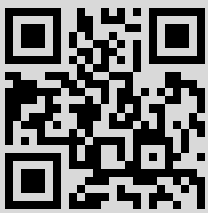
П. Ю. Козлов, А. Б. Скопенков, В поисках утраченной алгебры: в направлении Гаусса (подборка задач), *Матем. просв.*, 2008, выпуск 12, 127–143



В поисках утраченной алгебры: в направлении Гаусса* (подборка задач)

П. Ю. Козлов А. Б. Скопенков†

Listeners are prepared to accept unstated (but hinted) generalizations much more than they are able... to decode a precisely stated abstraction and to re-invent the special cases that motivated it in the first place.

P. Halmos, How to talk mathematics

Введение

Теорема Гаусса. [1)] *Калькулятор (вычисляющий числа с абсолютной точностью) имеет кнопки*

$$1, \quad +, \quad -, \quad \times, \quad : \quad \text{и} \quad \sqrt{}$$

(и неограниченную память). На этом калькуляторе можно вычислить число $\cos\frac{2\pi}{n}$ *тогда и только тогда, когда* $n = 2^\alpha p_1 \cdot \ldots \cdot p_l$, *где* $p_1, \ldots, p_l$ — *различные простые числа вида* $2^{2^s}+1$.

*Полный обновляемый текст находится по адресу: www.mccme.ru/circles/oim/materials/construc.pdf

†Частично поддержан Российским Фондом Фундаментальных Исследований, Гранты номер 05-01-00993, 07-01-00648a и 06-01-72551-NCNILa, Грантами Президента РФ НШ-4578.2006.1 и МД-4729.2007.1, а также стипендией П. Делиня, основанной на его Премии Бальзана 2004 года.

1)Переформулировка теоремы Гаусса в терминах построимости циркулем и линейкой правильных многоугольников приводится ниже (см. отступление) и не используется в остальном тексте. История этой знаменитой теоремы приводится в [6]. Строго говоря, теорема Гаусса не дает настоящего решения проблемы построимости правильных многоугольников, поскольку неизвестно, какие числа вида $2^{2^s}+1$ являются простыми. Однако теорема Гаусса дает, например, полиномиальный алгоритм выяснения построимости правильного n-угольника (n задано десятичной записью).

В этой заметке предлагается набросок *элементарного доказательства приведенной теоремы*. Оно не использует терминов «группа Галуа» (даже понятия «группа») и «поле» (доказательство невозможности использует квадратичные расширения только *множества рациональных чисел*). Несмотря на отсутствие этих *терминов*, *идеи* приводимых доказательств являются *отправными* для теории Галуа,[2)] которая (вместе с теорией групп) появилась в опыте *группировки* корней многочлена, с помощью которой их можно выразить через радикалы.[3)]

Нам кажется, что именно с *новых идей*, а не с *немотивированных определений*, полезно *начинать* изучение любой теории. Как правило, такие идеи наиболее ярко выражаются доказательствами, подобными приведенным здесь. Более подробно это обсуждается в философском отступлении, которое содержится в полном тексте заметки (см. примечание к заглавию статьи).

Приводимые доказательства *известны в математическом фольклоре*, однако авторам не удалось найти их в явном виде в литературе (кроме второго доказательства невозможности в теореме Гаусса [3]).

Элементарное доказательство *возможности* для $n = 17$ приводится в [6,9,13,15,16]. Для общего случая оно намечено в [4,6], где ясности доказательства немного мешает построение общей теории вместо доказательства конкретного результата.[4)]

Невозможность в теореме Гаусса не доказана явно в [4]. Однако первое доказательство невозможности в настоящей заметке (серия D) основано на идеях из [4] и поэтому его можно принять за рассуждение Гаусса. Элементарное изложение идеи неэлементарного доказательства невозможности приводится в [8]. Доказательства невозможности в теореме Гаусса являются алгебраическим выражением этой идеи «разбиения решений на пары». Простое доказательство *невозможности* из [3, гл. 5] намечено в серии E (отличие приводимого изложения в том, что необходимые понятия не вводятся немотивированно впрок, а естественно появляются в процессе размышления над проблемой). Еще одно доказательство невозможности, возникшее в ходе обсуждений с А. Я. Канелем-Беловым, приводится в приложении в полном тексте. По сути все доказательства очень близки.

Перед доказательствами невозможности в теореме Гаусса некоторые их идеи демонстрируются по одной и на простейших примерах (серия C). Эти

[2)] Конечно, *отправные* идеи любой теории не исчерпывают *всех* ее идей.

[3)] Вульгарно, но ярко, эти идеи можно выразить девизом *группируй и властвуй* или *объединяй и властвуй*.

[4)] Авторы лишь потому позволяют себе данное замечание по поводу изложения в [4], что преклоняются перед величием Гаусса, начавшего путь в науку с труднейших разделов чистой математики, а затем много занимавшегося приложениями и превратившего один из разделов географии в раздел математики.

примеры дают решение классических задач древности об удвоении куба и трисекции угла, ждавших своего решения два тысячелетия. Приводимое изложение основано на [10, 12]; оно немного более коротко и ясно за счет того, что не используется термин «поле». Ср. [5, §4.19].

Приводимые серии задач (в частности, доказательства возможности и невозможности) независимы друг от друга. В доказательствах используется определение построимости из второго отступления и эквивалентность теоремы Гаусса аналогичной теореме для *комплексного* калькулятора (задача А4).

Доказательства представлены в виде циклов задач (большинство задач снабжены указаниями или решениями). Решение задач потребует от многих читателей усилий (впрочем, опытный математик, не знакомый с теорией Галуа, с легкостью восстановит решения по приведенным указаниям или даже без них). Однако эти усилия будут сполна оправданы тем, что вслед за великими математиками в процессе изучения интересной проблемы читатель познакомится с некоторыми основными идеями алгебры. Надеюсь, это поможет читателю совершить собственные настолько же полезные открытия (не обязательно в математике)!

Общее замечание к формулировкам задач: если условие задачи является утверждением, то в задаче требуется это утверждение доказать.

Предварительная версия этой заметки представлялась А. Беловым-Канелем, П. Дергачом и авторами в виде цикла задач на Летней Конференции Турнира Городов в августе 2007 г. Сокращенный английский перевод (выполненный П. Дергачом и А. Скопенковым) доступен в интернете[5)].

В этой заметке использованы материалы занятий со школьниками по элементарному доказательству теоремы Гаусса, которые вели А. С. Голованов, А. И. Ефимов и второй автор. Аналогичные занятия вели А. Я. Белов-Канель, И. И. Богданов, Г. Р. Челноков и, возможно, другие. Мы благодарим их всех, а также Э. Б. Винберга, М. Н. Вялого, П. А. Дергача, А. А. Казначеева и В. В. Прасолова за полезные обсуждения.

Отступление: связь с построениями циркулем и линейкой

А1. Используя отрезки длины a, b и c, можно построить циркулем и линейкой отрезки длины $a+b$, $a-b$, ab/c, $\sqrt{ab}$.

Вещественное число называется *построимым*, если его можно получить на нашем калькуляторе (т. е. получить из 1 при помощи сложения,

[5)] См. `www.mccme.ru/circles/oim/materials/constreng.pdf`

вычитания, умножения, деления и извлечения квадратного корня из положительного числа). Например, числа

$$1+\sqrt{2},\quad \sqrt[4]{2}=\sqrt{\sqrt{2}},\quad \sqrt{2\sqrt{3}},\quad \sqrt{2}+\sqrt{3},\quad \sqrt{1+\sqrt{2}},\quad \frac{1}{1+\sqrt{2}}\quad \text{и}\quad \cos 3^\circ$$

построимы. Про последние два числа это не совсем очевидно.

А2. Любое построимое число можно построить циркулем и линейкой (далее слова «циркулем и линейкой» опускаются).

Этот простой (вытекающий из А1) результат был известен еще древним грекам. Он показывает, что из *выразимости* числа $\cos(2\pi/n)$ в теореме Гаусса вытекает *построимость* правильного n-угольника.

А3. *Основная теорема теории геометрических построений.* Обратное тоже верно: если отрезок длины a можно построить циркулем и линейкой, то число a построимо.

Этот несложный результат [9, 14] (доказанный лишь в 19-м веке) показывает, что из *невыразимости* в теореме Гаусса вытекает *непостроимость* соответствующих n-угольников.

Для его доказательства рассмотрите все возможные случаи появления новых объектов (точек, прямых, окружностей). Покажите, что координаты всех построенных точек и коэффициенты уравнений всех проведённых прямых и окружностей являются построимыми. См. детали в [9, 10, 12, 14].

Определение *комплексно построимого* комплексного числа аналогично определению построимого вещественного числа, только квадратные корни извлекаются из произвольных уже выраженных чисел и комплексно построимыми считаются оба значения квадратного корня.

А4. Комплексное число комплексно построимо тогда и только тогда, когда его вещественная и мнимая части (вещественно) построимы.

Указание: Если $\sqrt{a+bi}=u+vi$, то u, v выражаются через a и b с помощью арифметических операций и квадратных радикалов.

По поводу невыразимости вещественных чисел через вещественные (положительные) значения корней произвольной целой степени (из положительных чисел) см. [2].

А5. Если правильный mn-угольник построим, то и правильный m-угольник построим.

А6. Правильные 3-угольник и 5-угольник построимы.

А7. Правильный 120-угольник построим. Или, эквивалентно, угол 3° построим.

Указание: Если не получается, то см. следующие задачи.

А8. Если правильный n-угольник построим, то и правильный $2n$-угольник построим.

Указание: Получается делением угла пополам или применением формулы половинного угла.

А9. Пусть правильные m- и n-угольники построимы, причем числа m и n взаимно просты. Тогда правильный mn-угольник построим.

Указание: Так как m и n взаимно просты, то существуют целые a, b такие, что $am + bn = 1$.

Доказательство возможности в теореме Гаусса

Нетрудно доказать возможность в теореме Гаусса для $n \leqslant 16$.

Доказательство возможности в теореме Гаусса для $n = 5$. Видимо, приводимый способ сложнее придуманного Вами. Зато из него будет видно, что делать в общем случае. Достаточно выразить число $\varepsilon = \cos\frac{2\pi}{5} + i\sin\frac{2\pi}{5}$. Сразу это сделать трудно, поэтому сначала построим некоторые многочлены от ε. Мы знаем, что $\varepsilon + \varepsilon^2 + \varepsilon^3 + \varepsilon^4 = -1$. Поэтому

$$(\varepsilon + \varepsilon^4)(\varepsilon^2 + \varepsilon^3) = \varepsilon + \varepsilon^2 + \varepsilon^3 + \varepsilon^4 = -1.$$

Обозначим

$$A_0 := \varepsilon + \varepsilon^4 \text{ и } A_1 := \varepsilon^2 + \varepsilon^3.$$

Тогда по теореме Виета числа A_0 и A_1 являются корнями уравнения $t^2 + t - 1 = 0$. Поэтому можно выразить A_0 (и A_1). Поскольку $\varepsilon \cdot \varepsilon^4 = 1$, то по теореме Виета числа ε и ε^4 являются корнями уравнения $t^2 - A_0 t + 1 = 0$. Поэтому можно выразить ε (и ε^4).

В1. Если число $2^m + 1$ простое, то m — степень двойки.

Идея доказательства построимости в теореме Гаусса. Достаточно выразить число $\varepsilon = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$ для простого $n = 2^m + 1$ (тогда m обязано быть степенью двойки).

Сначала хорошо бы разбить сумму

$$\varepsilon + \varepsilon^2 + \cdots + \varepsilon^{n-1} = -1$$

на два слагаемых A_0 и A_1, *произведение* которых построимо (иными словами, *сгруппировать* хитрым образом корни уравнения $1 + \varepsilon + \varepsilon^2 + \cdots + \varepsilon^{n-1} = 0$). Тогда A_0 и A_1 построимы по теореме Виета. Затем хорошо бы разбить сумму A_0 на два слагаемых $A_0 = A_{00} + A_{01}$, произведение которых построимо, и аналогично разбить $A_1 = A_{10} + A_{11}$. И так далее, пока не построим $A_{0\ldots0} = \varepsilon$.

Однако придумать нужные группировки корней уравнения $1+\varepsilon+\varepsilon^2+\dots+\varepsilon^{n-1}=0$ совершенно нетривиально и возможно не для всех n. Как это можно придумать, описано в [7]. Здесь приведем лишь ответ, который очень прост.

Теорема о первообразном корне. Для любого простого p существует число g, для которого остатки от деления на p чисел $g^1, g^2, g^3, \dots, g^{p-1}=1$ различны.

Как строить нужные группировки, видно из задач B3a, B4a и B4c ниже.

B2. *Доказательство теоремы о первообразном корне.* Пусть p простое и a не делится на p.

(a) $p-1$ делится на наименьшее $k>0$, для которого $a^k \equiv 1 \pmod p$.

Указание: используйте малую теорему Ферма.

(b) Для любых целых n и a сравнение $x^n \equiv a \pmod p$ имеет не более n решений.

(c) Если $p-1$ делится на d, то сравнение $x^d \equiv 1 \pmod p$ имеет ровно d решений.

(d) Докажите теорему о первообразном корне для $p=2^m+1$. (Только этот частный случай нужен для теоремы Гаусса.)

(e)* Докажите теорему о первообразном корне для $p=2^m\cdot 3^n+1$.

(f)* Докажите теорему о первообразном корне для *произвольного* простого p.

(g)* Верно ли, что число 3 является первообразным корнем по модулю любого простого числа вида $p=2^m+1$?

Начиная с этого момента $p=2^m+1\geqslant 5$ — простое число и g — (любой) первообразный корень по модулю p.

B3. (a) Положим

$$A_0 := \varepsilon^{g^2}+\varepsilon^{g^4}+\varepsilon^{g^6}+\dots+\varepsilon^{g^{2^m}} \quad \text{и} \quad A_1 := \varepsilon^{g^1}+\varepsilon^{g^3}+\varepsilon^{g^5}+\dots+\varepsilon^{g^{2^m-1}}.$$

Докажите, что $A_0A_1=-\dfrac{p-1}{4}$. (Следующие задачи являются подсказками.)

(b) $g^k+g^l \equiv 0 \pmod p$ тогда и только тогда, когда $k-l \equiv \dfrac{p-1}{2} \pmod{p-1}$.

(c) $A_0A_1=\sum\limits_{s=1}^{2^m}\varepsilon^s\alpha(s)$, где $\alpha(s)$ равно числу решений (k,l) (в вычетах по модулю $p-1$) сравнения $g^{2k}+g^{2l+1}\equiv s \pmod p$.

(d) $\alpha(s)=\alpha(gs)$.

(e) $\alpha(s)$ не зависит от $s=1,\dots,2^m$.

B4. (a) Положим

$$A_{00} := \varepsilon^{g^4} + \varepsilon^{g^8} + \varepsilon^{g^{12}} + \cdots + \varepsilon^{g^{2^m}} \quad \text{и} \quad A_{01} := \varepsilon^{g^2} + \varepsilon^{g^6} + \varepsilon^{g^{10}} + \cdots + \varepsilon^{g^{2^m-2}}.$$

Докажите, что $A_{00}A_{01} = sA_0 + tA_1$ для некоторых целых чисел s и t $(s + t = \dfrac{p-1}{8})$. (Следующая задача является подсказкой.)

(b) Сравнение $g^{4k} + g^{4l+2} \equiv 1 \pmod p$ имеет столько же решений (k, l) (в вычетах по модулю $p-1$), сколько сравнение $g^{4k} + g^{4l+2} \equiv g^2 \pmod p$.

(c) Положим

$$A_{11} := \varepsilon^{g^1} + \varepsilon^{g^5} + \varepsilon^{g^9} + \cdots + \varepsilon^{g^{2^m-3}} \quad \text{и} \quad A_{10} := \varepsilon^{g^3} + \varepsilon^{g^7} + \varepsilon^{g^{11}} + \cdots + \varepsilon^{g^{2^m-1}}.$$

Докажите, что $A_{10}A_{11} = uA_0 + vA_1$ для некоторых целых чисел u и v $(u + v = \dfrac{p-1}{8})$.

(d) Закончите доказательство возможности в теореме Гаусса.

B5. Найдите явно выражение через квадратные радикалы числа

(a) A_0 из задачи B3a. (b) $\cos\dfrac{2\pi}{17}$. (c)* $\cos\dfrac{2\pi}{257}$. (d)* $\cos\dfrac{2\pi}{65537}$.

При помощи приведенного метода и компьютера эту задачу можно решить быстро, несмотря на следующую историю [11]. «Один слишком навязчивый аспирант довел своего руководителя до того, что тот сказал ему: „Идите и разработайте построение правильного многоугольника с 65 537 сторонами“. Аспирант удалился, чтобы вернуться через 20 лет с соответствующим построением (которое хранится в архивах в Геттингене).»

Замечание. Построимость можно доказывать по тому же плану без использования комплексных чисел. Приведем указание для случая правильного 17-угольника. Положим $a_k = \cos(2\pi k/17)$. Тогда $a_k = a_{17-k}$, $2a_ka_l = a_{k+l} + a_{k-l}$ и $a_1 + a_2 + a_3 + \cdots + a_8 = -1/2$. Сначала выразите $a_1 + a_2 + a_4 + a_8$ и $a_3 + a_5 + a_6 + a_7$. Затем выразите $a_1 + a_4$, $a_2 + a_8$, $a_3 + a_5$ и $a_6 + a_7$. Наконец, выразите a_1.

Указания и решения к доказательству возможности

Указание к B1. Если n нечетно, то $2^{kn} + 1$ делится на $2^k + 1$.

Указание к B2b. Докажем более общее утверждение: *многочлен степени n не может иметь более n корней в множестве $\mathbb{Z}/p\mathbb{Z}$ вычетов по модулю p (в котором имеются операции сложения и умножения по модулю p)*. Здесь многочленом называется бесконечный упорядоченный набор $(a_0, \ldots, a_n, \ldots)$ вычетов по модулю p, в котором лишь конечное число элементов отлично от нуля. Обычно многочлен записывается в виде $a_0 + {+}a_1x{+}\cdots{+}a_kx^k$ (если $a_{k+1} = a_{k+2} = \cdots = 0$). Эта запись дает отображение

$\mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$. Будьте осторожны: разным многочленам может соответствовать одно и то же отображение. *Корнем* многочлена $a_0+a_1x+\cdots+a_kx^k$ называется такой вычет x_0 по модулю p, что $a_0 + a_1x_0 + \cdots + a_kx_0^k = 0$.

Пусть многочлен $P(x)$ степени n имеет различные корни $x_1, \ldots, x_n$, x_{n+1} в множестве вычетов $\mathbb{Z}/p\mathbb{Z}$. Представьте его в виде

$$P(x) = b_n(x-x_1)\cdot\ldots\cdot(x-x_n)+b_{n-1}(x-x_1)\cdot\ldots\cdot(x-x_{n-1})+\cdots+b_1(x-x_1)+b_0$$

(«*интерполяция Ньютона*»). Последовательно подставляя в сравнение $P(x) \equiv 0 \pmod p$ вычеты $x_1, \ldots, x_n, x_{n+1}$, получим $b_0 \equiv b_1 \equiv \cdots \equiv b_{n-1} \equiv \equiv b_n \equiv 0 \pmod p$.

То же самое решение можно записать и так. Пусть P — многочлен. Тогда $P - P(a) = (x - a)Q$ для некоторого многочлена Q степени меньше $\deg P$. Поэтому если $P(a) = 0$, то $P = (x-a)Q$ для некоторого многочлена Q степени меньше $\deg P$. Теперь требуемое в задаче утверждение доказывается индукцией по степени многочлена P с использованием простоты числа p.

Первое указание к B2c. Заметьте, что многочлен $x^{p-1} - 1$ имеет ровно $p-1$ корень в множестве вычетов $\mathbb{Z}/p\mathbb{Z}$ и делится на $x^d - 1$. Докажите, что если многочлен степени a имеет ровно a корней и делится на многочлен степени b, то этот многочлен степени b имеет ровно b корней.

Второе указание к B2c. Если $p = kd$, то для любого a сравнение $y^k \equiv \equiv a \pmod p$ имеет не более k решений.

Указание к B2d. Если первообразного корня нет, то по 2a сравнение $x^{2^{m-1}} \equiv 1 \pmod p$ имеет $p - 1 = 2^m > 2^{m-1}$ решений.

Указание к B2e,f. Аналогично B2d.

Замечание к B2f. Из существования первообразного корня легко вывести, что для $p-1 = p_1^{a_1} \cdot \ldots \cdot p_k^{a_k}$ количество первообразных корней равно $(p-1)(1-\frac{1}{p_1}) \cdot \ldots \cdot (1-\frac{1}{p_k}) = \varphi(p-1)$.

Указание к B3c. Раскройте скобки и сгруппируйте равные слагаемые.

Указание к B3d. Если (a, b) — решение сравнения $g^{2k} + g^{2l+1} \equiv s \pmod p$, то $(b + 1, a)$ — решение сравнения $g^{2k} + g^{2l+1} \equiv gs \pmod p$. Если (a, b) — решение сравнения $g^{2k} + g^{2l+1} \equiv gs \pmod p$, то $(b, a - 1)$ — решение сравнения $g^{2k} + g^{2l+1} \equiv s \pmod p$.

Указание к B5c. (Написано с использованием решения задачи 4d из `http://www.turgor.ru/lktg/2007/5/index.php`, представленного Е. Лукьянцом, учеником ФМЛ 239 г. Санкт-Петербурга, и В. Соколовым, учеником гимназии №261 г. Санкт-Петербурга.) Положим

$$\overline{i_0 \ldots i_x} := i_0 2^0 + \cdots + i_x 2^x \quad \text{и} \quad A_{i_0 \ldots i_x} := \sum_{s=1}^{2^{m-x-1}} \varepsilon^{g^{-\overline{i_0 \ldots i_x}} + s 2^{x+1}}.$$

Тогда $A_{i_0\ldots i_x 0} + A_{i_0\ldots i_x 1} = A_{i_0\ldots i_x}$. При $x < m$ имеем

$$A_{i_0\ldots i_x 0} A_{i_0\ldots i_x 1} = \sum_{s=0}^{2^m} \alpha(s)\varepsilon^s = \sum_{(j_0\ldots j_x)} b_{j_0\ldots j_x} A_{j_0\ldots j_x} \quad \text{для некоторых } b_{j_0\ldots j_x} \in \mathbb{Z}.$$

Здесь в первом равенстве $\alpha(s)$ равно числу решений (k, l) (в вычетах по модулю $p-1$) сравнения

$$g^{-\overline{i_0\ldots i_x}+k2^{x+1}} + g^{-\overline{i_0\ldots i_x}+l2^{x+1}+2^x} \equiv s \pmod p.$$

По B3b $\alpha(0) = 0$ при $x < m$. Аналогично B3c $\alpha(s) = \alpha(sg^{2^x})$. Отсюда вытекает второе равенство.

Подготовка к доказательству невозможности в теореме Гаусса

C1. Не существует рациональных чисел a, b, c, d, для которых $\sqrt[3]{2} =$
(a) $a + \sqrt{b}$; (b) $a - \sqrt{b}$; (c) $\dfrac{1}{a+\sqrt{b}}$; (d) $a + \sqrt{b} + \sqrt{c}$; (e) $a + \sqrt{b} + \sqrt{c} + \sqrt{bc}$; (f) $a + \sqrt{b + \sqrt{c}}$; (g) $a + \sqrt{b} + \sqrt{c} + \sqrt{d}$.

Указание к C1c. Домножьте на сопряженное.

C2. Пусть нажатие кнопок «1» и четырех арифметических действий на калькуляторе из теоремы Гаусса бесплатны, а за извлечение корня нужно платить копейку.

(a) *Число A можно получить за r копеек тогда и только тогда, когда существуют такие $a_1, \ldots, a_{r-1} \in \mathbb{R}$, что*

$$\mathbb{Q} = Q_1 \subset Q_2 \subset Q_3 \subset \ldots \subset Q_{r-1} \subset Q_r \ni A, \quad \text{где } a_k \in Q_k,\ \sqrt{a_k} \notin Q_k,$$

а $Q_{k+1} = Q_k[\sqrt{a_k}] := \{\alpha + \beta\sqrt{a_k} \mid \alpha, \beta \in Q_k\}$ для любого $k = 1, \ldots, r-1$.

Указание: Это утверждение легко доказывается индукцией по количеству операций калькулятора, необходимых для получения числа, с применением домножения на сопряженное.

Такая последовательность называется *цепочкой квадратичных расширений* (это единый термин, термин «квадратичное расширение» мы не используем).

Итак, число A построимо тогда и только тогда, когда для некоторого r существует цепочка квадратичных расширений длины r, последнее множество которой содержит A.

Доказательство невозможности, основанное на рассмотрении аналогичных цепочек, называется в математической логике и программировании *индукцией по глубине формулы*.

(b) Оторвем у (комплексного аналога) калькулятора из теоремы Гаусса кнопку «:», но разрешим использовать все рациональные числа. Тогда

множество чисел, которые можно реализовать на калькуляторе, не изменится.

Указание: Следует из предыдущего.

(c) $\sqrt[3]{2}$ непостроимо. (Значит, удвоение куба циркулем и линейкой невозможно.)

Доказательство непостроимости числа $\sqrt[3]{2}$. Предположим, что $\sqrt[3]{2}$ построимо. Тогда существует такая цепочка квадратичных расширений

$$\mathbb{Q} = Q_1 \subset Q_2 \subset Q_3 \subset \ldots \subset Q_{r-1} \subset Q_r, \quad \text{что} \quad \sqrt[3]{2} \in Q_r \setminus Q_{r-1}.$$

Поскольку $\sqrt[3]{2} \notin \mathbb{Q}$, то $r \geqslant 2$. Значит,

$$\sqrt[3]{2} = \alpha + \beta\sqrt{a}, \quad \text{где} \quad \alpha, \beta, a \in Q_{r-1}, \quad \sqrt{a} \notin Q_{r-1} \quad \text{и} \quad \beta \neq 0.$$

Отсюда

$$2 = (\sqrt[3]{2})^3 = (\alpha^3 + 3\alpha\beta^2 a) + (3\alpha^2\beta + \beta^3 a)\sqrt{a} = u + v\sqrt{a}.$$

Поскольку $2 \in \mathbb{Q} \subset Q_{r-1}$, то $2 - u \in Q_{r-1}$. Так как

$$v\sqrt{a} = 2 - u \quad \text{и} \quad v \in Q_{r-1}, \quad \text{то} \quad 0 = v = 3\alpha^2\beta + \beta^3 a.$$

Так как $3\alpha^2 + \beta^2 a > 0$, получаем $\beta = 0$ — противоречие! □

C3. (a) Число $\cos(2\pi/9)$ является корнем уравнения $8x^3 - 6x + 1 = 0$.

(b) Не существует рациональных чисел a и b, для которых $\cos(2\pi/9) = a + \sqrt{b}$.

(c) Не существует рациональных чисел a, b, c, для которых $\cos(2\pi/9) = a + \sqrt{b + \sqrt{c}}$.

(d) Число $\cos(2\pi/9)$ не построимо (значит, трисекция угла $\pi/3$ циркулем и линейкой невозможна и правильный 9-угольник не построим).

(e) *Теорема.* Корни кубического уравнения с рациональными коэффициентами построимы тогда и только тогда, когда один из них рационален.

Указания к C3. (a) Выразите $\cos 3\alpha$ через $\cos\alpha$.

(b) Если $\cos(2\pi/9) = a + \sqrt{b}$, то число $a - \sqrt{b}$ тоже является корнем уравнения $8x^3 - 6x + 1 = 0$. Тогда по теореме Виета третий корень равен $-(a + \sqrt{b}) - (a - \sqrt{b}) = -2a \in \mathbb{Q}$.

(d) Следует из (a) и (e).

(e) См. следующую лемму.

C4. *Лемма о сопряжении.* В цепочке квадратичных расширений положим $a = a_k$ и определим отображение сопряжения $\overline{\cdot}\colon Q_k[\sqrt{a}] \to Q_k[\sqrt{a}]$ формулой $\overline{x + y\sqrt{a}} = x - y\sqrt{a}$. Тогда

(a) Это определение корректно.

(b) $\overline{z + w} = \overline{z} + \overline{w}$, $\quad \overline{zw} = \overline{z}\,\overline{w} \quad$ и $\quad \overline{z} = z \Leftrightarrow z = x + 0\sqrt{a} \in Q_{k-1}$.

(c) Если $z \in Q_k[\sqrt{a}]$ — корень многочлена P с рациональными коэффициентами, то $P(\overline{z}) = 0$.

(Сравните с леммой о комплексных корнях многочлена с вещественными коэффициентами.)

Доказательство теоремы С3е *о кубических уравнениях для уравнений, все три корня которых вещественны (этот частный случай достаточен для непостроимости правильного* 9*-угольника).* Часть «тогда» очевидна. Чтобы доказать часть «только тогда», предположим, что хотя бы один из корней построим. Для каждого из построимых корней z рассмотрим минимальную цепочку расширений

$$\mathbb{Q} = Q_1 \subset Q_2 \subset Q_3 \subset \ldots \subset Q_{r-1} \subset Q_r, \quad \text{для которой} \quad z_1 \in Q_r \setminus Q_{r-1}.$$

Возьмем корень $z = z_1$ с наименьшей длиной минимальной цепочки l.

Если кубическое уравнение не имеет рациональных корней, то $l \geqslant 2$. Значит,

$$z_1 = \alpha + \beta\sqrt{a}, \quad \text{где} \quad \alpha, \beta \in Q_{l-1}, \quad \sqrt{a} \notin Q_{l-1} \qquad \text{и} \quad \beta \neq 0.$$

Тогда число $z_2 := \overline{z}_1 = \alpha - \beta\sqrt{a}$ также является корнем кубического уравнения (по лемме о сопряжении). Поскольку

$$\beta \neq 0, \text{ то } \alpha - \beta\sqrt{a} \neq \alpha + \beta\sqrt{a}, \text{ т. е. } z_2 \neq z_1.$$

Обозначим z_3 третий корень кубического уравнения (возможно, $z_3 \in \{z_1, z_2\}$). По формуле Виета

$$z_1+z_2+z_3 = (\alpha+\beta\sqrt{a})+(\alpha-\beta\sqrt{a})+z_3 = 2\alpha+z_3 \in \mathbb{Q}, \quad \text{поэтому} \quad z_3 \in Q_{l-1}.$$

Следовательно, для корня z_3 существует цепочка меньшей длины, чем для z_1. Противоречие. □

С5. *Эта задача не используется при доказательстве теоремы Гаусса.*

(a)* Корни многочлена 4-ой степени с рациональными коэффициентами построимы тогда и только тогда, когда его *кубическая резольвента* [9, 14] имеет рациональный корень.

(b) Любое построимое число является алгебраическим, т. е. корнем некоторого многочлена с целыми коэффициентами. (Из этого и доказанной в 1883 г. Линдеманом трансцендентности числа π, влекущей трансцендентность числа $\sqrt{\pi}$, вытекает, что задача о квадратуре круга неразрешима циркулем и линейкой.)

(c) (Г. Челноков) Лешин калькулятор получается из комплексного гауссова добавлением кнопки извлечения кубического корня из комплексных чисел (которая дает все три значения корня). Гришин калькулятор получается из комплексного гауссова добавлением кнопки нахождения по комплексному числу a всех трех комплексных корней уравнения $a = \dfrac{3x - 4x^3}{1 - 3x^2}$. Будет ли множество «Лешиных» чисел совпадать с множеством «Гришиных»?

(d) (Г. Челноков) Если неприводимый над $\mathbb{Q}$ многочлен раскладывается над $\mathbb{Q}[\sqrt[4]{2}]$ ровно на четыре множителя (неприводимых над $\mathbb{Q}[\sqrt[4]{2}]$), то степень этого многочлена делится на 8.

Указание к C5b. Пусть $a{=}a_1$ и $b{=}b_1$ — построимые числа, а P и Q — многочлены с рациональными коэффициентами минимальной степени, корнями которых являются соответственно a и b. Пусть $a_2, \dots, a_m$ — все остальные комплексные корни многочлена P, а $b_2, \dots, b_n$ — все остальные комплексные корни многочлена Q. Заметим, что

$a+b$ — корень многочлена $P(x-b_1)\cdot\ldots\cdot P(x-b_n)$,
$a-b$ — корень многочлена $P(x+b_1)\cdot\ldots\cdot P(x+b_n)$,
ab — корень многочлена $P(\frac{x}{b_1})\cdot\ldots\cdot P(\frac{x}{b_n})$,
$\frac{a}{b}$ — корень многочлена $P(xb_1)\cdot\ldots\cdot P(xb_n)$,
$\sqrt{a}$ — корень многочлена $P(x^2)$.

Осталось доказать следующее вспомогательное утверждение.

Лемма. Пусть $R(x,y)$ — многочлен от двух переменных с рациональными коэффициентами, а $b_1, b_2, \dots, b_n$ — все комплексные корни многочлена Q с рациональными коэффициентами. Тогда многочлен от одной переменной $R(x,b_1)R(x,b_2)\cdot\ldots\cdot R(x,b_n)$ также имеет рациональные коэффициенты.

Первое доказательство невозможности в теореме Гаусса

Это доказательство наиболее похоже на доказательство возможности.

D1. Число $\cos(2\pi/7)$ не построимо (значит, правильный 7-угольник не построим).

D2. Пусть $n = 4k{+}3$ простое. Обозначим $f_s = \varepsilon^s{+}\varepsilon^{-s}$. Назовем *рангом* построимого числа наименьшую длину минимальной цепочки квадратичных расширений, последнее множество которой содержит данное число.

(a) Для любого k число $f_1^k + f_2^k + \dots + f_{(p-1)/2}^k$ рационально.

(b) После раскрытия скобок и приведения подобных в выражении $(x-f_1)(x-f_2)\cdot\ldots\cdot(x-f_{(p-1)/2})$ получается многочлен с рациональными коэффициентами.

(c) Ранги чисел $\varepsilon, \varepsilon^2, \dots, \varepsilon^{p-1}$ одинаковы.

(d) Ранги чисел $f_1, \dots, f_{(p-1)/2}$ одинаковы.

(e) Число $\cos(2\pi/n)$ не построимо.

D3. Обозначим $\varepsilon = \cos(2\pi/13) + i\sin(2\pi/13)$, $g = 2$ — первообразный корень по модулю 13,

$A_0 = \varepsilon^{g^0}{+}\varepsilon^{g^3}{+}\varepsilon^{g^6}{+}\varepsilon^{g^9}$, $A_1 = \varepsilon^{g^1}{+}\varepsilon^{g^4}{+}\varepsilon^{g^7}{+}\varepsilon^{g^{10}}$ и $A_2 = \varepsilon^{g^2}{+}\varepsilon^{g^5}{+}\varepsilon^{g^8}{+}\varepsilon^{g^{11}}$.

(a) $A_0^2 = 4 + A_1 + 2A_2$, $A_1^2 = 4 + A_2 + 2A_0$ и $A_2^2 = 4 + A_0 + 2A_1$.

(b) Числа A_0, A_1, A_2 являются корнями неприводимого кубического уравнения с рациональными коэффициентами.

(c) Числа A_0, A_1, A_2 имеют одинаковый ранг.

(d) Число $\cos(2\pi/13)$ не построимо.

D4. Число $\cos(2\pi/p)$ не построимо для

(a) $p = 3 \cdot 2^k + 1$ простого.

(b) p простого, $p \neq 2^m + 1$.

(c) $p = 289$.

(d) числа p, не являющегоеся произведением степени двойки и различных простых чисел вида $2^m + 1$.

Решение D1. Рассмотрим комплексное число

$$\varepsilon = \cos(2\pi/7) + i\sin(2\pi/7).$$

Так как $\varepsilon \neq 1$, то число ε удовлетворяет уравнению 6-ой степени

$$\varepsilon^6 + \varepsilon^5 + \varepsilon^4 + \varepsilon^3 + \varepsilon^2 + \varepsilon + 1 = 0.$$

Разделим обе части уравнения на ε^3. Положим

$$f := \varepsilon + \varepsilon^{-1}, \quad \text{тогда } \varepsilon^2 + \varepsilon^{-2} = f^2 - 2 \text{ и } \varepsilon^3 + \varepsilon^{-3} = f(\varepsilon^2 + \varepsilon^{-2} - 1).$$

Получим кубическое уравнение

$$f(f^2 - 3) + (f^2 - 2) + f + 1 = 0, \quad \text{то есть} \quad f^3 + f^2 - 2f - 1 = 0.$$

Кандидаты на рациональные корни этого уравнения $f = \pm 1$ отвергаются проверкой. Согласно теореме С3е о кубических уравнениях число $f = \varepsilon + \varepsilon^{-1}$ не построимо. Поэтому и ε не построимо (поясните).

Указания к D2. (a) Индукция по k.

(b) Следует из пункта (a) и из того, что любой симметрический многочлен от переменных $f_1, f_2, \ldots, f_{(p-1)/2}$ рационально выражается через многочлены вида $f_1^k + f_2^k + \cdots + f_{(p-1)/2}^k$.

(c) Так как для любых $s, t \in \{1, 2, \ldots, p-1\}$ существует такое k, что $\varepsilon^s = (\varepsilon^t)^k$, то ранги чисел $\varepsilon, \varepsilon^2, \ldots, \varepsilon^{p-1}$ одинаковы.

(d) Так как $\varepsilon^s + \varepsilon^{-s}$ рационально выражается через $\varepsilon + \varepsilon^{-1}$, то для любых $s, t \in \{1, 2, \ldots, p-1\}$ число $\varepsilon^s + \varepsilon^{-s}$ рационально выражается через $\varepsilon^t + \varepsilon^{-t}$ (аналогично приведенному решению задачи D1). Поэтому ранги чисел $f_1, \ldots, f_{(p-1)/2}$ одинаковы.

(Заметим, что $\operatorname{rk}(\varepsilon + \varepsilon^{-1}) = \operatorname{rk}\varepsilon - 1$.)

(e) Пусть $r := \operatorname{rk} f_s$. Значит, для некоторой цепочки квадратичных расширений

$$f_s = \alpha_s + \beta_s\sqrt{a}, \quad \text{где } \alpha_s, \beta_s, a \in Q_{r-1},\ \sqrt{a} \notin Q_{r-1} \text{ и } \beta_s \neq 0.$$

Тогда число $\overline{f}_s = \alpha_s - \beta_s\sqrt{a}$ также является корнем рассматриваемого многочлена (по лемме о сопряжении). Поскольку

$$\beta_s \neq 0, \quad \text{то} \quad \alpha_s - \beta_s\sqrt{a} \neq \alpha_s + \beta_s\sqrt{a}, \quad \text{т. е.} \quad \overline{f}_s \neq f_s.$$

Итак, корни $f_1, \dots, f_{(p-1)/2}$ разбиваются на пары сопряженных. Значит, $(p-1)/2$ четно — противоречие.

Указания к D3. (a) Докажем первую фомулу (остальные доказываются аналогично). Заметим, что $g^6 = -1$. Поэтому

$$A_0^2 = ((\varepsilon^{g^0} + \varepsilon^{-g^0}) + (\varepsilon^{g^3} + \varepsilon^{-g^3}))^2 =$$
$$= 2 + \varepsilon^{g^1} + \varepsilon^{-g^1} + 2 + \varepsilon^{g^4} + \varepsilon^{-g^4} + 2(\varepsilon^{g^0} + \varepsilon^{g^6})(\varepsilon^{g^3} + \varepsilon^{g^9}) = 4 + A_1 + 2A_2.$$

Последнее равенство верно, поскольку

$$(\varepsilon^{g^0} + \varepsilon^{g^6})(\varepsilon^{g^3} + \varepsilon^{g^9}) = \varepsilon^{g^0+g^3} + \varepsilon^{g^3+g^6} + \varepsilon^{g^6+g^9} + \varepsilon^{g^9+g^0} =$$
$$= \varepsilon^{g^0+g^3} A_0 = \varepsilon^{g^8} A_0 = A_2.$$

(В обеих формулах предпоследние равенства верны, поскольку $g = 2$.)

(b) Докажите, что $A_0 + A_1 + A_2$, $A_0^2 + A_1^2 + A_2^2$, $A_0^3 + A_1^3 + A_2^3$ рациональны.

(c) Пользуясь пунктом (a) и тем, что $A_0 + A_1 + A_2 = -1$, докажите, что любое A_i рационально выражается через любое A_j.

(d) Решение получается из пунктов (b) и (c) аналогично решению задачи D2e.

Вот идея другого решения, не использующего пункт (c). Пусть число A_0 имеет ранг r. Сопряжем его относительно Q_{r-1}. Полученное число будет одним из чисел A_i (поясните). Теперь легко понять, что числа A_i разбиваются на пары сопряженных, т. е. их четное число, что неверно.

Указания к D4. (a) Аналогично задаче D3.

(b) Предположите, что для $p = 2^k r + 1$ число $\cos\dfrac{2\pi}{p}$ построимо (где $r > 1$ — нечетное число). Выведите из этого, что числа

$$A_i = \varepsilon^{g^i} + \varepsilon^{g^{r+i}} + \dots + \varepsilon^{g^{(2^k-1)r+i}}, \quad 0 \leqslant i \leqslant r-1$$

имеют одинаковый ранг и являются корнями мнгочлена степени r с рациональными коэффициентами.

(c) Рассмотрите числа

$$A_0 = \varepsilon^{g^0} + \varepsilon^{g^{17}} + \dots + \varepsilon^{g^{272}},$$
$$A_1 = \varepsilon^{g^1} + \varepsilon^{g^{18}} + \dots + \varepsilon^{g^{273}},$$
$$A_{16} = \varepsilon^{g^{16}} + \varepsilon^{g^{33}} + \dots + \varepsilon^{g^{288}}.$$

Второе доказательство невозможности в теореме Гаусса

Идея этого доказательства выражается понятиями поля и размерности поля.

E1. *Полем* (числовым) называется подмножество множества $\mathbb{C}$ комплексных чисел, замкнутое относительно сложения, вычитания, умножения и деления.

(a) Следующие множества являются полями: $\mathbb{Q}$, множество построимых чисел, множество вещественных чисел, $\mathbb{Q}[\sqrt{2}] := \{\alpha + \beta\sqrt{2} \mid \alpha, \beta \in \mathbb{Q}\}$, каждое Q_k в цепочке квадратичных расширений и

$$\mathbb{Q}[\varepsilon] := \{\alpha_0 + \alpha_1\varepsilon + \alpha_2\varepsilon^2 + \cdots + \alpha_{12}\varepsilon^{12} \mid \alpha_i \in \mathbb{Q}\}, \quad \text{где } \varepsilon = \cos\frac{2\pi}{13} + i\sin\frac{2\pi}{13}\,.$$

(b) Любое поле содержит поле $\mathbb{Q}$.

(c) Любое поле, содержащее $\sqrt{2}$, содержит $\mathbb{Q}[\sqrt{2}]$.

(d) Любое поле, содержащее ε, содержит $\mathbb{Q}[\varepsilon]$.

E2. *Размерностью* $\dim F$ поля F называется наименьшее k, для которого существуют такие $b_2, b_3 \ldots, b_k \in F$, что

$$F = \{\alpha_1 + \alpha_2 b_2 + \alpha_3 b_3 + \cdots + \alpha_k b_k \mid \alpha_i \in \mathbb{Q}\},$$

если такое k существует.

(a) $\dim \mathbb{Q} = 1$.

(b) $\dim \mathbb{Q}[\sqrt{2}] = 2$.

(c) В цепочке квадратичных расширений

$$\dim Q_k = 2\dim Q_{k-1} \quad \text{при } k \geqslant 1.$$

(d) В цепочке квадратичных расширений $\dim Q_k = 2^{k-1}$.

(e)* Если $G \subset F$ — поля, то $\dim F$ делится на $\dim G$.

E3. (a) $\dim \mathbb{Q}[\cos\frac{2\pi}{13} + i\sin\frac{2\pi}{13}] \leqslant 12$.

(b) Если $\dim \mathbb{Q}[\cos\frac{2\pi}{13} + i\sin\frac{2\pi}{13}] < 12$, то $P(\varepsilon) = 0$ для некоторого многочлена P с рациональными коэффициентами степени меньше 12.

(c) Многочлен $\Phi(x) := x^{12} + x^{11} + \cdots + x + 1$ неприводим над $\mathbb{Q}$.

Указание: если не получается, то используйте лемму Гаусса и признак Эйзенштейна (см. ниже).

(d) $\dim \mathbb{Q}[\cos\frac{2\pi}{13} + i\sin\frac{2\pi}{13}] = 12$.

(e) Число $\cos(2\pi/13)$ не построимо.

E4. (a) *Лемма Гаусса.* Если многочлен с целыми коэффициентами неприводим над $\mathbb{Z}$, то он неприводим и над $\mathbb{Q}$ [14].

(b) *Признак Эйзенштейна.* Пусть p простое. Если для многочлена с целыми коэффициентами старший коэффициент не делится на p, остальные делятся на p, а свободный член не делится на p^2, то этот многочлен неприводим над $\mathbb{Z}$ [14].

E5. (a) $\dim \mathbb{Q}[\cos\frac{2\pi}{289} + i\sin\frac{2\pi}{289}] = 272$.

(b) Выведите из предыдущих пунктов, что число $\cos(2\pi/289)$ не построимо.

(c) Докажите невозможность в теореме Гаусса.

Указание к E2. (c) Докажите, что

$$Q_k = \{\alpha_1 + \alpha_2 b \mid \alpha_1, \alpha_2 \in Q_{k-1}\} \quad \text{для любого } b \in Q_k - Q_{k-1}.$$

(d) Следует из (a) и (c).

(e) *Размерностью* $\dim(F : G)$ поля F над полем G называется наименьшее k, для которого существуют такие $b_1, b_2, \dots, b_k \in F$, что

$$F = \{\alpha_1 b_1 + \alpha_2 b_2 + \alpha_3 b_3 + \dots + \alpha_k b_k \mid \alpha_i \in G\},$$

если такое k существует. Докажите, что $\dim F = \dim G \dim(F : G)$.

Указания к E3. (a) $1 + \varepsilon + \varepsilon^2 \dots + \varepsilon^{12} = 0$.

(b) По определению размерности существуют такие

$$b_1, \dots, b_{11} \in \mathbb{Q}[\cos\frac{2\pi}{13} + i\sin\frac{2\pi}{13}] \text{ и } \alpha_{kl} \in \mathbb{Q}, \text{ что}$$
$$\varepsilon^{j-1} = \alpha_{j,1} b_1 + \alpha_{j,2} b_2 + \dots + \alpha_{j,11} b_{11} \text{ для } j = 1, 2, \dots, 12.$$

Поэтому существуют такие рациональные $a_0, a_1, \dots, a_{12}$, не все равные 0, что $a_0 + a_1\varepsilon + \dots + a_{11}\varepsilon^{11} = 0$. Для доказательства последнего утверждения подставьте выражения для ε^i в последнее равенство, приравняйте к нулю коэффициенты при $b_1, \dots, b_{11}$ и докажите, что полученная система уравнений имеет нетривиальное рациональное решение.

(c) Примените признак Эйзенштейна к многочлену $((x+1)^{13} - 1)/x$ и лемму Гаусса.

(d) Следует из (a), (b) и (c).

(e) Следует из (d) и E2d.

Указание к E4b. Предположите противное и воспользуйтесь методом неопределенных коэффициентов.

Указание к E5a. Аналогично решению задачи E3d. Докажите неприводимость многочлена $\Phi(x) = 1 + x^{17} + x^{34} + x^{51} + \dots + x^{272}$ и воспользуйтесь ей.

Список литературы

[1] Алексеев В. Б. *Теорема Абеля*. М: Наука, 1976.

[2] Ван дер Варден Б. Л. *Алгебра*. М.: Наука, 1976.

[3] Винберг Э. Б. *Алгебра многочленов*. М.: Просвещение, 1980.

[4] Гаусс К. Ф. *Арифметические исследования* // Труды по теории чисел. М.: Изд-во АН СССР, 1959. С. 9–580.

[5] Гашков С. Б. *Современная элементарная алгебра в задачах и упражнениях*. М.: МЦНМО, 2006.

[6] Гиндикин С. *Дебют Гаусса* // Квант, №1, 1972. С. 2–11.

[7] Канель А. Я. *О построениях*. Готовится к печати.

[8] Кириллов А. А. *О правильных многоугольниках, функции Эйлера и числах Ферма* // Квант, №7, 1977. С. 2–9. Квант, №6, 1994. С. 15–18.

[9] Колосов В. А. *Теоремы и задачи алгебры, теории чисел и комбинаторики*. М: Гелиос, 2001.

[10] Курант Р., Роббинс Г. *Что такое математика*? М.: МЦНМО, 2004.

[11] Литлвуд Дж. *Математическая смесь*. М.: Наука, 1978.

[12] Манин Ю.И. *О разрешимости задач на построение с помощью циркуля и линейки* // Энциклопедия элементарной математики. Книга четвертая (геометрия). Под редакцией П. С. Александрова, А. И. Маркушевича и А. Я. Хинчина М.: Физматгиз, 1963.

[13] Постников М. М. *Теория Галуа*. М.: Гос. изд-во физ.-мат. л-ры, 1963.

[14] Прасолов В. В. *Многочлены*. М: МЦНМО, 1999, 2001, 2003.

[15] Прасолов В. В., Соловьев Ю. П. *Эллиптические функции и алгебраические уравнения*. М.: Факториал, 1997.

[16] Чеботарев Н. Н. *Основы теории Галуа*. Часть 1. Л., М.: Гостехиздат, 1934.

[17] Эдвардс Г. *Последняя теорема Ферма. Генетическое введение в алгебраическую теорию чисел*. М.: Мир, 1980.

П. Ю. Козлов: механико-математический факультет Московского государственного университета им. М. В. Ломоносова

А. Б. Скопенков: механико-математический факультет Московского государственного университета им. М. В. Ломоносова, Независимый московский Университет, Московский институт открытого образования
e-mail: `skopenko@mccme.ru`