Множественная сложность построения правильного многоугольника

Е. С. Коган

Эта работа иллюстрирует важный метод на примере решения алгоритмической задачи.

Будем рассматривать следующую операцию: к подмножеству $A \subset \mathbb{C}$, содержащему числа x, y, добавляется любое из чисел $x + y$, $x - y$, xy, или (если $y \neq 0$) x/y, или такое z, что $z^2 = x$.

Основная теорема. *Пусть p — простое число Ферма, т. е. простое число вида $2^m + 1$, где m — степень двойки с натуральным показателем, ε — первообразный корень степени p из единицы*:

$$\varepsilon := \cos \frac{2\pi}{p} + i \sin \frac{2\pi}{p}.$$

Тогда из $\{1\}$ можно получить некоторое множество, содержащее корни p-й степени из единицы: $1, \varepsilon, \varepsilon^2, \ldots, \varepsilon^{p-1}$, *за $12p^2$ добавлений, определённых выше*.

Назовём сложность, рассмотренную в основной теореме, *множественной сложностью*. Такое понятие сложности отличается от сложности как времени работы алгоритма, находящего корни степени p из 1. Однако последняя сложность также пропорциональна p^2. Об алгоритмах вычисления корней p-й степени из 1 см. [4], а также [5]. О строгих определениях различных понятий сложности см. [1]. Автор не исследовал соотношение введённого понятия множественной сложности с этими определениями. В любом случае основная теорема не претендует на новизну.

Замечание 1. Из основной теоремы можно вывести следующее утверждение.

Пусть p — простое число Ферма. Тогда существует такое действительное число C, не зависящее от p, что из единичного отрезка можно получить правильный p-угольник за $C \cdot p^2$ операций проведения окружности

с центром в одной точке и проходящей через другую и проведения прямой через две точки[1)].

Замечание 2. Из основной теоремы также можно вывести её вещественный аналог, который состоит в следующем.

Существует такое число C, что для любого простого числа Ферма p число $\cos(2\pi/p)$ можно получить из $\{1\}$ за $C \cdot p^2$ операций, аналогичных определённым выше, причём корни извлекаются только из положительных чисел.

Доказательство основной теоремы проводится аналогично [2, п. 5.3.4, с. 83–88]. Оценка же, получающаяся из доказательства построимости, приведённого в [2, конец п. 5.3.3, с. 83], пропорциональна p^3.

Идея доказательства основной теоремы для $p = 5$. Сначала выразим через радикалы некоторые многочлены от ε.

Заметим, что $(\varepsilon + \varepsilon^4)(\varepsilon^2 + \varepsilon^3) = \varepsilon + \varepsilon^2 + \varepsilon^3 + \varepsilon^4 = -1$. Обозначим $T_0 := \varepsilon + \varepsilon^4$ и $T_1 := \varepsilon^2 + \varepsilon^3$. Тогда по теореме Виета T_0 и T_1 являются корнями уравнения $t^2 + t - 1 = 0$. Отсюда можно выразить T_0 (и T_1). Поскольку $\varepsilon \cdot \varepsilon^4 = 1$, по теореме Виета числа ε и ε^4 являются корнями уравнения $t^2 - T_0 t + 1 = 0$. Отсюда можно выразить ε (и ε^4).

Идея доказательства основной теоремы в общем случае. Сначала хорошо бы разбить сумму $\varepsilon + \varepsilon^2 + \ldots + \varepsilon^{p-1} = -1$на два слагаемых T_0, T_1, которые можно получить добавлениями, описанными в начале статьи (иными словами, *сгруппировать* удачным образом корни уравнения $1 + x + x^2 + \ldots + x^{p-1} = 0$). Затем нужно разбить каждую сумму T_k на два слагаемых $T_{k,0}, T_{k,1}$, которые можно получить такими добавлениями. И так далее, пока не получим $T_{\underbrace{1,\ldots,1}_{s}} = \varepsilon$.

Теорема о первообразном корне, приведённая, например, в [2, п. 5.3.3, с. 82], позволяет закодировать ненулевые вычеты по модулю p вычетами по модулю $p-1$. А именно, выбрав первообразный корень g по модулю p, мы вычет k по модулю $p-1$ сопоставляем (ненулевому) остатку от деления g^k на p. Это кодирование использовано в группировках, построенных выше для $p = 5$.

Введём определения и обозначения, необходимые для доказательства.

Множество $A \subset \mathbb{C}$ *построимо за* n *операций из множества* $B \subset \mathbb{C}$, если какое-нибудь множество $A' \supset A$ можно получить из B за n добавлений, описанных в начале статьи. Используем следующие обозначения:

[1)] Известна история об аспиранте, который разработал построение правильного многоугольника с 65 537 сторонами за 20 лет (см. [3, с. 43]).

- $p = 2^m + 1$ — простое число Ферма;
- $q_k = 2^{k+1}$ $(k = 0, 1, \ldots, m)$;
- $s_k = 2^{m-k-1} - 1$ $(k = 0, 1, \ldots, m)$;
- ε — первообразный корень степени p из единицы;
- g — первообразный корень по модулю p;
- $T_{k,r} := \sum_{a=0}^{2^{m-k}-1} \varepsilon^{g^{2^k \cdot a + r}}$ для каждого $k \in \{0, 1, \ldots, m\}$, $r \in \mathbb{Z}_{2^m}$.
  В частности, $T_{0,0} = -1$, а $T_{m,r} = \varepsilon^{g^r}$. Также $T_{k,r_1} = T_{k,r_2}$ при $r_1 \equiv r_2 \pmod{2^k}$, поэтому это определение осмысленно и при $r \in \mathbb{Z}_{2^k}$;
- $N_{k,t}$ — число пар (c, d) вычетов по модулю 2^{m-k-1}, $k \in \{0, 1, \ldots, m-1\}$, удовлетворяющих сравнению

$$g^{q_k \cdot c + t} + g^{q_k \cdot d + 2^k + t} \equiv 1 \pmod{p}, \quad t \in \mathbb{Z}_{2^m}. \tag{1}$$

  Числа $T_{k,r}$ и $N_{k,t}$ зависят от m, но, поскольку m зафиксировано, оно не указывается.

Лемма 1. *Для любых вычетов $t_1, t_2 \in \mathbb{Z}_{2^m}$, сравнимых по модулю 2^k, $k \in \{0, 1, \ldots, m-1\}$, верно равенство $N_{k,t_1} = N_{k,t_2}$.*

Доказательство. Достаточно показать, что $N_{k,t} = N_{k,2^k+t}$. Для этого сопоставим каждому решению (c, d) сравнения (1) пару $(d, c-1)$. Эти пары дают все решения сравнения (1) при замене t на $2^k + t$, поскольку следующие сравнения равносильны:

$$g^{q_k \cdot c + t} + g^{q_k \cdot d + 2^k + t} \equiv 1 \pmod{p},$$
$$g^{q_k \cdot d + (2^k + t)} + g^{q_k \cdot (c-1) + 2^k + (2^k + t)} \equiv 1 \pmod{p}. \qquad \square$$

Лемма 2. *Для любых $k \in \{0, 1, \ldots, m-2\}$ и $r \in \mathbb{Z}_{2^m}$*

$$T_{k+1,r} T_{k+1,2^k+r} = \sum_{s=0}^{2^k-1} N_{k,r-s} T_{k,s}.$$

Доказательство. Имеем

$$T_{k+1,r} T_{k+1,2^k+r} = \left(\sum_{c=0}^{s_k} \varepsilon^{g^{q_k \cdot c + r}} \right) \cdot \left(\sum_{d=0}^{s_k} \varepsilon^{g^{q_k \cdot d + 2^k + r}} \right) =$$
$$= \sum_{c=0}^{s_k} \sum_{d=0}^{s_k} \varepsilon^{g^{q_k \cdot c + r} + g^{q_k \cdot d + 2^k + r}} \overset{(*)}{=} \sum_{s=0}^{2^m-1} N_{k,r-s} \varepsilon^{g^s} \overset{(**)}{=} \sum_{s=0}^{2^k-1} N_{k,r-s} T_{k,s}. \tag{2}$$

Равенство $(*)$ из (2) доказывается группировкой одинаковых слагаемых. Действительно, сравнение

$$g^{q_k \cdot c + r} + g^{q_k \cdot d + 2^k + r} \equiv g^s \pmod{p}$$

равносильно сравнению (1) для $t = r - s$. А сравнение

$$g^{q_k \cdot c + r} + g^{q_k \cdot d + 2^k + r} \equiv 0 \pmod{p}$$

не имеет решений, поскольку оно равносильно следующим:

$$\begin{aligned} g^{q_k \cdot c + r} &\equiv (-1) \cdot g^{q_k \cdot d + 2^k + r} \pmod{p}, \\ g^{q_k \cdot c + r} &\equiv g^{2^{m-1}} \cdot g^{q_k \cdot d + 2^k + r} \pmod{p}, \\ q_k \cdot c + r &\equiv 2^{m-1} + (q_k \cdot d + 2^k + r) \pmod{2^m}, \\ q_k \cdot (c - d) &\equiv 2^{m-1} + 2^k \pmod{2^m}, \\ 2(c - d) &\equiv 2^{m-k-1} + 1 \pmod{2^{m-k}}. \end{aligned}$$

Последнее сравнение не имеет решений, так как в левой части стоит чётное число, а в правой — нечётное (2^{m-k-1} чётно, так как $k \leqslant m-2$).

Равенство $(**)$ из (2) получается из леммы 1 группировкой одинаковых $N_{k,r-s}$. □

Замечание. При $k = m-1$ произведение $T_{k+1,r} T_{k+1,2^k+r}$ равно

$$T_{m,r} T_{m,2^{m-1}+r} = \varepsilon^{g^r} \cdot \varepsilon^{g^{2^{m-1}+r}} = \varepsilon^{g^r} \cdot \varepsilon^{-g^r} = 1.$$

Лемма 3. *Для любого целого числа k от 0 до $m-1$ множество*

$$A = \{0, 1, \ldots, p\} \cup \{T_{k+1,r} \mid r \in \mathbb{Z}_{2^{k+1}}\}$$

построимо за $11 \cdot 4^k$ операций из множества $B = \{0, 1, \ldots, p\} \cup \{T_{k,r} \mid r \in \mathbb{Z}_{2^k}\}$.

Доказательство. Во-первых, для любых $k \in \{0, 1, \ldots, m\}$ и $t \in \mathbb{Z}_{2^m}$ выполняется $N_{k,t} \leqslant p$, так как в сравнении (1) одному вычету c может соответствовать не больше одного вычета d. Следовательно, все $N_{k,t}$ содержатся в B.

Докажем, что множество $P := \{T_{k+1,r} T_{k+1,2^k+r} \mid r \in \mathbb{Z}_{2^k}\}$ построимо из B меньше чем за $2 \cdot 4^k$ операций; в определении P вычет r берётся по модулю 2^k, а не 2^{k+1}, так как $T_{k+1,r} T_{k+1,2^k+r} = T_{k+1,2^k+r} T_{k+1,2^k+(2^k+r)}$.

Из замечания к лемме 2 следует, что $P = \{1\} \subset B$ при $k = m-1$. Если же $k \leqslant m-2$, то множество $P' := \{N_{k,r-s} T_{k,s} \mid r, s \in \mathbb{Z}_{2^k}\}$ построимо из B за $2^k \cdot 2^k = 4^k$ операций умножения (можно для всех пар (r, s) добавить $N_{k,r-s} T_{k,s}$), а множество P по лемме 2 построимо из P' за $(2^k - 1) \cdot 2^k < 4^k$ операций умножения. Значит, множество P построимо из B меньше чем за $4^k + 4^k = 2 \cdot 4^k$ операций.

Далее, множество $P \cup B$ содержит

$$T_{k+1,r} + T_{k+1,2^k+r} = T_{k,r} \in B \quad \text{и} \quad T_{k+1,r} T_{k+1,2^k+r} \in P,$$

и для любых (комплексных) чисел x_1, x_2 множество $\{x_1, x_2\}$ построимо за 9 операций из множества $\{x_1 + x_2, x_1x_2\}$ (по формуле корней квадратного уравнения). Следовательно, $A' := \{T_{k+1,r} \mid r \in \mathbb{Z}_{2^{k+1}}\}$ построимо из $P \cup B$ за $9 \cdot 2^k$ операций, т. е. A' построимо из B за $2 \cdot 4^k + 9 \cdot 2^k \leqslant 11 \cdot 4^k$ операций. Кроме того, $\{0, 1, \ldots, p\} \subset B$, поэтому A также построимо из B за $11 \cdot 4^k$ операций. □

Доказательство основной теоремы. Из леммы 3 следует, что множество

$$\{T_{m,r} \mid r \in \{0, 1, \ldots, 2^m - 1\}\} = \{\varepsilon^r \mid r \in \{0, 1, \ldots, 2^m - 1\}\}$$

построимо из $\{1\}$ за

$$p + 1 + \sum_{k=0}^{m-1} 11 \cdot 4^k = p + 1 + 11 \cdot \frac{4^m - 1}{4 - 1} < p + 11 \cdot 4^m < 12p^2$$

операций. □

Благодарности

Благодарю Д. Мусатова, А. Савватеева и руководителя работы А. Скопенкова за ценные замечания и предложения при написании данной работы.

Список литературы

[1] *Абрамов С. А.* Лекции о сложности алгоритмов. М.: МЦНМО, 2012.

[2] *Заславский А. А., Скопенков А. Б., Скопенков М. Б.* Элементы математики в задачах. М.: МЦНМО, 2018. С. 82–90.

[3] *Литлвуд Дж.* Математическая смесь. М.: Физматлит, 1990.

[4] *Сафин А. Р.* Программа для построения правильных многоугольников циркулем и линейкой. https://www.mccme.ru/mmks/dec08/Safin.pdf

[5] *Berndt B., Evans R., Williams K.* Gauss and Jacobi sums. New York: John Wiley & Sons, Inc., 1998. (Canadian Mathematical Society Series of Monographs and Advanced Texts).

Евгений Сергеевич Коган, ученик 11 класса ГБОУ «Интеллектуал»
koganeser@gmail.com