

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	4
3	По следам Стёрмера	8
4	Об уравнениях в факториальных кольцах	9
5	Об уравнениях Лебега-Нагеля	12
6	К доказательству факториальности	13

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

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.

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

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.

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

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 $y > 1$.

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.

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

Нам неизвестен элементарный алгоритм, который по уравнению $(*)$ при $c > 1$ 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 $10^x - 7^y = 3$.

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

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

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 .

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.

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

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

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 .

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 .

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 .

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.

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

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 $w(p)$.

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 $D y_1$ делится на p ,
 (б) $w(p)$ делит $(p - \varepsilon)/2$, если $D y_1$ не делится на p , где

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

Задача 2.8. Пусть $p > 3$ простое число, делящее $D y_1$. Докажите, что $U_p \equiv p \pmod{p^2}$.

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

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

Для краткости запишем

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

Введём ещё одно обозначение:

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

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 .

Задача 2.11. Докажите, что

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

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 $n > 3$.

Задача 2.13. Рассмотрим целое $n > 3$.

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

(б) Докажите, что $q \geq 2n - 1$.

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

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

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.

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.

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 .

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 .

Задача 3.4. Докажите, что уравнение

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

не имеет решений в натуральных числах.

Задача 3.5. Докажите, что уравнение

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

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

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 .)

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.

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) $1 + 3i$, $3 + 4i$, $5 + 7i$.

Задача 4.4. Найдите все неприводимые гауссовы числа.

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.

Наибольшим общим делителем $\text{НОД}(a, b)$ 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 $\text{НОД}(a, b)$ в произвольном кольце не гарантируется, но он существует для факториальных колец (подумайте почему). Числа a и b называются *взаимно простыми*, если любой их $\text{НОД}(a, b)$ 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?

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 $u_1, u_2 \in R$.

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.

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 $u, v, w, r \in R$.

Задача 4.10. Опишите все решения уравнения

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

в целых числах.

Задача 4.11. Докажите, что все решения уравнения

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

в целых числах описываются формулами

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

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

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 $n \geq 2$.

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 $q \equiv 1 \pmod{4}$.

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 $n \geq 2$.

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 $q \equiv 1 \pmod{4}$.

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.

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.

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 .

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.

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 .

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 .

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.

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

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>