Когда косинус угла правильного n-угольника является квадратичной иррациональностью

Наталия Ленская

Утверждение. Число $\cos(2\pi/n)$ представимо в виде $a \pm \sqrt{b}$, где $a, b \in \mathbb{Q}$ тогда и только тогда, когда $n \in \{1; 2; 3; 4; 5; 6; 8; 10; 12\}$.

Доказываемое утверждение известно.

Гаусс и Ванцель нашли все n, при которых $\cos(2\pi/n)+i\sin(2\pi/n)$ и соответственно $\cos(2\pi/n)$, выражаются в квадратных радикалах (см., например, [S], [ZSS, \S9.2.5, \S9.4.4]). Приведенная версия, когда радикалов не более одного, не является частным случаем теоремы Гаусса-Ванцеля, но доказывается близким методом. Эта версия в чем-то более сложна, чем теорема Гаусса-Ванцеля, ибо требует неприводимости кругового многочлена Φ_n для произвольного n, а не только для $n = p^k$. В этом тексте приводится вывод утверждения из неприводимости кругового многочлена.

[S] A. Skopenkov, Yet another proof from the book: Gauss-Wantzel theorem (in Russian), Mat. Prosveschenie, 28 (2021), 133–141. `https://old.mccme.ru//free-books//matpros-28.html`

[ZSS] Элементы математики в задачах: через олимпиады и кружки к профессии, А. Заславский, А. Скопенков и М. Скопенков. Изд-во МЦНМО, 2017.
`http://www.mccme.ru/circles/oim/materials/sturm.pdf`

Лемма 1. При $n > 2$ существует такой неприводимый над $\mathbb{Q}$ многочлен $F_n(x)$ с рациональными коэффициентами степени $\varphi(n)/2$, что $F_n(\cos(\frac{2\pi}{n})) = 0$.

Доказательство. Обозначим через $\varepsilon_n = \cos(2\pi/n) + i\sin(2\pi/n)$, то есть корень n степени из единицы. Обозначим через $\Phi_n(x)$ многочлен с рациональными коэффициентами наименьшей степени, для которого ε_n является корнем. Я буду пользоваться следующим утверждением:

$$\deg \Phi_n(x) = \varphi(n) \text{ и } \Phi_n(x) = x^{\varphi(n)}\Phi_n(\frac{1}{x})^1$$

(то есть для любого целого положительного n последовательность коэффициентов многочлена $\Phi_n(x)$ симметрична; такие многочлены называют возвратными).

Пусть $n > 2$. Докажем, что тогда $\varphi(n)$ чётно. Действительно, k взаимно просто с n тогда и только тогда, когда $n-k$ взаимно просто с n, а также для четных n НОД$(n/2; n) = n/2 > 1$. Это задаёт разбиение чисел, взаимно простых с n, на пары. Значит, их количество, то есть $\varphi(n)$, чётно.

Определим многочлен $F_n(x)$ формулой $F_n(\frac{1}{2}(z + \frac{1}{z})) = \Phi_n(z)/z^{\varphi(n)/2}$. Такой многочлен существует и единственный в силу симметричности последовательности коэффициентов и того факта, что $a^k + b^k$ при $b = \frac{1}{a}$ выражается с рациональными коэффициентами через $(a + b)/2$ и $ab = 1$ по основной теореме о симметрических многочленах. Из этого также следует, что все коэффициенты многочлена рациональны. Покажем, что данный многочлен искомый.

Имеем $\cos(2\pi/n) = \frac{1}{2}(\varepsilon_n + \overline{\varepsilon_n}) = \frac{1}{2}(\varepsilon_n + \frac{1}{\varepsilon_n})$. Тогда $F_n(\cos(2\pi/n)) = F_n(\frac{1}{2}(\varepsilon_n + \frac{1}{\varepsilon_n})) = \Phi_n(\varepsilon_n)/\varepsilon_n^{\varphi(n)/2} = 0$, то есть мы получили, что $\cos(2\pi/n)$ является корнем этого многочлена.

[1] Доказательство этих утверждений приведено, например, в книге «Многочлены» Прасолова В.В.

Так как степень $\Phi_n(x)$ равна $\varphi(n)$, степень $F_n(x)$ равна $\varphi(n)/2$. В следующем абзаце покажем, что многочлен $F_n(x)$ неприводим над $\mathbb{Q}$.

Предположим противное. Пусть $F_n(x) = P(x)Q(x)$, где $P(x), Q(x) \in \mathbb{Q}[x]$. А также $\deg P = k < \varphi(n)/2 = \deg F_n$. Тогда

$$\Phi_n(x) = x^{\varphi(n)/2} F_n(\frac{1}{2}(x + \frac{1}{x})) = x^k P(\frac{1}{2}(x + \frac{1}{x})) \cdot x^{\varphi(n)/2-k} Q(\frac{1}{2}(x + \frac{1}{x})) = R(x)S(x)$$

для некоторых многочленов R, S с рациональными коэффициентами, что противоречит неприводимости над $\mathbb{Q}$ многочлена $\Phi_n(x)$. $\square$

Лемма 2. Множество чисел n таких, что $\varphi(n) \leqslant 4$, это $\{1; 2; 3; 4; 5; 6; 8; 10; 12\}$.

Доказательство. Как известно, $\varphi(n) = \prod_{p|n, p\in\mathbb{P}} (p-1)p^{\nu_p(n)-1}$, где $\nu_p(n)$ - степень вхождения простого p в n. Если $\varphi(n) \leqslant 4$, то n не имеет простых делителей больше 5. Если $5|n$, то $\varphi(n) \geqslant 5 - 1 = 4$, т.е. у $\varphi(n)$ нет иных отличных от 1 делителей, значит, $n \in \{5; 10\}$, $\varphi(5) = \varphi(10) = 4$, поэтому они оба подходят. Также так как $\varphi(n) < 6$, $\nu_3(n) < 2$. А в силу того, что $\varphi(n) < 8$, имеем $\nu_2(n) < 4$. Тогда все n такие, что $\varphi(n) \leqslant 4$ и $5 \nmid n$, лежат в множестве $\{1; 2; 3; 4; 6; 8; 12; 24; 48\}$. Имеем $\varphi(1) = 1$, $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(4) = 2$, $\varphi(5) = 4$, $\varphi(6) = 2$, $\varphi(8) = 4$, $\varphi(12) = 4$, $\varphi(24) = 8$, $\varphi(48) = 16$. Видно, что подходят все n, кроме 24 и 48. $\square$

Доказательство утверждения.

Если $n = 1$, то $\cos(2\pi/n) = \cos 2\pi = 1$, а если $n = 2$, то $\cos(2\pi/n) = \cos\pi = -1$. Таким образом, получаем, что $n = 1, 2$ подходят.

Теперь рассмотрим случай $n > 2$. Пусть $\cos(2\pi/n) = a \pm \sqrt{b}$, где $a, b \in \mathbb{Q}$. Рассмотрим многочлен $f(x) = (x - a - \sqrt{b})(x - a + \sqrt{b}) = (x - a)^2 - b \in \mathbb{Q}[x]$. Тогда заметим, что $f(\cos(2\pi/n)) = 0$. По лемме 1 $F_n(\cos(2\pi/n)) = 0$. Таким образом, мы нашли два многочлена над $\mathbb{Q}$, у которых есть общий корень. Поэтому степень их НОДа над $\mathbb{Q}$ больше нуля. Тогда так как $F_n(x)$ неприводим, то $F_n(x)$ делит $f(x)$. Следовательно $\varphi(n)/2 = \deg F_n(x) \leqslant \deg f(x) = 2$. Значит $\varphi(n) \leqslant 4$. Верно и обратное: если $\varphi(n) \leqslant 4$, то все корни многочлена $F_n(x)$ являются квадратичными иррациональностями (действительно, $F_n(x)$ — многочлен степени не выше второй; если $F_n(x) = ax + b$, то корень равен $-\frac{b}{a}$, а если $F_n(x) = ax^2 + bx + c$ при $a \neq 0$, то корни равны $-\frac{b}{2a} \pm \sqrt{\frac{b^2-4ac}{4a^2}}$). Но по лемме 2 множество всех n, функция Эйлера от которых не больше 4, — $\{1; 2; 3; 4; 5; 6; 8; 10; 12\}$. $\square$