c(ax_1y_2 + by_1x_2 + cy_1y_2).$$

Следовательно, ab и c взаимно просты по задаче 6.2. ■

Задача 6.4. Пусть R — евклидово кольцо, $a_1, \dots, a_n \in R$ и неприводимое $p \in R$ делит произведение $\prod_{i=1}^n a_i$. Докажите, что p делит a_i для некоторого i .

Решение. Докажем утверждение индукцией по n . База индукции для $n = 1$ тривиальна. Пусть $n > 1$ и $b = \prod_{i=2}^n a_i$. Если a_1 и p взаимно просты, то по задаче 6.3.а p делит b . Тогда по предположению индукции p делит a_i для некоторого $2 \leq i \leq n$. Если a_1 и p не взаимно просты, то $d = \text{НОД}(a_1, p)$ для некоторого необратимого $d \in R$. Тогда $p = du$ и $a_1 = dv$ для некоторых $u, v \in R$. Поскольку p неприводимо и d необратимо, то u обратимо, и p делит a_1 . ■

Далее установим некоторые полезные свойства евклидовых норм.

Задача 6.5. Пусть R — евклидово кольцо, и f — любая евклидова норма. Докажите, что:

- (а) $f(ab) = f(a)$ для любых ненулевого $a \in R$ и единицы $b \in R$;
- (б) $f(ab) > f(a)$ для любых ненулевого $a \in R$ и ненулевого необратимого $b \in R$;
- (в) $f(a) \geq f(1)$ для любого ненулевого $a \in R$, причем равенство достигается тогда и только тогда, когда a — единица в R .

Решение. (а) Пусть число c обратное к b . Тогда по свойству (i) евклидовой нормы имеем

$$f(a) \leq f(ab) \leq f((ab)c) = f(a(bc)) = f(a).$$

(б) Предположим противное, что $f(ab) = f(a)$ для некоторого $a \neq 0$ и необратимого b . Поделим a на ab с остатком: возьмем такие $q, r \in R$, что $a = (ab)q + r$. Тогда $r = a(1 - bq)$. Поскольку b необратим, то $1 - bq \neq 0$. Следовательно, $r \neq 0$. По следующему неравенству приходим к противоречию:

$$f(a) = f(ab) > f(r) = f(a(1 - bq)) \geq f(a).$$

(в) Если a обратим, то по пункту (а) имеем $f(a) = f(a \cdot 1) = f(1)$. Иначе по пункту (б) имеем $f(a) = f(a \cdot 1) > f(1)$. ■

Теперь мы готовы доказать Основную теорему арифметики для евклидовых колец.

Задача 6.6. Докажите, что любое евклидово кольцо R факториально, т.е.

- (а) любое ненулевое необратимое число из R имеет полное разложение в R ;
 (б) любые два полных разложения числа из R эквивалентны.

Решение. Возьмем евклидову норму f в R .

(а) От противного, возьмем ненулевое необратимое число $x \in R$ минимальной нормы, не имеющее полного разложения. Если x неприводимо, то x само является своим полным разложением. Противоречие. Иначе найдутся такие необратимые y и z , что $x = yz$. По задаче 6.5.6 имеем $f(x) > f(y)$ и $f(x) > f(z)$. Тогда y, z имеют полные разложения по минимальности выбора и произведение их полных разложений будет полным разложением для x . Противоречие.

(б) Докажем эквивалентность любых двух полных разложений индукцией по количеству m множителей в первом разложении.

База индукции: $m = 1$. Пусть $x = p_1 = q_1 \cdot \dots \cdot q_k$. Так как p_1 неприводимо, k должно равняться 1 (иначе p_1 раскладывается в произведение необратимых). Значит, $x = p_1 = q_1$, разложения эквивалентны тривиально.

Шаг индукции: предположим, что утверждение верно для всех разложений, длина первого из которых меньше m . Пусть даны два полных разложения:

$$x = p_1 \cdot \dots \cdot p_m = q_1 \cdot \dots \cdot q_k.$$

По задаче 6.4 для $p = p_1$, $n = k$ и $a_i = q_i$ имеем, что для некоторого i число p_1 делит q_i . Поскольку оба p_1 и q_i неприводимы, то тогда они ассоциированы: $q_i = up_1$ для некоторой единицы u кольца R . Не нарушая общности, можем считать, что $i = 1$ (иначе нужно взять композицию перестановки $(1i)$ с построенной ниже биекцией π).

Подставим это в исходное равенство и скоратим на p_1 :

$$x/p_1 = p_2 \cdot \dots \cdot p_m = (uq_2) \cdot q_3 \cdot \dots \cdot q_k.$$

Таким образом, мы получили два полных разложения числа x/p_1 , причем первое разложение состоит из $m - 1$ множителя.

По предположению индукции эти разложения эквивалентны: $m - 1 = k - 1 \implies m = k$, и существует биекция $\pi' : \{2, \dots, m\} \rightarrow \{2, \dots, k\}$ такая, что p_j ассоциировано с соответствующим множителем второго разложения.

Дополним биекцию π' до биекции $\pi : \{1, \dots, m\} \rightarrow \{1, \dots, k\}$, положив $\pi(1) = 1$ и $\pi(j) = \pi'(j)$ при $j \geq 2$. Получим искомую эквивалентность. ■

Задача 6.7. Докажите, что следующие кольца евклидовы: (а) $\mathbb{Z}[i\sqrt{2}]$; (б) $\mathbb{Z}[\omega]$.

Решение. (а) Докажем, что функция $N(x) = a^2 + 2b^2$ для $x = a + bi\sqrt{2} \in \mathbb{Z}[i\sqrt{2}]$ является евклидовой нормой кольца $\mathbb{Z}[i\sqrt{2}]$.

Доказательство свойства (i): для ненулевых $x, y \in \mathbb{Z}[i\sqrt{2}]$ имеем

$$N(xy) = N(x)N(y) \geq N(x),$$

т.к. N мультипликативна и $N(y) \geq 1$ (поскольку $y \neq 0$).

Для доказательства (ii) запишем комплексное число a/b в виде $u + vi\sqrt{2}$ для некоторых рациональных чисел u, v . Выберем целые числа x и y , ближайšie к u и v соответственно, то есть $|u - x| \leq 1/2$ и $|v - y| \leq 1/2$. Тогда $q = x + yi\sqrt{2}$ и $r = a - bq$ принадлежат $\mathbb{Z}[i\sqrt{2}]$. Кроме того,

$$\begin{aligned} N(r) &= N(a - bq) = N(b)N(a/b - q) = N(b)N\left((u - x) + (v - y)i\sqrt{2}\right) \\ &= N(b)((u - x)^2 + 2(v - y)^2) \leq N(b)((1/2)^2 + 1/2) \\ &= 3N(b)/4 < N(b). \end{aligned}$$

(б) Докажем, что функция $N(x) = a^2 - ab + b^2$ для $x = a + b\omega \in \mathbb{Z}[\omega]$ является евклидовой нормой кольца $\mathbb{Z}[\omega]$.

Доказательство свойства (i): для ненулевых $x, y \in \mathbb{Z}[\omega]$ имеем

$$N(xy) = N(x)N(y) \geq N(x),$$

т.к. N мультипликативна и $N(y) \geq 1$ (поскольку $y \neq 0$).

Для доказательства (ii) запишем комплексное число a/b в виде $u + v\omega$ для некоторых рациональных чисел u, v . Выберем целые числа x и y , ближайšie к u и v соответственно, то есть $|u - x| \leq 1/2$ и $|v - y| \leq 1/2$. Тогда $q = x + y\omega$ и $r = a - bq$ принадлежат $\mathbb{Z}[\omega]$. Кроме того,

$$\begin{aligned} N(r) &= N(a - bq) = N(b)N(a/b - q) = N(b)N((u - x) + (v - y)\omega) \\ &= N(b)((u - x)^2 - (u - x)(v - y) + (v - y)^2) \leq N(b)((1/2)^2 + (1/2)^2 + (1/2)^2) \\ &= 3N(b)/4 < N(b). \end{aligned}$$

■

Список литературы

1. Cai, Z. (2025). An Effective Method for Solving a Class of Transcendental Diophantine Equations. arXiv. <https://arxiv.org/abs/2510.11753>
2. Bennett, M. A. (2001). On some exponential equations of S. S. Pillai. Canadian Journal of Mathematics, 53(5), 897–922.
3. Klazar, M. (2010). Størmer's solution of the unit equation $x - y = 1$. Unpublished manuscript, Department of Applied Mathematics, Charles University, Prague. Retrieved from <https://kam.mff.cuni.cz/%7Eklazar/othertexts.html>
4. Lehmer, D. H. (1964). On a Problem of Størmer. Illinois Journal of Mathematics, 8(1), 57–79.
5. Daems, J. (2002). A Cyclotomic Proof of Catalan's Conjecture: Master's Thesis. Leiden: Universiteit Leiden, 64 p.
6. Grechuk, B., Wilcox, A. (2024). Polynomial Diophantine Equations: A Systematic Approach. Springer. <https://doi.org/10.1007/978-3-031-62949-5>
7. Andreescu, T., Andrica, D., Cucurezeanu, I. (2010). An introduction to Diophantine equations: A problem-based approach. Birkhäuser.
8. <https://artofproblemsolving.com/community/c6h418604p2361782>
9. <https://mathoverflow.net/questions/206645/on-a-result-attributed-to-w-ljunggren-and-t-nagell>
10. <https://mathoverflow.net/questions/285507/a-modification-of-the-ljunggren-nagell-equation>
11. <https://artofproblemsolving.com/community/c6h254153p1389586>
12. <https://artofproblemsolving.com/community/c6h3524470p34235849>
13. <https://artofproblemsolving.com/community/c6h553400p3215430>
14. <https://mathoverflow.net/questions/490280/on-a-paper-of-wilhelm-ljunggren>
15. <https://artofproblemsolving.com/community/c6h3048886p27466981>