Семнадцатиугольник и закон взаимности Гаусса

Бурда Ю. Кадец Л.

В этой заметке обсуждается как построить семнадцатиугольник при помощи циркуля и линейки и как данное построение связано с квадратичным законом взаимности Гаусса.

1. Введение

Теория Галуа позволяет дать полный ответ на вопрос о возможности построения правильного n-угольника с помощью циркуля и линейки:

Теорема 1. *Правильный n-угольник можно построить циркулем и линейкой если и только если n имеет вид $n = 2^m \cdot p_1 \cdot \ldots \cdot p_k$, где $p_1, \ldots, p_k$ — различные простые числа вида $2^{2^s} + 1$.*

К сожалению теория Галуа позволяет лишь судить о возможности того или иного построения и подсказывает некоторые шаги на пути к нему, но явное построение приходится находить отдельно в каждом конкретном случае.

Тем более удивительно, что построение семнадцатиугольника с помощью циркуля и линейки было придумано *до* появления теории Галуа. Первым это построение нашёл Гаусс в конце восемнадцатого века, спустя много столетий после того как правильные 3-, 4-, 5-, 6-, 8-, 10-, 12-, 15- и 16-угольники были построены древними геометрами.

В этой заметке представлен способ построения правильного 17-угольника. Описание построения не использует никаких идей, которые не были известны в то время, когда Гаусс его придумал. Увы, некоторые действия в этом построении выглядят несколько загадочно и могут быть куда лучше поняты в свете более общей теории. Объяснения такого рода даны в замечаниях 1 и 2. В замечании 3 мы объясняем связь построения 17-угольника с другими работами Гаусса, а именно, с квадратичным законом взаимности.

Благодарности. Мы благодарим Аскольда Георгиевича Хованского, чьи замечательные лекции по теории Галуа вдохновили нас задуматься о построении 17-угольника. Мы также благодарим Бориса Кадеца, который

сообщил нам нескольких крайне красивых доказательств квадратичного закона взаимности.

2. План построения

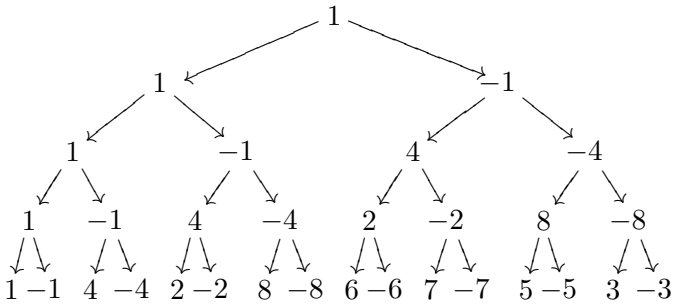
Если отождествить плоскость $\mathbb{R}^2$ с плоскостью комплексных чисел $\mathbb{C}$ (с отмеченными точками 0 и 1), то задача о построении правильного n-угольника переходит в задачу о построении примитивного корня из единицы ξ степени n (например $\xi = e^{2\pi i/n}$). Действительно, если это число построено, то его степени являются вершинами правильного n-угольника.

В дальнейшем мы будем часто использовать следующее построение: если числа z_1 и z_2 являются решениями квадратного уравнения $z^2+az+b = 0$, и точки a и b уже построены, то точки z_1 и z_2 можно построить циркулем и линейкой. Это построение основывается на формуле для решений квадратного уравнения, в которой присутствуют лишь операции сложения, вычитания, умножения, деления и извлечения квадратного корня. Все эти операции с уже построенными точками можно выполнить с помощью циркуля и линейки.

Наш план тогда сводится к нахождению явных квадратных уравнений со следующими свойствами:

- первое из этих уравнений имеет целочисленные коэффициенты;
- коэффициенты каждого из уравнений либо целые числа, либо (с точностью до знака) совпадают с корнями предыдущего уравнения;
- число ξ является одним из решений последнего уравнения.

Эти уравнения будут продвигать нас вниз по следующей диаграмме:



Стрелки в этом дереве ведут от чисел к их квадратным корням по модулю 17.

С каждым узлом дерева мы свяжем число $\sum_i \xi^i$, где суммирование производится по набору тех чисел i из самого нижнего ряда, до которых можно добраться по стрелкам из данного узла.

Ниже мы покажем, что числа, связанные с узлами в каждой строке, удовлетворяют квадратным уравнениям с коэффициентами, которые являются либо целыми числами, либо (с точностью до знака) числами, связанными с узлами предыдущей строки.

Замечание 1. Минимальным уравнением над полем $\mathbb{Q}$, которому удовлетворяет примитивный корень из единицы ξ простой степени p, является уравнение $1 + x + \ldots + x^{p-1} = 0$. Его группа Галуа — циклическая группа $G = \mathbb{Z}_p^*$. Для каждого делителя d числа $p - 1$ эта группа содержит единственную подгруппу порядка d. В частности если $p = 2^k + 1$, подгруппы группы G образуют башню $G = G_k \supset G_{k-1} \supset \ldots \supset G_0 = \{1\}$, где G_m имеет порядок 2^m. Соответствие Галуа сопоставляет этой башне подгрупп цепочку квадратичных расширений полей $\mathbb{Q}(\xi) = L_0 \supset L_1 \supset \ldots \supset L_k = \mathbb{Q}$.

Вычеты из m-й строки дерева составляют группу G_m. Числа $\sum\limits_{i \in G_m} \xi^i$, связанные с узлами диаграммы, порождают расширение $L_m/\mathbb{Q}$. Коэффициенты квадратного уравнения, которое мы находим на m-м шаге, находятся в поле L_{m-1}, а его корни порождают расширение L_m/L_{m-1}.

3. Шаг номер 0

Пусть $\xi \neq 1$ — корень из единицы степени p. Тогда

$$\sum_{i=1}^{p-1} \xi^i = \frac{\xi^p - \xi}{\xi - 1} = -1.$$

Таким образом, с корнем дерева связано число -1.

4. Первый шаг — квадратичные вычеты

Теорема 2. *Пусть Q — множество квадратичных вычетов по модулю нечётного простого числа p. Пусть ξ — примитивный корень из единицы степени p и пусть $x = \sum\limits_{i \in Q} \xi^i$.*

Для p вида $p = 4m + 1$ выполняется $x^2 + x - \dfrac{p-1}{4} = 0$.

Для p вида $p = 4m - 1$ выполняется $x^2 + x + \dfrac{p+1}{4} = 0$.

Замечание 2. Для любого нечётного простого p группа $\mathbb{Z}_p^*$ содержит единственную подгруппу индекса 2, а именно группу Q квадратичных вычетов по модулю p. Группа $\mathbb{Z}_p^*$ является группой Галуа расширения Галуа $\mathbb{Q}(\xi)/\mathbb{Q}$: элемент $m \in \mathbb{Z}_p^*$ действует автоморфизмом, переводящим ξ в ξ^m.

Орбита числа $x = \sum_{i \in Q} \xi^i$ при действии этой группы состоит из двух элементов. Таким образом, x является корнем некоторого квадратного уравнения с рациональными коэффициентами. Теорема 2 предоставляет явный вид этого уравнения.

Доказательство теоремы 2. Чтобы найти x, мы вычислим $y = \sum_{i=0}^{p-1} \xi^{i^2}$ и используем тождество $y = 2x - 1$. Комплексное сопряжение числа y равно $\overline{y} = \sum_{i=0}^{p-1} \xi^{-i^2}$, а значит,

$$y\overline{y} = \left(\sum_{i=0}^{p-1} \xi^{i^2}\right)\left(\sum_{i=0}^{p-1} \xi^{-j^2}\right) = \sum_{i,j=0}^{p-1} \xi^{i^2-j^2}.$$

Коэффициент при ξ^k в этой формуле равен количеству решений (i, j) сравнения $i^2 - j^2 \equiv k \mod p$. Обратимой заменой координат $(a, b) = (i - j, i + j)$ это сравнение переводится в сравнение $ab \equiv k \mod p$. У последнего сравнения $p - 1$ решений, если $k \neq 0$, и $2p - 1$ решений, если $k = 0$.

Таким образом,

$$y\overline{y} = 2p - 1 + (p - 1)\sum_{k=1}^{p-1} \xi^k = 2p - 1 - (p - 1) = p.$$

Если $p \equiv 1 \mod 4$, то $\overline{y} = y$. Действительно, так как -1 является квадратичным вычетом по модулю p, выражение $\sum_{i=0}^{p-1} \xi^{-i^2}$ не отличается от выражения $\sum_{i'=0}^{p-1} \xi^{i'^2}$.

Если $p \equiv -1 \mod 4$, то $\overline{y} = -y$. Действительно, так как -1 не является квадратичным вычетом по модулю p, в выражении $y + \overline{y}$ каждая степень ξ встречается ровно дважды. А значит, $y + \overline{y} = 2\sum_{k=0}^{p-1} \xi^k = 0$.

В обоих случаях окончательный результат следует из тождества $y = 2x - 1$.

Из теоремы следует, что числа, связанные с узлами во второй строке, являются решениями уравнения $x^2 + x - \frac{17-1}{4} = 0$, то есть $x_1, x_2 = \frac{-1 \pm \sqrt{17}}{2}$.

Замечание 3. Интересно заметить, что вычисление из доказательства теоремы 2 можно использовать для простого и элегантного доказательства квадратичного закона взаимности Гаусса.

Чтобы выяснить, является ли p квадратичным вычетом по модулю простого числа q, достаточно выяснить, принадлежит ли $\sqrt{p}$ полю $\mathbb{F}_q$ вычетов по модулю q.

Поле $\mathbb{F}_q$ состоит в точности из q корней уравнения $y^q = y$, так что элемент y расширения поля $\mathbb{F}_q$ находится в $\mathbb{F}_q$ в точности когда $y^q = y$.

Пусть, как и раньше, $y = \sum_{i=0}^{p-1} \xi^{i^2}$, где ξ — примитивный корень из единицы степени p, лежащий в некотором расширении поля $\mathbb{F}_q$.

Вычисление из доказательства теоремы 2 показывает, что если $p \equiv 1 \mod 4$, то $y = \sqrt{p}$ и находится в $\mathbb{F}_q$, если и только если $y^q = y$. Однако в расширениях поля $\mathbb{F}_q$ имеет место формула $(a+b)^q = a^q + b^q$, а значит, $y^q = \sum_{i=0}^{p-1} \xi^{i^2 q}$. Таким образом, $y^q = y$ в точности тогда, когда q является квадратичным вычетом по модулю p.

Итак, если $p \equiv 1 \mod 4$ и $q \neq p$ — простые числа, то p является квадратичным вычетом по модулю q тогда и только тогда, когда q является квадратичным вычетом по модулю p.

Если $p \equiv -1 \mod 4$, то $y = \sqrt{-p}$ и те же рассуждения показывают, что $-p$ является квадратичным вычетом по модулю q тогда и только тогда, когда q является квадратичным вычетом по модулю p.

5. Шаг второй, несколько тригонометрических тождеств

Лемма 1. *Для любого* $\xi \neq \pm 1$

$$(\xi + \xi^{-1})(\xi^2 + \xi^{-2})(\xi^4 + \xi^{-4}) \cdot \ldots \cdot (\xi^{2^n} + \xi^{-2^n}) = \frac{\xi^{2^{n+1}} - \xi^{-2^{n+1}}}{\xi - \xi^{-1}}\,.$$

Это тождество легко проверить, домножив обе части равенства на $\xi - \xi^{-1}$, а затем n раз использовав тождество $(\xi^{2^k} - \xi^{2^k})(\xi^{2^k} + \xi^{2^k}) = (\xi^{2^{k+1}} - \xi^{2^{k+1}})$.

Следствие 1. *Если* $\xi \neq \pm 1$ *— корень из единицы степени* p, *где* $p = 2^{n+1} + 1$, *то*

$$(\xi + \xi^{-1})(\xi^2 + \xi^{-2})(\xi^4 + \xi^{-4}) \cdot \ldots \cdot (\xi^{2^n} + \xi^{-2^n}) = -1.$$

Пусть теперь $c_k = \xi^k + \xi^{-k}$.

Лемма 2. *Для любых* s, t

$$c_s \cdot c_t = c_{s+t} + c_{s-t}\,.$$

Замечание 4. Если ξ равен $e^{i\alpha}$, то $c_k = 2\cos k\alpha$. В этом случае лемма 2 следует из формулы $2\cos(s\alpha)\cos(t\alpha) = \cos((s+t)\alpha) + \cos((s-t)\alpha)$, а

следствие 1 следует из тождества

$$2^n \cos\alpha \cos(2\alpha) \cos(4\alpha) \cdot \ldots \cdot \cos(2^n\alpha) = \frac{\sin(2^{n+1}\alpha)}{\sin\alpha}\,.$$

Найдём теперь квадратное уравнение с корнями $c_1 + c_4$ и $c_2 + c_8$.

Сумма корней этого уравнения — число $c_1 + c_2 + c_4 + c_8$, которое мы нашли на прошлом шаге: это корень x_1 уравнения $x^2 + x - 4 = 0$.

Чтобы найти произведение $(c_1 + c_4)(c_2 + c_8)$ будем рассуждать так: из следствия 1, применённого к корню из единицы ξ, мы находим $c_1c_2c_4c_8 = -1$. То же следствие, применённое к корню из единицы ξ^3, приводит к тождеству $c_3c_6c_{12}c_{24} = -1$, то есть $c_3c_6c_5c_7 = -1$.

Подставляя тождества $c_3c_5 = c_2 + c_8$, $c_6c_7 = c_1 + c_4$ в $c_3c_6c_5c_7 = -1$, получаем $(c_1 + c_4)(c_2 + c_8) = -1$.

Таким образом, $c_1 + c_4$ и $c_2 + c_8$ являются решениями y_1, y_2 уравнения $y^2 - x_1y - 1 = 0$, где x_1 — решение уравнения $x^2 + x - 4 = 0$.

Так же находим, что $c_3 + c_5$ и $c_6 + c_7$ являются решениями y_3, y_4 уравнения $y^2 - x_2y - 1 = 0$, где x_2 — другой корень уравнения $x^2 + x - 4 = 0$.

6. Шаг третий

Сумма чисел c_1 и c_4 равна $c_1 + c_4 = y_1$, а их произведение равно $c_1c_4 = c_3 + c_5 = y_3$. Следовательно, c_1, c_4 являются решениями уравнения $z^2 - y_1z + y_3 = 0$.

7. Последний шаг

Поскольку $\xi + \xi^{-1} = c_1$ и $\xi \cdot \xi^{-1} = 1$, то ξ и ξ^{-1} являются корнями уравнения $w^2 - c_1w + 1 = 0$.

8. Подведение итогов

При решении четырёх квадратных уравнений, выписанных выше, нам приходится четыре раза выбирать один из двух корней. Таким образом, мы можем получить 16 различных ответов, являющихся различными примитивными корнями из единицы степени 17.

Если мы выберем $\xi = e^{2\pi i/17}$, то мы можем проследить, какие корни нам следует выбирать, чтобы найти ξ:

$$c_1 + c_2 + c_4 + c_8 = \frac{-1 + \sqrt{17}}{2}\,,$$

$$c_3 + c_5 + c_6 + c_7 = \frac{-1 - \sqrt{17}}{2}\,,$$

$$c_1 + c_4 = \frac{\frac{-1+\sqrt{17}}{2} + \sqrt{\frac{17-\sqrt{17}}{2}}}{2} = A,$$
$$c_3 + c_5 = \frac{\frac{-1-\sqrt{17}}{2} + \sqrt{\frac{17+\sqrt{17}}{2}}}{2} = B,$$
$$c_1 = \frac{A + \sqrt{A^2 - 4B}}{2} = C,$$
$$\xi = \frac{C + \sqrt{C^2 - 4}}{2}\,.$$

Юрий Бурда, Univ. of Toronto
Email: yburda@math.toronto.edu
Люся Кадец, Univ. of Toronto
Email: lucy.kadets@math.toronto.edu