# Сложность алгоритмов при построениях циркулем и линейкой

М. В. Алехнович, А. Я. Канель-Белов, А. О. Сулейкин

Статья посвящена решению задачи 32.9 (выпуск 32, с. 181). Пусть на плоскости отмечены две точки $A$ и $B$ и задано натуральное число $n$. Наша цель — построить на прямой, проходящей через эти точки, третью точку $C$ так, чтобы длина отрезка $AC$ была в $n$ раз больше длины отрезка $AB$, с помощью линейки и (или) циркуля (при этом прямая $AB$ считается проведённой). На каждом шаге мы можем либо проводить линейкой прямую через две отмеченные точки, либо строить окружность с центром в отмеченной точке радиусом, равным расстоянию между отмеченными точками. При пересечении проведённых прямых и окружностей возникают новые отмеченные точки. Обозначим через Ц($n$) минимальное число шагов, необходимое при решении задачи одним циркулем, а через ЦЛ($n$) — число шагов, необходимых при решении её циркулем и линейкой. Задача заключается в оценке асимптотического поведения функций Ц($n$) и ЦЛ($n$). Основной результат работы заключается в следующем. Существуют такие константы $c_1, c_2 > 0$, что:

$$\text{а)}\ c_1 \ln n \leqslant \text{Ц}(n) \leqslant c_2 \ln n; \quad \text{б)}\ c_1 \ln\ln n \leqslant \text{ЦЛ}(n) \leqslant \frac{c_2 \ln n}{\ln\ln n}.$$

Наиболее интересный результат получается при нижней оценке функции ЦЛ($n$), где совершенно неожиданно возникают чисто алгебраические понятия, такие как высота числа и др.

Над статьёй совместно работали М. В. Алехнович и А. Я. Канель-Белов. Работа была завершена А. Я. Канель-Беловым и А. О. Сулейкиным.

## § 1. Используемые обозначения и вспомогательные утверждения

В этой статье будут рассматриваться несколько способов построений на плоскости (построения одним циркулем, циркулем и линейкой, одной линейкой и т. д.). С каждым способом построения связаны свои алгоритмы для достижения того или иного результата (деление отрезка пополам, увеличение его в $n$ раз и т. п.). Будем говорить, что способ построения $P$ *эквивалентен* способу $Q$ (обозначение: $P \sim Q$), если существует такая константа $c > 0$, что для любого алгоритма построения

для $P$, работающего за $k$ операций, существует имитирующий его алгоритм для $Q$, который работает не более чем за $c \cdot k$ операций, и наоборот, для любого алгоритма для $Q$ существует имитирующий алгоритм для $P$, причём время работы увеличивается не более чем в $c$ раз. Далее, если $f(x)$ — функция, то через $O(f(x))$, как обычно, обозначается любая такая функция $g(x)$, что существует константа $c > 0$, для которой $g(x) \leqslant c \cdot f(x)$ для всех $x$. В частности, $O(1)$ означает ограниченное число. Везде в данной работе в качестве $O(1)$ можно взять число 100. Если же

$$\lim_{x\to\infty} \left(\frac{g(x)}{f(x)}\right) = 0,$$

то $g(x) = o(f(x))$. Сформулируем без доказательства следующие известные факты.

Лемма 1.1. *Существуют алгоритмы построения за $O(1)$ действий*

а) *отрезка, равного по длине сумме двух отрезков, с помощью одного циркуля*;

б) *отрезка, равного по длине произведению двух отрезков, с помощью циркуля и линейки*;

в) *отрезка, равного по длине квадратному корню из заданного отрезка, с помощью циркуля и линейки.* □

Лемма 1.2. *Справедливо равенство*

$$\lim_{n\to\infty} \left(\frac{\Gamma^{-1}(n)}{\frac{\ln n}{\ln\ln n}}\right) = 1. \qquad \square$$

Напомним, что $\Gamma(x)$ — гамма-функция от действительной переменной, которая на натуральных числах совпадает с функцией $(n-1)!$, а $\Gamma^{-1}(x)$ — функция, обратная к $\Gamma(x)$.

## § 2. О формализации и роли математических понятий

Много говорят о *формализме*, неудобстве его восприятия, важность содержательной стороны противопоставляют формальной и т. д. Но тем не менее *формализация* — нечто очень важное и ценное. Почему?

Формализация необходима, чтобы сделать рассуждение объектом изучения средствами математики. Конструирование формализации даёт лучшее понимание сути и выявляет подводные камни, и, наконец, после формализации появляется возможность не приводить каждый

раз одно и то же рассуждение, а сослаться на теорему. Эта деятельность сродни *переводу*, и существуют *приёмы перевода* («нечто» — множество объектов, «определяет» — существует функция и т. д.). Этот математический канцелярит важно знать, так как если на него отвлекаться, то уйдёт суть. Когда мы решаем трудную задачу, мы строим воображаемый автомат, её решающий, но при этом необходимые понятия надо перевести на доступный для него язык. Формализация — не для нас, а для «автомата». Между формализацией и программированием, их трудностями есть глубокая связь. Например, тригонометрия автоматизирует рассуждения, связанные с подобными треугольниками. Автоматизированные и формализованные рассуждения суть *вычисления*.

Имея дополнительно формальный перевод, идею легче увидеть и применить. (Впрочем, любая переформулировка полезна, но работа с математическим объектом бывает удобнее.) Формализация не исчерпывает сущности (см. П. Флоренского о комплексных числах), объект может иметь много формализаций, каждая — взгляд со своей стороны. Например, *бесконечно малое* может быть формализовано как *дифференциал* (с помощью касательного отображения) или как в нестандартном анализе. Процедура формализации раскрывает важные вещи, и не формализуемое до конца нельзя до конца и понять. На самом деле кроме формального есть и другие уровни чёткости, так что формализацию и обоснование можно рассматривать в более широком контексте перевода.

Интересно, что в школьном курсе нет полной строгости. Например, такие важные понятия, как «теорема», «доказательство», не имели строгих определений. Они появились только в XX веке. Чтобы построить теорему, из которой вытекала бы её собственная недоказуемость, а тем самым — пример недоказуемого и неопровержимого утверждения, понадобилась формализация понятий «теорема», «доказательство» (удивительно, до какой степени она оказалась непростой!). Понятие *алгоритма* было формализовано, когда было установлено наличие алгоритмически неразрешимых проблем. В частности, таковой является проблема останова.

Дело в том, что в математике могут моделироваться не только объекты природы, но и сами рассуждения и математические конструкции. *Формализация* — это и есть такое моделирование. Только она делает из рассуждения математический объект. Это часто нужно в доказательствах невозможности чего-либо. Например, чтобы доказать разрешимость кубического уравнения в радикалах, достаточно вывести формулу, но чтобы доказать *неразрешимость* общего уравнения пятой

степени в радикалах, потребовалось формализовать само понятие *разрешимости* (что и сделал Абель). Эти алгебраические концепции, возникшие в начале XIX века, изменили лицо алгебры.

### 2.1. Радикалы и невозможность удвоения куба

Пусть $K$ — некоторое *поле*, т. е. множество (комплексных) чисел, замкнутое относительно арифметических операций, т. е. операций сложения, вычитания, умножения и деления (кроме деления на нуль). Над полями можно строить арифметику и производить все привычные конструкции, в частности рассматривать *векторные пространства* над $K$, их базисы, изучать размерности. *Расширение поля* $K$ набором чисел $\{x_i\}$ (обозначение: $K' > K$) есть множество чисел, получающееся из поля $K$ и набора $\{x_i\}$ с помощью арифметических операций. Иными словами, это минимальное по включению поле $K'$, содержащее $K \cup \{x_i\}$. Эти два понятия выглядят совершенно невинно, однако их достаточно для решения знаменитых задач древности об удвоении куба и трисекции угла. Мы это продемонстрируем, чтобы читатель отнёсся с должным уважением и к другим понятиям теории полей, отражающим глубокие идеи, которые необходимо не спеша продумать[1)].

Чтобы доказать возможность построения циркулем и линейкой, достаточно понимания процедуры с позиции обычного здравого смысла. Однако для доказательства *невозможности* необходимо саму процедуру построения сделать математическим объектом, т. е. *формализовать*. (Аналогичные разговоры следует вести при изучении построения одной линейкой.) Прежде всего, если задан единичный отрезок, несложно проверить, что все длины, которые мы можем построить, выражаются через 1 с помощью арифметических действий и вычисления квадратного корня[2)].

Начнём с упражнения, доступного читателю, знающему, как делить многочлены с остатком.

---

[1)] Короткие тексты с большой концентрацией идей весьма коварны (например, при изучении цепных дробей также сталкиваются с большим числом идей в коротком тексте, отсюда возникают методические проблемы). Такие тексты надо изучать *очень медленно*.

[2)] Координаты точки пересечения двух прямых выражаются через угловые коэффициенты прямых с помощью арифметических операций, а координаты точек пересечения окружности и прямой выражаются через координаты центра окружности, угловой коэффициент прямой и радиус окружности с помощью арифметических действий и операции извлечения квадратного корня; ситуация с пересечением двух окружностей аналогична.

Упражнение. Даны многочлен $P$ третьей степени и многочлен $Q$ второй степени, оба с рациональными коэффициентами. Докажите, что если $P$ и $Q$ имеют общий корень, то многочлен $P$ имеет рациональный корень.

Этот факт легко обобщается для произвольного числового поля.

Упражнение. Даны многочлен $P$ третьей степени и многочлен $Q$ второй степени, оба с коэффициентами из поля $K$. Докажите, что если $P$ и $Q$ имеют общий корень, то многочлен $P$ имеет корень в $K$.

*Квадратичным расширением $K'$ поля $K$* называется расширение поля $K$ корнем квадратного трёхчлена с коэффициентами из $K$.

Упражнение. Докажите, что каждый элемент из $K'$ либо принадлежит $K$, либо является корнем квадратного уравнения с коэффициентами из $K$.

Следствие 2.1. *Пусть поле $K$ есть квадратичное расширение поля $L$. Пусть многочлен $P$ с коэффициентами из $L$ имеет степень* 3 *и не имеет корня в $L$. Тогда у него нет и корня в $K$.* □

Следствие 2.2. *Пусть поле $K_{i+1}$ есть квадратичное расширение поля $K_i$, $i = 0, \ldots, n$, а многочлен $P$ с коэффициентами из $K_0$ имеет степень* 3 *и не имеет корня в $K_0$. Тогда у него нет и корня в $K_n$.* □

Предположим, что $\sqrt[3]{2}$ выражается через квадратные радикалы. Тогда существует такая *башня* (*квадратичных*) *расширений*, т. е. цепочка полей $K_0 = \mathbb{Q} \subset K_1 \subset \ldots \subset K_n$, что

- $\sqrt[3]{2} \in K_n$;
- $K_i$ есть квадратичное расширение поля $K_{i-1}$ для любого $i$, $1 \leqslant i \leqslant n$.

Понятие *башни квадратичных расширений* даёт формализацию понятия *разрешимости в квадратных радикалах*.

Следующее утверждение означает невозможность удвоения куба.

Следствие 2.3. *Корень уравнения $x^3 - 2 = 0$ не выражается в квадратных радикалах*[3)]. □

Для доказательства невозможности удвоения куба в пятимерном пространстве (т. е. невозможности построения $\sqrt[5]{2}$) достаточно ввести

[3)] В преподавании при разговоре о доказательстве невозможности удвоения куба с помощью циркуля и линейки (и аналогично о доказательстве невозможности трисекции угла) опять говорим о *процедуре формализации*, о том, как формализовать понятие *разрешимости уравнения в радикалах*, а также *разрешимости уравнения в квадратных радикалах*. Затем следует ввести понятие *башни* (*квадратичных*) *расширений*.

ещё одно понятие. Пусть $K' > K$ — расширение поля $K$. Тогда $K'$ можно рассматривать как векторное пространство над $K$, ибо любой элемент поля $K'$ можно умножить на любой другой элемент поля $K'$, в том числе и на элемент поля $K$. Размерность поля $K'$ над $K$ есть *степень поля $K'$ над $K$*, она обозначается $[K' : K]$.

Упражнение. Пусть $K'' > K' > K$. Докажите, что

$$[K'' : K] = [K'' : K'] \cdot [K' : K].$$

Указание. Пусть $\{e_i\}_{i=1}^n$ — базис поля $K'$ над $K$, а $\{f_j\}_{j=1}^m$ — базис поля $K''$ над $K'$. Тогда $\{e_i f_j\}_{i=1 j=1}^{n \quad m}$ есть базис поля $K''$ над $K$.

Иными словами, размерность подполя делит размерность поля. Если $K' \neq K$ есть квадратичное расширение поля $K$, то $[K' : K] = 2$. Если $F > K$ получается башней квадратичных расширений, то $[F : K]$ есть степень двойки. С другой стороны, $\mathbb{Q}[\sqrt[5]{2}]$ имеет размерность 5 над $\mathbb{Q}$, а пятёрка не делит степень двойки.

Упражнение. Докажите, что $\sqrt[5]{2}$ не выражается в квадратных и кубических радикалах.

Мы рекомендуем читателю обратиться к материалам 32-й Летней конференции международного математического Турнира городов.

## 2.2. Построения одной линейкой

Та же ситуация возникает с алгоритмами и с построением циркулем и линейкой.

Задача. Докажите, что с помощью одной линейки нельзя опустить из данной точки на прямую перпендикуляр.

Решение. Будем действовать от противного. Пусть существует правило (алгоритм), по которому мы можем опустить из данной точки перпендикуляр на данную прямую. Что это значит? Казалось бы, всё тут яснее ясного. Попробуйте, не читая дальше, определить понятие *алгоритма* сами. Оказывается, сконструировать определение такого, казалось бы, «очевидного» понятия далеко не просто! При этом до сих пор нам хватало интуитивного понимания для успешного проведения построений, а сейчас понадобилось определение. Разве это не удивительно?

*Процедура построения одной линейкой* состоит из следующих шагов.

1. Построение прямой, соединяющей две данные ранее построенные точки.
2. Построение точки пересечения ранее построенных прямых.

3. Взятие «произвольной» точки в ранее построенной области (на луче, прямой, отрезке, области плоскости, ограниченной ранее построенными линиями).

Шаг 3 не однозначен, результат не должен от него зависеть (подробности см. в разделе, посвящённом *глазомеру*).

Упражнение. Определите по аналогии процедуру построения циркулем и линейкой.

Перейдём к **решению**. Найдём образ прямой и не лежащей на ней точки при некотором аффинном преобразовании. Получим также прямую и не лежащую на ней точку. Будем поэтапно выполнять алгоритм построения перпендикуляра для прямой и её образа. Все шаги алгоритма сохранятся, ибо при аффинном преобразовании отрезок переходит в отрезок, прямая в прямую и т. д.

Но в результате выполнения алгоритма мы построим перпендикуляр. Его образ, коль скоро наш алгоритм корректно строит перпендикуляры, также будет перпендикуляром к образу прямой. С другой стороны, при правильно подобранном аффинном преобразовании образ уже перпендикуляром не будет. Мы получили противоречие. Значит, предположение неверно и с помощью одной линейки нельзя опустить перпендикуляр на прямую.

Следующая задача также неразрешима.

Задача. Докажите, что с помощью одной линейки нельзя провести через данную точку прямую, параллельную данной прямой.

Решение. При аффинном преобразовании параллельность сохраняется, так что предыдущее решение нуждается в модификации. Построение одной линейкой имеет более глубокие корни — проективные. Предположим, некий профессор Nobody изобрёл алгоритм и собирается осчастливить человечество своим открытием. Он демонстрирует его на слайде. Когда он проводит прямую, на экране тоже проводится прямая, когда он находит точку пересечения — на экране тоже строится точка пересечения.

Может, однако, так случиться, что линия, соединяющая точку пересечения двух прямых и источник света, будет параллельна плоскости экрана. Этого не произойдёт, если слайд параллелен плоскости экрана. Не произойдёт этого и если зафиксировать процесс построения и затем достаточно мало скосить плоскость экрана.

При этом, скосив экран подходящим образом, можно добиться, чтобы в результате на экране параллельная пара прямых перестала

быть параллельной. Но при этом процесс построения на экране будет по-прежнему корректным. Профессор Nobody оконфузился. Получили противоречие.

**Задачи**

1. Дана окружность. Можно ли построить её центр с помощью одной линейки?
2. Дана окружность, в которой проведён диаметр. Можно ли построить её центр с помощью одной линейки?
3. Проведите прямую, проходящую через недоступную точку пересечения двух прямых и точку, лежащую а) между прямыми; б) по одну сторону от прямых. (*Указание*. Воспользуйтесь конфигурацией из теоремы Дезарга.)
4. Дана недоступная прямая $T$, заданная двумя точками пересечения пар прямых $M_1, M_2$ и $N_1, N_2$ соответственно. Постройте прямую, проходящую через точку $P$ и пересекающую данную прямую $L$ на недоступной прямой $T$.
5. Даны окружность и точка. Одной линейкой постройте касательную к окружности, проходящую через эту точку, если точка а) лежит на окружности; б) не лежит.
6. Дана некоторая окружность с центром. Постройте с помощью одной линейки следующее:
   а) перпендикуляр из данной точки на данную прямую;
   б) отрезок на данной прямой с концом в данной точке, равный данному отрезку;
   в) точки пересечения прямой с окружностью, центр которой — данная точка, а радиус равен длине данного отрезка;
   г) точки пересечения двух окружностей, центры которых — данные точки, а радиусы — данные отрезки.
7. Даны две параллельные прямые. С помощью одной линейки разделите пополам отрезок, лежащий на одной из данных прямых.
8. Даны две параллельные прямые и отрезок, лежащий на одной из них. Удвойте этот отрезок.
9. Даны две параллельные прямые. Разделите отрезок, лежащий на одной из них, на $n$ равных частей.
10. Даны две параллельные прямые и точка $P$. Проведите через точку $P$ прямую, параллельную данным прямым.
11. Даны окружность, её диаметр $AB$ и точка $P$. Проведите через точку $P$ перпендикуляр к прямой $AB$ (см. [6])

## § 3. Построение одним циркулем

Известно (теорема Мора — Маскерони), что любое построение с помощью циркуля и линейки в принципе можно осуществить одним циркулем (прямые задаются парами точек). Доказательство этой теоремы основано на двух конструкциях:

1) построение точек пересечения окружности и прямой (в случае, когда центр окружности не лежит на прямой, это лёгкое упражнение);
2) построение точки пересечения двух прямых.

Последняя конструкция представляет собой основную трудность. Один из путей её осуществления — построение образов прямых и точек при инверсии. Однако процедура построения инверсного образа одним циркулем может потребовать сколь угодно большого числа действий (когда точка или прямая находятся близко к центру инверсии). И это не случайно: хотя без линейки и можно обойтись, её наличие может существенно экономить количество операций. На XXI Всероссийской математической олимпиаде была предложена следующая задача.

Задача. Пусть Ц($n$) — минимальное число линий, необходимых для увеличения отрезка в $n$ раз с помощью одного циркуля, а ЦЛ($n$) — с помощью циркуля и линейки. Докажите, что отношение Ц($n$)/ЦЛ($n$) не ограничено.

Приведём решение. Вначале докажем лемму.

Лемма 3.1. *Справедливо неравенство* $1 \leqslant \dfrac{\text{Ц}(n)}{\log_2 n} \leqslant O(1)$.

Доказательство. По условию мы можем строить циркулем окружности с центром в построенных ранее точках, причём имеем право делать раствор, равный какому-то уже построенному расстоянию. Ясно, что диаметр множества всех точек может увеличиться после построения одной окружности не более чем вдвое. Поэтому $\text{Ц}(n) \geqslant \log_2 n$. Но так как мы умеем строить сумму двух отрезков за $O(1)$ действий, мы сможем построить число $n$ за $O(\log_2 n)$ действий (достаточно рассмотреть двоичное разложение числа $n$). □

Для решения задачи остаётся заметить, что с помощью линейки мы можем за несколько действий возводить в квадрат (лемма 1.1). Таким образом, $\text{ЦЛ}(2^{2^n}) \leqslant O(n)$, а с другой стороны, $\text{Ц}(2^{2^n}) \geqslant 2^n$, и, значит,

$$\frac{\text{ЦЛ}(2^{2^n})}{\text{Ц}(2^n)} \geqslant \frac{2^n}{O(n)},$$

что при $n \to \infty$ стремится к бесконечности. Задача решена.

## § 4. Построение циркулем и линейкой

Перейдём к более подробному изучению построений. Мы убедились, что отношение Ц($n$)/ЦЛ($n$) не ограничено. В частности, при $n = 2^{2^k}$ и $k \to \infty$ это отношение стремится к бесконечности. Возникает вопрос: верно ли, что наличие линейки существенно экономит количество построений при всех $n \to \infty$?

Иными словами, равен ли предел $\lim\limits_{n\to\infty} \dfrac{\text{Ц}(n)}{\text{ЦЛ}(n)}$ бесконечности? Поскольку Ц($n$) имеет порядок $\ln n$ (по лемме 3.1), достаточно доказать следующий результат.

Лемма 4.1 (верхняя оценка). *Справедливо неравенство*

$$\text{ЦЛ}(n) \leqslant O\Big(\frac{\ln n}{\ln\ln n}\Big).$$

Доказательство. Приведём алгоритм построения. Представим $n$ в факториальной системе счисления:

$$n = a_1 \cdot 1! + a_2 \cdot 2! + \ldots + a_{[\Gamma^{-1}(n)]}[\Gamma^{-1}(n)]!, \quad a_i \leqslant i.$$

Будем строить число $n$ в три этапа.

1. Последовательно построим числа $1, 2, 3, \ldots, [\Gamma^{-1}(n)]$. Это требует $[\Gamma^{-1}(n)]$ сложений.
2. Последовательно построим числа $1!, 2!, 3!, \ldots, [\Gamma^{-1}(n)]$. Это требует не более $[\Gamma^{-1}(n)]$ умножений.
3. Пользуясь полученными числами, построим число $n$. Этот этап потребует не более $[\Gamma^{-1}(n)]$ сложений и $[\Gamma^{-1}(n)]$ умножений.

Поскольку каждое сложение и умножение можно осуществить за $O(1)$ операций (лемма 1.1) и

$$\Gamma^{-1}(n) = O\Big(\frac{\ln n}{\ln\ln n}\Big),$$

этот алгоритм обеспечивает нужную оценку. □

Итак,

$$\text{ЦЛ}(n) = O\Big(\frac{\ln n}{\ln\ln n}\Big).$$

Оказывается, эта асимптотика является точной. А именно, имеет место следующая лемма.

Лемма 4.2 (достижимость верхней оценки). *Существует такая константа $c > 0$, что для бесконечно многих $n$ выполняется неравенство*

$$\text{ЦЛ}(n) \geqslant \frac{c_2 \ln n}{\ln\ln n}.$$

Прежде чем перейти к доказательству, опишем его идею. Она состоит в том, что существует не более $(6n)!$ алгоритмов построения, работающих за $n$ шагов, и соответственно не более $(6n)!$ возможных результатов, которые не могут покрывать все числа от 1 до $(6n)!+1$.

Сформулируем вспомогательные утверждения.

Лемма 4.3. а) *Если проведено $n$ линий, то имеется не более чем $n^2$ точек пересечения.* б) *Если имеется не более чем $n^2$ точек пересечения, то можно провести не более $(n^2)^3$ прямых или окружностей.* □

Следствие 4.4. *Число способов построения за $n$ действий не превышает $(n!)^6 < (6n)!$.* □

Доказательство леммы 4.2. Выпишем по порядку все числа, которые могут быть получены в результате $n$ действий. Их не более $(6n)!$. Поэтому всегда существует натуральное $k$, меньшее чем $(6n)!$, которое не выписано. Это значит, что увеличение отрезка в $k$ раз не может быть получено за $n$ действий, где $n = [\Gamma^{-1}(k)/6]$. Итак, мы получили, что для бесконечного множества натуральных чисел $k \in \mathbb{N}$ выполняется неравенство

$$\text{ЦЛ}(k) \geqslant \frac{\Gamma^{-1}(k)}{6} \geqslant \frac{c_1}{6}\frac{\ln n}{\ln\ln n},$$

где $c_1$ — константа из леммы 1.2. □

Итак, для бесконечно многих $n$ (даже для «большинства») оценка $\ln n/\ln\ln n$ для ЦЛ$(n)$ существенно не улучшается. Тем не менее для некоторых «хороших» $n$ её улучшить можно. Например, имеет место следующий результат.

Лемма 4.5. *Если $n$ является степенью двойки, то* $\text{ЦЛ}(n) \leqslant O(\ln\ln n)$.

Доказательство. Пусть $n = 2^t$. Рассмотрим двоичное разложение числа $t$:

$$t = a_0 + 2a_1 + \ldots + 2^r a_r, \quad \text{где } r = [\log_2 n].$$

Тогда за $r$ операций умножения мы можем построить числа $1, 2, \ldots, 2^r$ и ещё за $r-1$ операцию умножения построить

$$n = 2^{a_0}\cdot 4^{a_1}\cdot\ldots\cdot(2^r)^{a_r}.$$

Остаётся заметить, что $r \sim \ln\ln n$. □

## 4.1. Основной результат. Нижняя оценка сложности

Предыдущее предложение показывает, что нижняя оценка в основной теореме достигается. Легко доказать аналогичное утверждение для $n = q^k$. Итак, для некоторых $n$ можно обойтись лишь $c\ln\ln n$ опе-

рациями. А каков самый удачный случай? Существуют ли такие $n$, которые можно построить ещё быстрее? Оказывается, асимптотика $\ln\ln n$ тоже является точной. Имеет место следующий результат.

Теорема 4.6 (нижняя оценка). *Существует такая константа $c>0$, что для любого $n$ выполнено неравенство* $\text{ЦЛ}(n) > c\ln\ln n$.

Это основной результат данной работы.

Чтобы понять общую ситуацию, начнём с изучения более простого случая. Рассмотрим задачу на построение одной линейкой. Сформулируем её так.

Задача. Дан единичный квадрат, в котором отмечены середины сторон. Оцените количество операций $\text{ЦЛ}(n)$, необходимое для построения отрезка длины $n$.

Следующая лемма аналогична лемме 1.1.

Лемма 4.7. *Пусть на плоскости отмечены вершины квадрата. Тогда с помощью одной линейки за $O(1)$ действий можно построить*

а) *сумму двух отрезков, лежащих на одной прямой, так, чтобы отрезок-сумма принадлежал той же прямой;*

б) *произведение двух отрезков, лежащих на одной прямой, так, чтобы отрезок-произведение принадлежал той же прямой.* □

Таким же способом, что и в предыдущем случае, можно доказать аналоги лемм 4.1, 4.2, 4.5.

Лемма 4.8.

а) *Существует такое $C$, что для всех $n$ выполнено неравенство*

$$\text{Л}(n) \leqslant C\frac{\ln n}{\ln\ln n}.$$

б) *Существует такое $c$, что для бесконечного множества значений $n$ выполнено неравенство*

$$\text{ЦЛ}(n) \geqslant c\frac{\ln n}{\ln\ln n}.$$

в) *Для любого числа $k$ существует такая константа $c(k)$, что*

$$\text{ЦЛ}(k^q) \leqslant c(k)\ln\ln(k^q).$$ □

Теперь перейдём к доказательству более простого аналога теоремы 4.6.

Теорема 4.9. *Существует такая константа $c>0$, что для любого $n$ выполнено неравенство $\text{Л}(n) > c\ln\ln n$.*

Доказательство. Введём на плоскости декартову систему координат и будем записывать уравнения всех возникающих линий и точек в аналитическом виде. Прямой будем считать набор из трёх коэффициентов, задающих её уравнение, точкой — пару координат. Очевидно, что можно выразить координаты точки пересечения прямых через коэффициенты этих прямых с помощью не более чем 30 операций из множества $\{+, -, \cdot, /\}$. Аналогично можно выразить коэффициенты прямой, проходящей через пару точек, через координаты этих точек не более чем за 30 операций из множества $\{+, -, \cdot, /\}$. Первоначально у нас отмечены точки $(0,0)$, $(0,1)$, $(1,0)$, $(1,1)$. Если мы докажем, что за $k$ арифметических операций из чисел 0, 1 мы не можем получить число, большее чем $2^{2^k}$, то утверждение будет доказано. Заметим, что все числа, возникающие в наших построениях, рациональны. Определим высоту $\mathrm{ht}(q) = \mathrm{ht}(m/n)$ рационального числа $q$, представленного в виде несократимой дроби $m/n$, как $|m| + |n|$.

Тогда

1) $\mathrm{ht}\Big(\Big(\frac{m}{n}\Big)^{-1}\Big) = \mathrm{ht}\Big(\frac{m}{n}\Big)$;

2) $\mathrm{ht}\Big(-\Big(\frac{m}{n}\Big)\Big) = \mathrm{ht}\Big(\frac{m}{n}\Big)$;

3) $\mathrm{ht}\Big(\frac{m_1}{n_1}\frac{m_2}{n_2}\Big) = |m_1 \cdot m_2| + |n_1 \cdot n_2| \leqslant$
$\leqslant (|m_1| + |n_1|) \cdot (|m_2| + |n_2|) = \mathrm{ht}\Big(\frac{m_1}{n_1}\Big) \cdot \mathrm{ht}\Big(\frac{m_2}{n_2}\Big)$;

4) $\mathrm{ht}\Big(\frac{m_1}{n_1} + \frac{m_2}{n_2}\Big) = |m_1 \cdot n_2 + m_2 \cdot n_1| + |n_1 \cdot n_2| \leqslant$
$\leqslant (|m_1| + |n_1|) \cdot (|m_2| + |n_2|) = \mathrm{ht}\Big(\frac{m_1}{n_1}\Big) \cdot \mathrm{ht}\Big(\frac{m_2}{n_2}\Big)$.

Таким образом, если $h$ — максимальная высота построенных нами чисел, то после выполнения любой операции максимальная высота не превышает $h^2$. Это означает, что если мы выполнили $k$ операций, то высота результата не превышает

$$\underbrace{\big(((2^2)^2)\dots\big)^2}_{k \text{ раз}} = 2^{2^k}.$$

Доказательство теоремы 4.9 завершено. □

Перейдём к **доказательству теоремы 4.6**.

Будем, как и в теореме 4.9, использовать аналитическое представление прямых и окружностей. Задача о построении циркулем и линейкой переводится на аналитический язык. С одной стороны, ариф-

метические операции и операция извлечения квадратного корня имеют интерпретацию на языке геометрических построений, а с другой стороны, координаты точек пересечения прямых или окружностей выражаются как корни линейных или квадратных уравнений.

В частности, любое число, которое можно построить с помощью циркуля и линейки, выражается через квадратные радикалы. (Поскольку числа $\pi$ и $\sqrt[3]{2}$ не выражаются через квадратные радикалы, а $\cos(\varphi/3)$ не выражается с помощью квадратных радикалов через $\cos(\varphi)$, три знаменитые проблемы древности о квадратуре круга, трисекции угла и удвоении куба оказались неразрешимыми.) Подробнее об алгебраических задачах, связанных с геометрическими построениями и решением уравнений в радикалах, рассказано в книге [1].

Итак, для доказательства основной теоремы следует показать, что за $n$ применений арифметических операций и операции извлечения корня нельзя построить числа, большие $m^{m^n}$, где $m$ — некоторая константа. Основная трудность состоит именно в наличии операции извлечения корня.

Как и в доказательстве предыдущей теоремы, постараемся определить *высоту* — «размер» числа — и проверить, что она растёт не слишком быстро. Для того чтобы избежать трудностей с корнем, мы будем представлять возникающие алгебраические числа в виде матриц с целыми коэффициентами. При этом извлечение корня будет преобразовываться в расширение матрицы до вдвое большего размера.

Если определять *высоту числа* стандартным образом — как сумму модулей коэффициентов его минимального многочлена, то нужные оценки не получатся. Дело в том, что высоты суммы и произведения $\mathrm{ht}(\alpha+\beta)$ и $\mathrm{ht}(\alpha\beta)$ оцениваются как $\mathrm{ht}(\alpha)^{\deg\beta}\,\mathrm{ht}(\beta)^{\deg\alpha}$. Нетрудно показать, что степень полученных не более чем за $n$ шагов чисел не превосходит $2^n$. В самом деле, квадратичное расширение удваивает размерность построенного числового поля. Поэтому размерность поля, порождённого значениями координат точек, построенных не более чем за $n$ шагов, не превосходит $2^n$. Степень алгебраического числа не больше размерности числового поля, в котором оно лежит. Таким образом, высота числа, построенного за $n$ шагов, оценивается величиной

$$\underbrace{(2^{2^n})^{2^n}\dots}_{n\text{ раз}} = 2^{n^2},$$

что позволяет получить лишь нижнюю оценку $\sqrt{\ln\ln n}$.

Однако оценки

$$\mathrm{ht}(\alpha)^{\deg\beta}\,\mathrm{ht}(\beta)^{\deg\alpha}$$

получаются с помощью техники симметрических многочленов. А это означает, что, используя эти оценки, мы работаем в нормальном замыкании числового поля, порождённого всеми ранее построенными величинами, которое в нашем случае может иметь степень $2^{2^n}$, что много больше, чем степень того расширения, которое нам нужно. Поэтому, чтобы не иметь дело с лишними расширениями, мы пользуемся представлением чисел матрицами.

## 4.2. Основные конструкции

Пусть $k$ — некоторое *числовое поле*, т. е. множество алгебраических чисел, замкнутое относительно арифметических операций. (Число называется *алгебраическим*, если оно является корнем уравнения с целыми коэффициентами.) Мы будем изображать элементы поля $k$ с помощью целочисленных матриц. При этом сумме чисел отвечает сумма соответствующих матриц, а произведению — произведение. Таким образом, мы работаем с некоторым коммутативным подкольцом $K_1 \subseteq M_n$.

Кроме того, мы будем всегда помнить, какое число какой матрице соответствует. Это значит, что вместе с подкольцом $K_1 \subseteq M_n$ всякий раз фиксируется некоторый гомоморфизм (т. е. отображение, сохраняющее операции сложения и умножения) из $K_1$ в поле действительных чисел. Этот гомоморфизм будет обозначаться через $F$.

Несколько сложнее обстоит дело с операцией извлечения квадратного корня из матрицы $A$. В исходном кольце $K_1$ осуществление такой операции может оказаться затруднительным, поэтому мы воспользуется следующим трюком из линейной алгебры: перейдём к другому матричному кольцу $K_2$, в котором корень из элемента, соответствующего $A$, строится явно.

Итак, пусть у нас есть матрица $A$, из которой нужно извлечь квадратный корень. Покажем, как расширить кольцо $K_1$ и доопределить гомоморфизм $F$ так, чтобы $A$ была квадратом некоторой матрицы. Рассмотрим кольцо $K_1' \subseteq M_{2n}$, $K_1' \simeq K_1$, где элементы кольца $K_1$ связаны с элементами кольца $K_1'$ следующим образом:

$$X \mapsto \begin{pmatrix} X & 0 \\ 0 & X \end{pmatrix}.$$

Обозначим $B = \begin{pmatrix} 0 & A \\ 1 & 0 \end{pmatrix}$. При этом $B^2 = \begin{pmatrix} A & 0 \\ 0 & A \end{pmatrix}$. Новое кольцо $K_2$ порождено кольцом $K_1'$ и элементом $B$. Нетрудно видеть, что $K_2$ — коммутативное кольцо, являющееся расширением кольца $K_1'$. При этом мож-

но доопределить гомоморфизм $F$ из $K_2$ в поле действительных чисел так, что $F(B)=\sqrt{F(A)}$. Отметим, что если в кольце $K_1$ уже существовал элемент $x$, дающий в квадрате $A$, то в $K_2$ появятся *делители нуля* (элементы с нулевым умножением). В самом деле, $(x-\sqrt{A})(x+\sqrt{A})=0$. Если же извлекается корень из делителя нуля, то могут возникнуть и *нильпотенты* (элементы, степени которых равны нулю), ибо

$$\left(\sqrt{x-\sqrt{A}}\cdot\sqrt{x+\sqrt{A}}\right)^2=0.$$

Теперь можно считать, что вместо чисел мы оперируем с матрицами. В самом начале у нас есть единичная матрица из кольца $M_1$ над $\mathbb{Z}$. Операции извлечения квадратного корня соответствует не алгебраическая операция, а расширение нашего кольца, при котором размер матриц увеличивается вдвое.

Чтобы обойти трудности, связанные с делением, воспользуемся той же конструкцией, что и при построении множества рациональных чисел с помощью пар целых. Мы будем работать с парами матриц и операциями

$$(A,B)+(C,D)=(AD+BC,BD),\ (A,B)\cdot(C,D)=(AC,BD),\ (A,B)^{-1}=(B,A)$$

и $\sqrt{(A,B)}=(\sqrt{A},\sqrt{B})$. Таким образом, при извлечении корня из дроби размер матриц будет увеличиваться в 4 раза.

Определим теперь для произвольной матрицы $A$ понятие *высоты* $\mathrm{ht}(A)$ как максимум модулей коэффициентов матрицы $A$. За высоту «дроби» $(A,B)$ примем максимум из высот матриц $A$ и $B$. Высота матриц, как нетрудно убедиться, обладает следующими свойствами.

Лемма 4.10.

а) *Справедливо неравенство* $\mathrm{ht}(A+B)\leqslant \mathrm{ht}\,A+\mathrm{ht}\,B$.

б) *Если* $A,B\in M_n$, *то* $\mathrm{ht}(A\cdot B)\leqslant n\cdot\mathrm{ht}\,A\cdot\mathrm{ht}\,B$.

в) *Справедливо равенство* $\mathrm{ht}\sqrt{A}=\mathrm{ht}\,A$. □

Из леммы 4.10 непосредственно получается следующий результат.

Лемма 4.11.

а) *Если мы произвели над парами матриц* $n$ *операций, то размер получившихся матриц не превосходит* $4^n$.

б) *Если мы произвели над парами матриц* $n$ *операций, то максимальная высота получившихся матриц не превосходит*

$$\underbrace{4^n\left(\ldots\left(4^n((4^n)^2)\right)^2\ldots\right)^2}_{n\ раз}=(4^n)^{(1+2+\ldots+2^n)}\leqslant 4^{n2^{n+1}}\leqslant 5^{5^n}.$$ □

Итак, мы получили пару матриц $A$ и $B$ высоты не более чем $5^{5^n}$. Теперь наша цель — оценить высоту $F(A)/F(B)$. Нам понадобятся несколько фактов и понятий из линейной алгебры.

*Характеристическим многочленом* матрицы $A$ называется многочлен от $x$, равный $\det(A - xE)$ (если формально раскрыть определитель), где $E$ — единичная матрица.

Хорошо известна следующая теорема.

Теорема 4.12 (Гамильтон — Кэли). *Если $f(x)$ — характеристический многочлен матрицы $B$, то $f(B) = 0$.* □

Теперь нам надо оценить коэффициенты и корни характеристического многочлена матрицы $A$, построенной за $n$ операций из предыдущей леммы.

Лемма 4.13. *Пусть $A$ — матрица из $M_n$, $\mathrm{ht}(A) < h$. Тогда модули коэффициентов её характеристического многочлена*

$$f(x) = (-1)^n x^n + a_{n-1}x^{n-1} + \ldots + a_0$$

*удовлетворяют оценке $|a_i| \leqslant (n!)^2 h^n$.*

Доказательство. Раскрывая формально определитель матрицы $A - xE$, получаем сумму, состоящую из $n!$ произведений вида

$$(a_{i_1 j_1} - x) \cdot (a_{i_2 j_2} - x) \cdot \ldots \cdot (a_{i_{l-1} j_{l-1}} - x) \cdot a_{i_l j_l} \cdot \ldots \cdot a_{i_n j_n}.$$

Модули коэффициентов при степенях $x$ в каждом из таких слагаемых не превосходят коэффициента при соответствующей степени в $(x + h)^n$, который, в свою очередь, не больше $n! \cdot h^n$. Отсюда получаем, что модули коэффициентов характеристического многочлена не больше $(n!)^2 h^n$. □

Лемма 4.14. *Пусть $f(x)$ — такой многочлен с целыми коэффициентами степени $n$, что модуль каждого его коэффициента не превышает $m$. Пусть $x$ — его корень. Тогда*

а) $|x| \leqslant n \cdot m$;

б) *если $x$ отличен от нуля, то $|1/x| \leqslant n \cdot m$.*

Доказательство. Докажем сначала пункт а). Предположим, что $x_0$ — корень и $x_0 > n \cdot m$. Но

$$|f(x_0)| = |a_n \cdot x_0^n + a_{n-1}x_0^{n-1} + \ldots + a_0| \geqslant$$
$$\geqslant |a_n \cdot x_0^n| - n \cdot (m \cdot x_0^{n-1}) \geqslant (x_0^{n-1}) \cdot (x_0 - n \cdot m) > 0.$$

Получили противоречие. Отсюда вытекает правильность оценки из пункта а).

Для доказательства пункта б) достаточно заметить, что если $x_0$ — корень многочлена $f(x)$, то $x_0^{-1}$ — корень многочлена, полученного при выписывании коэффициентов многочлена $f(x)$ в обратном порядке. □

### 4.3. Завершение доказательства теоремы 4.6

Допустим, что мы получили число $k$ за $n$ операций. На языке наших матриц это означает, что мы получили такую пару матриц $(A, B)$, что $k = F(A)/F(B)$, где $F(X)$ — наш гомоморфизм из матриц в числа.

Положим $a = F(A)$, $b = F(B)$. Оценим $a$ сверху.

Пусть $f(x)$ — характеристический многочлен матрицы $A$. Тогда по теореме Гамильтона — Кэли $f(A) = 0$, а значит, и $F(f(A)) = f(F(A)) = f(a) = 0$.

По лемме 4.11 высота матрицы $A$ не превышает $5^{5^n}$, следовательно, по лемме 4.13 модули коэффициентов многочлена $f(x)$ не превосходят

$$(n!)^2 \cdot (5^{5^n})^n = (n!)^2 \cdot 5^{n \cdot 5^n}.$$

Так как $a$ — корень многочлена $f(x)$, по лемме 4.14 получаем оценку

$$k \leqslant n \cdot (n!)^2 \cdot 5^{n \cdot 5^n},$$

а это выражение, начиная с некоторого $n$, меньше чем $6^{6^n}$.

Аналогично получается верхняя оценка $b^{-1} < 6^{6^n}$ с той лишь разницей, что мы оцениваем не сам корень характеристического многочлена, а обратную ему величину.

Итак, $k < 6^{6^n} \cdot 6^{6^n} < 7^{7^n}$ для всех $n > n_0$. Доказательство теоремы 4.6 завершено. □

Утверждение этой теоремы выглядит совершенно элементарно и невинно. Однако при доказательстве потребовалось довольно глубокое применение линейной алгебры. Неожиданным образом стали работать такие вещи, как расширения колец, матричные представления, теорема Гамильтона — Кэли, оценки определителей.

Замечание 4.15. Трюк, связанный с переходом к матрицам большего размера, проходит не только для операции извлечения квадратного корня, но и в общем случае. Чтобы присоединить корень уравнения

$$x^k = A_1 x^{k-1} + \ldots + A_k, \qquad (*)$$

надо перейти к матрицам в $k$ раз большего размера и в качестве $x$ взять матрицу

$$\begin{pmatrix} 0 & \ldots & 0 & 1 \\ 0 & \ldots & 1 & 0 \\ 0 & 1 & \ldots & 0 \\ A_1 & A_2 & \ldots & A_k \end{pmatrix}.$$

Так выглядит матрица оператора умножения на корень $x$ уравнения $(*)$ в базисе $1, x, \ldots, x^{k-1}$. При этом 1 переходит в $x$, $x$ — в $x^2$, …, $x^{k-1}$ — в $A_1 x^{k-1} + \ldots + A_k$ (см. [3]).

Основную теорему из данной работы можно обобщить так: высота числа, получившегося за $n$ последовательных алгебраических расширений, каждое из которых получено присоединением корня многочлена ограниченной степени с целыми ограниченными коэффициентами, имеет порядок, не больший $t^{t^n}$, где $t$ — некоторая константа.

Замечание 4.16. При доказательстве этой теоремы мы встретились с изучением коммутативных матричных алгебр. Опишем (без доказательства), как устроены гомоморфизмы таких алгебр в числовые поля. Пусть $A$ — подалгебра алгебры $(n \times n)$-матриц, действующая на $n$-мерном пространстве $V$; $a_1, a_2, \ldots, a_k$ — её образующие. Тогда $V$ разлагается в прямую сумму «жордановых клеток» — таких подпространств $V_I = V_{\lambda_{I_1} \lambda_{I_2} \ldots \lambda_{I_k}}$, что $a_j - \lambda_{I_j} E$ является нильпотентом на $V_{\lambda_{I_1} \lambda_{I_2} \ldots \lambda_{I_k}}$. Любому гомоморфизму $\varphi\colon A \to \mathbf{F}$ отвечает ограничение алгебры $A$ на некоторое инвариантное одномерное подпространство (содержащееся в некотором $V_I$), при этом $\varphi(a_s) = \lambda_{I_s}$. Множество всех гомоморфизмов алгебры $A$ в поле называется её спектром и обозначается $\mathrm{spec}(A)$. (Напомним, что спектральные линии веществ отвечают собственным значениям операторов в квантовой механике.)

## § 5. Введение глазомера и комплексных чисел

В этой части мы постараемся понять, почему время построения одним циркулем так сильно отличается от времени построения циркулем и линейкой. Одна из причин заключается в том, что уравнение второй степени не всегда имеет решение в поле действительных чисел, из-за чего две окружности (окружность и прямая) на плоскости часто не имеют точек пересечения.

Отметим, что процедура построения, которая рассматривалась выше, несколько отличается от обычной процедуры. Дело в том, что обычно разрешается операция выбора так называемой «произвольной» точки, прямой или окружности. Эта операция формализуется следующим образом.

Определение 5.1. Введём новый способ построения точек. Мы можем задать любую отмеченную точку $O$ и (не обязательно отмеченный) радиус $R$ и отметить некоторую точку, лежащую вне окружности с центром $O$ и радиусом $R$ (т. е. точку, удалённую от $O$ на расстоя-

ние, большее $R$). При этом алгоритм построения считается корректным, если результат не зависит от того, какая именно точка выбрана во внешности окружности с центром $O$. Назовём этот способ применением *слабого глазомера*.

*Сильный вариант глазомера* определяется так. Мы можем задать любую (не обязательно отмеченную) точку $P$ и любой (не обязательно отмеченный) радиус $\varepsilon$ и отметить точку из окрестности $U_\varepsilon(P)$. Алгоритм считается корректным, если конечный результат не зависит от того, куда именно в заданной окрестности попала отмеченная точка. Этот способ назовём применением сильного глазомера. Очевидно, что с помощью сильного глазомера можно имитировать слабый глазомер.

После того как мы определили два варианта глазомера, становится возможным с помощью комбинирования допустимых инструментов получать много новых способов построения на плоскости (Ц, Ц + Сильный глазомер, ЦЛ + Слабый глазомер и т. д.).

Постараемся понять, насколько эффективнее становятся способы построения, если в них добавить глазомер. Впоследствии окажется, что Ц + Слабый глазомер $\sim$ ЦЛ + Слабый глазомер $\sim$ ЦЛ + Сильный глазомер.

Из элементарной геометрии известно, что любое построение циркулем и линейкой можно выполнить одним лишь циркулем (в традиционном смысле) за число действий, превышающее ЦЛ лишь в константу раз. Дело в том, что, выбирая «произвольные» точки общего положения, можно добиваться того, что нужные линии имеют точки пересечения.

Лемма 5.2. *С помощью применения слабого глазомера и циркуля можно находить точки пересечения прямой, заданной двумя точками, и окружности, а также точку пересечения двух прямых, заданных по двум точкам, за время, не большее $O(1)$ построений.*

Доказательство. Задача о нахождении точки пересечения прямой и окружности — несложное упражнение, поэтому единственным трудным фактом в лемме является алгоритм построения точки пересечения двух прямых. Схема этого алгоритма состоит в том, чтобы инверсией перевести эти прямые в окружности, найти точку их пересечения и отразить её обратно (см. [4, с. 31–33]). Это и будет точка пересечения заданных прямых.

Сложность заключается в том, что с помощью одного циркуля можно быстро строить инверсные образы не всех точек и прямых, а лишь тех, которые удалены от центра инверсии на расстояние порядка ра-

диуса окружности, относительно которой делается инверсия. Поэтому надо выбрать центр и радиус этой окружности так, чтобы каждая из заданных прямых и точка их пересечения располагались на расстоянии порядка радиуса.

Для этой цели мы выбираем с помощью слабого глазомера точку $X$, удалённую от наших пар точек (задающих прямые) и точки их пересечения на расстояние $l$, много большее диаметра множества, составленного из этих точек. Далее мы строим правильный шестиугольник с вершиной в точке $X$ и с центром в одной из точек, задающих прямые. Одна из вершин шестиугольника удалена от обеих прямых и наших точек на расстояние порядка $l$ (т. е. не больше чем $2l$ и не меньше чем $l/6$). □

Следствие 5.3. Ц + *Слабый глазомер* ∼ ЦЛ + *Слабый глазомер*. □

Постараемся понять, что означает выбор случайной точки на алгебраическом языке. Любой алгоритм построения циркулем (циркулем и линейкой) может иметь следующую трактовку.

Определение 5.4. Пусть имеется некоторое множество чисел (отмеченные точки). За один шаг можно выбрать любые два числа из этого множества и добавить в него их сумму, произведение, частное или корень из элемента, принадлежащего множеству. Будем называть этот способ построением с помощь *калькулятора*.

Лемма 5.5. ЦЛ ∼ *Калькулятор*.

Доказательство. Поставим в соответствие каждому алгоритму построения циркулем (циркулем и линейкой) алгоритм на калькуляторе, записав координаты точек пересечения прямых и окружностей в аналитической форме. Это можно сделать, так как существует алгебраическая формула, выражающая точку пересечения двух окружностей (двух прямых, прямой и окружности) через уравнения этих окружностей. С другой стороны, для любого алгоритма построения на калькуляторе существует эквивалентный алгоритм построения циркулем и линейкой. В самом деле, с помощью ЦЛ возможно реализовать все арифметические операции и операцию извлечения квадратного корня. □

Введение возможности глазомера на калькуляторе соответствует тому, что наш калькулятор работает не только с числами, но и с выражениями в радикалах от некоторого набора переменных $x_1, x_2, \ldots, x_n$. Каждой переменной $x_i$ соответствует её область определения — некоторый отрезок $[a_i, b_i]$ (если глазомер сильный) или $[a_i, +\infty)$ (если глазомер слабый), который мы задаём, выбирая случайную точку.

Алгоритм вычисления считается корректным, если для любого набора значений $x_1, \ldots, x_n$ из области определения наше выражение-результат определено на нём и не зависит от выбора точек.

Следующая лемма означает возможность «избавления от иррациональности в знаменателе».

Лемма 5.6. *Пусть $f(x_1, x_2, \ldots, x_n)$ — функция, выражающаяся через операции из множества $\{+, -, \cdot, \sqrt{}\}$. Тогда существует функция $g(x_1, x_2, \ldots, x_n)$, обладающая тем же свойством и такая, что*

$$f(x_1, \ldots, x_n) \cdot g(x_1, \ldots, x_n) = P(x_1, \ldots, x_n),$$

*где $P$ — полином.* □

Ясно, что мы можем представить наше выражение на калькуляторе в виде

$$\frac{f_1(x_1, x_2, \ldots, x_n)}{f_2(x_1, x_2, \ldots, x_n)},$$

где $f_1, f_2$ — выражения, не использующие деление. По лемме 5.6 из того, что выражение $f_1/f_2$ не зависит от выбора переменных $x_i \in [a_i, b_i]$, следует, что это выражение является константой для всех значений, для которых оно определено. В каких случаях выражение, составленное из операций $\{+, \cdot, -, /, \sqrt{}\}$, может быть не определено? Либо когда возникает корень из отрицательного числа (отсутствие пересечений), либо когда возникает деление на нуль, которое при построении циркулем (циркулем и линейкой) соответствует некоторому вырождению (концентрическим окружностям или параллельным прямым). Чтобы избавиться от трудностей с извлечением квадратного корня, мы выйдем на комплексную плоскость $\mathbb{C}^2$. Мы покажем, что «комплексные» операции можно осуществить «вещественными» средствами. Остаётся следить только за тем, чтобы знаменатель не обращался в нуль.

## 5.1. Комплексные построения

Пусть мы работаем в комплексной плоскости $\mathbb{C}^2$. Прямые задаются уравнениями $ax + by + c = 0$, где $a, b, c$ — комплексные числа; окружности — уравнениями $(x + a)^2 + (y + b)^2 = r^2$, где $a, b, r$ — комплексные числа. Мы можем также обобщить понятие калькулятора, позволяя ему оперировать с комплексными числами, и получить *комплексный калькулятор*. Для комплексного калькулятора можно так же, как и для вещественного, определить понятие сильного и слабого глазомера (сильный позволяет выбирать точку в любом открытом множестве, а слабый — в любой окрестности бесконечности вида $\{|z| > R\}$).

Лемма 5.7. ЦЛ *на комплексной плоскости* ∼ *Комплексный калькулятор* ∼ *Вещественный калькулятор* ∼ ЦЛ *на вещественной плоскости*.

Доказательство. Мы уже убедились в эквивалентности Вещественный калькулятор ∼ ЦЛ на вещественной плоскости. Эквивалентность ЦЛ на комплексной плоскости ∼ Комплексный калькулятор доказывается аналогично.

Таким образом, осталось показать эквивалентность комплексных и вещественных калькуляторов. В самом деле, комплексное число $z = x + iy$ можно рассматривать как пару вещественных чисел $x$ и $y$. Арифметическим операциям над комплексными числами соответствуют арифметические операции над их вещественными и мнимыми частями. Несколько сложнее обстоит дело с операцией извлечения квадратного корня. Для этого можно воспользоваться следующими формулами:

$$\sqrt{z} = \sqrt{|z|} \cdot \left(\cos\frac{\varphi}{2} + i \cdot \sin\frac{\varphi}{2}\right),$$

где

$$|z| = \sqrt{x^2 + y^2}, \quad \varphi = \arg z, \quad \cos\varphi = \frac{x}{|z|}, \quad \sin\varphi = \frac{y}{|z|}.$$

Косинус и синус половинного угла выражаются по формулам

$$\cos\left(\frac{\varphi}{2}\right) = \sqrt{\frac{1+\cos\varphi}{2}}, \quad \sin\left(\frac{\varphi}{2}\right) = \sqrt{\frac{1-\cos\varphi}{2}}. \qquad \square$$

Из этой леммы вытекают следующие эквивалентности: Вещественный калькулятор + Сильный глазомер ∼ Комплексный калькулятор + Сильный глазомер, Вещественный калькулятор + Слабый глазомер ∼ Комплексный калькулятор + Слабый глазомер.

Отметим, что если бы мы работали с кубическими корнями, то с помощью вещественного калькулятора нельзя было бы сымитировать комплексный. Дело в том, что для извлечения кубического корня из комплексного числа нужно уметь не только извлекать кубические корни из вещественных чисел, но и решать задачу «трисекции угла» (т. е. нахождения $\cos(\varphi/3)$ по $\cos\varphi$).

Покажем, что на комплексной плоскости Ц ∼ ЦЛ. Опишем сначала идею доказательства. Мы знаем, что циркуль с помощью глазомера может находить точку пересечения двух прямых (прямой и окружности). Правда, при этом нам нужно выбирать некоторые «случайные» точки из заданной окрестности. Как будет показано ниже, вместо них можно выбирать произвольные точки плоскости с одним лишь ограничением, чтобы было обеспечено наличие нужных пересечений. В вещественном случае наблюдаются «неприятности» двух типов: извлечение

корня из отрицательного числа и деление на нуль. После перехода в комплексную плоскость остаются только «вырождения», связанные с делением на нуль, а таковых должно быть не слишком много. В некоторых случаях их удаётся избежать путём имитации случайного выбора: если построить много разных точек, то какие-нибудь из них могут подойти для алгоритма в качестве «случайных» и вырождения не произойдёт. Перейдём к доказательствам.

Несложно доказать следующее утверждение.

Лемма 5.8. *Пусть выбрана система координат и отмечены точки с координатами* $(0,0)$, $(x,0)$, $(y,0)$ (*где* $x$ *и* $y$ *— вещественные числа*). *Тогда за* $O(1)$ *действий одним циркулем без глазомера можно отметить точку с координатами* $(x,y)$. □

Лемма 5.9. *Пусть* $P(x_1, x_2, \ldots, x_n)$ *— полином степени* $k$, *отличный от тождественного нуля. Пусть* $A = \{a_1, a_2, \ldots, a_k, a_{k+1}\}$ *— некоторый набор различных чисел. Тогда переменным* $x_1, \ldots, x_n$ *можно присвоить значения из* $A$ *так, что* $P$ *не обратится в нуль на этих значениях.*

Доказательство. Так как многочлен $P$ не является тождественным нулём, существует такой набор значений $c_1, c_2, \ldots, c_n$, что $P$ не обращается в нуль. Фиксируем все значения, кроме первого, и будем рассматривать $P$ как многочлен от одной переменной $P(x_1)$, степень которого не больше $k$. Тогда для $x_1$ можно подобрать значение $c_1'$ из множества $A$ так, что $P(x_1) \neq 0$. Так мы получим такой набор $c_1', c_2, \ldots, c_n$, что $P$ не обращается в нуль. Действуя по индукции, можно получить набор значений, целиком состоящий из элементов $A$ и такой, что $P$ не обращается в нуль. □

Следствие 5.10. *Пусть имеется алгоритм для калькулятора с сильным* (*слабым*) *глазомером, работающий с вещественными или комплексными числами и использующий* $n$ *случайных переменных* $x_1$, $x_2$, …, $x_n$. *Тогда в качестве случайных переменных могут быть использованы любые* $n$ *чисел* $a_1, a_2, \ldots, a_n$, *для которых результат калькулятора определён.* □

Следствие 5.11. ЦЛ + *Сильный глазомер* ∼ ЦЛ + *Слабый глазомер*.

Доказательство. Так как ЦЛ + Сильный глазомер ∼ Вещественный калькулятор + Сильный глазомер и ЦЛ + Слабый глазомер ∼ Комплексный калькулятор + Слабый глазомер, достаточно показать эквивалентность глазомеров для калькулятора, оперирующего с комплексными числами. Для этого нужно выбрать «случайные» перемен-

ные, используя слабый глазомер, так, чтобы знаменатель не обратился в нуль. □

Теорема 5.12. Ц *на* $\mathbb{C}^2 \sim$ ЦЛ *на* $\mathbb{C}^2$.

Доказательство. Докажем, что с помощью одного циркуля на комплексной плоскости можно построить точку пересечения двух прямых, заданных по двум точкам, не используя глазомер. По лемме 5.2 существует алгоритм построения, использующий глазомер, работающий за 100 операций. Пусть этот алгоритм требует выбора $n$ случайных точек $(x_1, y_1)$, $(x_2, y_2)$, …, $(x_n, y_n)$. Рассмотрим соответствующее построение на калькуляторе. Пусть мы получили в пересечении точку $(x, y)$, где

$$x = \frac{f_1(x_1, y_1, \ldots, x_n, y_n)}{f_2(x_1, y_1, \ldots, x_n, y_n)}, \quad y = \frac{f_3(x_1, y_1, \ldots, x_n, y_n)}{f_4(x_1, y_1, \ldots, x_n, y_n)}.$$

Пусть $f_2 \cdot f_4 \cdot g = P$, где $P$ — полином степени $k$. Рассмотрим множество $A = \{1, 2, 3, \ldots, k+1\}$. По лемме 5.9 переменным $x_1, y_1, \ldots, x_n, y_n$ можно присвоить значения из $A$ так, чтобы знаменатель не обратился в нуль. По лемме 5.8 мы можем отметить точки $(x_i, y_i)$ за время $200 \cdot (k+1)$ (сначала строим точки $(1, 0), (2, 0), \ldots, (k+1, 0)$, а потом уже строим $(x_i, y_i)$). Если теперь мы применим алгоритм с глазомером и будем выбирать эти точки вместо случайных точек, мы корректно построим точку пересечения данных прямых. Абсолютно аналогично доказывается, что за постоянное число операций можно найти точки пересечения прямой и окружности. Мы доказали, что на комплексной плоскости Ц $\sim$ ЦЛ. □

## § 6. Заключительные замечания. Задачи и перспективы

В данной работе мы рассмотрели задачи, связанные со сложностью вычислений. Нашей главной целью было не столько получить те или иные результаты, сколько показать читателю, как естественным образом одна за другой возникают задачи и как строится научное исследование.

Результаты, изложенные в предложениях 4.1, 4.2, 4.5 и в теореме 4.6, следует считать окончательными. Почему все оценки сложности следует осуществлять с точностью до постоянного множителя? Дело в том, что вычисление соответствующих констант представляется нереальным. При этом те или иные «инженерные» улучшения ничего принципиально нового не дают. Построение оптимальных алгоритмов

скорее относится к области головоломок. А головоломки интересны тогда, когда они изящны, т. е. оперируют малым материалом.

Для дальнейшего знакомства с задачами, относящимися к построениям с ограничениями, мы отсылаем читателя к брошюре [4]. Наша же цель — познакомить читателя с математическими задачами, которые непосредственно примыкают к теме данной статьи и решение которых нам неизвестно.

1. Верно ли, что $Л(n)/ЦЛ(n)$ не ограничено? Иными словами, может ли операция извлечения корня существенно сокращать «рациональные вычисления»?
2. Позволяет ли глазомер существенно экономить вычисления? Если перевести это на язык «калькулятора», то верно ли, что недетерминированный способ построения позволяет в некоторых случаях получить существенный выигрыш? Выигрыш этот может быть достигнут только за счёт того, что трансцендентные промежуточные параметры позволяют избегать появления нуля в знаменателе. Но можно ли за ограниченное число линий эти параметры сымитировать? Более общая задача такова: показать эквивалентность детерминированной и недетерминированной вычислительных схем.
3. Мы рассматривали только квадратичные расширения. Однако, действуя так же, как и в доказательстве теоремы 4.6, можно получить аналогичные результаты для расширений бóльших порядков (см. замечание 4.15). Вместе с тем возникают дополнительные вопросы: даёт ли комплексный калькулятор в случае извлечения кубических корней существенное преимущество над вещественным (в случае вычисления целых чисел)? Верно ли, что наличие возможностей вычисления разных корней, например кубического и квадратного, приводит к существенным упрощениям в вычислениях различных классов чисел?
4. Пусть числа $x_i$ задаются системой $k$ уравнений $\{P_j(\vec{x}) = 0\}$, где $P_j(\vec{x}) = P_j(x_1, \ldots, x_k)$ — многочлен степени $n$ от $k$ переменных, причём $n \ll k$. Интересно было бы получить оценку на высоты чисел $\{x_i\}$.

Наиболее перспективным представляется подход, связанный с построением матричного представления факторкольца $C[\vec{x}]/\mathrm{id}(\{P_j(\vec{x})\})$. Высоту можно оценить исходя из размеров матриц и величины коэффициентов. Размер же матриц можно оценить как $k^\gamma$, где $\gamma$ — размер базиса Грёбнера идеала $\mathrm{id}(\{P_j(\vec{x})\})$, порождённого набором многочленов $\{P_j(\vec{x})\}$.

Для дальнейшего знакомства с проблематикой, связанной со сложностью алгебраических вычислений, советуем обратиться к учебнику [5].

Результаты, изложенные в предложениях 4.1, 4.2, 4.5, были получены независимо С. Б. Гашковым. Авторы приносят благодарность О. Н. Попову за идею доказательства предложения 4.1.

## Список литературы

[1] *Алексеев В. Б.* Теорема Абеля в задачах и решениях. М.: Наука, 1976.

[2] *Ван дер Варден Б. Л.* Алгебра. М.: Наука, 1979.

[3] *Ленг С.* Алгебра. М.: Мир, 1968.

[4] *Костовский А. Н.* Геометрические построения одним циркулем. Сер. Популярные лекции по математике. Вып. 29. М.: Наука, 1984.

[5] *Латышев В. Н.* Комбинаторная теория колец. Сложность алгебраических алгоритмов. М.: МГУ, 1987.

[6] *Канель-Белов А. Я.*, *Нилов Ф. К.*, *Радзивиловский Л. В.* Задача Мишустина // Потенциал. 2022. № 11. С. 19–22.

---

Михаил Владимирович Алехнович, университет Сан-Диего

Алексей Яковлевич Канель-Белов, МФТИ, университет Бар-Илана
kanelster@gmail.com

Аллан Олегович Сулейкин, мехмат МГУ
allan.suleykin@math.msu.ru