Множественная сложность построения правильного многоугольника *

Евгений Коган

Аннотация

Given a subset of $\mathbb{C}$ containing x, y, one can add $x+y$, $x-y$, xy or (when $y \neq 0$) x/y or any z such that $z^2 = x$. Let p be a prime Fermat number. We prove that it is possible to obtain from $\{1\}$ a set containing all the p-th roots of 1 by $12p^2$ above operations. This problem is different from the standard estimation of complexity of an algotihm computing the p-th roots of 1.

К подмножеству $A \subset \mathbb{C}$ содержащему числа x, y можно добавить любое из чисел $x+y$, $x-y$, xy или (если $y \neq 0$) x/y или любое z такое, что $z^2 = x$.

Основная теорема. Пусть $p = 2^m + 1$ — простое число Ферма, $\varepsilon := \cos\frac{2\pi}{p} + i\sin\frac{2\pi}{p}$. Тогда из $\{1\}$ можно получить некоторое множество, содержащее числа $1, \varepsilon, \varepsilon^2, \ldots, \varepsilon^{p-1}$, за $12p^2$ добавлений, определенных выше.

Эта проблема отличается от стандартной оценки сложности алгоритма, находящего корни степени p из 1. Об этой оценке можно см. [2] и [3]. Известна история об аспиранте, который разработал построение правильного многоугольника с 65537 сторонами за 20 лет (см. [4]).

Замечание. Из основной теоремы можно вывести следующее утверждение:

*This paper is prepared under the supervision of Arkadiy Skopenkov and is submitted to the Moscow Mathematical Conference for High-School Students. Readers are invited to send their remarks and reports on this paper to mmks@mccme.ru

Пусть p — простое число Ферма, т. е. простое число вида $2^m + 1$, где m — степень 2. Тогда существует действительное число C, не зависящее от p, такое, что за $C \cdot p^2$ операций проведения окружности с центром в одной точке и проходящей через другую и проведения прямой через две точки из единичного отрезка можно получить правильный p-угольник.

Формализация аналогична основной теореме.

Замечание. Из основной теоремы также можно вывести ее вещественный аналог, который состоит в следующем:

Существует такое число C, что для любого простого числа Ферма p число $\cos\frac{2\pi}{p}$ можно получить из $\{1\}$ за $C \cdot p^2$ операций, аналогичным определенным выше, но при которых корень можно брать только из положительных чисел.

Доказательство основной теоремы аналогично [1, п. 5.3.4]. Оценка же, получающаяся из доказательства построимости, приведенном в [1, конец п. 5.3.3], пропорциональна $p^2 \log_2 p$.

Введем определения и обозначения, необходимые для доказательства.

Множество $A \subset \mathbb{C}$ *построимо за* n *операций из* $B \subset \mathbb{C}$, если какое-нибудь множество $A' \supset A$ можно получить из B за n операций, описанных выше.

Обозначим через

- g — первообразный корень по модулю p;
- $T_{k,r} := \sum\limits_{a=0}^{2^{m-k}-1} \varepsilon^{g^{2^k} \cdot a + r}$ для каждого $k \in \{0, 1, \ldots, m\}$, $r \in \mathbb{Z}_{2^k}$.

  В частности, $T_{0,0} = -1$, а $T_{m,r} = \varepsilon^r$;
- $N_{k,t,m}$ — число пар (c, d) вычетов по модулю 2^{m-k-1}, являющихся решениями сравнения

$$g^{2^{k+1} \cdot c + t} + g^{2^{k+1} \cdot d + 2^k + t} \equiv 1 \pmod{p}, \tag{1}$$

  где $k \in \{0, 1, \ldots, m-1\}$, $t \in \mathbb{Z}_{2^m}$. Если m зафиксировано, мы будем опускать его и писать $N_{k,t} := N_{k,t,m}$.

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 $N_{k,t_1} = N_{k,t_2}$.

Доказательство. Пусть $t_1 \equiv t_2 \pmod{2^{k+1}}$. Обозначим через $l := \dfrac{t_1 - t_2}{2^{k+1}}, c' := c + l, d' := d + l$. Тогда:

$$g^{2^{k+1}\cdot c + t_1} + g^{2^{k+1}\cdot d + 2^k + t_1} \equiv 1 \pmod{p}$$

$$g^{2^{k+1}\cdot (c+l) + t_2} + g^{2^{k+1}\cdot (d+l) + 2^k + t_2} \equiv 1 \pmod{p}$$

$$g^{2^{k+1}\cdot c' + t_2} + g^{2^{k+1}\cdot d' + 2^k + t_2} \equiv 1 \pmod{p}$$

Следовательно, $N_{k,t_1} = N_{k,t_2}$.

Для завершения доказательства леммы 1 достаточно показать, что $N_{k,t} = N_{k,2^k+t}$. Обозначим через $c' := d, d' := c - 1$. Тогда:

$$g^{2^{k+1}\cdot c + t} + g^{2^{k+1}\cdot d + 2^k + t} \equiv 1 \pmod{p}$$

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

$$g^{2^{k+1}\cdot c' + (2^k + t)} + g^{2^{k+1}\cdot d' + 2^k + (2^k + t)} \equiv 1 \pmod{p}$$

□

Лемма 2. Для любого целого числа k от 1 до $m - 1$ множество

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

построимо из множества

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

за $11 \cdot 4^k$ операций.

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

Во-вторых,

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

(во втором равенстве мы воспользовались леммой 1), а множество $\{N_{k,r-s} T_{k,s} \mid r, s \in \mathbb{Z}_{2^k}\}$ построимо из B за $2^k \cdot 2^k$ операций. Из этого

вытекает, что множество $P := \{T_{k+1,r}T_{k+1,2^k+r} \mid r \in \mathbb{Z}_{2^k}\}$ построимо из B за $2^k \cdot 2^k + (2^k - 1) \cdot 2^k < 2 \cdot 4^k$ операций.

Далее, 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 $x_{1,2} = = \frac{-b \pm \sqrt{b^2-4c}}{2}$). При этом множество $P \cup B$ содержит

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

Следовательно, $\left\{T_{k+1,r} \mid r \in \mathbb{Z}_{2^{k+1}}\right\}$ 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 построимо из B за $11 \cdot 4^k$ операций. □

Доказательство основной теоремы. Из леммы 2 следует, что множество

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

построимо из $\{1\}$ за

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

операций. □

Список литературы

[1] А.А. Заславский, А.Б. Скопенков, М.Б. Скопенков, *Элементы математики в задачах*, Издательство МЦНМО (2018)

[2] Bruce C. Berndt, Ronald J. Evans, and Kenneth S. Williams, *Gauss and Jacobi Sums*, Canadian Mathematical Society Series of Monographs and Advanced Texts, Volume 21, John Wiley & Sons (1998)

[3] А.Р. Сафин, *Программа для построения правильных многоугольников циркулем и линейкой* [электронный ресурс], https://www.mccme.ru/mmks/dec08/Safin.pdf (2008)

[4] Дж. Литлвуд, *Математическая смесь*, Наука (1973)