Еще одно доказательство из Книги: теорема Гаусса о разрешимости в радикалах

А. Скопенков, https://users.mccme.ru/skopenko/

Аннотация. Известно, что

$$\cos\frac{2\pi}{3}=-\frac{1}{2},\quad \cos\frac{2\pi}{4}=0,\quad \cos\frac{2\pi}{5}=\frac{\sqrt{5}-1}{4},$$

$$\cos\frac{2\pi}{6}=\frac{1}{2},\quad \cos\frac{2\pi}{8}=\frac{1}{\sqrt{2}}.$$

Как обобщить эти формулы на $\cos(2\pi/n)$?

Рассмотрим калькулятор с кнопками

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

Калькулятор вычисляет числа с абсолютной точностью и имеет неограниченную память. При делении на 0 он выдает ошибку. Калькулятор оперирует с вещественными числами и при извлечении квадратного корня из отрицательного числа выдает ошибку.

Теорема Гаусса. *Число* $\cos(2\pi/n)$ *можно получить на калькуляторе тогда и только тогда, когда* $n = 2^\alpha p_1 \dots p_l$, *где* $p_1, \dots, p_l$ *— различные простые числа вида* $2^{2^s} + 1$.

Будет приведено малоизвестное простое доказательство части «тогда» этой теоремы. Для понимания доказательства достаточно начальных сведений о многочленах, комплексных чисел и сравнениях по модулю. На простых примерах, свободных от технических деталей, мы познакомимся с отправными идеями теории Галуа.

Подготовительные задачи к лекции.

Вещественное число называется *вещественно построимым*, если его можно получить на калькуляторе (т.е. получить из 1 при помощи сложений, вычитаний, умножений, делений и извлечений квадратного корня из положительных чисел).

1. Число $\cos(2\pi/n)$ построимо для $n = 3, 4, 5, 6, 8, 10, 15$.

2. Если $\cos(2\pi/n)$ построимо, то $\cos(\pi/n)$ построимо.

3. Если $\cos(2\pi/n)$ и $\cos(2\pi/m)$ построимы и m, n взаимно просты, то $\cos(\pi/mn)$ построимо.

4. Если $(u + vi)^2 = a + bi$ и a, b построимы, то u, v построимы.

5. Решите систему уравнений (x, y, z, t — неизвестные, a, b, c, d известны):

(a) $\begin{cases} x + y + z + t = a \\ x + y - z - t = b \\ x - y + z - t = c \\ x - y - z + t = d \end{cases}$ (b) $\begin{cases} x + y + z + t = a \\ x + iy - z - it = b \\ x - y + z - t = c \\ x - iy - z + it = d \end{cases}$

6. Обозначим

$$\beta := \frac{1+i\sqrt{3}}{2} \quad \text{и} \quad T(x) := x+\beta x^3+\beta^2 x^9+\beta^3 x^{27}+\beta^4 x^{81}+\beta^5 x^{243}.$$

Докажите, что $T(x) \equiv \beta\, T(x^3) \mod x^7-1$.

ТЕОРЕМА ГАУССА О РАЗРЕШИМОСТИ В РАДИКАЛАХ

Сформулированную выше теорему Гаусса можно переформулировать в терминах *построимости циркулем и линейкой* правильных n-угольников.

То, что называлось построимостью, будем аккуратнее называть *вещественной построимостью*. Слово «построимость» будет обозначать *комплексную построимость*, определенную далее.

Например, вещественно построимы числа

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

Строго говоря, теорема Гаусса не дает настоящего решения проблемы вещественной построимости чисел $\cos(2\pi/n)$, поскольку неизвестно, какие числа вида $2^{2^s}+1$ являются простыми. Однако теорема Гаусса дает, например, быстрый алгоритм выяснения построимости числа $\cos(2\pi/n)$.

История этой знаменитой теоремы здесь не приводится, см. книгу С. Гиндикина. Часть «только тогда» доказана Ванцелем, поэтому «теорема Гаусса-Ванцеля» — более точное, но менее общепринятое название.

Теорема Гаусса интересна современному человеку как решение пробной задачи об *исследовании операций*.

Здесь будет приведено *малоизвестное простое элементарное доказательство теоремы Гаусса.* Оно получено из имеющегося в книге Г. Эдвардса «Теория Галуа» некоторым упрощением.

Edwards H. M. Galois Theory. Springer Verlag, 1984.

Комплексный калькулятор имеет те же кнопки, что и определенный выше вещественный, но оперирует с комплексными числами и при нажатии кнопки $\sqrt{}$ выдает оба значения корня. На (комплексном или вещественном) калькуляторе можно получить число, если на нем можно получить *множество* чисел, содержащих заданное число.

Комплексное число называется **построимым**, если его можно получить на комплексном калькуляторе.

Лемма о комплексификации. *(a) Число* $\cos(2\pi/n)$ *построимо тогда и только тогда, когда число* $\varepsilon_n := \cos(2\pi/n) + i\sin(2\pi/n)$ *построимо.*
(b) Комплексное число построимо тогда и только тогда, когда его вещественная и мнимая части вещественно построимы.

Указание к доказательству. Часть «только тогда» в (a) очевидна.
Часть «только тогда» в (a) следует из равенства $2\cos(2\pi/n) = \varepsilon_n + \varepsilon_n^{-1}$.
Часть «тогда» в (b) очевидна.
(Заметим, что на калькуляторе нет кнопок *Re* и *Im*.)
Для доказательства части «только тогда» в (b) напишите $\sqrt{a+bi} = u + vi$ и выразите u, v через a и b с помощью четырех арифметических операций и квадратных радикалов.
QED

План доказательства построимости в теореме Гаусса

Лемма об умножении. *Если ε_n и ε_m построимы и m, n взаимно просты, то ε_{2n} и ε_{mn} построимы.*

Доказательство получается из формул $\varepsilon_{2n} \in \sqrt{\varepsilon_n}$ и $\varepsilon_{mn} = \varepsilon_m^x \varepsilon_n^y$, где x и y — целые числа, для которых $nx + my = 1$. QED

Доказательство построимости в теореме Гаусса. По леммам о комплексификации и об умножении достаточно доказать, что ε_n построимо для любого простого $n = 2^{2^s} + 1$. Так как $n - 1 = 2^m$, то по лемме об умножении ε_{n-1} построимо. Значит, построимость числа ε_n вытекает из следующей леммы. QED

Основная Лемма. *Если n простое, то из чисел 1 и $\beta := \varepsilon_{n-1}$ можно получить множество чисел, содержащее $\varepsilon := \varepsilon_n$, используя четыре арифметические операции и извлечения корней $(n-1)$-й степени (при которых получаются все $n-1$ значений корня).*

Идея доказательства построимости на примере числа $\varepsilon := \varepsilon_5$

Во-первых,

$$T_0 := \varepsilon + \varepsilon^2 + \varepsilon^4 + \varepsilon^8 = -1.$$

Сначала докажем построимость числа

$$T_2 := \varepsilon - \varepsilon^2 + \varepsilon^4 - \varepsilon^8.$$

При замене ε на ε^2 число T_2 переходит в $-T_2$. Значит, T_2^2 не меняется при этой замене. Поэтому T_2^2 не меняется при двукратной и трехкратной таких заменах, т. е. при заменах ε на ε^4 и ε на $\varepsilon^8 = \varepsilon^3$. Итак, для любого k число T_2^2 не меняется при замене ε на ε^k.

Раскроем скобки в произведении T_2^2 и заменим ε^5 на 1. Получим равенство

$$T_2^2 = a_0 + a_1\varepsilon + a_2\varepsilon^2 + a_3\varepsilon^3 + a_4\varepsilon^4 \quad \text{для некоторых} \quad a_k \in \mathbb{Z}.$$

Так как для любого k число T_2^4 не меняется при замене ε на ε^k, то $a_1 = a_2 = a_3 = a_4$. Поэтому $T_2^2 = a_0 - a_1 \in \mathbb{Z}$. Значит, T_2 построимо.

Обозначим

$$T_1 := \varepsilon + i\varepsilon^2 - \varepsilon^4 - i\varepsilon^8 \qquad \text{и} \qquad T_3 := \varepsilon - i\varepsilon^2 - \varepsilon^4 + i\varepsilon^8.$$

Тогда $T_0 + T_1 + T_2 + T_3 = 4\varepsilon$. Поэтому достаточно доказать построимость чисел T_1 и T_3. Сделаем это для T_1; доказательство для T_3 аналогично.
При замене ε на ε^2 число T_1 переходит в $-iT_1$. Значит, T_1^4 при этой замене не меняется. Поэтому T_1^4 не меняется при двукратной и трҷхкратной замене такого вида, т. е. при замене ε на ε^4 и ε на $\varepsilon^8 = \varepsilon^3$. Итак, для любого k число T_1^4 не меняется при замене ε на ε^k.
Раскроем скобки в произведении T_1^4 и заменим ε^5 на 1. Получим равенство

$$T_1^4 = a_0 + a_1\varepsilon + a_2\varepsilon^2 + a_3\varepsilon^3 + a_4\varepsilon^4 \quad \text{для некоторых} \quad a_k \in \mathbb{Z} + i\mathbb{Z}.$$

Так как для любого k число T_1^4 не меняется при замене ε на ε^k, то $a_1 = a_2 = a_3 = a_4$. Поэтому $T_1^4 = a_0 - a_1 \in \mathbb{Z} + i\mathbb{Z}$.
Значит, T_1 построимо.

Корректировка идеи: многочлены вместо чисел

В приведенных рассуждениях нужно обосновать корректность определения «замены ε на ε^k». Обоснование для общего случая трудное; читатель может найти пример такого рассуждения в §24 книги Эдвардса. Поэтому вместо того, чтобы его приводить, мы немного изменим доказательство; именно этим приводимое доказательство проще данного в книге Эдвардса. Вместо работы с *числами* мы будем работать с *многочленами* и подставлять в них ε в качестве аргумента. Два многочлена с комплексными коэффициентами называются *сравнимыми по модулю многочлена* p, если их разность делится (в $\mathbb{C}[x]$) на p.

Доказательство построимости числа $\varepsilon := \varepsilon_5$.
Определим многочлен $T_1(x) := x + ix^2 - x^4 - ix^8$. Определим многочлены $T_0(x)$, $T_2(x)$ и $T_3(x)$ формулами, аналогичными вышенаписанным. Как и выше, $(T_0 + T_1 + T_2 + T_3)(\varepsilon) = 4\varepsilon$. Поэтому достаточно доказать построимость каждого из чисел $T_r(\varepsilon)$, $r = 1, 2, 3$. Имеем

$$iT_1(x^2) \underset{x^5-1}{\equiv} T_1(x) \quad \Longrightarrow \quad T_1^4(x^2) \underset{x^5-1}{\equiv} T_1^4(x) \quad \Longrightarrow$$
$$\Longrightarrow \quad T_1^4(x^k) \underset{x^5-1}{\equiv} T_1^4(x) \quad \text{для любого } k.$$

Возьмем многочлен $a_0 + a_1x + a_2x^2 + a_3x^3 + a_4x^4$ с коэффициентами в $\mathbb{Z} + i\mathbb{Z}$, сравнимый с $T_1^4(x)$ по модулю $x^5 - 1$. Тогда $a_k = a_{2k \mod 5}$ для любого $k = 1, 2, 3, 4$. Значит, $a_1 = a_2 = a_4 = a_3$. Поэтому $T_1^4(\varepsilon) = a_0 - a_1 \in \mathbb{Z} + i\mathbb{Z}$. Значит, $T_1(\varepsilon)$ построимо. Аналогично $T_2(\varepsilon)$ и $T_3(\varepsilon)$ построимы. QED

Задача. (a) Решите подготовительную задачу 6.
(b) Приведите вычисление на комплексном калькуляторе числа ε_7, при котором извлекаются только корни второй и третьей степени. Сколько раз при этом извлекается корень третьей степени?
(c) Докажите, что на комплексном калькуляторе можно получить число ε_7 так, чтобы только один раз извлекать корень третьей степени и не извлекать корней большей степени.

Задача. Число ε_{17} построимо.
Указание. Обозначим

$$\beta := \varepsilon_{16} \quad \text{и} \quad T(x) := x + \beta x^6 + \beta^2 x^{36} + \beta^3 x^{216} + \ldots + \beta^{15} x^{6^{15}}.$$

Докажите, что $T(x) \underset{x^{17}-1}{\equiv} \beta T(x^6)$.

Теорема о первообразном корне

При доказательстве построимости числа ε_5 мы использовали различность остатков от деления чисел $2, 2^2, 2^3, 2^4$ на 5. При решении задачи Вы использовали аналогичное свойство чисел 3 и 7, 6 и 17. Для общего случая необходимо следующее обобщение.

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

Указание к доказательству для $p = 2^m + 1$ (только этот случай нужен для теоремы Гаусса). Если первообразного корня нет, то сравнение $x^{2^{m-1}} \underset{p}{\equiv} 1$ имеет $p - 1 = 2^m > 2^{m-1}$ решений. QED

Доказательство основной леммы для общего случая.
Обозначим через g первообразный корень по модулю n.
Обозначим

$$\mathbb{Z}[\beta] := \{b_0 + b_1\beta + b_2\beta^2 + \ldots + b_{n-2}\beta^{n-2} \ : \ b_0, b_1, \ldots, b_{n-2} \in \mathbb{Z}\}.$$

Для $r = 0, 1, 2, \ldots, n-2$ возьмем «резольвенту Лагранжа»

$$T_r(x) := x + \beta^r x^g + \beta^{2r} x^{g^2} + \ldots + \beta^{(n-2)r} x^{g^{n-2}} \in \mathbb{Z}[\beta][x].$$

$$\text{Тогда} \quad (T_0 + T_1 + \ldots + T_{n-2})(\varepsilon) = (n-1)\varepsilon.$$

Имеем $T_0(\varepsilon) = -1$. Поэтому достаточно доказать лемму с заменой ε на каждое из чисел $T_r(\varepsilon)$, $r = 1, 2, \ldots, n-2$.
Так как

$$\beta^r T_r(x^g) \underset{x^n-1}{\equiv} T_r(x), \quad \text{то} \quad T_r^{n-1}(x^g) \underset{x^n-1}{\equiv} T_r^{n-1}(x).$$

Возьмем многочлен $a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1}x^{n-1}$ с коэффициентами в $\mathbb{Z}[\beta]$, сравнимый с $T_r^{n-1}(x)$ по модулю $x^n - 1$. Тогда $a_1 = a_g = a_{g^2 \bmod n} = a_{g^3 \bmod n} = \ldots$. Значит, $a_1 = a_2 = \cdots = a_{n-1}$. Поэтому $T_r^{n-1}(\varepsilon) = a_0 - a_1 \in \mathbb{Z}[\beta]$.
Значит, лемма верна с заменой ε на $T_r(\varepsilon)$. QED

Задача для исследования. Для каких n число $\cos(2\pi/n)$
(a) рационально?
(b)* представимо в виде $a + \sqrt{b}$, где $a, b \in \mathbb{Q}$?
(c)* можно получить на вещественном калькуляторе, если разрешается извлекать корни *любых* степеней, а не только квадратные?

См. подробнее §9 (в бумажной версии §5) следующей книги. *Элементы математики в задачах: через олимпиады и кружки к профессии Сборник под редакцией А. Заславского, А. Скопенкова и М. Скопенкова. Изд-во МЦНМО, 2018.* `http://www.mccme.ru/circles/oim/materials/sturm.pdf`.