Множественная сложность построения правильного многоугольника *

Е.С. 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 result is different from the standard estimation of complexity of an algorithm 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 — простое число Ферма, т.е. простое число вида $2^m + 1$, где m — степень 2, $\varepsilon := \cos\frac{2\pi}{p} + i\sin\frac{2\pi}{p}$. Тогда из $\{1\}$ можно получить некоторое множество, содержащее числа $1, \varepsilon, \varepsilon^2, \ldots, \varepsilon^{p-1}$, за $12p^2$ добавлений, определенных выше.

Эта работа может быть интересна читателю, так как на примере решения алгоритмической задачи иллюстрирует важный математический метод.

Назовем *множественной сложностью* сложность, рассмотренную в основной теореме. 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] и, возможно, [5]. О строгих

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

определениях различных понятий сложности см. [1]. Видимо, понятие множественной сложности совпадает с одним из сформулированных в этой книге, возможно, со сложностью как глубиной формулы. В любом случае, основная теорема не претендует на новизну. Даже если рассмотренное понятие сложности новое, доказательство не содержит новых идей.

Замечание. Из основной теоремы можно вывести следующее утверждение:

Пусть p — простое число Ферма. 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.

Известна история об аспиранте, который разработал построение правильного многоугольника с 65537 сторонами за 20 лет (см. [3]).

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 [2, п. 5.3.4]. Оценка же, получающаяся из доказательства построимости, приведенном в [2, конец п. 5.3.3], пропорциональна p^3.

Следующее изложение идеи доказательства заимствованно из [2, п. 5.3.4].

Идея доказательства основной теоремы для $p = 5$. Сразу выразить число ε через радикалы трудно, поэтому сначала выразим некоторые «многочлены от ε». Мы знаем, что $\varepsilon + \varepsilon^2 + \varepsilon^3 + \varepsilon^4 = -1$. Поэтому

$$(\varepsilon + \varepsilon^4)(\varepsilon^2 + \varepsilon^3) = \varepsilon + \varepsilon^2 + \varepsilon^3 + \varepsilon^4 = -1.$$

Обозначим

$$T_0 := \varepsilon + \varepsilon^4 \quad \text{и} \quad T_1 := \varepsilon^2 + \varepsilon^3.$$

Тогда по теореме Виета числа T_0 и T_1 являются корнями уравнения $t^2 + t - 1 = 0$. Поэтому можно выразить T_0 (и T_1). Поскольку $\varepsilon \cdot \varepsilon^4 = 1$, по теореме Виета числа ε и ε^4 являются корнями уравнения $t^2 - T_0 t + 1 = 0$. Поэтому 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 2 слагаемых T_0, T_1, которые можно получить добавлениями, описанными перед теоремой 1 (иными словами, *сгруппировать* хитрым образом корни уравнения $1 + x + x^2 + \ldots + x^{p-1} = 0$). Затем нужно разбить каждую сумму T_k на 2 слагаемых $T_{k,0}, T_{k,1}$, которые можно получить такими добавлениями. И так далее, пока не получим $T_{\underbrace{1,\ldots,1}_{s}} = \varepsilon$.

Однако придумать нужные группировки чисел $1, \varepsilon, \varepsilon^2, \ldots, \varepsilon^{p-1}$ — нетривиальная задача.

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

Введем 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 с. 1.

Обозначим через

- $p = 2^m + 1$ — простое Ферма;
- 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 $k \in \{0, 1, \ldots, m\}$, $r \in \mathbb{Z}_{2^m}$.

  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}, являющихся решениями сравнения

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

где $k \in \{0, 1, \dots, m-1\}$, $t \in \mathbb{Z}_{2^m}$.

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

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

Доказательство. Достаточно показать, что $N_{k,t} = N_{k,2^k+t}$. Для этого сопоставим каждому решению (c, d) сравнения (1) пару $(d, c-1)$. Эта пара будет решением сравнения (1) для t, замененного на $2^k + t$, поскольку следующие сравнения равносильны:

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

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

□

Лемма 2. Для любых $k \in \{0, 1, \dots, m-2\}$ 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.

$$T_{k+1,r}T_{k+1,2^k+r} = \left(\sum_{c=0}^{2^{m-k-1}-1} \varepsilon^{g^{2^{k+1}\cdot c+r}}\right) \cdot \left(\sum_{d=0}^{2^{m-k-1}-1} \varepsilon^{g^{2^{k+1}\cdot d+2^k+r}}\right) =$$

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

Доказательство равенства $(*)$ получается группировкой одинаковых слагаемых. Действительно, сравнение

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

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

$$g^{2^{k+1}\cdot c+r} + g^{2^{k+1}\cdot d+2^k+r} \equiv 0 \pmod p$$

не имеет решений, поскольку оно равносильно следующим:

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

Последнее сравнение не имеет решений, так как в левой части стоит четное число, а в правой нечетное (2^{m-k-1} четно, т. к. $k \le m-2$).

Равенство $(**)$ получается из леммы 1 путем группировки одинаковых $N_{k,r-s}$.

$\square$

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 1 до $m-1$ множество

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

построимо из множества

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

за $11\cdot 4^k$ операций.

Доказательство. Во-первых, для любых $k\in\{0,1,\dots,m\}$ 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.

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 берется по модулю 2^k, а не 2^{k+1}, т. к. $T_{k+1,r}T_{k+1,2^k+r} = T_{k+1,2^k+r}T_{k+1,2^k+(2^k+r)}$.

Из замечания после леммы 2 следует, что $P=\{1\}\subset B$ при $k = m-1$. Если же $k\le m-2$, 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 $x_{1,2}=\frac{-b\pm\sqrt{b^2-4c}}{2}$). Следовательно, $A':=\left\{T_{k+1,r}\mid r\in\mathbb{Z}_{2^{k+1}}\right\}$ 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, $\{0,1,\ \dots\ ,p\}\subset B$, поэтому A также построимо из B за $11\cdot 4^k$ операций. $\square$

Доказательство основной теоремы. Из леммы 3 следует, что множество

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

построимо из $\{1\}$ за

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

операций. $\square$

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.: Наука, 1973.

[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 // Canadian Mathematical Society Series of Monographs and Advanced Texts. Volume 21. John Wiley & Sons, 1998.