Первообразные корни и построение правильных многоугольников с помощью циркуля и линейки

Савватеев Алексей Владимирович

Берендеевы поляны, 18–20 августа 2019 г.

Комплексные числа

Напишем многочлен с корнями 1,2,–3 (нам понадобится многочлен с другими корнями). Он равен

$$P(x) = (x-1)(x-2)(x+3) = x^3 - 7x + 6.$$

Напишем для $P(x)$ формулу Кардано:

$$\begin{aligned}
x &= \alpha + \beta \\
(\alpha+\beta)^3 - 7(\alpha+\beta) + 6 &= 0 \\
\alpha^3 + \beta^3 + (\alpha+\beta)(3\alpha\beta - 7) + 6 &= 0 \\
\begin{cases} 3\alpha\beta = 7 \\ \alpha^3 + \beta^3 = -6 \end{cases} & \\
(y-\alpha^3)(y-\beta^3) &= 0 \\
y = -3 \pm \sqrt{9 - \frac{343}{27}} & \\
x = \sqrt[3]{-3 - \frac{\sqrt{-100}}{27}} + \sqrt[3]{-3 + \frac{\sqrt{-100}}{27}} & \\
x = \sqrt[3]{-3 - \frac{10i}{3\sqrt{3}}} + \sqrt[3]{-3 + \frac{10i}{3\sqrt{3}}} &
\end{aligned}$$

и при правильном извлечении кубических корней получим те же самые три корня (для каждого α^3 будет однозначно определяться β^3).

Определение 1. Комплексные числа $\mathbb{C}$ — расширение $\mathbb{R}$, получаемое из него добавлением формального символа i со свойством $i^2 = -1$.

Свойства.

- $\mathbb{C}$ — поле ($(x+iy) + (a+ib) = (x+a) + i(y+b)$ и т.п.)
- Если нарисовать $\mathbb{C}$ на плоскости, ставя в соответствие точке (x, y) число $x+iy$, сумма комплексных чисел будет суммой векторов.
- Поставим каждому числу $z \in \mathbb{C}$ в соответствие $\arg z$ — угол между Ox и лучом из $(0,0)$ в z и $|z|$ — длину вектора от $(0,0)$ в z. Тогда при умножении комплексных чисел аргументы чисел будут складываться, а модули умножаться. Т.е. при умножении всех точек плоскости на одно конкретное (ненулевое) число z происходит поворотная гомотетия с коэффициентом $|z|$ и углом $\arg z$.
- Аналогично, при инверсии ($z \mapsto \frac{1}{z}$) будет так: $\arg\frac{1}{z} = -\arg z$, $|\frac{1}{z}| = \frac{1}{|z|}$.
- Поставим в соответствие числу $z = x+iy$ число $\overline{z} = x - iy$ — сопряжённое число (геометрически это отражение относительно Ox). Тогда при арифметических операциях сопряжение сохраняется ($\overline{z} + \overline{t} = \overline{z+t}$ и т.п.) и $|z|^2 = z\overline{z}$.
- Корень n-й степени извлекается из любого ненулевого комплексного числа ровно n способами — это вершины правильного n-угольника.

Построение фигур

Треугольник $72°, 72°, 36°$

Заметим, что если у этого треугольника провести биссектрису большого угла, он разобьётся на 2 равнобедренных, поэтому если его малая сторона 1, а большая x, то $x - 1 = \dfrac{1}{x}$, т.е. $x = \dfrac{1+\sqrt{5}}{2}$. Чтобы построить этот отрезок, построим прямоугольный треугольник со сторонами 1 и 2, тогда половина его гипотенузы будет $\dfrac{\sqrt{5}}{2}$. ■

Правильный пятиугольник

Построим треугольник с углами $72°, 72°, 36°$ и опишем вокруг него окружность, затем построим серединные перпендикуляры к его большим сторонам и пересечём с окружностью. Получатся 2 точки, которые вместе с треугольником образуют правильный пятиугольник. ■

Правильный пятиугольник II

Будем строить решения уравнения $z^5 = 1$ в комплексных числах. Пусть его решения — $1, \xi, \xi^2, \xi^{-2}, \xi^{-1}$. Заметим, что по теореме Виета (или из-за поворотов) сумма решений равна 0, т.е. $(\xi + \xi^{-1})(\xi^2 + \xi^{-2}) = -1$. Пусть левая скобка α, а правая — β, тогда по теореме Виета α и β — корни уравнения $x^2 + x - 1 = 0$. Найдём α (положительный корень, равный $\frac{\sqrt{5}-1}{2}$), построим его на вещественной оси (пусть это точка A), тогда пересечение серединного перпендикуляра к OA с единичной окружностью даст 2-ю и 3-ю вершины пятиугольника. ■

Правильный 17-угольник

Пусть $\xi = \cos\frac{2\pi}{17} + i\sin\frac{2\pi}{17}$ — «первый» корень 17-й степени из единицы. Будем строить ξ, или, что аналогично, $\xi + \xi^{-1}$. Аналогично предыдущему построению заметим, что $(\xi + \xi^{-1})(\sum\limits_{j=1}^{8}\xi^j) = -1$. Разобьём степени ξ на две группы: в α степени $\pm1, \pm2, \pm4, \pm8$, в β все остальные.

Пусть мы это доказали. Тогда α и β — корни уравнения $x^2 + x - 4 = 0$, т.е. $(\alpha, \beta) = \dfrac{\pm\sqrt{17}-1}{2}$. Тогда очевидно, что

$$\alpha = \frac{\sqrt{17}-1}{2},\ \beta = \frac{-\sqrt{17}-1}{2}.$$

Теперь разобьём каждую из α и β на 2 группы: пусть в γ_1 степени $\pm1, \pm4$, в γ_2 — $\pm2, \pm8$, в γ_3 — $\pm3, \pm5$, в γ_4 — $\pm6, \pm7$. Тогда окажется, что $\gamma_1\gamma_2 = \gamma_3\gamma_4 = -1$ и по теореме Виета (и 4) все γ_i построимы (большие корни — соответственно, γ_1 и γ_3. Наконец, разобьём γ_1 на две группы — в δ_1 степени ±1, а в δ_2 — ±4. Тогда $\delta_1 + \delta_2 = \gamma_1, \delta_1\delta_2 = \gamma_3$. По теореме Виета строим δ_1 (больший корень уравнения $x^2 - \gamma_1 x + \gamma_3 = 0$), строим точку A с этой координатой на вещественной оси, тогда серединный перпендикуляр к отрезку OA даст две вершины 17-угольника. ■

В дальнейших леммах имеются в виду правильные многоугольники.

Лемма 1. Если m-угольник построим, то и $2m$-угольник тоже.
Лемма 2. Если mn-угольник построим, то m- и n-угольники тоже.
Обе леммы очевидны.

Лемма 3. Если $(m, n) = 1$, то существуют $k, l \in \mathbb{Z}$ такие, что $km + ln = 1$.

Доказательство. Пусть $d > 0$ — минимальное представимое в виде $km + ln = d$. Заметим, что $m \vdots d$. Действительно, следующее после d число, которое можно получить — это $2d$, затем $3d$ и т.п., т.к. иначе можно было бы получить число, меньшее d. Аналогично $n \vdots d$. Тогда $(m, n) \geq d$, значит, $d = 1$. ■

Лемма 4. Если m- и n-угольники построимы и $(m, n) = 1$, то mn-угольник тоже.

Доказательство. По 3 существуют такие k и l, что $km - ln = 1$. Значит, если построить эти многоугольники на одной окружности с общей вершиной, какие-то две вершины будут на расстоянии $\frac{1}{mn}$ от длины окружности. ■

Школьная теория полей

Определение 2. Абелева Группа — множество $(G, \oplus, \ominus)$ с определёнными на нём операциями $\oplus$ и $\ominus$ со следующими свойствами:

- $\forall a, b \in G\ a \oplus b, \ominus a \in G$;
- $\forall a, b \in G\ a \oplus b = b \oplus a$ (коммутативность);
- $\forall a, b, c \in G\ a \oplus (b \oplus c) = (a \oplus b) \oplus c$ (ассоциативность);
- $\exists e \in G \forall a \in G\ a \oplus e = a$;
- $\forall a \in G\ a \oplus (\ominus a) = e$ (обратимость).

Определение 3. Поле — множество $\mathbb{F}$ с определёнными на нём операциями $+, -, \cdot, /$ со следующими свойствами:

- $(\mathbb{F}, +, x \mapsto -x)$ — абелева группа;
- $(\mathbb{F}/0, \cdot, x \mapsto 1/x)$ — абелева группа;
- Выполняется дистрибутивность ($\forall a, b, c \in \mathbb{F}\ a \cdot (b + c) = a \cdot b + a \cdot c$).

Первообразные

Определение 4. Первообразный корень по модулю p — такой остаток q, что все ненулевые остатки по модулю p являются степенями q в каком-то порядке.

Теорема 5. Первообразный корень существует для всех простых p.

Обозначим $aS = \{ab|b \in S\}$.

Лемма 6. Если $S \subset \mathbb{F}_p$, то $|aS| = |S|$. В частности, $a\mathbb{F}_p^* = \mathbb{F}_p^*$.

Доказательство. Вытекает из 6. ■

Теорема 7 (малая теорема Ферма). Если $n \not| p$, то $n^{p-1} \equiv 1 \mod p$.

Доказательство. Заметим, что $(p-1)! \equiv n \cdot (2n) \cdot \ldots \cdot (p-1)n = (p-1)!n^{p-1} \mod p$, откуда следует утверждение задачи. ■

Определение 5. Порядок a по модулю p (обозначается $ord_p(a)$) — минимальное такое натуральное k, что $a^k \equiv 1 \mod p$.

Лемма 8. $ord_p(a)|p-1$.

Доказательство. Заметим, что все числа разбиваются на множества вида $a_1^n, a_2^n, \ldots$. Пусть $ord_p(a_1) = l$. Тогда до тех пор, пока есть не рассмотренные числа, будем брать одно из них (b) и добавлять к рассмотренным числа вида $b \cdot a^n$. Тогда на каждом шаге все рассматриваемые числа различные и добавляется l чисел за шаг, откуда всё следует. ■

Теорема 9 (Безу). Пусть $P(x)$ — многочлен с коэффициентами из кольца. Тогда если α — корень P, то $P \vdots (x-\alpha)$. (упражнение на 1 балл)

Лемма 10. Пусть $P(x)$ — многочлен с коэффициентами из поля. Тогда если $\alpha_1, \ldots, \alpha_n$ — корни P, то $P \vdots (x-\alpha_1)\ldots(x-\alpha_n)$. (упражнение на 1 балл)

Лемма 11. У многочлена степени n с коэффициентами из поля не более n корней. (упражнение на 1 балл)

Лемма 12 (Гаусс). Пусть S — множество остатков от 1 до $\frac{p-1}{2}$. Тогда $|\{n, -n\} \cap aS| = 1$ для всех n и $a \not\equiv 0$ и, кроме того, $a^{\frac{p-1}{2}} = (-1)^m$, где m — количество таких $n \leq \frac{p-1}{2}$, что в aS есть $-n$.

Доказательство. Первая часть очевидна из принципа Дирихле. Вторая часть следует из того, что $(\frac{p-1}{2})! \equiv (-1)^m \cdot a(2a)\ldots(\frac{p-1}{2}a)$. ■

Определение 6. Функция Эйлера $\varphi(d)$ — количество натуральных чисел, меньших s и взаимно простых с ним

Лемма 13. $d = \sum\limits_{l|d} \varphi(l)$ для всех d.

Доказательство. Напишем дроби $\frac{1}{d}, \frac{2}{d}, \ldots, \frac{n}{d}$ и сократим их. Заметим, что дробей с знаменателем l ровно $\varphi(l)$, откуда всё следует. ■

Доказательство теоремы 5. Пусть $d|n$. Тогда $x^n - 1 = (x^d - 1)\Psi(x)$, где у Ψ степень $n-d$. Значит, по 11 есть ровно d решений уравнения $x^d - 1 = 0$, т.е. существует ровно d чисел с порядком, делящим d. Обозначим $\psi(d) = |\{a|ord_p(a) = d\}|$. Тогда по 13 $d = \sum\limits_{l|d} \psi(l)\ \forall d|n$. Значит, $\psi \equiv \varphi$, в частности, $\psi(p-1) = \varphi(p-1) > 0$. ■

Финал

Лемма 14. Если $2^k + 1 \in \mathbb{P}$, то $k = 2^l$ для натурального n. (такие числа называются числами Ферма)

Лемма 15. Если для p такого вида a — не первообразный, то $a^{\frac{p-1}{2}} \equiv 1 \mod p$.

Доказательство. По 7 это либо 1, либо -1, и -1 не подходит. ■

Утверждение. Число построимо тогда и только тогда, когда существует список квадратных уравнений, последнее из которых имеет это число решением.

Теорема 16. Если $p > 3 \in \mathbb{P}$ таково, что правильный p-угольник построим, то 3 — первообразный корень по модулю p.

Лемма 17. Простые числа Ферма, большие 3, сравнимы с 5 по модулю 12.

Доказательство теоремы 16 #1. Докажем по индукции, что для чисел, сравнимых с 5 по модулю 12, 12 даёт нечётное количество минусов. База для 17 очевидна, шаг очевиден. ■

Доказательство теоремы 16 #2. Заметим, что такие p имеют вид $2^{2^n} + 1$. Применим закон квадратичной взаимности Гаусса: $\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = (-1)^{\frac{p-1}{2}} = 1$. Заметим, что $\left(\frac{p}{3}\right) = \left(\frac{-1}{p}\right) = -1$, значит, и $\left(\frac{3}{p}\right) = -1$. С другой стороны, $\text{ord } n \mod p = 2^k$, а значит, и $\frac{p-1}{\text{ord } n \mod p} = 2^k$, но мы доказали, что это нечётное число, значит, это 1. ■

Идея построения. Вначале разбиваем сумму всех ξ на слагаемые вида $\xi^{3^{2^k(m+1)}}$ и на $\xi^{3^{2^{k+1}}}$, где k — номер шага (например, вначале разбиваем на чётные и нечётные степени тройки). Тогда после каждого шага каждая сумма строится.