# Теорема Гаусса о построении правильных многоугольников

# Заметка Гаусса 1 июня 1796 в немецкой газете

Всякому начинающему геометру известно, что можно геометрически (т. е. циркулем и линейкой) строить разные правильные многоугольники, а именно: треугольник, пятиугольник, пятнадцатиугольник и те, которые получаются из каждого из них путём последовательного удвоения числа его сторон. Это было известно во времена Евклида, и, как кажется, с тех пор было распространено убеждение, что дальше область элементарной геометрии не распространяется: по крайней мере, я не знаю удачной попытки распространить её в эту сторону. Тем более кажется мне заслуживающим внимания открытие, что, кроме этих правильных многоугольников, может быть геометрически построено множество других, например, семнадцатиугольник.

# Теорема Гаусса—Ванцеля

Правильный $n$-угольник можно построить с помощью циркуля и линейки тогда и только тогда, когда $n$ есть произведение степени двойки и различных простых чисел Ферма.

# Числа Ферма

$$F_k = 2^{2^k} + 1,\ k \in \mathbb{N}_0$$

| $k$ | $F_k$ |
|---|---|
| 0 | 3 |
| 1 | 5 |
| 2 | 17 |
| 3 | 257 |
| 4 | 65537 |

# Составное число Ферма

$$F_5 = 4294967297 = 641 \cdot 6700417$$

Леонард Эйлер, 1732 г.

# Из книги Дж. Литлвуда „Математическая смесь“

Один слишком навязчивый аспирант довёл своего руководителя до того, что тот сказал ему: «Идите и разработайте построение правильного многоугольника с 65537 сторонами». Аспирант удалился, чтобы вернуться через 20 лет с соответствующим построением

# Из статьи Гаусса

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.

# Числовые поля

Множество $\mathbb{C}$ комплексных чисел является **полем**: оно замкнуто относительно сложения, вычитания, умножения и деления (исключая деление на 0).

Всякое подмножество в $\mathbb{C}$ с тем же свойством и содержащее числа 0 и 1 называется **числовым полем.**

Примеры: $\mathbb{Q} \subset \ldots \subset \mathbb{R} \subset \mathbb{C}$

$\mathbb{N}, \mathbb{Z}, (0, \infty)$ не поля

# Присоединение $\sqrt{2}$

Найдём наименьшее поле, содержащее $\sqrt{2}$, т. е. замкнём множество

$$\mathbb{Q} \cup \{\sqrt{2}\}$$

относительно четырёх арифметических действий.

# Присоединение $\sqrt{2}$: этап I

Замкнём $\mathbb{Q} \cup \{\sqrt{2}\}$ относительно умножения:

$$\mathbb{Q} \cup \mathbb{Q}\sqrt{2}$$

# Присоединение $\sqrt{2}$: этап II

Замкнём $\mathbb{Q} \cup \mathbb{Q}\sqrt{2}$ относительно сложения:

$$\mathbb{Q} + \mathbb{Q}\sqrt{2} = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$$

Это множество замкнуто относительно сложения, вычитания и деления.

# Присоединение $\sqrt{2}$: этап III

Оказывается, $\mathbb{Q} + \mathbb{Q}\sqrt{2}$ замнкуто также относительно деления:

$$\frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{a^2 - 2b^2},$$

$$(0, 0) \neq (a, b) \in \mathbb{Q} \times \mathbb{Q}$$

Обозначение: $\mathbb{Q}(\sqrt{2}) = \mathbb{Q} + \mathbb{Q}\sqrt{2}$.

# Квадратичные расширения

Пусть $K$ — поле, $d \in K$, но $\sqrt{d} \notin K$. Тогда

$$\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} \mid a, b \in K\}$$

# Квадратичные расширения

Пусть $L$ — *расширение* поля $K$ размерности 2, т.е. $L$ — поле, отличное от $K$ и

$$L = \{a + b\alpha \mid a, b \in K\}$$

для всех $\alpha \in L \setminus K$. Тогда

$$L = K(\sqrt{d})$$

для некоторого $d \in K$.

# Построение правильного 17-угольника

сводится к построению цепочки квадратичных расширений

$$\mathbb{Q} \subset \mathbb{Q}(\alpha) \subset \mathbb{Q}(\alpha)(\beta) \subset \mathbb{Q}(\cos \tfrac{2\pi}{17})$$

# Присоединение $\sqrt[3]{2}$

Замкнём $\mathbb{Q} \cup \{\sqrt[3]{2}\}$ относительно сложения, вычитания и умножения:

$$\mathbb{Q} + \mathbb{Q}\sqrt[3]{2} + \mathbb{Q}\sqrt[3]{4} =$$

$$= \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q}\}$$

# Присоединение $\sqrt[3]{2}$

$$\frac{1}{a + b\sqrt[3]{2} + c\sqrt[3]{4}} = A + B\sqrt[3]{2} + C\sqrt[3]{4}$$

$$\mathbb{Q} \ni A, B, C = ?$$

Пример: $\dfrac{1}{\sqrt[3]{4}+\sqrt[3]{2}+3}$

$$f(x) = x^3 - 2 = (x^2 + x + 3)(x - 1) - 2x + 1$$
$$g(x) = x^2 + x + 3 = (2x - 1)\left(\tfrac{1}{2}x + \tfrac{3}{4}\right) + \tfrac{15}{4}$$

$$\begin{aligned}\tfrac{15}{4} &= g(x) - (g(x)(x-1) - f(x))\left(\tfrac{1}{2}x + \tfrac{3}{4}\right) = \\ &= f(x)\left(\tfrac{1}{2}x + \tfrac{3}{4}\right) + g(x)\left(-\tfrac{1}{2}x^2 - \tfrac{1}{4}x + \tfrac{7}{4}\right)\end{aligned}$$

$$\frac{1}{\sqrt[3]{4}+\sqrt[3]{2}+3} = -\frac{2\sqrt[3]{4}+\sqrt[3]{2}-7}{15}$$

# Сопряжённые числа

Числа $a + b\sqrt{2}$ и $a - b\sqrt{2}$ $(a, b \in \mathbb{Q},\ b \neq 0)$ — сопряжённые квадратичные иррациональности.

А какие сопряжённые у числа $a + b\sqrt[3]{2}$?

# Алгебраические числа

Число $\alpha \in \mathbb{C}$ называется **алгебраическим,** если оно является корнем некоторого ненулевого многочлена с рациональными коэффициентами:

$$\alpha \in \mathbb{A} \iff \exists f \in \mathbb{Q}[x] \setminus \{0\}\ f(\alpha) = 0.$$

# Минимальный многочлен

$\mu_\alpha(x) = x^n + \ldots$ — многочлен наименьшей степени над $\mathbb{Q}$ с корнем $\alpha$. Он неприводим, т. е. не раскладывается в произведение многочленов меньшей степени

$$\boxed{\mathbb{Q}(\alpha) = \{a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1} \mid a_0, \ldots, a_{n-1} \in \mathbb{Q}\}}$$

— поле и векторное пространство над $\mathbb{Q}$ с базисом $1, \alpha, \ldots, \alpha^{n-1}$

# Сопряжённые числа

— это корни одного неприводимого над $\mathbb{Q}$ многочлена:

$$\mu_\alpha(x) = (x - \alpha_1)\dots(x - \alpha_n) \iff$$

$$\iff \alpha_1, \dots, \alpha_n \text{ — сопряжённые к } \alpha$$

Например,

$$\{\sqrt[3]{2}, \sqrt[3]{2}\varepsilon, \sqrt[3]{2}\varepsilon^2\}, \text{ где } \varepsilon = \tfrac{-1+i\sqrt{3}}{2} \in \sqrt[3]{1}.$$

Это набор корней двучлена $x^3 - 2$, неприводимого над $\mathbb{Q}$.

## Сопряжённые к числу $a + b\sqrt[3]{2} + c\sqrt[3]{4},\ a, b, c \in \mathbb{Q}$

$$a + b\sqrt[3]{2} + c\sqrt[3]{4}$$

$$a + b\sqrt[3]{2}\varepsilon + c\sqrt[3]{4}\varepsilon^2$$

$$a + b\sqrt[3]{2}\varepsilon^2 + c\sqrt[3]{4}\varepsilon$$

# Сопряжённые к числу $f(\alpha)$

Пусть $\alpha \in \mathbb{A}$, $f(x) \in \mathbb{Q}[x]$. Тогда сопряжённые к числу $f(\alpha)$:

$$f(\alpha_1), \ldots, f(\alpha_n),$$

где $\alpha_1, \ldots, \alpha_n$ — сопряжённые к $\alpha$.

# Круговое поле $\mathbb{Q}(\varepsilon)$, $\varepsilon = \varepsilon_{17} = \cos\frac{2\pi}{17} + i\sin\frac{2\pi}{17}$

$$\mu_\varepsilon(x) = \frac{x^{17}-1}{x-1} = x^{16} + x^{15} + \ldots + x + 1$$

— неприводимый над $\mathbb{Q}$ многочлен

Наша задача — построить цепочку квадратичных расширений

$$\mathbb{Q} \subset \mathbb{Q}(\alpha) \subset \mathbb{Q}(\alpha)(\beta) \subset \mathbb{Q}(\cos\tfrac{2\pi}{17}) \subset \mathbb{Q}(\varepsilon)$$

# Как найти $\alpha$?

$$\alpha = a_0 + a_1\varepsilon + a_2\varepsilon^2 + \ldots + a_{15}\varepsilon^{15},\ a_0, \ldots, a_{15} \in \mathbb{Q}$$

Его сопряжённые:

$$\begin{aligned}
\alpha_1 &= a_0 + a_1\varepsilon + a_2\varepsilon^2 + \ldots + a_{15}\varepsilon^{15} \\
\alpha_2 &= a_0 + a_1\varepsilon^2 + a_2\varepsilon^4 + \ldots + a_{15}\varepsilon^{30} \\
\alpha_3 &= a_0 + a_1\varepsilon^3 + a_2\varepsilon^6 + \ldots + a_{15}\varepsilon^{45} \\
&\ldots \\
\alpha_{16} &= a_0 + a_1\varepsilon^{16} + a_2\varepsilon^{32} + \ldots + a_{15}\varepsilon^{240}
\end{aligned}$$

Сколько среди них должно быть разных?

# Сменим базис!

Расположим степени $\varepsilon$, чтобы каждая следующая была (одной и той же) степенью предыдущей, например, так:

$$\varepsilon, \varepsilon^2, \varepsilon^4, \varepsilon^8, \ldots$$

Подходит?

# Первообразный корень по модулю 17: 3

$$\mathbb{Z}_{17}^{*} = \{1, 3, 3^2, \ldots, 3^{15}\}$$

$$\{\varepsilon, \varepsilon^2, \varepsilon^3, \ldots, \varepsilon^{16}\} =$$

$$= \{\varepsilon, \varepsilon^3, \varepsilon^{3^2}, \ldots, \varepsilon^{3^{15}}\}$$

# Как найти $\alpha$? Вторая попытка

$$\alpha = a_0\varepsilon + a_1\varepsilon^3 + a_2\varepsilon^{3^2} + \ldots + a_{15}\varepsilon^{3^{15}},\ a_0, \ldots, a_{15} \in \mathbb{Q}$$

Его сопряжённые:

$$\alpha_0 = a_0\varepsilon + a_1\varepsilon^3 + a_2\varepsilon^{3^2} + \ldots + a_{15}\varepsilon^{3^{15}}$$

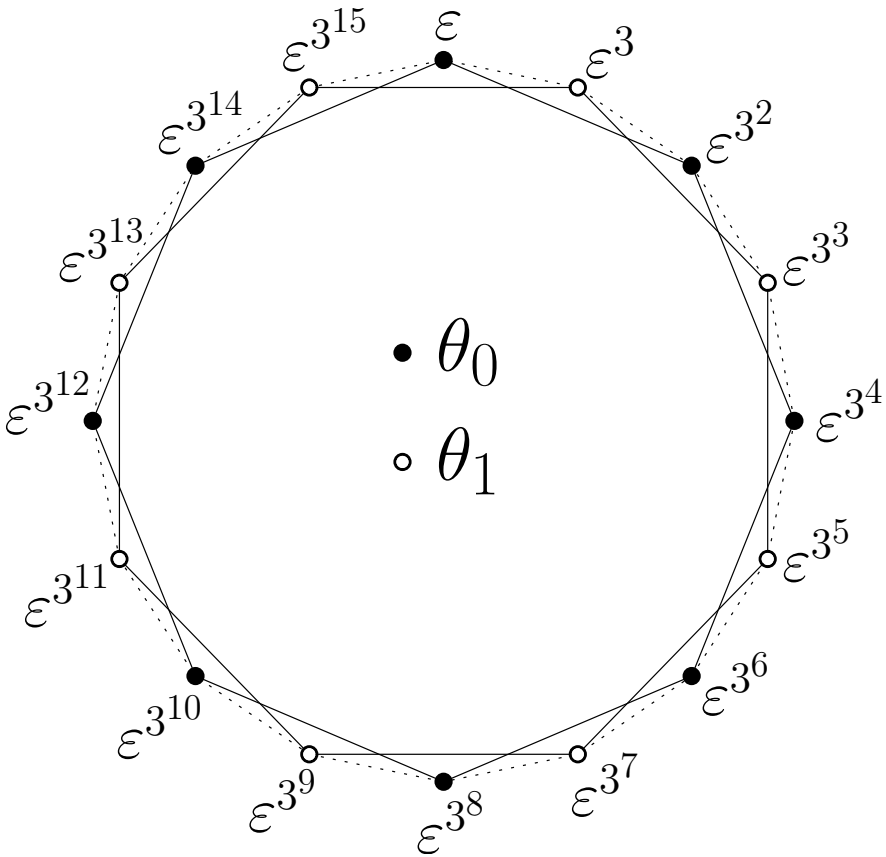
$$\alpha_1 = a_0\varepsilon^3 + a_1\varepsilon^{3^2} + a_2\varepsilon^{3^3} + \ldots + a_{15}\varepsilon$$

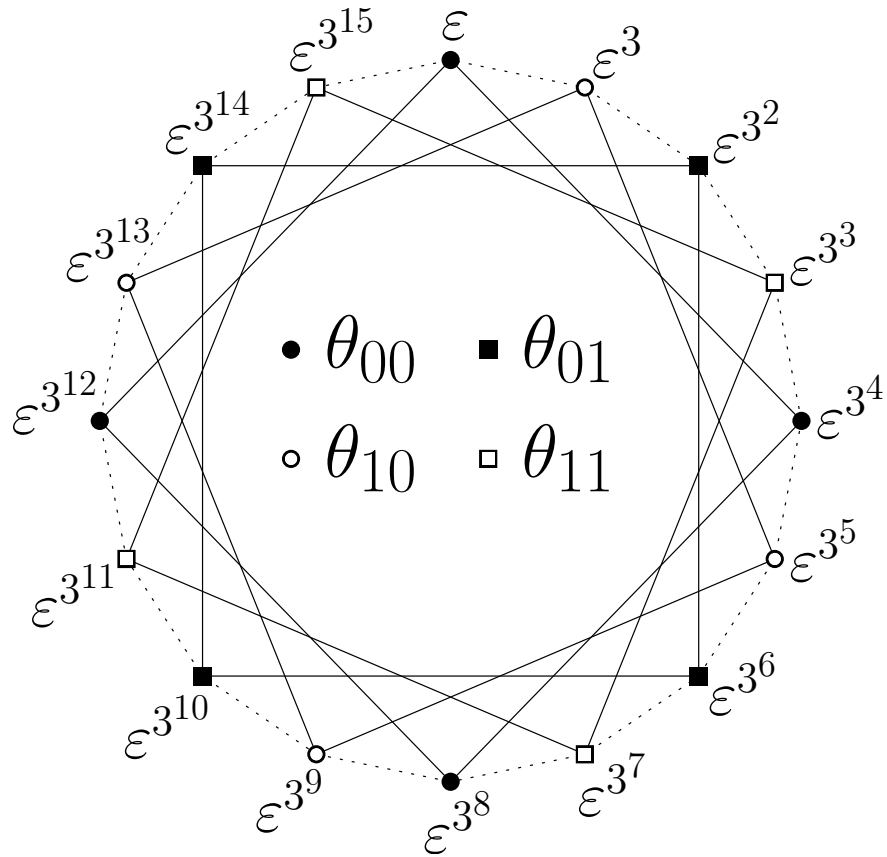
$$\alpha_2 = a_0\varepsilon^{3^2} + a_1\varepsilon^{3^3} + a_2\varepsilon^{3^4} + \ldots + a_{15}\varepsilon^3$$

$$\ldots$$

$$\alpha_{15} = a_0\varepsilon^{3^{15}} + a_1\varepsilon + a_2\varepsilon^3 + \ldots + a_{15}\varepsilon^{3^{14}}$$

# 2-периоды и 4-периоды Гаусса для $p = 17$



Сопряжённые $\alpha_j = \sum\limits_{k\in\mathbb{Z}_{16}} a_k \varepsilon^{3^{j+k}} \in \mathbb{Q}(\varepsilon_{17})$, $j \in \mathbb{Z}_{16}$

$$(0)\ \alpha_0 = \alpha_1 \iff a_0 = a_1 = \ldots = a_{15} \iff \deg\alpha = 1$$

$$(1)\ \alpha_0 = \alpha_2 \iff \begin{cases} a_0 = a_2 = \ldots = a_{14} \\ a_1 = a_3 = \ldots = a_{15} \end{cases} \iff \deg\alpha \in \{1, 2\}$$

$$(2)\ \alpha_0 = \alpha_4 \iff \begin{cases} a_0 = a_4 = a_8 = a_{12} \\ a_1 = a_5 = a_9 = a_{13} \\ a_2 = a_6 = a_{10} = a_{14} \\ a_3 = a_7 = a_{11} = a_{15} \end{cases} \iff \deg\alpha \in \{1, 2, 4\}$$

$$(3)\ \alpha_0 = \alpha_8 \iff \begin{cases} a_0 = a_8, \quad a_4 = a_{12} \\ a_1 = a_9, \quad a_5 = a_{13} \\ a_2 = a_{10}, \quad a_6 = a_{14} \\ a_3 = a_{11}, \quad a_7 = a_{15} \end{cases} \iff \deg\alpha \in \{1, 2, 4, 8\}$$

# Базисы в подполях башни

$\mathbb{Q} = K_0 \xrightarrow{2} K_1 \xrightarrow{2} K_2 \xrightarrow{2} K_3 \xrightarrow{2} K_4 = \mathbb{Q}(\varepsilon)$ при $p = 17$

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| $\theta_\varnothing = \varepsilon + \varepsilon^3 + \varepsilon^{3^2} + \varepsilon^{3^3} + \ldots + \varepsilon^{3^{15}} = -1$ | | | | | | | |
| $\theta_0 = \varepsilon + \varepsilon^{3^2} + \varepsilon^{3^4} + \ldots + \varepsilon^{3^{14}}$ | | | | $\theta_1 = \varepsilon^3 + \varepsilon^{3^3} + \varepsilon^{3^5} + \ldots + \varepsilon^{3^{15}}$ | | | |
| $\underbrace{\varepsilon + \varepsilon^{3^4} + \varepsilon^{3^8} + \varepsilon^{3^{12}}}_{\theta_{00}}$ | | $\underbrace{\varepsilon^{3^2} + \varepsilon^{3^6} + \varepsilon^{3^{10}} + \varepsilon^{3^{14}}}_{\theta_{01}}$ | | $\underbrace{\varepsilon^3 + \varepsilon^{3^5} + \varepsilon^{3^9} + \varepsilon^{3^{13}}}_{\theta_{10}}$ | | $\underbrace{\varepsilon^{3^3} + \varepsilon^{3^7} + \varepsilon^{3^{11}} + \varepsilon^{3^{15}}}_{\theta_{11}}$ | |
| $\underbrace{\varepsilon + \varepsilon^{3^8}}_{\theta_{000}=c_1}$ | $\underbrace{\varepsilon^{3^4} + \varepsilon^{3^{12}}}_{\theta_{001}=c_4}$ | $\underbrace{\varepsilon^{3^2} + \varepsilon^{3^{10}}}_{\theta_{010}=c_8}$ | $\underbrace{\varepsilon^{3^6} + \varepsilon^{3^{14}}}_{\theta_{011}=c_2}$ | $\underbrace{\varepsilon^3 + \varepsilon^{3^9}}_{\theta_{100}=c_3}$ | $\underbrace{\varepsilon^{3^5} + \varepsilon^{3^{13}}}_{\theta_{101}=c_5}$ | $\underbrace{\varepsilon^{3^3} + \varepsilon^{3^{11}}}_{\theta_{110}=c_7}$ | $\underbrace{\varepsilon^{3^7} + \varepsilon^{3^{15}}}_{\theta_{111}=c_6}$ |
| $\varepsilon$ \| $\varepsilon^{3^8}$ | $\varepsilon^{3^4}$ \| $\varepsilon^{3^{12}}$ | $\varepsilon^{3^2}$ \| $\varepsilon^{3^{10}}$ | $\varepsilon^{3^6}$ \| $\varepsilon^{3^{14}}$ | $\varepsilon^3$ \| $\varepsilon^{3^9}$ | $\varepsilon^{3^5}$ \| $\varepsilon^{3^{13}}$ | $\varepsilon^{3^3}$ \| $\varepsilon^{3^{11}}$ | $\varepsilon^{3^7}$ \| $\varepsilon^{3^{15}}$ |

$K_1 = \mathbb{Q}(\theta_0) = \mathbb{Q}(\theta_1)$

$K_2 = \mathbb{Q}(\theta_{00}) = \mathbb{Q}(\theta_{01}) = \mathbb{Q}(\theta_{10}) = \mathbb{Q}(\theta_{11})$

$K_3 = \mathbb{Q}(\theta_{000}) = \ldots = \mathbb{Q}(\theta_{111})$, $\varepsilon = e^{\frac{2\pi i k}{17}} \Rightarrow \theta_{000} = 2\cos\frac{2\pi k}{17}$

$K_4 = \mathbb{Q}(\varepsilon^{3^k}), \forall k$

# Построение правильного 17-угольника: шаг 1

$$\theta_0 + \theta_1 = -1$$

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

$$= \underline{\varepsilon^{3+3^2} + \varepsilon^{3^3+3^4} + \ldots + \varepsilon^{3^{15}+3^{16}}} +$$

$$+ \varepsilon^{3+3^4} + \varepsilon^{3^3+3^6} + \ldots + \varepsilon^{3^{15}+3^2} +$$

$$+ \ldots +$$

$$+ \varepsilon^{3+3^{14}} + \varepsilon^{3^3+3^{16}} + \ldots + \varepsilon^{3^{15}+3^{12}} +$$

$$+ \underline{\varepsilon^{3+3^{16}} + \varepsilon^{3^3+3^2} + \ldots + \varepsilon^{3^{15}+3^{14}}} =$$

$$= -4$$

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

# Построение правильного 17-угольника: шаг 2

$$\theta_{00} + \theta_{01} = \theta_0$$

$$\begin{aligned}
\theta_{01}\theta_{00} &= (\varepsilon^{3^2} + \varepsilon^{3^6} + \varepsilon^{3^{10}} + \varepsilon^{3^{14}})(\varepsilon^{3^4} + \varepsilon^{3^8} + \varepsilon^{3^{12}} + \varepsilon^{3^{16}}) \\
&= \underline{\varepsilon^{3^2+3^4} + \varepsilon^{3^6+3^8} + \varepsilon^{3^{10}+3^{12}} + \varepsilon^{3^{14}+3^{16}}} + \\
&+ \varepsilon^{3^2+3^8} + \varepsilon^{3^6+3^{12}} + \varepsilon^{3^{10}+3^{16}} + \varepsilon^{3^{14}+3^4} + \\
&+ \varepsilon^{3^2+3^{12}} + \varepsilon^{3^6+3^{16}} + \varepsilon^{3^{10}+3^4} + \varepsilon^{3^{14}+3^8} + \\
&+ \underline{\varepsilon^{3^2+3^{16}} + \varepsilon^{3^6+3^4} + \varepsilon^{3^{10}+3^8} + \varepsilon^{3^{14}+3^{12}}} = \\
&= \underline{\theta_1} + \theta_0 = -1.
\end{aligned}$$

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

# Другой способ — тригонометрический

$$c_k := \varepsilon^k + \varepsilon^{-k} \text{ — удвоенные косинусы}$$

$$c_k c_l = c_{k+l} + c_{k-l},\ k, l \in \mathbb{Z}_{17}.$$

$$c_k = c_{17-k}$$

$$\begin{aligned}
\theta_{01}\theta_{00} &= (c_1 + c_4)(c_2 + c_8) = \\
&= c_1 c_2 + c_1 c_8 + c_4 c_2 + c_4 c_8 = \\
&= c_1 + c_3 + c_7 + c_8 + c_2 + c_6 + c_4 + c_5 = \\
&= -1.
\end{aligned}$$

# Построение правильного 17-угольника: шаг 3

$$c_1 = \theta_{000},\ c_4 = \theta_{001};\quad c_1 + c_4 = \theta_{00}$$

$$c_1 c_4 = c_3 + c_5 = \theta_{10}$$

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

# Построение правильного 17-угольника: шаг 3

$$\begin{aligned}
\theta_{10}\theta_{00} &= (c_1 + c_4)(c_3 + c_5) = \\
&= c_2 + c_4 + c_4 + c_6 + c_1 + c_7 + c_1 + c_9 = \\
&= 2\theta_{00} + \theta_{01} + \theta_{11} = -1 + \theta_{00} - \theta_{10} \Longrightarrow \\
&\Longrightarrow \ \theta_{10} = \frac{\theta_{00} - 1}{\theta_{00} + 1}
\end{aligned}$$

# Построение правильного 17-угольника: всё вместе

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

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

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

$$\theta_{10} = \frac{\theta_{00} - 1}{\theta_{00} + 1}$$

# 2-периоды Гаусса

- $p$ — любое нечётное простое число, $\mathbb{Z}_p^* = \langle g \rangle$;
- $Q = \langle g^2 \rangle$ — группа квадратичных вычетов по модулю $p$ ($\mathbb{Z}_p^* = Q \sqcup gQ$);
- $\varepsilon = \varepsilon_p \in K$, где $K$ — поле, $\operatorname{char} K \neq p$;
- $\theta_0 = \sum\limits_{k \in Q} \varepsilon^k$, $\theta_1 = \sum\limits_{k \in gQ} \varepsilon^k$ — 2-периоды Гаусса ($\theta_0 + \theta_1 = -1$).
- $S = \sum\limits_{j \in \mathbb{Z}_p} \varepsilon^{j^2} = 2\theta_0 + 1$,
- $S_a = \sum\limits_{j \in \mathbb{Z}_p} \varepsilon^{aj^2}$, где $a \in \mathbb{Z}_p^*$.

# 2-периоды Гаусса

$$S_a = \begin{cases} 2\theta_0 + 1 = S, & \text{если } a \in Q, \\ 2\theta_1 + 1 = -S, & \text{если } a \notin Q, \end{cases}$$

$$\boxed{S_a = \left(\frac{a}{p}\right) S}$$

# 2-периоды Гаусса

$$S^2 = \begin{cases} p, & \text{если } p \equiv 1 \pmod 4, \text{ в частности, } \sqrt{p} \in K(\varepsilon), \\ -p, & \text{если } p \equiv -1 \pmod 4, \text{ в частности, } \sqrt{-p} \in K(\varepsilon) \end{cases}$$

$$SS_{-1} = \sum_{i,j \in \mathbb{Z}_p} \varepsilon^{i^2 - j^2}$$

Коэффициент при $\varepsilon^k$:

$$\left|\{(i,j) \in \mathbb{Z}_p \times \mathbb{Z}_p \mid i^2 - j^2 = k\}\right| =$$

$$= \left|\{(a,b) \in \mathbb{Z}_p \times \mathbb{Z}_p \mid ab = k\}\right| = \begin{cases} p-1, & k \neq 0, \\ 2p-1, & k = 0, \end{cases}$$

$$\Longrightarrow \quad SS_{-1} = 2p - 1 + (p-1) \sum_{l=1}^{p-1} \varepsilon^l = p.$$

# 2-периоды Гаусса

$$\{\theta_0, \theta_1\} = \begin{cases} \dfrac{-1 \pm \sqrt{p}}{2}, & \text{если } p \equiv \quad 1 \pmod 4, \\ \dfrac{-1 \pm \sqrt{-p}}{2}, & \text{если } p \equiv -1 \pmod 4. \end{cases}$$

# Квадратичный закон взаимности Гаусса

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \quad \text{при различных простых} \quad p, q \geqslant 3,$$

В поле $K = \mathbb{Z}_q(\varepsilon)$: $S^q = S_q = \left(\frac{q}{p}\right) S$, поэтому

$S^q = S \Leftrightarrow \left(\frac{q}{p}\right) = 1$. С другой стороны, $S^q = S \Leftrightarrow S \in \mathbb{Z}_q$. Это равносильно следующему:

- при $p \equiv 1 \pmod 4$: $\sqrt{p} \in Q \Leftrightarrow \left(\frac{p}{q}\right) = 1$;
- при $p \equiv -1 \pmod 4$:
  $\sqrt{-p} \in Q \Leftrightarrow \left(\frac{-p}{q}\right) = 1 \Leftrightarrow (-1)^{\frac{q-1}{2}} \left(\frac{p}{q}\right) = 1$