По мотивам задачника «Математического просвещения»

Семь этюдов об одном несовпадении

Н. Н. Осипов

> *— Видите, Балаганов, что можно сделать из простой швейной машины Зингера? Небольшое приспособление — и получилась прелестная колхозная сноповязалка.*
>
> И. Ильф, Е. Петров. *Золотой телёнок*

На одной недавней математической олимпиаде[1)] её участникам была предложена следующая

Задача. *Докажите, что числа* $\operatorname{arctg}(4/3)$ *и* π *несоизмеримы.*

Иными словами, требовалось показать, что число

$$\frac{\operatorname{arctg}(4/3)}{\pi}$$

иррационально. Если привлечь комплексные числа, то это утверждение можно сформулировать так: *число*

$$\frac{3+4\sqrt{-1}}{5}$$

[1)] *Региональная студенческая олимпиада по математике*, состоявшаяся в апреле 2010 года. Регулярно проводится Институтом математики Сибирского федерального университета (Красноярск) и обычно собирает команды университетов Абакана, Кемерово, Новосибирска, Улан-Удэ и самого Красноярска.

не является корнем из единицы. Таким образом, решение задачи сводится к доказательству такого факта: *при любом* $n = 1, 2, \ldots$ *равенство*

$$(3 + 4\sqrt{-1})^n = 5^n \qquad (*)$$

невозможно. Кому-то это может показаться очевидным: в самом деле, ведь не может быть, чтобы мнимое комплексное число $(3 + 4\sqrt{-1})^n$ оказалось равным вещественному числу 5^n. Но почему, собственно, первое число является мнимым? Как это можно доказать? И вообще, какие есть способы аккуратно опровергнуть равенство $(*)$?

В дальнейшем изложении мы будем использовать некоторые стандартные понятия и факты из теории колец и теории многочленов. Все необходимые для понимания предварительные сведения читатель при желании сможет найти, например, в книгах [1] и [6].

Этюд I. Канонический эпиморфизм

В *факторкольце* $R_1 = \mathbb{Z}[\sqrt{-1}]/I_1$ *кольца целых гауссовых чисел*

$$\mathbb{Z}[\sqrt{-1}] = \{a + b\sqrt{-1} : (a, b) \in \mathbb{Z}^2\}$$

по *идеалу* $I_1 = (5)$ имеем $5 = 0$ и $(3 + 4\sqrt{-1})^2 = 3 + 4\sqrt{-1}$. Но тогда

$$5^n = 0, \quad (3 + 4\sqrt{-1})^n = 3 + 4\sqrt{-1}$$

при любом натуральном n, и равенство $(*)$ не может быть верным.

А в факторкольце $R_2 = \mathbb{Z}[\sqrt{-1}]/I_2$, где $I_2 = (1+2\sqrt{-1})$, ещё нагляднее:

$$5^n = 0, \quad (3 + 4\sqrt{-1})^n = 1,$$

поскольку по-прежнему $5 = 0$, но теперь $3 + 4\sqrt{-1} = 1$.

Отметим кстати, что кольцо R_1 состоит из $25 = 5^2$ элементов и не является полем (ибо, например, содержит *делители нуля* $1 \pm 2\sqrt{-1}$), а R_2 — поле из 5 элементов (в отличие от $I_1 \subset I_2$, идеал I_2 уже *максимален*).

Этюд II. Факториальное кольцо

Поскольку $3 + 4\sqrt{-1} = (2 + \sqrt{-1})^2$ и $5 = (2 + \sqrt{-1})(2 - \sqrt{-1})$, равенство $(*)$ можно переписать в виде

$$(2 + \sqrt{-1})^n = (2 - \sqrt{-1})^n.$$

Но это равенство невозможно, поскольку в *евклидовом* (а значит, и *факториальном*) кольце $\mathbb{Z}[\sqrt{-1}]$ оба числа $2 \pm \sqrt{-1}$ являются *простыми*, причём *неассоциированными*.

Противоречивость равенства $(*)$ также станет очевидной, если заметить, что число $1+2\sqrt{-1}$ — простой делитель 5, который не делит $3+4\sqrt{-1}$ ввиду равенства $3 + 4\sqrt{-1} = 2(1 + 2\sqrt{-1}) + 1$.

Этюд III. Циклотомические многочлены

Хорошо известно, что *циклотомический многочлен* порядка n

$$\Phi_n(x) = \prod_{\text{НОД}\,(a,n)=1} (x - \zeta_n^a), \quad \zeta_n = \exp\,(2\pi\sqrt{-1}/n),$$

имеет целочисленные коэффициенты и неприводим над полем рациональных чисел $\mathbb{Q}$. Как следствие, любой многочлен $f(x) \in \mathbb{Q}[x]$, имеющий общие корни с $\Phi_n(x)$, обязан делиться на $\Phi_n(x)$. В частности, справедливо неравенство

$$\deg f(x) \geqslant \deg \Phi_n(x) = \varphi(n), \qquad (\dagger)$$

где $\varphi(n)$ — *функция Эйлера*.

Пусть теперь n — наименьшее натуральное число, для которого равенство $(*)$ справедливо. Тогда

$$\frac{3 + 4\sqrt{-1}}{5} = \zeta_n^a$$

для некоторого a, взаимно простого с n. Поскольку число слева — *квадратичная иррациональность*, имеем $\varphi(n) \leqslant 2$, откуда $n \in \{1, 3, 4, 6\}$. Но, как показывает непосредственная проверка, для этих значений n равенство $(*)$ не выполняется.

Фактически из $(\dagger)$ вытекает следующая более общая

Теорема. *Если* $\varphi/\pi \in \mathbb{Q}$ *и* $\cos\varphi \in \mathbb{Q}$, *то* $\cos\varphi \in \{0, \pm 1/2, \pm 1\}$.

Действительно, если $\varphi = 2\pi a/n$, где $0 \leqslant a < n$ и НОД $(a, n) = 1$, то

$$2\cos\varphi = \zeta_n^a + \zeta_n^{-a},$$

откуда ζ_n^a — корень $f(x) = x^2 - (2\cos\varphi)x + 1 \in \mathbb{Q}[x]$.

Другие доказательства этой теоремы будут даны в этюдах V и VI.

Этюд IV. Диадический показатель

Из равенства $(*)$ вытекает, что мнимая часть числа

$$(3 + 4\sqrt{-1})^n = (2 + \sqrt{-1})^{2n} = X_n + Y_n\sqrt{-1}$$

должна быть нулевой. Применив *биномиальную формулу*, найдём

$$Y_n = 2(-1)^{n-1} \sum_{k=0}^{n-1} (-1)^k C_{2n}^{2k+1} 2^{2k}.$$

Если равенство $Y_n = 0$ записать в виде

$$C_{2n}^1 = -\sum_{k=1}^{n-1} (-1)^k C_{2n}^{2k+1} 2^{2k},$$

станет понятно, что оно невозможно. Действительно,

$$C_{2n}^{2k+1} = \frac{C_{2n}^{1} C_{2n-1}^{2k}}{2k+1},$$

поэтому при $k \geqslant 1$ имеем

$$\nu_2(C_{2n}^{2k+1} 2^{2k}) = \nu_2\left(\frac{C_{2n}^{1} C_{2n-1}^{2k} 2^{2k}}{2k+1}\right) \geqslant \nu_2(C_{2n}^{1}) + 2k > \nu_2(C_{2n}^{1}),$$

где $\nu_2(m)$ — 2-*адический показатель* натурального числа m, т. е. такое целое число $l \geqslant 0$, что m делится на 2^l, но не делится на 2^{l+1}.

Этюд V. Многочлены Чебышёва и целые алгебраические числа

При любом $n = 1, 2, \ldots$ двучлен $z^n + 1/z^n$ можно представить в виде многочлена $p_n(y)$ от $y = z + 1/z$, при этом $p_n(y)$ нормирован и имеет целые коэффициенты. В самом деле, имеем

$$p_0(y) = 2, \quad p_1(y) = y, \quad p_{n+1}(y) = y p_n(y) - p_{n-1}(y).$$

Если $z = \cos\varphi + \sqrt{-1}\sin\varphi$, то $y = 2\cos\varphi$ и из *формулы Муавра* получим

$$p_n(y) = z^n + 1/z^n = 2\cos(n\varphi) = 2T_n(\cos\varphi) = 2T_n(y/2),$$

где $T_n(x)$ — *многочлен Чебышёва* 1-го рода.

Теперь запишем равенство $(*)$ в виде $z^n = 1$, где

$$z = \frac{3 + 4\sqrt{-1}}{5}.$$

Тогда $y = 6/5$, а также

$$p_n(y) = p_n(6/5) = z^n + 1/z^n = 2.$$

Итак, $6/5$ оказывается рациональным, но не целым корнем нормированного многочлена с целыми коэффициентами $p_n(y) - 2$, что невозможно.

Это рассуждение — ещё один способ доказательства теоремы из этюда III. Его можно сделать совсем кратким, если заметить, что число

$$y = 2\cos\varphi = \zeta_n^a + \zeta_n^{-a} = \zeta_n^a + \zeta_n^{n-a}$$

является *целым алгебраическим* (поскольку таково ζ_n, а целые алгебраические числа образуют кольцо). Но в таком случае условие $y \in \mathbb{Q}$ равносильно условию $y \in \mathbb{Z}$, а значит, $\cos\varphi \in \{0, \pm 1/2, \pm 1\}$.

Этюд VI. Динамические системы

Рассмотрим итерационный процесс, заданный формулой

$$x_{k+1} = 2x_k^2 - 1 \quad (k = 0, 1, 2, \ldots).$$

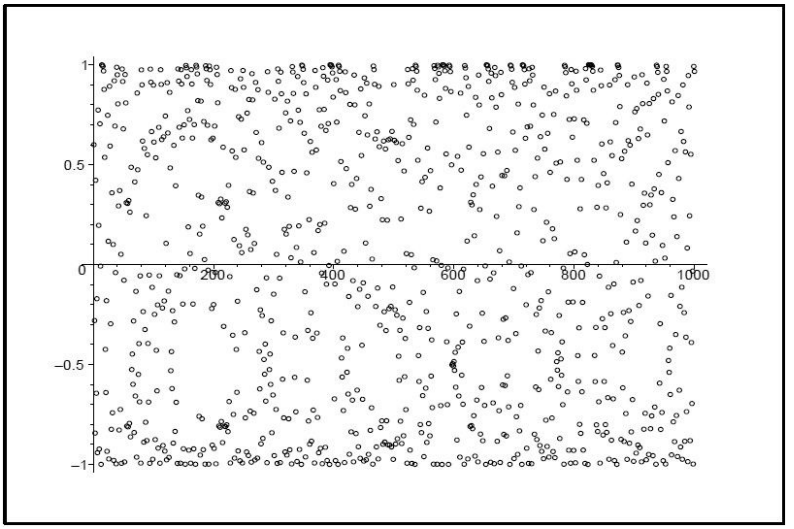

Рис. 1. Первая тысяча членов последовательности $\{x_k\}$ *при* $x_0 = 3/5$

Введём обозначение: $I_{\mathbb{Q}} = \{r \in \mathbb{Q} : -1 \leqslant r \leqslant 1\}$.

Предложение. *При* $x_0 \in I_{\mathbb{Q}} \setminus \{0, \pm 1/2, \pm 1\}$ *все члены последовательности* $\{x_k\}$ *попарно различны.*

В описанной ситуации поведение последовательности $\{x_k\}$ выглядит хаотическим (см. рис. 1). Для доказательства предложения нам понадобится

Лемма. *Пусть* $f(x) = 2x^2 - 1$. *Для* $k = 1, 2, \ldots$ *положим*

$$f_k(x) = \underbrace{f(\ldots(f}_{k}(x)\ldots).$$

Тогда рациональные корни уравнения $f_k(x) = x$ *суть* 1 *и* $-1/2$.

Доказательство. При $k > 1$ справедливо представление

$$f_k(x) = 2^{2^k-1}x^{2^k} + \ldots + 1.$$

Поэтому любой рациональный корень x_0 многочлена $f_k(x) - x$ должен иметь вид $\pm 1/2^l$, где l — некоторое целое неотрицательное число. Имеем

$$f_k(x_0) = f_2(y_0) = 8y_0^4 - 8y_0^2 + 1 = x_0,$$

где $y_0 = f_{k-2}(x_0)$ — рациональное число (считаем $f_0(x) = x$). Но, как нетрудно убедиться, уравнение вида

$$8y^4 - 8y^2 + 1 = \pm 1/2^l$$

имеет рациональные корни только тогда, когда его правая часть равна 1 или $-1/2$.

Переходя к доказательству предложения, заметим, что если $x_{N+k} = x_N$, то $f_k(x_N) = x_N$ и по лемме $x_N \in \{0, \pm 1/2, \pm 1\}$. Но в таком случае, как нетрудно проверить, $x_{N-1} \in \{0, \pm 1/2, \pm 1\}$ и т. д. — противоречие.

Расскажем ещё о двух других способах доказательства предложения, в каждом из которых эксплуатируется представление рациональных чисел x_k в виде несократимых дробей:

$$x_k = \frac{a_k}{b_k}\,, \quad \text{НОД}\,(a_k, b_k) = 1.$$

I. Первый способ совсем короткий. Имеем

$$x_{k+1} = \frac{a_{k+1}}{b_{k+1}} = \frac{2a_k^2 - b_k^2}{b_k^2}\,. \qquad (\ddagger)$$

Так как $d_k = \text{НОД}\,(2a_k^2 - b_k^2, b_k^2) \in \{1, 2\}$, то

$$b_{k+1} = \frac{b_k^2}{d_k} \geqslant \frac{b_k^2}{2} > b_k\,,$$

как только $b_k > 2$. Осталось заметить, что $b_0 > 2$.

Подобные элементарные рассуждения составляют основу интересного сюжета о том, как из одной известной рациональной точки на данной *эллиптической кривой* можно изготовить бесконечную последовательность рациональных точек этой кривой.

Приведём один пример. Пусть S — положительное рациональное число, E_S — эллиптическая кривая, определяемая уравнением

$$Sy^2 = x^3 - x.$$

Теорема. *Если кривая E_S содержит хотя бы одну рациональную точку $P_0 = (x_0, y_0)$ с $y_0 \neq 0$, то таких точек на ней бесконечно много.*

Доказательство. Проведём в точке P_0 касательную к E_S. Она пересечёт E_S в некоторой другой точке P^*. Обозначим через P_1 точку, симметричную P^* относительно прямой $y = 0$. Говорят, что точка P_1 получена *удвоением* точки P_0 (такая терминология связана с некоторой естественной *операцией сложения* точек эллиптической кривой).

Пусть $P_1 = (x_1, y_1)$. Простые, но несколько громоздкие вычисления дают

$$x_1 = \frac{(x_0^2 + 1)^2}{4x_0(x_0^2 - 1)}\,, \quad y_1 = \frac{x_0^6 - 5x_0^4 - 5x_0^2 + 1}{8Sx_0y_0(x_0^2 - 1)}\,.$$

Поскольку $y_1 \neq 0$, ибо многочлен

$$x^6 - 5x^4 - 5x^2 + 1 = (x^2 + 1)(x^2 - 2x - 1)(x^2 + 2x - 1)$$

не имеет рациональных корней, из точки P_1 удвоением можно получить точку $P_2 = (x_2, y_2)$, из точки P_2 аналогичным образом получить точку $P_3 = (x_3, y_3)$ и т. д. Покажем, что все точки P_k будут попарно различны.

Пусть $x_k = a_k/b_k$ — запись в виде несократимой дроби. Тогда, как легко видеть,

$$b_1 = \frac{4|a_0(a_0^2 - b_0^2)|}{d_0}\, b_0, \quad d_0 = \text{НОД}\,((a_0^2 + b_0^2)^2, 4a_0b_0(a_0^2 - b_0^2)).$$

Нетрудно проверить, что $d_0 \in \{1, 4\}$. Поскольку $|a_0(a_0^2 - b_0^2)| > 1$, имеем $b_1 > b_0$. Аналогично $b_2 > b_1$ и т. д. Таким образом, знаменатели b_k рациональных чисел x_k монотонно возрастают, а значит, все x_k и тем более P_k попарно различны.

Кривая E_S примечательна тем, что её рациональным точкам, отличным от $(0, 0)$ и $(\pm 1, 0)$, соответствуют прямоугольные треугольники площади S с рациональными длинами сторон. Доказанную теорему можно сформулировать так: *если существует хотя бы один такой треугольник, то их существует бесконечно много* (утверждение, которое впервые высказал П. Ферма). Однако вопрос существования для данного S хотя бы одного треугольника с требуемым свойством оказывается весьма нетривиальным (подробнее об этом см., например, в брошюре [5]).

II. Второй способ основан на следующем соображении. Пусть p — простой делитель b_0. Тогда для $k = 0, 1, \ldots$ имеем

$$\nu_p(b_k) = \begin{cases} 2^k \nu_p(b_0), & \text{если } p > 2, \\ 2^k(\nu_2(b_0) - 1) + 1, & \text{если } p = 2, \end{cases}$$

где $\nu_p(m)$ — *p-адический показатель*, определяемый аналогично 2-адическому показателю (см. этюд IV). Доказательство проводится по индукции с использованием рекуррентного соотношения (‡). В частном случае это рассуждение можно найти, например, в опубликованном решении следующей фольклорной задачи: *доказать иррациональность градусной меры угла φ при условии* $\cos\varphi = 1/3$ (см. [3]).

Теперь можно дать ещё одно доказательство теоремы из этюда III.

Пусть $x_0 = \cos\varphi \in I_{\mathbb{Q}} \setminus \{0, \pm 1/2, \pm 1\}$. Тогда

$$x_k = \cos\,(2^k\varphi), \quad k = 0, 1, 2, \ldots,$$

и по предложению в последовательности $\{x_k\}$ не должно быть совпадений. Но так не бывает, если $\varphi/\pi \in \mathbb{Q}$.

Некоторые элементарные свойства последовательности $\{x_k\}$ рассмотрены в статье [2].

Этюд VII. Трансцендентные числа и мера иррациональности

Утверждение об иррациональности числа

$$\beta_0 = \frac{\operatorname{arctg}(4/3)}{\pi}$$

означает, что это число не может быть корнем многочлена 1-й степени с целыми коэффициентами. Но на самом деле оно не является корнем вообще никакого многочлена с целыми коэффициентами. Иными словами, это число — *трансцендентное*. Этот факт вытекает из следующей теоремы.

Теорема Гельфонда (1934). Если α, β — алгебраические числа, причём $\alpha \notin \{0, 1\}$, $\beta \notin \mathbb{Q}$, то число α^β трансцендентно.

Доказательство этой весьма нетривиальной теоремы, решающей *7-ю проблему Гильберта*, читатель может найти в книге [7]. В нашем случае имеем

$$(-1)^{\beta_0} = \exp(\beta_0 \log(-1)) = \exp(\beta_0 \pi \sqrt{-1}) = \frac{3 + 4\sqrt{-1}}{5},$$

а последнее число, очевидно, алгебраическое.

Иррациональное число β_0 является вещественным, а для таких чисел представляет интерес вопрос о том, насколько хорошо они приближаются рациональными дробями.

Мерой иррациональности $\mu(\beta)$ числа $\beta \in \mathbb{R} \setminus \mathbb{Q}$ называют нижнюю грань таких чисел $\mu > 0$, что неравенство

$$\left|\beta - \frac{p}{q}\right| < \frac{1}{q^\mu} \qquad (\S)$$

имеет лишь конечное множество решений $(p, q) \in \mathbb{Z}^2$. Если чисел μ с указанным свойством нет, то полагают $\mu(\beta) = \infty$ (такие числа β существуют и называются *числами Лиувилля*). Опираясь на *принцип Дирихле*, легко показать, что при $\mu = 2$ неравенство (§) имеет бесконечно много решений, поэтому всегда $\mu(\beta) \geqslant 2$.

Теорема Рота (1955). Если $\beta \in \mathbb{R} \setminus \mathbb{Q}$ — алгебраическое число, то для любого $\mu > 2$ неравенству (§) удовлетворяет конечное множество пар $(p, q) \in \mathbb{Z}^2$.

Итак, $\mu(\beta) = 2$ для любого алгебраического числа $\beta \in \mathbb{R} \setminus \mathbb{Q}$. Доказательство теоремы Рота также очень сложно и к тому же неэффективно, поскольку не позволяет указать явной оценки $q \leqslant q_0 = q_0(\beta, \mu)$ для возможных решений (p, q) неравенства (§) (см., например, [4]).

Вместе с тем для любой вещественной квадратичной иррациональности β такую оценку выписать вполне можно. Это связано с тем, что можно

предъявить в явном виде такую константу $c = c(\beta) > 0$, что неравенство

$$\left|\beta - \frac{p}{q}\right| \geqslant \frac{c(\beta)}{q^2}$$

будет верно для любых $(p, q) \in \mathbb{Z}^2$. Так, например, для $\beta = \sqrt{2}$ годится $c = 1/4$.

Для меры иррациональности $\mu(\beta)$ трансцендентных чисел $\beta \in \mathbb{R}$, не являющихся числами Лиувилля, обычно известны только верхние оценки (некоторые конкретные результаты читатель сможет найти по ссылке [10]).

Про число β_0 известно, что оно не число Лиувилля, при этом можно указать явную оценку $\mu(\beta_0) \leqslant a_0$ его меры иррациональности. Такого рода факты вытекают из степенной оценки для *линейной формы от логарифмов алгебраических чисел*, которую впервые получил Фельдман в 1968 году (см. [7]).

В частности, для числа

$$\beta_0 = \frac{\log(\alpha_1)}{\log(\alpha_2)}, \quad \alpha_1 = \frac{3 + 4\sqrt{-1}}{5}, \quad \alpha_2 = -1$$

речь идёт о линейной форме $\Lambda = q_1 \log(\alpha_1) + q_2 \log(\alpha_2)$, для которой справедлива оценка типа

$$|\Lambda| > L^{-b_0},$$

где $L = \max\{|q_1|, |q_2|, 2\}$, при этом константа b_0, зависящая только от α_1, α_2, а также от выбранных значений $\log(\alpha_1)$, $\log(\alpha_2)$, может быть явно вычислена. Для получения этого результата Фельдман усовершенствовал метод оценки линейной формы от логарифмов алгебраических чисел, предложенный в 1966 году Бейкером (см. [8]).

Однако константа b_0 (и, следовательно, константа a_0) оказывается очень большой, поэтому для практических приложений выгоднее применять оценку типа

$$|\Lambda| > \exp(-c_0 \log^2 L),$$

худшую по порядку, но с относительно небольшой константой c_0, также зависящей только от α_1, α_2, $\log(\alpha_1)$, $\log(\alpha_2)$. Пример такой оценки читатель сможет найти в работе [9].

Список литературы

[1] Винберг Э. Б. *Курс алгебры*. М.: Факториал Пресс. 2001.

[2] Иванов О.А. *Современная математика в школьных задачах* // Соросовский образовательный журнал. № 6. 2000. С. 110–116.

[3] Канель-Белов А. Я. *Решение задачи* 12.1 // Математическое просвещение. Сер. 3. Вып. 15. 2011. С. 236–237.

[4] Касселс Дж. *Введение в теорию диофантовых приближений*. М.: Мир. 1961.

[5] Острик В. В., Цфасман М. А. *Алгебраическая геометрия и теория чисел*: *рациональные и эллиптические кривые*. М.: МЦНМО. 2001.

[6] Прасолов В. В. *Многочлены*. М.: МЦНМО. 2001.

[7] Фельдман Н.И. *Седьмая проблема Гильберта*. М.: МГУ. 1982.

[8] Baker A. *Transcendental Number Theory*. Cambridge: Cambridge Univ. Press. 1975.

[9] Laurent M., Mignotte M., Nesterenko Y. *Formes linéaires en deux logarithmes et déterminants d'interpolation* // J. Number Theory. Vol. 55. 1995. P. 285–321.

[10] `http://mathworld.wolfram.com/IrrationalityMeasure.html`

Н. Н. Осипов
Email: `nnosipov@rambler.ru`