Гауссовы суммы

В.СЕНДЕРОВ, А. СПИВАК

Правильные многоугольники

Проведем векторы из центра O правильного n-угольника во все его вершины $A_1, A_2, \ldots, A_n$ (на рисунке 1 $n = 7$). Получим систему векторов, сумма которых равна нулю:

$$\overrightarrow{OA_1} + \overrightarrow{OA_2} + \ldots + \overrightarrow{OA_n} = \vec{0}. \qquad (1)$$

Доказательство равенства (1) очень простое: если бы сумма не равнялась нулю, то при повороте каждого из векторов на угол $360°/n$ сумма должна была бы одновременно и повернуться на угол $360°/n$, и остаться неизменной, поскольку при повороте векторы переходят «по циклу» друг в друга.

Неудивительно, что равенство (1) используется во многих задачах планиметрии (см., например, статью «Вписанные многоугольники», в этом номере журнала). Немецкий математик К.Ф.Гаусс (1777–1855) в трактате «Арифметические исследования», опубликованном в 1801 году, рассмотрел более сложные, чем (1), формулы. Неожиданным образом они оказались очень важны для теории чисел. Соответствующие суммы векторов получили название «гауссовых сумм». Рассказу о них и посвящена статья.

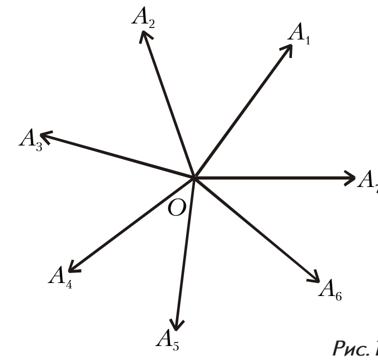

Рис.1

Задача М1648

Начнем с задачи «Задачника «Кванта».

М1648. *Из центра правильного многоугольника, вписанного в ок-*

*ружность радиусом 1, в некоторые вершины этого многоугольника проведены векторы. Может ли длина суммы этих векторов равняться а) 1998; б)** $\sqrt{1998}$?

Ответ на оба вопроса задачи утвердительный. Начнем построение примера к пункту а). Длина суммы $\overrightarrow{OB_2} + \overrightarrow{OB_3} + \overrightarrow{OB_4}$ векторов рисунка 2 равна 2. Чтобы построить систему векторов, длина суммы которых равна 3, помимо шестиугольника рассмотрим пятиугольник (рис.3).

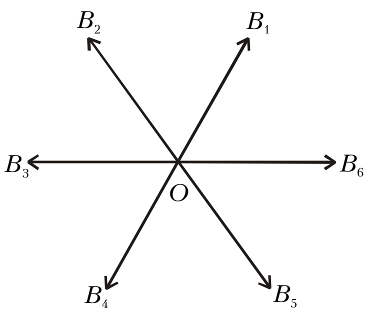

Рис.2

Благодаря формуле (1) сумма четырех векторов $\overrightarrow{OC_1} + \overrightarrow{OC_2} + \overrightarrow{OC_3} + \overrightarrow{OC_4}$, проведенных из центра в четыре вершины правильного пятиугольника, противоположна вектору $\overrightarrow{OC_5}$, соединяющему центр с пятой вершиной пятиугольника. И вершины пятиугольника, и вершины шестиугольника лежат в вершинах правильного 30-угольника.

Аналогично, чтобы построить систему векторов, длина суммы которых равна 4, добавим еще 6 векторов $\overrightarrow{OA_1}, \ldots, \overrightarrow{OA_6}$, соединяющих центр с вершинами семиугольника (см. рис.1). Продолжая в таком же духе, мы и получим пример к пункту а).

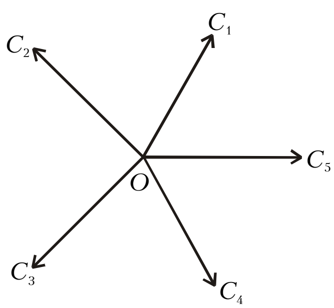

Рис.3

Формальное описание изложенной конструкции таково. Пусть $n_1, n_2, \ldots, n_{1998}$ – попарно взаимно простые числа. Рассмотрим правильный $n_1 n_2 \ldots n_{1998}$-угольник. Зафиксируем некоторую его вершину A. Назовем «выделенным» n_i-угольником ($i = 1, \ldots, 1998$) правильный n_i-угольник, одной из вершин которого является точка A, а другие вершины являются вершинами $n_1 n_2 \ldots n_{1998}$-угольника. Выделенные n_i-угольник и n_j-угольник ($i \neq j$) имеют, благодаря взаимной простоте чисел n_i и n_j, единственную общую вершину A. Рассмотрим векторы, идущие из центра O многоугольника во все вершины всех выделенных n_i-угольников, кроме A. Их сумма равна $-1998\overrightarrow{OA}$, что и требовалось.

б) В следующем разделе статьи мы построим с привлечением комплексных чисел сумму длиной $\sqrt{n}$ при любом натуральном n, а пока предлагаем ряд упражнений. Тот, кто справится с ними, получит решение пункта б), не использующее никаких выходящих за рамки школьной программы понятий (но, к сожалению, существенно использующее специфику числа $\sqrt{1998}$).

Упражнение 1. Воспользовавшись приемом решения пункта а), докажите, что если можно представить в искомом виде (т.е. в виде суммы векторов, проведенных из центра вписанного в единичную окружность правильного многоугольника в его вершины) некоторый вектор $\vec{v}$, то можно представить в таком виде и вектор $a\vec{v}$, где a – натуральное число.

Упражнение 2. Докажите, что если можно представить в искомом виде вектор длиной x, то можно представить в таком виде и вектор длиной а) $x\sqrt{a^2+b^2}$, б) $x\sqrt{a^2+2b^2}$, где a и b – натуральные числа.

Замечание. Если в искомом виде можно представить некоторый вектор длиной $\sqrt{m}$, то можно представить и вектор длиной $\sqrt{2m}$. Поэтому в дальнейшем мы можем искать вектор длиной $\sqrt{n}$ только для нечетных n.

Упражнение 3. Решите пункт б) задачи М1648.

Указание. $\sqrt{1998} = \sqrt{3^2+18^2} \cdot \sqrt{2^2+2\cdot 1^2}$.

Корни из единицы

Сейчас мы запишем равенство (1) в довольно неожиданном виде. Для этого рассмотрим уравнение $z^n - 1 = 0$ и разложим его левую часть на множители:

$$(z-1)\left(z^{n-1} + z^{n-2} + \ldots + z + 1\right) = 0.$$

Значит, если $z^n = 1$ и $z \neq 1$, то

$$z^{n-1} + z^{n-2} + \ldots + z + 1 = 0. \qquad (2)$$

В статье «Многочлены деления круга» («Квант» №1 за 1998 год) рассказано о том, что уравнение $z^n = 1$ имеет n решений – «корней из единицы». Они являются вершинами правильного n-угольника, вписанного в единичную окружность, и имеют вид

$$\zeta^k = \cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n},$$

где $\zeta = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$, $k = 1, \ldots, n$. Сумма всех корней n-й степени из единицы (при $n > 1$) равна 0:

$$1 + \zeta + \ldots + \zeta^{n-2} + \zeta^{n-1} = 0.$$

Это, по сути, и есть равенство (1)!

Зная все n корней $\zeta, \zeta^2, \ldots, \zeta^n (=1)$ многочлена $z^n - 1$, мы можем разложить его на множители:

$$z^n - 1 = (z-\zeta)\left(z-\zeta^2\right)\ldots\left(z-\zeta^{n-1}\right)(z-1). \qquad (3)$$

Сократив обе части на $z - 1$, получим

$$z^{n-1} + z^{n-2} + \ldots + z + 1 = (z-\zeta)\left(z-\zeta^2\right)\ldots\left(z-\zeta^{n-1}\right). \qquad (4)$$

Подставим в последнее равенство вместо z число 1:

$$n = (1-\zeta)\left(1-\zeta^2\right)\ldots\left(1-\zeta^{n-1}\right). \qquad (5)$$

Упражнение 4. Чтобы получить равенство (5), мы подставили $z = 1$ в равенство (4), которое получилось делением на $z - 1$ обеих частей равенства (3). Объясните, почему так делать можно, хотя «на ноль делить нельзя».

Пусть n – нечетное число. Тогда все множители правой части (5) можно разбить на комплексно сопряженные (т.е. симметричные относительно оси абсцисс) пары чисел $1 - \zeta^k = 1 - \cos\frac{2\pi k}{n} - i\sin\frac{2\pi k}{n}$ и $1 - \zeta^{n-k} = 1 - \cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n}$ (рис. 4). Взяв из каждой пары сопряженных множителей только один множитель, мы получим число, модуль которого – квадратный корень из

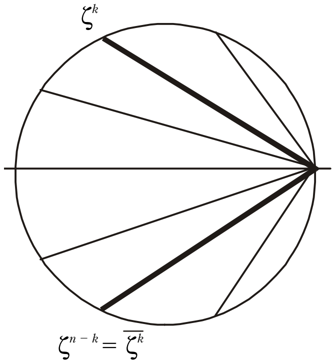

Рис.4

модуля произведения:

$$\sqrt{n} = \left|(1-\zeta)\left(1-\zeta^2\right)\ldots(1-\zeta)^{(n-1)/2}\right|. \qquad (6)$$

Раскрыв скобки в произведении, стоящем в формуле (6) под знаком модуля, мы получим вектор, длина которого равна $\sqrt{n}$. Он оказывается суммой корней из единицы. (Знаки вычитания нас не смущают, поскольку корень из единицы, взятый со знаком минус, все равно является корнем некоторой степени из единицы.) Если некоторые корни из единицы встретятся в этой сумме неоднократно, то можно применить прием пункта а) и по одному, вводя все новые простые числа, заменять такие корни.

Упражнение 5. Выпишите равенство, аналогичное равенству (6), для четного n.

Упражнение 6. а) Найдите произведение $A_1A_n \cdot A_2A_n \cdot \ldots \cdot A_{n-1}A_n$ длин сторон и диагоналей, выходящих из вершины A_n правильного n-угольника $A_1A_2\ldots A_n$, вписанного в окружность единичного радиуса. б) Найдите произведение длин всех сторон и диагоналей правильного n-угольника, вписанного в окружность радиуса R.

Упражнение 7. Пусть $ABCDE$ – правильный пятиугольник, вписанный в окружность с центром O. Если $AO = 1$ и если точка P симметрична точке O относительно точки A, докажите, что $PB \cdot PC = \sqrt{31}$.

Упражнение 8. а) Выведите из равенства (6), что если n нечетное, то

$$2^{(n-1)/2}\sin(\pi/n)\sin(2\pi/n)\cdot\ldots\cdot\sin\left(\frac{n-1}{2}\pi\Big/n\right) = \sqrt{n}.$$

б) Найдите произведение

$$\sin(\pi/n)\sin(2\pi/n)\cdot\ldots\cdot\sin\left(\frac{n-2}{2}\pi\Big/n\right),$$

где n – четное число.

К сожалению, формула (6) дает только длину, а не направление вектора. Получить вектор длиной $\sqrt{n}$ известного направления проще всего при помощи формул для гауссовых сумм (см. следующий раздел). Можно обойтись и более простыми (но, к сожалению, менее естественными) средствами – применив к формуле упражнения 8 а) формулу $\sin\alpha\sin\beta = \frac{1}{2}\left(\cos(\alpha-\beta)-\cos(\alpha+\beta)\right)$ преобразования произведения синусов в разность косинусов и аналогичные формулы для произведения синуса и косинуса и для произведения косинусов, можно получить формулу вида

$$\sum_k 2\cos\frac{m_k}{2n}\pi = \sqrt{n},$$

где m_k – целые числа. Далее можно воспользоваться тем, что удвоенный косинус любой рациональной доли угла π есть сумма сопряженных корней из единицы (а именно, $2\cos\frac{m_k}{2n}\pi = \eta^{m_k} + \eta^{-m_k}$, где $\eta = \cos(\pi/n) + i\sin(\pi/n)$ – корень $2n$-степени из единицы).

Упражнение 9. Представьте в виде суммы корней из единицы числа а) $\sqrt{2}$; б) $\sqrt{3}$; в) $\sqrt{5}$.

Гауссовы суммы

Обозначим

$$S_n = 1 + \zeta + \zeta^4 + \zeta^9 + \ldots + \zeta^{(n-1)^2}.$$

Упражнение 10. Вычислите S_n при а) $n = 1, 2, \ldots, 6$; б*) $n = 7$; в) $n = 8, 9, 10$.

После ряда безуспешных попыток Гаусс в 1811 году доказал, что

$$S_n = \begin{cases} \sqrt{n}, & n \equiv 1 \pmod 4, \\ 0, & n \equiv 2 \pmod 4, \\ i\sqrt{n}, & n \equiv 3 \pmod 4, \\ (1+i)\sqrt{n}, & n \equiv 0 \pmod 4). \end{cases}$$

В 1835 году Дирихле при помощи рядов Фурье получил другое доказательство этого факта. К сожалению, оно тоже слишком сложное и не может здесь обсуждаться.

Абсолютную величину S_n, в отличие от точного значения этого числа, найти легко. Мы сделаем это в случае, когда n – нечетное число. Поскольку модуль числа равен корню из произведения числа и его сопряженного, достаточно доказать формулу

$$S_n\overline{S_n} = n, \qquad (7)$$

т. е.

$$\left(1 + \zeta + \zeta^4 + \zeta^9 + \ldots + \zeta^{(n-1)^2}\right) \times \left(1 + \overline{\zeta} + \overline{\zeta^4} + \overline{\zeta^9} + \ldots + \overline{\zeta^{(n-1)^2}}\right) = n.$$

Как известно, $\overline{\zeta} = \zeta^{-1}$. Раскроем скобки. При умножении взятого из первой скобки числа ζ^{k^2}, где $k = 0, \ldots, n-1$, на взятое из второй скобки слагаемое ζ^{-m^2}, где $m = 0, \ldots, n-1$, получаем $\zeta^{k^2-m^2}$. Обозначим через a и b остатки от деления на n чисел $k-m$ и $k+m$. Очевидно, $\zeta^{k^2-m^2} = \zeta^{ab}$. Любой паре остатков $(a; b)$ соответствует единственная пара $(k; m)$. (Докажите!) Поэтому при суммировании встретятся по одному разу все n^2 разных пар $(a; b)$ и, следовательно,

$$S_n\overline{S_n} = \sum_{b=0}^{n-1}\sum_{a=0}^{n-1}\zeta^{ab}.$$

При $b = 0$ все n слагаемых вида ζ^{ab} равны 1. При $1 \le b < n$ сумма $\sum_{a=0}^{n-1}\zeta^{ab}$ равна 0. Равенство (7) доказано.

Упражнение 11. Докажите, что а) если $n = 4k + 2$, где $k \in \boldsymbol{N}$, то $S_n = 0$; б) если $n = 4k$, где $k \in \boldsymbol{N}$, то $|S_n| = \sqrt{2n}$.

Упражнение 12*. Докажите, что если p – нечетное простое число, то $S_p^2 = (-1)^{(p-1)/2}p$.