Как придумать построение правильного семнадцатиугольника

А. Л. Канунников

Какие правильные n-угольники можно построить с помощью циркуля и линейки? Этот вопрос интересовал ещё древнегреческих геометров. Они знали построение при $n = 3, 4, 5, 15$ и умели удваивать число сторон. Продвижений не было две тысячи лет, пока в 1796 году не произошёл прорыв: 18-летний Иоганн Карл Фридрих Гаусс (1777–1855) научился строить правильный 17-угольник, а вскоре решил задачу окончательно. Это было первое большое открытие будущего «короля математиков», как называли Гаусса, и он им очень дорожил — даже завещал выгравировать на своей могиле правильный 17-угольник, вписанный в круг.

Несмотря на геометрическую постановку задачи, она решается методами алгебры и теории чисел, и Гаусс посвятил ей раздел в своём монументальном труде «Арифметические исследования» [1].

Слово Гауссу:

> *«Читатель может удивиться, что это исследование помещено именно в настоящем труде, который, на первый взгляд, посвящён совершенно чуждому этим вопросам предмету; однако само сочинение убедительно покажет, в какой тесной связи с высшей арифметикой эти вопросы находятся»* [1, с. 509].

> *«В то время как возможность деления круга на три и пять частей была известна уже ко временам Евклида, к этим сведениям на протяжении* 2000 *лет не было добавлено ничего нового…»* [1, с. 571].

При поддержке Московского центра фундаментальной и прикладной математики, грант «Структурная теория и комбинаторно-логические методы в теории алгебраических систем».

Вместе с работами Лагранжа о перестановках корней уравнений (1776) исследования Гаусса подготовили почву для настоящей революции в алгебре. Дело в том, что циркулем и линейкой строятся только те отрезки, длины которых выражаются в квадратных радикалах, а разрешимость уравнений в радикалах (любой степени) — центральная проблема алгебры того времени. Окончательно её решил замечательный математик Эварист Галуа (1811–1832), вдохновлённый идеями Лагранжа и Гаусса. Галуа полностью преобразил алгебру, заложив основы таких её современных разделов, как теория групп и теория полей. Теорию Галуа для двучленных уравнений фактически разработал Гаусс, обобщив и расширив свои исследования по построению правильных многоугольников.

Вершины правильного n-угольника Гаусс интерпретирует как комплексные корни n-й степени из единицы[1)]. Ключевая идея Гаусса — группировать их в суммы, которые он называет *периодами*. Далее Гаусс находит те n, при которых эти периоды удаётся выразить в квадратных радикалах. Самое трудное и красивое — упорядочить корни должным образом для разбиения на периоды. Для простых n (к которым всё сводится) это упорядочение становится возможным благодаря замечательному факту — существованию первообразного корня по любому простому модулю. Эта теорема, также впервые доказанная Гауссом, стала настоящей жемчужиной теории чисел и алгебры.

Замечательное открытие Гаусса переплетается и с другими его результатами, ставшими классикой. Недаром оно обсуждается с разных сторон во многих книгах и статьях.

- Периоды Гаусса тесно связаны с его учением о квадратичных вычетах. Так, с помощью периодов Гаусс концептуально передоказал важнейший *квадратичный закон взаимности* [1, с. 643–648]. Упрощённое рассуждение, использующее более поздние идеи, см. в [4].
- В. А. Кириченко [10] частично переизлагает теорию периодов Гаусса на современном языке. Основные цели этого миникурса — «реклама замечательной книги [1] и доступное введение в теорию Галуа».
- П. Ю. Козлов и А. Б. Скопенков [12] приводят два доказательства теоремы Гаусса, предваряя их задачами, подводящими к ключевым идеям. Оба доказательства восходят к оригинальной работе [1] Гаусса, но изложение переработано и содержит оригинальные идеи авторов.

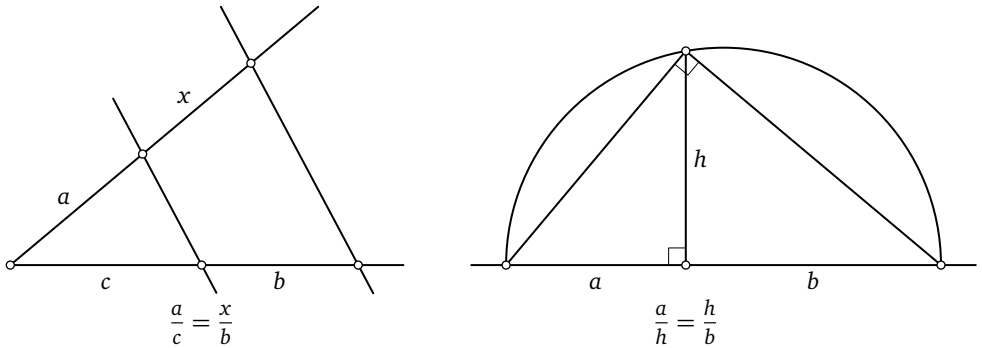
[1)] Такая интерпретация была известна уже почти век — она основана на формуле Муавра (1707).

- М. М. Постников [14] излагает теорию Гаусса деления круга, *опираясь на выросшую из неё* теорию Галуа. Этот путь предполагает глубокую алгебраическую подготовку.
- М. Н. Аршинов и Л. Е. Садовский [3, глава 5], а также С. Г. Гиндикин [6, глава «Король математиков»] объясняют построение правильного 17-угольника с помощью группы автоморфизмов, т. е. опять-таки с точки зрения теории Галуа.

Главная цель нашей статьи — показать, как прийти к открытию Гаусса естественным путём, используя сравнительно простые средства — основы теории алгебраических чисел. Им мы посвятили отдельную статью «Алгебраические числа как векторы» [8] в этом выпуске. Там можно найти необходимые определения и обозначения. Мы также передокажем результаты построенной Гауссом теории, используя более современный язык и развитую технику.

§ 1. Что известно из «Начал» Евклида

Задачам на построение циркулем и линейкой и, в частности, построению правильных многоугольников посвящена IV книга трактата Евклида «Начала» (около 300 г. до н. э.) — главного труда античной математики. В нём описано, как по отрезкам a, b, c построить отрезки ab/c и $\sqrt{ab}$ (рис. 1). Это позволяет на числовой прямой с отмеченными точками $0, 1$ и $a, b > 0$ отметить точки $a \pm b$, $ab/1$, $(a \cdot 1)/b$, $\sqrt{a \cdot 1}$. Таким образом, можно отметить все числа, которые получаются из рациональных с помощью арифметических действий и извлечения квадратных корней. Такие числа часто называют *поликвадратичными*.



$\frac{a}{c} = \frac{x}{b}$ $\qquad$ $\frac{a}{h} = \frac{h}{b}$

Рис. 1

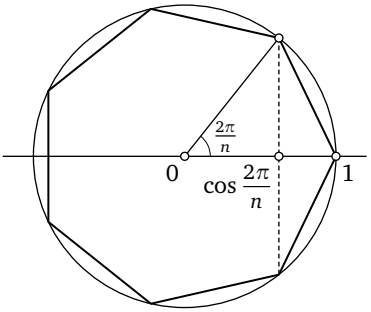


Рис. 2

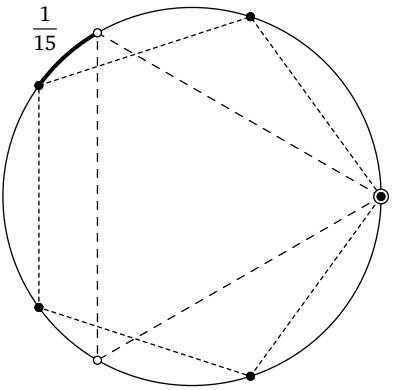


Рис. 3

Заметим теперь, что построение правильного n-угольника или деление окружности на n равных частей равносильно построению числа[2)] $\cos(2\pi/n)$ (рис. 2). При $n = 3, 4$ это тривиально. Случай $n = 5$ посложнее (см., например, [7, задача 5]):

$$\cos\frac{2\pi}{5} = \frac{\sqrt{5}-1}{4}. \tag{1}$$

Чтобы построить правильный 15-угольник, впишем в окружность правильные треугольник и пятиугольник, имеющие общую вершину (рис. 3). Ближайшие из отмеченных точек заключают дугу, равную $1/15$ окружности, поскольку $\frac{1}{15} = 2 \cdot \frac{1}{5} - \frac{1}{3}$. Вообще, при взаимно простых m и n, имея $1/m$ и $1/n$ части окружности, можно построить $1/(mn)$ её часть: по алгоритму Евклида находим такие целые a и b, что $am + bn = 1$, т. е.

$$\frac{1}{mn} = a \cdot \frac{1}{n} + b \cdot \frac{1}{m}.$$

Наконец, умея строить $1/n$ часть окружности, легко построить и $1/(2n)$ часть, проведя биссектрису угла. Таким образом, с учётом разложения чисел на простые множители задача сведена к такой:

$$\begin{gathered}\text{при каких простых } p > 2 \text{ и натуральных } k \\ \text{можно построить правильный } p^k\text{-угольник?}\end{gathered} \tag{2}$$

Ответ на этот вопрос заведомо положителен, если

$$\text{число } \cos\frac{2\pi}{p^k} \text{ поликвадратично.} \tag{3}$$

[2)] Построить число $a \in \mathbb{R}$ — значит отметить точку с координатой a на числовой прямой (здесь и далее — циркулем и линейкой). Фраза «построить отрезок длины a» осмысленна только при $a > 0$.

Выполняется ли это условие для каких-то ещё знаменателей вида p^k, кроме 3 и 5? Является ли оно не только достаточным, но и необходимым? На эти вопросы никто не знал ответов до конца XVIII века…

§ 2. Почему вдруг 17?

Забегая вперёд, отметим, что правильный 17-угольник можно построить с помощью полученной Гауссом [1, с. 571] формулы, которая после упрощений принимает вид

$$\cos\frac{2\pi}{17}=\frac{\sqrt{17}-1}{16}+\frac{1}{16}\sqrt{34-2\sqrt{17}}+\frac{1}{8}\sqrt{17+3\sqrt{17}-\sqrt{170+38\sqrt{17}}}. \quad (4)$$

Покажем, как вывести эту формулу, а также как установить поликвадратичность числа $\cos(2\pi/17)$ без вычислений. Но обо всём по порядку.

Условие (3) на самом деле является и достаточным, и необходимым ввиду следующей теоремы.

Теорема 1. *Поликвадратичные числа и только они строятся циркулем и линейкой.*

Основные идеи доказательства. В § 1 мы показали, что действительные поликвадратичные числа строятся. Переход от построения «реальных отрезков» к «мистическим мнимым числам» заслуживает комментария. Комплексные числа — вполне реальные точки на плоскости, и их тоже можно отмечать циркулем и линейкой. Имея на комплексной плоскости точки $0, 1$ и $a, b \neq 0$, совсем легко построить точки $a \pm b$ и также несложно построить точки ab, $\frac{a}{b}$, $\sqrt{a}$: модули строятся как в § 1, а аргументы (углы) соответственно складываются (для ab), вычитаются (для a/b) и делятся пополам (для $\sqrt{a}$). Итак, любые (комплексные) поликвадратичные числа строятся циркулем и линейкой.

В обратную сторону теорема не столь очевидна, хотя главная идея лежит на поверхности: циркулем и линейкой строятся прямые и окружности, а они задаются линейными и квадратными уравнениями. Вот более подробное рассуждение.

Пусть уже построено некоторое множество чисел и все они поликвадратичны. Казалось бы, мы можем только проводить прямые и окружности через построенные комплексные числа на плоскости, а также строить окружности построенных радиусов с построенными центрами. Все такие прямые и окружности задаются уравнениями степени 1 и 2 с поликвадратичными коэффициентами, а значит, точки пересечения имеют

поликвадратичные координаты. Однако нельзя забывать, что при построении можно также выбирать произвольные точки, причём иногда это просто необходимо (попробуйте, к примеру, построить центр данной окружности). Конечно, произвольные точки не считаются построенными циркулем и линейкой, но точка, полученная с их помощью и *не зависящая от их выбора*, считается построенной. А раз так, то произвольные точки можно считать поликвадратичными. Также следует учесть, что в ряде случаев произвол ограничен: точка случайно выбирается на данной прямой или окружности, а то и вовсе *достаточно близко* к уже построенной. Остаётся заметить, что множество поликвадратичных чисел содержит всюду плотное подмножество $\mathbb{Q}+i\mathbb{Q}$. За более полным и детальным доказательством мы отсылаем читателя к [14, глава 5], [16].

Теорема 1 прокладывает мостик от геометрической формулировки (2) к эквивалентной алгебраической (3), поэтому мы откладываем в сторону циркуль и линейку и вооружаемся инструментами из алгебры — алгебраическими числами и расширениями полей. Основы этой теории начали формироваться как раз в трактате Гаусса [1], были существенно развиты в работах Галуа, а полностью были разработаны во второй половине XIX века усилиями Куммера, Кронекера, Гильберта и др. Вы можете ознакомиться с ними по статье «Алгебраические числа как векторы» [8] в этом выпуске.

Переформулируем условие поликвадратичности на языке расширений полей. Поскольку присоединение квадратного радикала приводит к расширению степени 2, то всякое поликвадратичное число α содержится в некоторой башне полей вида

$$\mathbb{Q} = K_0 \xrightarrow{2} K_1 \xrightarrow{2} \dots \xrightarrow{2} K_m. \tag{5}$$

По теореме о размерности башни [8, теорема 9] получаем

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] \mid [K_m : \mathbb{Q}] = 2^m,$$

а по теореме [8, теорема 8] получаем $\alpha \in \mathbb{A}$ и $\deg \alpha = [\mathbb{Q}(\alpha) : \mathbb{Q}]$[3]. Мы доказали простое, но важное необходимое условие поликвадратичности.

Теорема 2. *Всякое поликвадратичное число — алгебраическое, и его степень есть степень двойки.*

[3] Напомним, что $\deg \alpha$, где α — алгебраические число, — это степень минимального многочлена числа α.

Это условие не достаточно, см. далее задачу 2.

Итак, для выполнения условия (3) необходимо, чтобы $\deg \cos(2\pi/p^k)$ было степенью двойки.

Пример 1. Найдём минимальные многочлены для чисел $\cos\frac{2\pi}{9}$ и $\cos\frac{2\pi}{7}$.

а) По формуле тройного угла

$$4\cos^3\frac{2\pi}{9} - 3\cos\frac{2\pi}{9} = \cos\frac{2\pi}{3} = -\frac{1}{2},$$

откуда $\cos(2\pi/9)$ — корень многочлена $8x^3 - 6x + 1$. Этот многочлен неприводим над $\mathbb{Q}$ (после замены $2x = y$ получаем многочлен $y^3 - 3y + 1$, не имеющий рациональных корней), а потому является минимальным для числа $\cos(2\pi/9)$.

б) Сумма комплексных корней двучлена $x^7 - 1$ по теореме Виета равна 0, поэтому сумма их действительных частей

$$1 + 2\cos\frac{2\pi}{7} + 2\cos\frac{4\pi}{7} + 2\cos\frac{6\pi}{7}$$

тоже равна 0. Обозначив $c = \cos(2\pi/7)$, имеем:

$$1 + 2c + 2(2c^2 - 1) + 2(4c^3 - 3c) = 0 \quad \Leftrightarrow \quad (2c)^3 + (2c)^2 - 2(2c) - 1 = 0.$$

При этом многочлен $y^3 + y^2 - 2y - 1$ не имеет корней в $\mathbb{Q}$.

Значит, $\deg \cos(2\pi/7) = \deg \cos(2\pi/9) = 3$, поэтому *правильные семиугольник и девятиугольник построить нельзя*.

В общем случае работать с косинусом неудобно. Скажем, для чисел $\cos(2\pi/13)$ и $\cos(2\pi/17)$ такие рассуждения, как в примере 1б, приведут (после громоздких вычислений) к многочленам степеней 6 и 8 соответственно, и для доказательства их неприводимости над $\mathbb{Q}$ уже будет недостаточно отсутствия рациональных корней. Препятствие преодолевается изящно и естественно. Вспомним, откуда вообще взялся косинус. Это абсцисса вершины правильного n-угольника (рис. 2), или, алгебраически, действительная часть корня из единицы

$$\varepsilon_n = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}. \tag{6}$$

Будучи корнем двучлена, число ε_n гораздо удобнее для исследования[4)], нежели $\cos(2\pi/n)$, причём они оба либо строятся циркулем и линейкой,

[4)] Гаусс: «*Между тем ни одно уравнение не является столь простым для рассмотрения и удобным для нашей цели, как уравнение* $x^n - 1 = 0$ *...*» [1, с. 512]. О связи минимальных многочленов чисел ε_n и $\cos(2\pi/n)$ см. также [8, пример 11].

либо нет. Отметим, что восстановление вершин ε_n и ε_n^{-1} по их проекции $\cos(2\pi/n)$ (рис. 2) — геометрическое решение квадратного уравнения

$$x^2 - 2\cos\frac{2\pi}{n}x + 1 = 0 \quad \Leftrightarrow \quad x = \varepsilon_n, \varepsilon_n^{-1}.$$

В частности, при $n > 2$ (когда $\varepsilon_n \neq \pm 1$) имеем

$$\mathbb{Q}\Big(\cos\frac{2\pi}{n}\Big) \xrightarrow{2} \mathbb{Q}(\varepsilon_n) \quad \text{и} \quad \deg\varepsilon_n = 2\deg\cos\frac{2\pi}{n}.$$

Итак, нам нужно найти минимальный многочлен $\mu_{\varepsilon_n}(x)$ для $n = p^k$. Гаусс [1, п. 341] рассмотрел только случай $k = 1$, доказав довольно сложным методом, что многочлен

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \ldots + x + 1$$

неприводим над $\mathbb{Q}$, а значит, $\Phi_p(x) = \mu_{\varepsilon_p}(x)$. Позднее нашли простое доказательство: сделать замену $x - 1 = y$ и применить признак Эйзенштейна [8, теорема 1], согласно которому многочлен

$$\Phi_p(y+1) = \frac{(y+1)^p - 1}{y} = y^{p-1} + py^{p-2} + \ldots + C_p^k y^{k-1} + \ldots + C_p^2 y + p \quad (7)$$

неприводим, так как $C_p^k = \dfrac{p!}{k!(p-k)!}$ кратно p при $k = 1, \ldots, p-1$.

Более общо: число ε_{p^k} является корнем многочлена

$$\Phi_{p^k}(x) = \frac{x^{p^k} - 1}{x^{p^{k-1}} - 1} = \Phi_p(x^{p^{k-1}})$$

степени $p^k - p^{k-1}$ (среди корней степени p^k из единицы исключаем корни степени p^{k-1}).

Задача 1. Докажите, что многочлен $\Phi_{p^k}(x)$ неприводим над $\mathbb{Q}$. (Мы определили в [8, пример 9] круговые многочлены $\Phi_n(x)$ и упомянули без доказательства, что они неприводимы для любого n.)

Из задачи 1 следует, что $\deg\varepsilon_{p^k} = p^{k-1}(p-1)$. Когда это число — степень двойки? Ввиду нечётности p, тогда и только тогда, когда $k = 1$ и $(p-1)$ — степень двойки: $p - 1 = 2^l$. Если l делится на нечётное d, то $2^l + 1$ делится на $2^{l/d} + 1$. Поскольку $2^l + 1 = p$ — простое, с необходимостью $d = 1$. Значит, l не имеет нечётных делителей, кроме единицы, т. е. l — степень двойки, и p имеет вид $F_j = 2^{2^j} + 1$, где j целое неотрицательное. Числа такого вида называются *числами Ферма*. Первые пять из них простые:

$$F_0 = 3, \quad F_1 = 5, \quad F_2 = 17, \quad F_3 = 257, \quad F_4 = 65\,537.$$

Ферма полагал, что все F_j простые, но Эйлер это опроверг, показав, что $F_5 = 2^{32} + 1 = 4\,294\,967\,297$ кратно 641. До сих пор неизвестно, существуют ли другие простые числа Ферма. (См. [9], где связь чисел Ферма с построением правильных многоугольников объясняется другим интересным способом.)

Итак, «круг подозреваемых» резко сузился, и мы подошли к главному вопросу: *для каких простых чисел Ферма p можно построить правильный p-угольник*? Важно понимать, что ответ «для всех» не следует из теоремы 2, ведь она даёт лишь необходимое условие поликвадратичности, надежду построить башню (5), для которой $K_m \supseteq \mathbb{Q}(\varepsilon_p)$.

Задача 2. а) Докажите, что сопряжённые (т. е. корни того же минимального многочлена) с поликвадратичными числами тоже поликвадратичны. б) Пользуясь этим, приведите пример неприводимого над $\mathbb{Q}$ многочлена степени 4, корни которого не поликвадратичны.

Оказывается, *построить башню можно для всех простых чисел Ферма*, и в этом состоит замечательный результат Гаусса — наиболее сложная часть следующей знаменитой теоремы.

Теорема 3 (Гаусс — Ванцéль). *Правильный n-угольник строится циркулем и линейкой в точности тогда, когда n — произведение степени двойки и различных простых чисел Ферма* (*возможно, ни одного*).

На самом деле Гаусс доказал только утверждение «если». Вот что он пишет [1, с. 572] по поводу того, что других n нет: «Хотя границы нашего сочинения не позволяют провести этого доказательства, мы думаем, что надо всё же на это указать для того, чтобы кто-либо не пытался искать ещё других случаев, кроме тех, которые указаны нашей теорией, например, не надеялся бы свести на геометрические построения деление окружности на $7, 11, 13, 19, \ldots$ частей и не тратил бы зря своего времени». Аккуратное доказательство всё же следовало провести, и это сделал французский математик Пьер Ванцель [2] — выше мы фактически воспроизвели его рассуждение. Отметим, что Ванцель известен главным образом работой [2], в которой он доказал неразрешимость ещё двух классических задач на построение, также восходящих к древним грекам.

Теорема 4 (Ванцель [2]). *Удвоение куба и трисекция угла невыполнимы циркулем и линейкой.*

В самом деле, удвоение куба равносильно построению числа $\sqrt[3]{2}$, имеющего, очевидно, степень 3. А доказанная выше невозможность построить правильный девятиугольник (пример 1а) равносильна невыполнимости трисекции угла $2\pi/3$. (Неразрешимость третьей знаменитой проблемы —

квадратуры круга — следует из трансцендентности числа π, доказанной Линдеманом в 1882 году.)

Вот мы и поняли, «почему вдруг 17»: это следующее за пятёркой простое число Ферма. Теперь главное: как построить башню, оставаясь в рамках элементарной теории алгебраических чисел.

§ 3. Как прийти к периодам Гаусса

Разберём подробно случай $p = 17$. Положим $\varepsilon = \varepsilon_{17} = \cos\frac{2\pi}{17} + i\sin\frac{2\pi}{17}$. Попробуем построить башню квадратичных расширений

$$\mathbb{Q} = K_0 \xrightarrow{2} K_1 \xrightarrow{2} K_2 \xrightarrow{2} K_3 \xrightarrow{2} K_4 = \mathbb{Q}(\varepsilon). \tag{8}$$

Как найти промежуточные поля K_1, K_2, K_3? Все числа из $K_1 \setminus \mathbb{Q}$ имеют степень 2 над $\mathbb{Q}$, все числа из $K_2 \setminus K_1$ имеют степень 2 над K_1, а значит, степень 4 над $\mathbb{Q}$ и т. д. Степень алгебраического числа, напомним, равна количеству сопряжённых с ним. Поле $\mathbb{Q}(\varepsilon)$ имеет базис $1, \varepsilon, \ldots, \varepsilon^{15}$ над $\mathbb{Q}$ [8, теорема 8]. Вместо 1 можно взять ε^{16} — они взаимозаменяемы ввиду равенства $1 + \varepsilon + \ldots + \varepsilon^{16} = 0$. Так удобнее, поскольку

$$\varepsilon, \varepsilon^2, \varepsilon^3, \ldots, \varepsilon^{15}, \varepsilon^{16} \tag{9}$$

— это не только базис, но и набор сопряжённых чисел. Разложим произвольное $\alpha \in \mathbb{Q}(\varepsilon)$ по этому базису:

$$\alpha = a_1\varepsilon + a_2\varepsilon^2 + \ldots + a_{16}\varepsilon^{16}, \quad \text{где } a_1, \ldots, a_{16} \in \mathbb{Q}. \tag{10}$$

Это многочлен от ε, и в такой ситуации список сопряжённых с α даёт следующая теорема.

Теорема 5 [8, теорема 6]. *Если $\beta_1, \ldots, \beta_n$ — все сопряжённые с алгебраическим числом β, то для любого многочлена $f(x) \in \mathbb{Q}[x]$ все сопряжённые с $f(\beta)$ суть $f(\beta_1), \ldots, f(\beta_n)$.*

Таким образом, подставив в (10) вместо ε его сопряжённые $\varepsilon^2, \ldots, \varepsilon^{16}$, получим все сопряжённые с α:

$$\begin{aligned} &a_1\varepsilon + a_2\varepsilon^2 + a_3\varepsilon^3 + \ldots, \\ &a_1\varepsilon^2 + a_2\varepsilon^4 + a_3\varepsilon^6 + \ldots, \\ &a_1\varepsilon^3 + a_2\varepsilon^6 + a_3\varepsilon^9 + \ldots, \\ &\ldots\ldots\ldots\ldots\ldots\ldots \end{aligned} \tag{11}$$

Среди этих чисел *какие-то должны повторяться*, коль скоро $\deg\alpha < 16$. Показатели степеней в k-й сумме из (11) равны $k, 2k, 3k, \ldots, 16k$ и дают

все ненулевые остатки при делении на 17. Поэтому, заменив показатели их остатками, мы получим разложения по тому же базису (9). Например, второе число равно

$$a_1\varepsilon^2 + a_2\varepsilon^4 + \ldots + a_8\varepsilon^{16} + a_9\varepsilon + \ldots + a_{16}\varepsilon^{15}.$$

Таким образом, равенство каких-то из чисел (11) означает равенство их коэффициентов при одинаковых степенях ε. К сожалению, эти степени перемешиваются хаотично, оттого условия на коэффициенты получаются громоздкими.

Чтобы решить проблему, *переупорядочим* базисные элементы (9) так, чтобы при подстановке в них вместо ε любого сопряжённого числа они сдвигались по циклу. Попробуем, например, расположить степени ε так, чтобы при подстановке ε^2 вместо ε они сдвинулись по циклу на единицу. Тогда после ε будет стоять ε^2, затем $(\varepsilon^2)^2 = \varepsilon^{2^2}$, $(\varepsilon^2)^{2^2} = \varepsilon^{2^3}$ и т. д. Выпишем ли мы так весь ряд (9)? Так как $2^4 \equiv -1 \pmod{17}$, то $2^8 \equiv 1 \pmod{17}$, поэтому девятым числом окажется $\varepsilon^{2^8} = \varepsilon$, т. е. зацикливание произойдёт раньше времени и мы выпишем лишь половину степеней ε. Не стоит огорчаться — мы просто не угадали с *первообразным корнем* по модулю 17 — двойка им не является. По определению, целое a называется первообразным корнем по модулю простого p, если степени $a, a^2, \ldots, a^{p-1}$ дают все ненулевые остатки при делении на p. Легко проверить, что по модулю 17 одним из первообразных корней является тройка. Поэтому, последовательно возводя ε в куб, мы выпишем все числа (9), см. рис. 4:

$$\{1, 3, 3^2, \ldots, 3^{15}\} \equiv \{1, 2, \ldots, 16\} \pmod{17} \quad \Rightarrow$$
$$\Rightarrow \quad \{\varepsilon, \varepsilon^3, \varepsilon^{3^2}, \ldots, \varepsilon^{3^{15}}\} = \{\varepsilon, \varepsilon^2, \varepsilon^3, \ldots, \varepsilon^{16}\}.$$

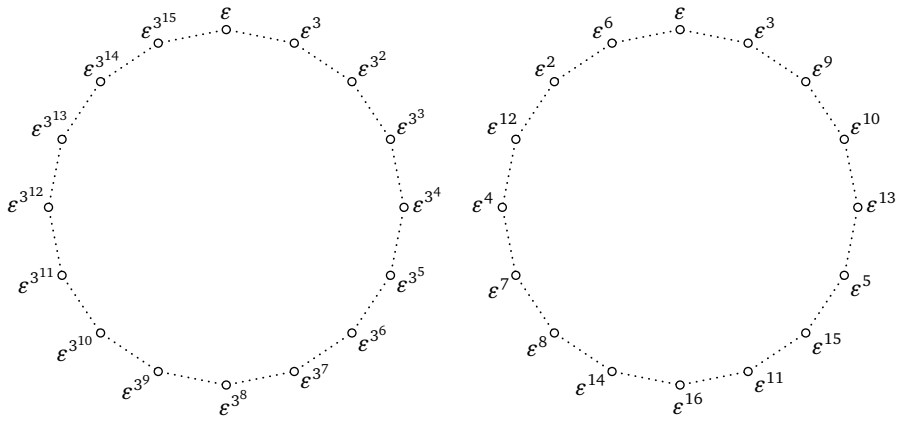


Рис. 4

Задача 3. Пусть целое a не кратно простому p. Как известно, по малой теореме Ферма $a^{p-1} \equiv 1 \pmod p$. Пусть k — наименьшее натуральное число со свойством $a^k \equiv 1 \pmod p$.

а) Докажите, что $k \mid p-1$.

б) Докажите следующее: a — первообразный корень по модулю $p \iff$ $\iff k = p-1 \iff k \neq (p-1)/q$ ни для какого простого делителя q числа $p-1$. (Например, при $p=17$ это значит, что $a^{(17-1)/2} = a^8 \not\equiv 1 \pmod{17}$. Этому условию не удовлетворяет $a=2$: $2^8 = 16^2 \equiv (-1)^2 \equiv 1 \pmod{17}$, зато удовлетворяет $a=3$: $3^8 = 81^2 \equiv (-4)^2 \equiv -1 \pmod{17}$.)

Феликс Клейн [11, с. 45]:

«30 мая 1796 года для Гаусса[5] наступает день его творческого крещения… Гаусс уже в течение долгого времени занимался группировкой корней из единицы, опираясь на созданную им теорию „первообразных корней“. И вот однажды утром, когда он был ещё в постели, он внезапно ясно и отчётливо осознал, что из его теории следует возможность построения правильного семнадцатиугольника. Как мы уже отмечали, это событие оказалось поворотным пунктом в жизни Гаусса. Он принимает решение полностью посвятить себя не филологии, а математике».

Выпишем сопряжённые с произвольным числом из $\mathbb{Q}(\varepsilon)$, разложенным по переупорядоченному базису.

Следствие 1 (теоремы 5). *Сопряжённые с любым числом $\alpha = \alpha_0 \in \mathbb{Q}(\varepsilon)$ имеют вид*:

$$\begin{aligned}
\alpha_0 &= a_0\varepsilon + a_1\varepsilon^3 + a_2\varepsilon^{3^2} + \ldots + a_{15}\varepsilon^{3^{15}},\\
\alpha_1 &= a_1\varepsilon + a_2\varepsilon^3 + a_3\varepsilon^{3^2} + \ldots + a_0\varepsilon^{3^{15}},\\
\alpha_2 &= a_2\varepsilon + a_3\varepsilon^3 + a_4\varepsilon^{3^2} + \ldots + a_1\varepsilon^{3^{15}},\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
\alpha_{14} &= a_{14}\varepsilon + a_{15}\varepsilon^3 + a_0\varepsilon^{3^2} + \ldots + a_{13}\varepsilon^{3^{15}},\\
\alpha_{15} &= a_{15}\varepsilon + a_0\varepsilon^3 + a_1\varepsilon^{3^2} + \ldots + a_{14}\varepsilon^{3^{15}},
\end{aligned} \tag{12}$$

где $a_0, \ldots, a_{15} \in \mathbb{Q}$.

Теперь, когда коэффициенты в каждой строчке получаются циклическим сдвигом из предыдущей, приравнивать их не составляет труда. Так, если $\alpha_0 = \alpha_1$, то по цепочке $a_0 = a_1 = a_2 = \ldots = a_{15}$, поэтому все α_i равны $a_0(\varepsilon + \varepsilon^2 + \ldots + \varepsilon^{16}) = -a_0$. Если $\alpha_0 = \alpha_2$, то коэффициенты повторяются через один: $a_0 = a_2 = \ldots = a_{14}$ и $a_1 = a_3 = \ldots = a_{15}$, поэтому числа α_j тоже

[5] Напомним, ему всего 18 лет.

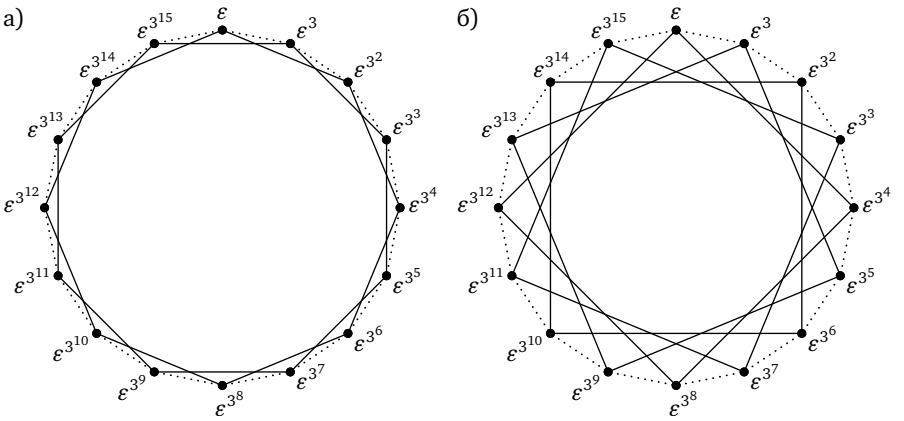


Рис. 5

повторяются через один. Важный пример такой пары чисел — две суммы степеней ε, взятых через одну:

$$\theta_0 = \varepsilon + \varepsilon^{3^2} + \varepsilon^{3^4} + \ldots + \varepsilon^{3^{14}}, \quad \theta_1 = \varepsilon^3 + \varepsilon^{3^3} + \varepsilon^{3^5} + \ldots + \varepsilon^{3^{15}}. \tag{13}$$

Гаусс называет их 2-*периодами* (рис. 5а). Поскольку они сопряжены и имеют степень 2, они образуют пару корней квадратного уравнения над $\mathbb{Q}$. Вскоре мы покажем, как его составить (что и делал Гаусс), но сейчас продолжим рассуждение без вычислений — путь к башне прощупывается! Взяв в 2-периодах каждое второе слагаемое, получим 4-*периоды* (рис. 5б), которые в свою очередь разбиваются на 8-*периоды* (на картинке это диаметры). Периоды одной длины Гаусс называет *однотипными*.

Замечание. 8-периоды равны удвоенным косинусам:

$$\varepsilon^{3^k} + \varepsilon^{3^{k+8}} = \varepsilon^{3^k} + \varepsilon^{-3^k} = 2\cos\frac{2\pi\cdot 3^k}{17}, \quad k = 1, \ldots, 8.$$

Периоды удобно организовать в таблицу:

<table>
<tr><td colspan="4">$\theta_0 = \varepsilon + \varepsilon^{3^2} + \varepsilon^{3^4} + \ldots + \varepsilon^{3^{14}}$</td><td colspan="4">$\theta_1 = \varepsilon^3 + \varepsilon^{3^3} + \varepsilon^{3^5} + \ldots + \varepsilon^{3^{15}}$</td></tr>
<tr><td colspan="2">$\underbrace{\varepsilon + \varepsilon^{3^4} + \varepsilon^{3^8} + \varepsilon^{3^{12}}}_{\theta_{00}}$</td><td colspan="2">$\underbrace{\varepsilon^{3^2} + \varepsilon^{3^6} + \varepsilon^{3^{10}} + \varepsilon^{3^{14}}}_{\theta_{01}}$</td><td colspan="2">$\underbrace{\varepsilon^3 + \varepsilon^{3^5} + \varepsilon^{3^9} + \varepsilon^{3^{13}}}_{\theta_{10}}$</td><td colspan="2">$\underbrace{\varepsilon^{3^3} + \varepsilon^{3^7} + \varepsilon^{3^{11}} + \varepsilon^{3^{15}}}_{\theta_{11}}$</td></tr>
<tr><td>$\underbrace{\varepsilon + \varepsilon^{3^8}}_{\theta_{000}}$</td><td>$\underbrace{\varepsilon^{3^4} + \varepsilon^{3^{12}}}_{\theta_{001}}$</td><td>$\underbrace{\varepsilon^{3^2} + \varepsilon^{3^{10}}}_{\theta_{010}}$</td><td>$\underbrace{\varepsilon^{3^6} + \varepsilon^{3^{14}}}_{\theta_{011}}$</td><td>$\underbrace{\varepsilon^3 + \varepsilon^{3^9}}_{\theta_{100}}$</td><td>$\underbrace{\varepsilon^{3^5} + \varepsilon^{3^{13}}}_{\theta_{101}}$</td><td>$\underbrace{\varepsilon^{3^3} + \varepsilon^{3^{11}}}_{\theta_{110}}$</td><td>$\underbrace{\varepsilon^{3^7} + \varepsilon^{3^{15}}}_{\theta_{111}}$</td></tr>
</table>

Обратите внимание, что при замене ε на ε^3 периоды не разрушаются, а лишь переставляются с однотипными, при этом структура таблицы сохраняется.

Как периоды помогут нам построить башню (8)? Поскольку d-периоды имеют степень d, имеем $[\mathbb{Q}(\theta_*) : \mathbb{Q}] = 2$, $[\mathbb{Q}(\theta_{**}) : \mathbb{Q}] = 4$ и т. д. Казалось бы, искомая башня имеет вид

$$\mathbb{Q} \subset \mathbb{Q}(\theta_*) \subset \mathbb{Q}(\theta_{**}) \subset \mathbb{Q}(\theta_{***}) = \mathbb{Q}\Big(\cos\frac{2\pi}{17}\Big) \subset \mathbb{Q}(\varepsilon), \tag{14}$$

но… включения не очевидны! Возникают следующие вопросы:

Q1 *Верны ли какие-нибудь включения вида* (14)?
Q2 *Верны ли равенства*

$$\mathbb{Q}(\theta_0) = \mathbb{Q}(\theta_1), \quad \mathbb{Q}(\theta_{00}) = \mathbb{Q}(\theta_{01}) = \mathbb{Q}(\theta_{10}) = \mathbb{Q}(\theta_{11}) \quad \textit{и т. д.}?$$

Чтобы ответить на эти вопросы, опишем все возможные совпадения среди чисел (12). Пусть есть какое-то совпадение: $\alpha_j = \alpha_{j+d}$ для некоторых j и d. Тогда

$$\begin{gathered}\text{коэффициенты } a_k \text{ повторяются с шагом } d \text{ по кругу:}\\ a_k = a_l \text{ при всех } k \equiv l \pmod d,\\ \text{а тогда с тем же шагом повторяются и сами числа (12).}\end{gathered} \tag{15}$$

Если при этом $d > 0$ выбрано наименьшим, то d делит 16 (если $16 = dq + r$, $0 \leqslant r < d$, то $\alpha_0 = \alpha_d = \alpha_{2d} = \ldots = \alpha_r$, откуда $r = 0$) и различных среди чисел (12) ровно d. *Это и есть* $\deg\alpha$. (В частности, при $d = 16$ совпадений нет и $\deg\alpha = 16$.) Теперь для каждого делителя d числа 16 рассмотрим множество U_d чисел $\alpha \in \mathbb{Q}(\varepsilon)$, удовлетворяющих условию (15). В этом условии не требуется минимальность d, поэтому

$$U_d = \{\alpha \in \mathbb{Q}(\varepsilon) \mid \deg\alpha \leqslant d\} = \{\alpha \in \mathbb{Q}(\varepsilon) \mid \deg\alpha \text{ — делитель } d\}. \tag{16}$$

Теперь включения очевидны:

$$\mathbb{Q} = U_1 \subset U_2 \subset U_4 \subset U_8 \subset U_{16} = \mathbb{Q}(\varepsilon),$$

но возникает новый вопрос:

Q3 *Почему U_d — поля*?

Задача 4. Докажите, что:
а) $\mathbb{Q}(\theta_0) = \mathbb{Q}(\theta_1) = U_2$;
б) $\mathbb{Q}(\theta_{000}) = \ldots = \mathbb{Q}(\theta_{111}) = U_8$ (используйте тригонометрию).

Итак, мы поняли, как прийти к открытым Гауссом периодам, но теперь надо завершить рассуждение, в правильности которого сомнений нет. Надо ответить на вопрос Q1 или равносильный ему Q3.

§ 4. Завершение доказательства теоремы Гаусса — Ванцеля

Для каждого делителя d числа 16 мы определили множество U_d чисел

$$a_0\varepsilon + a_1\varepsilon^3 + a_2\varepsilon^{3^2} + \ldots + a_{15}\varepsilon^{3^{15}},$$

у которых коэффициенты a_k повторяются с шагом d по кругу. Вынося повторяющиеся коэффициенты за скобки, получим в скобках суммы степеней ε с шагом d, т. е. не что иное как d-периоды. Обозначим их $\sigma_0, \ldots, \sigma_{d-1}$ — тогда каждое число из U_d однозначно запишется в виде

$$a_0\sigma_0 + a_1\sigma_1 + \ldots + a_{d-1}\sigma_{d-1}.$$

Это значит, что U_d — векторное пространство над $\mathbb{Q}$ с базисом $\sigma_0, \ldots, \sigma_{d-1}$. В частности, U_d замкнуто относительно сложения и вычитания, но нужна ещё замкнутость относительно умножения и деления. Следующая теорема даёт ответы на все вопросы Q1, Q2, Q3.

Теорема 6. *Для любого d-периода σ_j имеем $U_d = \mathbb{Q}(\sigma_j)$. В частности, U_d — поле.*

Доказательство. Как мы отметили, $\dim_{\mathbb{Q}} U_d = d$. Поле $\mathbb{Q}(\sigma_j)$ тоже имеет размерность d над $\mathbb{Q}$, поэтому достаточно доказать включение $\mathbb{Q}(\sigma_j) \subseteq U_d$. Но U_d состоит из чисел, у которых не более d сопряжённых, см. (16). А всякое число из $\mathbb{Q}(\sigma_j)$ имеет вид $f(\sigma_j)$ для некоторого многочлена $f(x) \in \mathbb{Q}[x]$, и по теореме 5 его сопряжённые суть $f(\sigma_0), \ldots, f(\sigma_{d-1})$, среди которых, очевидно, не более d различных. □

Итак, башня квадратичных расширений для 17-угольника построена.

Задача 5. Модифицируя доказательство теоремы 6, покажите, что полями U_d ($d = 1, 2, 4, 8, 16$) исчерпываются все подполя в $\mathbb{Q}(\varepsilon)$. Тем самым, построенная башня единственна.

Построение башни для любого простого числа Ферма p аналогично — нужно только найти первообразный корень по модулю p. Напомним, это такое целое g, что $\{1, 2, \ldots, p-1\} \equiv \{1, g, g^2, \ldots, g^{p-2}\} \pmod p$. Его существование — ещё один блестящий результат Гаусса, классика теории чисел.

Теорема 7 [1, п. 54]. *По любому простому модулю существует первообразный корень.*

Задача 6. Найдите какие-нибудь первообразные корни по модулям 7, 11, 13. (Воспользуйтесь задачей 3.)

Задача 7. Докажите теорему 7 в интересующем нас случае, когда p — простое число Ферма. Воспользуйтесь тем, что $\mathbb{Z}_p$ — поле и что многочлен степени n с коэффициентами из любого поля имеет не более n корней.

Легко проследить, что последующие рассуждения аналогичны разобранному случаю $p = 17$: многочлен $\Phi_p(x) = (x^p - 1)/(x - 1)$ неприводим над $\mathbb{Q}$ (см. § 2) и имеет множество корней $\{\varepsilon, \varepsilon^2, \ldots, \varepsilon^{p-1}\} = \{\varepsilon, \varepsilon^g, \ldots, \varepsilon^{g^{p-2}}\}$, где $\varepsilon = \cos(2\pi/p) + i\sin(2\pi/p)$. Определяем периоды. Для этого разбиваем сумму $\varepsilon + \varepsilon^g + \varepsilon^{g^2} + \ldots + \varepsilon^{g^{p-2}}$ на две — с чётными и нечётными номерами (это 2-периоды). Каждую из этих сумм разбиваем так же ещё на две, и т. д. ($p - 1$ — степень двойки). Теорема 6, очевидно, справедлива и в этой общей ситуации, и мы заключаем, что от поля $\mathbb{Q}$ к полю $\mathbb{Q}(\varepsilon)$ можно прийти последовательными квадратичными расширениями. Теорема 3 Гаусса — Ванцеля полностью доказана.

Конструктивно ли наше доказательство, т. е. можно ли с его помощью построить правильный p-угольник? Да, поскольку каждое расширение степени 2 получается присоединением квадратного радикала [8, теорема 9], который вычисляется алгоритмически. Проще всего последовательно присоединять сами периоды, имея в виду их следующее свойство.

Теорема 8. *Пусть период* θ_* (*где* $*$ — *двоичное слово*) *распался на два*: $\theta_* = \theta_{*0} + \theta_{*1}$. *Тогда* θ_{*0} *и* θ_{*1} — *пара сопряжённых над полем* $\mathbb{Q}(\theta_*)$.

Доказательство. С периодом θ_{*0} сопряжены над $\mathbb{Q}$ все периоды того же типа. По теореме 6 получаем $\mathbb{Q}(\theta_{*0}) \supset \mathbb{Q}(\theta_*)$, причём это расширение степени 2, следовательно, период θ_{*0} сопряжён над $\mathbb{Q}(\theta_*)$ ещё ровно с одним однотипным периодом, обозначим его $\theta_?$. Тогда

$$x^2 - (\theta_{*0} + \theta_?)x + \theta_{*0}\theta_? \in \mathbb{Q}(\theta_*)[x] \quad \text{и} \quad \theta_{*0} + \theta_? \in \mathbb{Q}(\theta_*).$$

Коэффициенты при степенях ε в сумме $\theta_{*0} + \theta_?$ повторяются с подходящим шагом только при $\theta_? = \theta_{*1}$. □

Таким образом, на каждом шаге нужно вычислять произведение $\theta_{*0}\theta_{*1}$.

Замечание. Сам Гаусс не рассуждал в терминах полей , а последовательно составлял для периодов квадратные уравнения. Также с помощью вычислений с периодами он доказал следующие их свойства, из которых вытекает ответ на вопрос Q2 и частично — на вопрос Q3:

— произведение однотипных периодов равно сумме периодов того же типа [1, с. 522–524];
— каждый период является многочленом над $\mathbb{Q}$ от любого периода того же типа [1, с. 524–526].

§ 5. Вычисление периодов при $p = 17$

2-периоды. При раскрытии скобок в выражении

$$\theta_1\theta_0 = (\varepsilon^3 + \varepsilon^{3^3} + \ldots + \varepsilon^{3^{15}})(\varepsilon^{3^2} + \varepsilon^{3^4} + \ldots + \varepsilon^{3^{16}}) \tag{17}$$

получится сумма $8^2 = 64$ слагаемых. Как известно, Гаусс вычислял много и с завидной для докомпьютерной эпохи точностью. И хотя рутинные вычисления никогда не были для него преградой, он владел высокой культурой счёта. Ещё в семь лет маленький Карл поразил школьного учителя, быстро сосчитав сумму $1 + 2 + \ldots + 100 = \frac{100 \cdot 101}{2} = 5050$. Вот и произведение (17) Гаусс вычислил с помощью удачной группировки, собрав члены $\varepsilon^{3^{2k+1}}\varepsilon^{3^{2l}}$ с одинаковой разностью $2k + 1 - 2l \pmod{16}$:

$$\begin{aligned}(\varepsilon^{3+3^2} + \varepsilon^{3^3+3^4} + \ldots + \varepsilon^{3^{15}+3^{16}}) + (\varepsilon^{3+3^4} + \varepsilon^{3^3+3^6} + \ldots + \varepsilon^{3^{15}+3^2}) + \\ + (\varepsilon^{3+3^6} + \varepsilon^{3^3+3^8} + \ldots + \varepsilon^{3^{15}+3^4}) + (\varepsilon^{3+3^8} + \varepsilon^{3^3+3^{10}} + \ldots + \varepsilon^{3^{15}+3^6}) + \\ + (\varepsilon^{3+3^{10}} + \varepsilon^{3^3+3^{12}} + \ldots + \varepsilon^{3^{15}+3^8}) + (\varepsilon^{3+3^{12}} + \varepsilon^{3^3+3^{14}} + \ldots + \varepsilon^{3^{15}+3^{10}}) + \\ + (\varepsilon^{3+3^{14}} + \varepsilon^{3^3+3^{16}} + \ldots + \varepsilon^{3^{15}+3^{12}}) + (\varepsilon^{3+3^{16}} + \varepsilon^{3^3+3^2} + \ldots + \varepsilon^{3^{15}+3^{14}}).\end{aligned}$$

Полученные восемь сумм разбиты на четыре пары, в каждой из которых встречаются все степени $\varepsilon^3, \ldots, \varepsilon^{3^{16}}$ по разу (так как показатели всякий раз выстраиваются в геометрическую прогрессию со знаменателем 3, например, $3 + 3^2 \to 3^3 + 3^2 \to 3^3 + 3^4 \to \ldots$). Каждая такая сумма равна -1, поэтому $\theta_0\theta_1 = -4$. Таким образом, $(x - \theta_0)(x - \theta_1) = x^2 + x - 4$, откуда

$$\theta_0, \theta_1 = \frac{-1 \pm \sqrt{17}}{2}$$

(вопрос выбора знаков обсудим позже).

Упростим дальнейшие вычисления, оперируя с 8-периодами или удвоенными косинусами:

$$c_k = 2\cos\frac{2\pi k}{17} = \varepsilon^k + \varepsilon^{-k}, \quad k = 1, \ldots, 8.$$

Они удовлетворяют равенствам $c_k = c_{17-k}$ и $c_k c_l = c_{k+l} + c_{k-l}$, в которых индексы можно рассматривать по модулю 17 ввиду 2π-периодичности косинуса.

4-периоды. Имеем

$$\theta_{00}\theta_{01} = (c_1 + c_4)(c_2 + c_8) = c_3 + c_1 + c_8 + c_7 + c_6 + c_2 + c_5 + c_4 = -1,$$

значит, $(x - \theta_{00})(x - \theta_{01}) = x^2 - \theta_0 x - 1$, откуда

$$\theta_{00}, \theta_{01} = \frac{\theta_0 \pm \sqrt{\theta_0^2 + 4}}{2} = \frac{\theta_0 \pm \sqrt{8 - \theta_0}}{2}.$$

8-периоды. Поскольку $\theta_{000}\theta_{001} = c_1c_4 = c_3 + c_5 = \theta_{10}$, получаем, что

$$\theta_{000}, \theta_{001} = \frac{\theta_{00} \pm \sqrt{\theta_{00}^2 - 4\theta_{10}}}{2}.$$

Памятуя о равенстве $\mathbb{Q}(\theta_{10}) = \mathbb{Q}(\theta_{00})$, выразим θ_{10} через θ_{00}. Проще всего это сделать так:

$$\theta_{00}\theta_{10} = (c_1 + c_4)(c_3 + c_5) = c_2 + c_4 + c_4 + c_6 + c_1 + c_7 + c_1 + c_8 =$$
$$= -1 + c_1 + c_4 - c_3 - c_5 = -1 + \theta_{00} - \theta_{10} \quad \Rightarrow \quad \theta_{10} = \frac{\theta_{00} - 1}{\theta_{00} + 1}.$$

О выборе знаков. В наших формулах три знака $\pm$, и мы пока не знаем, какому знаку отвечает какой период в каждой найденной паре. В этом может помочь тригонометрия: на отрезке $[0; \pi]$ косинус убывает, поэтому $c_1 > \ldots > c_4 > 0 > c_5 > \ldots > c_8$. Далее, $c_1 > c_2 > \cos(\pi/3) = 1/2$ и

$$\theta_0 = c_1 + c_2 + c_4 + c_8 > \frac{1}{2} + \frac{1}{2} + 0 + (-1) = 0,$$

значит,

$$\theta_0 = \frac{-1 + \sqrt{17}}{2}.$$

Аналогично можно сравнить и 4-периоды. Интересно, что Гаусс для этой цели использовал десятичные приближения [1, с. 540, п. 354] с избыточной точностью — 10 знаков после запятой! Однако давайте подумаем, так ли обязательно определяться со знаками. Что если просто вместо $\pm$ везде поставить $+$? Именно, последовательно построим отрезки:

$$a = \frac{-1 + \sqrt{17}}{2}, \quad b = \frac{a + \sqrt{8 - a}}{2}, \quad c = \frac{b + \sqrt{b^2 - 4 \cdot \dfrac{b-1}{b+1}}}{2}. \qquad (18)$$

Мы знаем, что $c = c_k$ — один из 8-периодов, т. е.

$$\frac{c}{2} = \cos\frac{2\pi k}{17}$$

при каком-то $k \in \{1, \ldots, 8\}$. Так вот, при каком именно — совершенно неважно для построения 17-угольника! Дело в том, что, последовательно откладывая дугу $2\pi k/17$ на окружности 16 раз, мы разделим окружность на 17 равных частей, каким бы ни было k. Просто при $k > 1$ точки деления будут появляться не подряд и мы сделаем несколько оборотов. С алгебраической точки зрения все первообразные корни 17-й степени из единицы равноправны, и в принципе любой из них мы могли бы принять за ε (не обязательно $\cos(2\pi/17) + i\sin(2\pi/17)$).

Задача 8. Определитесь со знаками ± в парах периодов $\{\theta_{00}, \theta_{01}\}$ и $\{\theta_{000}, \theta_{001}\}$ и убедитесь, что $\theta_{000} = c_1 = c$.

Замечание. Чтобы вывести формулу (4) для $\cos(2\pi/17)$, нужно упростить выражение под последним радикалом в (18). Используя равенства $a^2 = 4 - a$, $b^2 = ab + 1$ и $b = (a + \sqrt{8 - a})/2$, можно получить следующую формулу:

$$b^2 - 4 \cdot \frac{b-1}{b+1} = \frac{1}{4}\left(17 + 3\sqrt{17} - \sqrt{170 + 38\sqrt{17}}\right).$$

В трактате Гаусса [1, с. 571] стоит $\sqrt{34 - 2\sqrt{17}} + 2\sqrt{34 + 2\sqrt{17}}$ вместо $\sqrt{170 + 38\sqrt{17}}$ (Гаусс выражал θ_{10} в радикалах, а не через θ_{00}). Легко проверить, возведя в квадрат, что эти числа равны.

Для двух других простых чисел Ферма 257 и 65 537 вычисления лучше поручить компьютеру [15]. Впрочем, в XIX веке находились отважные, которые проделывали их вручную. Так, 257-угольник был построен Ришело, а в библиотеке Гёттингенгского университета хранится солидных размеров чемодан с построением 65 537-угольника!.. По этому поводу Дж. Литлвуд [13, с. 43] рассказал следующую историю: «Один слишком навязчивый аспирант довёл 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…»

§ 6. Связь 2-периодов с квадратичными вычетами

Отдельного внимания заслуживают 2-периоды, тесно связанные с квадратичными вычетами. Любопытно, что построение пятиугольника начинается с $\sqrt{5}$ (см. (1)), а построение 17-угольника — с $\sqrt{17}$. Это не похоже на случайное совпадение. Посмотрим, чему равны 2-периоды

$$\theta_0 = \varepsilon^{g^2} + \varepsilon^{g^4} + \ldots + \varepsilon^{g^{p-1}}, \quad \theta_1 = \varepsilon^{g} + \varepsilon^{g^3} + \ldots + \varepsilon^{g^{p-2}}$$

для других простых $p > 2$, не обязательно чисел Ферма. Как и ранее,

$$\varepsilon = \cos\frac{2\pi}{p} + i\sin\frac{2\pi}{p}$$

и g — любой первообразный корень по модулю p. Зависят ли 2-периоды от выбора g? Заметим, что все $(p-1)/2$ показателей $g^2, g^4, \ldots, g^{p-1}$ в периоде θ_0 являются *квадратичными вычетами* по модулю p, т. е., по определению, квадратами ненулевых вычетов. С другой стороны, этих квадратов не больше, чем $(p-1)/2$: все ненулевые вычеты можно записать

в симметричной форме $\pm1, \pm2, \ldots, \pm(p-1)/2$, поэтому их квадраты суть $1^2, 2^2, \ldots, ((p-1)/2)^2$. Итак,

$$\{g^2, g^4, \ldots, g^{p-1}\} \equiv \left\{1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2\right\} \pmod p \tag{19}$$

— это в точности все квадратичные вычеты по модулю p. Значит, 2-*периоды не зависят от выбора* g:

$$\theta_0 = \sum_{k=1}^{(p-1)/2} \varepsilon^{k^2}, \quad \theta_1 = -1 - \theta_0. \tag{20}$$

Пример 2. При $p = 3$:

$$\theta_0 = \varepsilon = \frac{-1+i\sqrt{3}}{2}, \quad \theta_1 = \varepsilon^2 = \frac{-1-i\sqrt{3}}{2}.$$

Здесь $\theta_1 = \bar\theta_0 \notin \mathbb{R}$, в отличие от случаев $p = 5, 17$.

Задача 9. При $p=7$ имеем $\theta_0 = \varepsilon^2 + \varepsilon^4 + \varepsilon$, $\theta_1 = \varepsilon^3 + \varepsilon^6 + \varepsilon^5$. Вычислите $\theta_0\theta_1$, а затем найдите θ_0, θ_1. (Вы увидите, что и здесь «замешан» $\sqrt{p}$, а точнее, $\sqrt{-p}$, как и в случае $p = 3$.)

Чтобы обобщить наши наблюдения при $p = 3, 5, 7, 17$ и выдвинуть гипотезу для любого p, давайте поймём, когда 2-периоды действительны (как при $p = 5, 17$), а когда — комплексно-сопряжены (как при $p = 3, 7$). Поскольку сумма сопряжённых чисел действительна, то $\theta_0, \theta_1 \in \mathbb{R}$, если сопряжённые корни попадают в один период. В противном случае $\theta_1 = \bar\theta_0$. Обобщим рис. 5а на любое нечётное p. Сопряжённые корни расположены на разных концах диаметров, а в один 2-период попадают корни, идущие через один. Значит, сопряжённые корни окажутся в одном 2-периоде, если число диаметров чётно, и в разных, если нечётно. Число диаметров равно $(p-1)/2$, что чётно при $p \equiv 1 \pmod 4$. Теперь мы готовы сформулировать гипотезу:

$$\{\theta_0, \theta_1\} = \begin{cases} \dfrac{-1 \pm \sqrt{p}}{2} & \text{при } p \equiv 1 \pmod 4, \\ \dfrac{-1 \pm i\sqrt{p}}{2} & \text{при } p \equiv 3 \pmod 4. \end{cases} \tag{21}$$

Вот план доказательства (подробности см. [1, с. 545, 868], [4]):

1) рассмотреть сумму $S = \sum_{k=0}^{p-1} \varepsilon^{k^2}$ и показать, что $S = 1 + 2\theta_0$;

2) доказать, что $S\bar S = p$, сгруппировав слагаемые после раскрытия скобок должным образом;

3) $\bar S = \begin{cases} S, & p \equiv 1 \pmod 4, \\ -S, & p \equiv 3 \pmod 4 \end{cases} \Rightarrow S^2 = \begin{cases} p, & p \equiv 1 \pmod 4, \\ -p, & p \equiv 3 \pmod 4 \end{cases} \Rightarrow (21).$

Замечание. Определиться в (21) со знаками — задача весьма непростая, и Гаусс думал над ней не один год. В конце концов он доказал, что $S = \sqrt{p}$ при $p \equiv 1 \pmod 4$ и $S = i\sqrt{p}$ при $p \equiv 3 \pmod 4$ [1, с. 594–618]. (Выше при $p = 17, 7$ мы в этом убедились с помощью простых оценок.) На этом пути Гаусс не только передоказал центральный результат теории квадратичных вычетов — квадратичный закон взаимности, но и создал теорию гауссовых сумм, которая и по сей день является мощным средством в аналитической теории чисел. Надеемся, читатель оценил теперь не только красоту открытия Гаусса, но и его огромное значение.

Задача 10. Докажите, что $\mathbb{Q}(\sqrt{7}, \sqrt{11}, \sqrt{13}) \subseteq \mathbb{Q}(\varepsilon_{4004})$.

Решения задач

1. Снова сделаем замену $x = y + 1$:

$$\Phi_{p^k}(x) = \Phi_p(x^{p^{k-1}}) = \Phi_p((y+1)^{p^{k-1}}) = f(y).$$

Этот многочлен имеет свободный член $f(0) = \Phi_p(1) = p$. А поскольку

$$(a+b)^{p^s} \equiv a^{p^s} + b^{p^s} \pmod p$$

при всех целых a, b (индукция по s), то

$$f(y) \equiv \Phi_p(y^{p^{k-1}} + 1) \pmod p.$$

Старший коэффициент этого многочлена равен 1, а остальные кратны p по аналогии с (7). Значит, многочлен $f(y)$ неприводим по признаку Эйзенштейна [8, теорема 1].

2. а) Для $\alpha \in \mathbb{C}$ обозначим через $\sqrt{\alpha}$ одно из значений корня. Возьмём любую бесконечную башню вида

$$\mathbb{Q} = K_0 \xrightarrow{2} K_1 \xrightarrow{2} \dots \xrightarrow{2} K_m \to \dots$$

и докажем индукцией по m, что сопряжённые ко всякому $\alpha \in K_m \setminus K_{m-1}$ поликвадратичны. Для $m = 1$ это очевидно, пусть $m > 1$. Имеем $\alpha = a + b\sqrt{c}$, где $a, b, c \in K_{m-1}$. По предположению индукции сопряжённые к a, b, c поликвадратичны. Остаётся показать, что сопряжённые к α имеют вид $a' \pm b'\sqrt{c'}$, где a', b', c' — сопряжённые к a, b, c. Ввиду [8, теорема 6] достаточно установить, что всякое сопряжённое к $\sqrt{c}$ имеет вид $\pm\sqrt{c'}$. Это так, поскольку $\sqrt{c}$ — корень многочлена $\mu_c(x^2) \in \mathbb{Q}[x]$.

б) Из пункта а) следует, что если α — любое поликвадратичное число, $\alpha_1, \ldots, \alpha_n$ — все его сопряжённые и $L = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$, то $[L : \mathbb{Q}]$ — степень двойки. Построим при $n = 4$ такое α, что $[L : \mathbb{Q}]$ кратно 3.

Идея Лагранжа решения уравнения 4-й степени с неизвестными корнями $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ состоит в переходе к вспомогательному кубическому уравнению с корнями $\alpha_1\alpha_2 + \alpha_3\alpha_4$, $\alpha_1\alpha_3 + \alpha_2\alpha_4$, $\alpha_1\alpha_4 + \alpha_2\alpha_3$, оно называется *резольвентой Феррари*. Можно вычислить, что для многочлена $P(x) = x^4 + ax^2 + bx + c$ резольвента имеет вид

$$R(x) = y^3 - ay^2 - 4cy + 4ac - b^2.$$

Поэтому достаточно подобрать такие $a, b, c \in \mathbb{Q}$, чтобы многочлены P и R были неприводимы над $\mathbb{Q}$. Тогда присоединение к $\mathbb{Q}$ любого корня многочлена R приведёт к расширению степени 3, откуда $3 \mid \dim_{\mathbb{Q}} L$. Подойдут значения $a = 0$, $b = 2$, $c = -2$: многочлен $x^4 + 2x - 2$ неприводим по признаку Эйзенштейна, а многочлен $y^3 + 8y - 4$ неприводим ввиду отсутствия рациональных корней.

Отметим без доказательства такой критерий: *число α поликвадратично в точности тогда, когда степень поля разложения его минимального многочлена есть степень двойки*. Для доказательства, по-видимому, не обойтись без соответствий Галуа [5, с. 471].

3. а) Пусть $p - 1 = kq + r$, где $0 \leqslant r < k$. Тогда $a^r = a^{p-1} : (a^k)^q = 1$, откуда $r = 0$ ввиду минимальности k.

б) Любая степень a сравнима по модулю p ровно с одной из степеней $a, a, a^2, \ldots, a^k \equiv 1$, так как $a^{k+1} \equiv a$ и т. д. Поэтому если все вычеты $a, a^2, \ldots, a^{p-1}$ различны, то $k = p - 1$. Обратно, если $a^m \equiv a^n$ при некоторых $0 \leqslant m < n < k$, то $a^{n-m} \equiv 1$, хотя $n - m < k$. Тем самым первые два условия равносильны. Третье условие, очевидно, равносильно второму.

4. а) $\mathbb{Q}(\theta_0) = \mathbb{Q} + \mathbb{Q}\theta_0$, $\mathbb{Q}(\theta_1) = \mathbb{Q} + \mathbb{Q}\theta_1$, $U_2 = \mathbb{Q}\theta_0 + \mathbb{Q}\theta_1$, причём $\theta_0 + \theta_1 = -1$, откуда следуют оба равенства.

б) Поскольку $\cos n\phi$ — многочлен Чебышёва от $\cos \phi$, получаем

$$\mathbb{Q}\Big(\cos \frac{2\pi n}{17}\Big) \subseteq \mathbb{Q}\Big(\cos \frac{2\pi}{17}\Big).$$

Если $17 \nmid n$, то $nm \equiv 1 \pmod{17}$ для некоторого m, откуда

$$\mathbb{Q}\Big(\cos \frac{2\pi}{17}\Big) \subseteq \mathbb{Q}\Big(\cos \frac{2\pi n}{17}\Big).$$

Далее,

$$U_8 = \mathbb{Q}\cos \frac{2\pi}{17} + \ldots + \mathbb{Q}\cos \frac{16\pi}{17} \subseteq \mathbb{Q}\Big(\cos \frac{2\pi}{17}\Big).$$

Обратное включение следует из равенства размерностей:

$$\dim_{\mathbb{Q}} U_8 = \dim_{\mathbb{Q}} \mathbb{Q}\Big(\cos\frac{2\pi}{17}\Big) = 8.$$

5. Пусть K — любое подполе в $\mathbb{Q}(\varepsilon)$ и n — наименьшее число со свойством $K \subseteq U_{2^n}$. Тогда K содержит число $\alpha \in U_{2^n} \setminus U_{2^{n-1}}$. Так как $\mathbb{Q}(\alpha) \subseteq K \subseteq U_{2^n}$ и $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg\alpha = 2^n = \dim_{\mathbb{Q}} U_{2^n}$, то $\mathbb{Q}(\alpha) = K = U_{2^n}$.

6. По модулю 7 двойка не подходит: $2^3 \equiv 1 \pmod 7$, а тройка подходит: $3^2, 3^3 \not\equiv 1 \pmod 7$. По модулям 11 и 13 двойка подходит: $2^2, 2^5 \not\equiv 1 \pmod{11}$ и $2^2, 2^3 \not\equiv 1 \pmod{13}$.

7. Если по модулю простого $p = 2^{2^m} + 1$ нет первообразного корня, то $a^{(p-1)/2} = a^{2^{2^m-1}} \equiv 1$ для всех $a \in \mathbb{Z}_p \setminus 0$. Это означает, что многочлен $x^{(p-1)/2} - 1$ имеет в поле $\mathbb{Z}_p$ вдвое больше корней, чем его степень. Противоречие.

8. Поскольку $\theta_{000} = c_1 > c_4 = \theta_{001}$ и $c_2 > c_8$, то $\theta_{00} = c_1 + c_4 > c_2 + c_8 = \theta_{01}$ и в формулах для периодов θ_{00} и θ_{000} следует выбрать знак $+$.

9. Имеем:

$$\begin{aligned}\theta_0\theta_1 &= (\varepsilon + \varepsilon^2 + \varepsilon^4)(\varepsilon^3 + \varepsilon^5 + \varepsilon^6) = \\ &= \varepsilon^4 + \varepsilon^6 + 1 + \varepsilon^5 + 1 + \varepsilon^8 + 1 + \varepsilon^9 + \varepsilon^{10} = \\ &= (\varepsilon + \varepsilon^2 + \varepsilon^3 + \varepsilon^4 + \varepsilon^5 + \varepsilon^6) + 3 = 2,\end{aligned}$$

откуда θ_0, θ_1 — корни трёхчлена $x^2 + x + 2$, т. е. $\dfrac{-1 + \sqrt{-7}}{2}$. Далее,

$$\operatorname{Im}\theta_0 = \sin\frac{2\pi}{7} + \sin\frac{4\pi}{7} + \sin\frac{8\pi}{7} > 0,$$

поэтому $\theta_0 = \dfrac{-1 + i\sqrt{7}}{2}$ и $\theta_1 = \dfrac{-1 - i\sqrt{7}}{2}$.

Список литературы

[1] *Гаусс К. Ф.* Арифметические исследования. (Др. назв.: Труды по теории чисел.) М.: АН СССР, 1959.

[2] *Wantzel P. L.* Recherches sur les moyens de reconnaître si un Problème de Géométrie peut se résoudre avec la règle et le compas // Journal de Mathématiques Pures et Appliquées. 1837. Vol. 2. P. 366–372.

[3] *Аршинов М. Н.*, *Садовский Л. Е.* Грани алгебры. М.: Факториал пресс, 2008.

[4] *Бурда Ю.*, *Кадец Л.* Семнадцатиугольник и закон взаимности Гаусса // Математическое просвещение. Сер. 3. Вып. 17. М.: МЦНМО, 2013. С. 61–67.

[5] *Винберг Э. Б.* Курс алгебры. М.: МЦНМО, 2019.

[6] *Гиндикин С. Г.* Рассказы о физиках и математиках. М.: МЦНМО, 2018.

[7] *Канунников А. Л.* Магия комплексных чисел // Квант. 2017. № 5. С. 5–11, 51–52.

[8] *Канунников А. Л.* Алгебраические числа как векторы // Математическое просвещение. Сер. 3. Вып. 26. М.: МЦНМО, 2020. С. 111–142.

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

[10] *Кириченко В. А.* Построения циркулем и линейкой и теория Галуа. Летняя школа «Современная математика», 2005. http://www.mccme.ru/dubna/2005/material.htm

[11] *Клейн Ф.* Лекции о развитии математики в XIX столетии. Т. 1. М.: Наука, 1989.

[12] *Козлов П. Ю.*, *Скопенков А. Б.* В поисках утраченной алгебры: в направлении Гаусса (подборка задач) // Математическое просвещение. Сер. 3. Вып. 12. М.: МЦНМО, 2008. С. 127–143. (Обновляемый текст: https://arxiv.org/abs/0804.4357)

[13] *Литлвуд Дж.* Математическая смесь. М.: Наука, 1990.

[14] *Постников М. М.* Теория Галуа. М.: Факториал пресс, 2003.

[15] *Сафин А.* Программа для построения правильных многоугольников циркулем и линейкой // Московская математическая конференция школьников, 2008. http://www.mccme.ru/mmks/dec08/Safin.pdf

[16] *Хованский А. Г.* Построения циркулем и линейкой // Математическое просвещение. Сер. 3. Вып. 17. М.: МЦНМО, 2013. С. 42–60.

Андрей Леонидович Канунников, мехмат МГУ,
Московский центр фундаментальной и прикладной математики
andrew.kanunnikov@gmail.com