Дальневосточный математический журнал. 2024. Т. 24. № 1. С. 45–54

УДК 511.321 + 511.31
MSC2020 11B39

© И. Д. Кан[1]

Достижимость неравенств из теоремы Ламе

В настоящей работе доказывается следующий результат. Число шагов в алгоритме Евклида для двух натуральных аргументов, меньший из которых имеет v цифровых разрядов в десятичной системе счисления, не превосходит целой части от дроби $(v+\lg(\sqrt{5}/\Phi))/\lg\Phi$, где $\Phi = (1+\sqrt{5})/2$, причем эта оценка достигается при каждом натуральном v. Доказывается также, что для двух других известных верхних оценок длины алгоритма Евклида справедливы частичная или асимптотическая достижимости.

Ключевые слова: *теорема Ламе, алгоритм Евклида.*

DOI: https://doi.org/10.47910/FEMJ202405

1. История вопроса

Знаменитый алгоритм Евклида находит, чему для двух заданных отрезков целой длины равна их максимальная общая единица измерения. Пусть, скажем, длины этих отрезков равны a и b, где $a \geqslant b$. Тогда положим $a = r_0$, $b = r_1$ и произведем серию делений с остатком. Первоначально a делится с остатком на b: пусть при этом получатся неполное частное q_1 и остаток r_2. Затем b делится с остатком на этот остаток r_2, в результате чего появляется частное q_2 и остаток r_3 и так далее. Как только в какой-то момент при делении с остатком произошло деление нацело, то делитель в этом делении — и есть наибольший общий делитель чисел a и b. Другими словами, НОД натуральных чисел a и b равен последнему ненулевому остатку в алгоритме Евклида.

Этот алгоритм выражается алгебраически следующими формулами: пусть

$$\begin{aligned}
&a = r_0 = q_1 b + r_2, && 0 < r_2 < b,\\
&b = r_1 = q_2 r_2 + r_3, && 0 < r_3 < r_2,\\
&r_2 = q_3 r_3 + r_4, && 0 < r_4 < r_3,\\
&\dots && \dots\\
&r_{n-2} = q_{n-1} r_{n-1} + r_n, && 0 < r_n < r_{n-1},\\
&r_{n-1} = q_n r_n + 0, && 0 = r_{n+1} < r_n,
\end{aligned}$$

[1] Московский авиационный институт (национальный исследовательский университет), 125993, г. Москва, Волоколамское шоссе, 4. Электронная почта: igor.kan@list.ru

тогда
$$r_n = \text{НОД}(a, b).$$

Заметим, что в таких обозначениях алгоритм Евклида требует именно n делений с остатком: каждому из этих действий соответствует некоторое неполное частное q_j, где j пробегает значения от 1 до n.

Пусть v — количество цифр в десятичной записи меньшего из двух аргументов алгоритма Евклида, $n = n(v)$ — максимальное число делений с остатком в этом алгоритме при заданном значении v. Известна классическая теорема об алгоритме Евклида, доказанная Г. Ламе в 1845 году.

Формулировка теоремы Ламе. *Выполнено следующее соотношение между v и n:*
$$n \leqslant 5v. \tag{1}$$

Другими словами, максимальное количество делений с остатком, необходимое для вычисления наибольшего общего делителя двух натуральных чисел с помощью алгоритма Евклида, не превосходит пятикратного количества цифр в десятичной записи меньшего из этих двух чисел.

Теорема Ламе вошла во многие учебники по теории чисел. Для доказательства этой теоремы обычно сравнивают остатки из алгоритма Евклида
$$r_1, r_2, r_3, \ldots, r_n,$$
записанные в обратном порядке, с числами Фибоначчи F_n:
$$0, 1, 1, 2, 3, 5, 8, 13, \ldots$$
(здесь $F_0 = 0, F_1 = 1$ и для всех натуральных n выполнено рекуррентное соотношение $F_{n+1} = F_n + F_{n-1}$, которым и определяются числа Фибоначчи). Так, известно неравенство, выполненное для каждого $i = 0, 1, \ldots, n-1$:
$$r_{n-i} \geqslant F_{i+2}. \tag{2}$$

Неравенство (2) легко доказывается индукцией по i. Далее для чисел Фибоначчи, как правило, применяется индуктивно доказываемое неравенство
$$F_j \geqslant \Phi^{j-2}, \qquad j = 1, 2, \ldots,$$
где $\Phi = (\sqrt{5}+1)/2$. При подстановке этого неравенства в (2) получается оценка
$$r_{n-i} \geqslant \Phi^i. \tag{3}$$

Учитывая, что $b = r_1$, получаем, что, с одной стороны, $b < 10^v$ как v-значное число, и, с другой стороны,
$$10^v > b = r_1 \geqslant \Phi^{n-1} \tag{4}$$
на основании неравенства (3). Логарифмируя, из (4) получаем
$$n < \frac{v}{\lg \Phi} + 1. \tag{5}$$

Отсюда, так как $\lg\Phi > 0.2$, и получается неравенство (1).

Такая схема доказательства применяется, например, в [1]. Таким образом, неравенство (1) является огрублением более точной оценки (5). Эта оценка (5) сформулирована также и во втором томе “Искусства программирования” Д. Кнута как более точная по сравнению с теоремой Ламе [2]. Однако на самом деле оценка (5) также является точной не всегда — не при каждом значении v. Например, неравенство

$$n \leqslant \left[\frac{v}{\lg\Phi} + 1\right], \tag{6}$$

следующее из (5) непосредственно, при $v=4$ дает оценку $n \leqslant 20$ — в то время как правильный ответ равен в этом случае 19.

Одна из целей настоящей работы состоит в уточнении неравенства (6) при сохранении структуры этой формулы. Так, подобно соотношению (6), в итоговом выражении для величины n внутри квадратных скобок, представляющих собой целую часть числа (округление до ближайшего целого в меньшую сторону), будет находиться также некоторая линейная неоднородная функция от аргумента v.

2. Основной результат статьи

Пусть величины n и v имеют определенный выше смысл. Главная цель настоящей работы состоит в доказательстве следующей теоремы.

Теорема 1. *Во-первых, выполнено равенство*

$$n = \left[\frac{v + \lg\frac{\sqrt{5}}{\Phi}}{\lg\Phi}\right]. \tag{7}$$

Во-вторых, для любого ρ из интервала $(0,1)$ и для любого положительного числа ε найдется бесконечно много v таких, что для чисел v и $n=n(v)$ справедливо неравенство

$$\left| n - \left(\frac{v + \lg\frac{\sqrt{5}}{\Phi}}{\lg\Phi} - \rho\right)\right| < \varepsilon. \tag{8}$$

В-третьих, неравенство (6) выполняется как равенство для бесконечно многих v (но не для всех v).

В-четвертых, неравенство (1) выполняется как равенство тогда и только тогда, когда $v \leqslant 3$.

Замечание 1. Пусть, как и выше, меньший из двух аргументов алгоритма Евклида представляет собой v-значное число. Оценку длины алгоритма Евклида для этого случая назовем *достижимой...*

... *частично*, если она выполняется как равенство только для конечного количества значений v;

... *асимптотически*, если она выполняется как равенство не для всех натуральных значений v, но для бесконечного их количества;

... *тотально*, если она выполняется как равенство для всех натуральных значений v.
Тогда формулы (1), (6) и (7) представляют собой частично, асимптотически и тотально достижимые оценки длины алгоритма Евклида соответственно.

3. Свойства чисел Фибоначчи

В этом разделе напоминаются и, как правило, доказываются, в основном известные свойства чисел Фибоначчи, необходимые для вывода теоремы 1. Эти и многие другие свойства можно найти, например, в книге [3].

3.1. Четность чисел Фибоначчи. *Число F_n четно тогда и только тогда, когда n делится на 3.*

Доказательство этого свойства. Обозначим через $(F_n)_2$ остатки чисел F_n от деления на 2. Напомним, что числа F_n удовлетворяют рекуррентному соотношению $F_{n+1}=F_n+F_{n-1}$. Поэтому числа $(F_n)_2$ также удовлетворяют аналогичному рекуррентному соотношению

$$(F_{n+1})_2 \equiv (F_n)_2 + (F_{n-1})_2 \pmod 2. \tag{9}$$

Следовательно, как только два соседних числа $(F_{n-1})_2$ и $(F_n)_2$ при каком-либо натуральном n совпадут одновременно с двумя аналогичными числами при меньшем значении n, то с этого момента все элементы последовательности $\{(F_n)_2\}$ начнут повторяться — эта последовательность станет циклической. Но, вычисляя элементы последовательности $\{(F_n)_2\}$ по формуле (9), получаем:

$$0, 1, 1, 0, 1, 1, \ldots$$

Мы видим, что последовательность $\{(F_n)_2\}$ зациклилась: она вся состоит из повторяющихся участков

$$(0, 1, 1),$$

состоящих из 3 элементов, ввиду чего равен нулю в точности каждый третий ее элемент, начиная с нулевого. Свойство доказано.

3.2. Делимость чисел Фибоначчи на 5. *Число F_n делится на 5 тогда и только тогда, когда n делится на 5.*

Доказательство этого свойства. Обозначим через $(F_n)_5$ остатки чисел F_n от деления на 5. Числа $(F_n)_5$ также удовлетворяют аналогичному рекуррентному соотношению

$$(F_{n+1})_5 \equiv (F_n)_5 + (F_{n-1})_5 \pmod 5. \tag{10}$$

Следовательно, как только два соседних числа $(F_{n-1})_5$ и $(F_n)_5$ при каком-либо натуральном n совпадут одновременно с двумя аналогичными числами при меньшем значении n, то с этого момента все элементы последовательности $\{(F_n)_5\}$ начнут повторяться. Действительно: вычисляя элементы последовательности $\{(F_n)_5\}$ по формуле (10), получим, что эта последовательность состоит из повторяющихся участков

$$(0, 1, 1, 2, 3, 0, 3, 3, 1, 4, 0, 4, 4, 3, 2, 0, 2, 2, 4, 1), \tag{11}$$

содержащих по 20 элементов в каждом из них. При этом в (11) равен нулю в точности каждый пятый элемент, начиная с нулевого. Свойство доказано.

3.3. Делимость чисел Фибоначчи на 10. *Число F_n делится на 10 тогда и только тогда, когда n делится на 15.*

Доказательство этого свойства. В двух предыдущих пунктах было показано, что F_n делится на 2 и на 5 тогда и только тогда, когда n делится, соответственно, на 3 и на 5. Но делимость на 10 равносильна одновременной делимости на 2 и на 5, а делимость на 15 — делимости на 3 и на 5 одновременно. Следовательно, F_n делится на 10 тогда и только тогда, когда n делится на 15. Свойство доказано.

3.4. Делимость чисел Фибоначчи на 10 и на 61. *Если F_n делится на 10, то F_n делится и на 61. Поэтому F_n никогда не равно целой степени числа 10.*

Доказательство этого свойства проведем по индукции. В частности, число $F_0 = 0$ делится и на 10, и на 61.

Согласно доказанному, все остальные числа Фибоначчи, кратные числу 10, можно получить из числа F_0, последовательно прибавляя к его индексу (к нулю) число 15 нужное количество раз. Это дает основу для проведения индуктивного шага. Так, согласно [3], при любых натуральных n и k выполняется формула

$$F_{n+k} = F_k F_{n-1} + F_{k+1} F_n, \tag{12}$$

которую легко доказать индукцией, например, по переменной k. В частности, для произвольного n, делящегося на 15, при $k = 15$ из (12) получаем

$$F_{n+15} = F_{15} F_{n-1} + F_{16} F_n = 610 F_{n-1} + F_{16} F_n = 61 \left(10 F_{n-1} + F_{16} \frac{F_n}{61} \right). \tag{13}$$

Поэтому, согласно (13), если F_n делилось на 61, то и F_{n+15} будет делиться на 61. Свойство доказано.

3.5. Расположение трех чисел на прямой. *Речь идет о таких трех числах: $\Phi^{n+1}/\sqrt{5}$, 10^v и F_{n+1} при натуральных n и v. Каждое из двух неравенств*

$$F_{n+1} < 10^v \leqslant \frac{\Phi^{n+1}}{\sqrt{5}} \tag{14}$$

и

$$\frac{\Phi^{n+1}}{\sqrt{5}} < 10^v \leqslant F_{n+1} \tag{15}$$

не имеет решений в целых числах n и v.

Доказательство этого свойства. Здесь нам потребуется формула Бине:

$$F_k = \frac{\Phi^k - \overline{\Phi}^k}{\sqrt{5}},$$

где $\overline{\Phi} = -1/\Phi$, легко доказываемая математической индукцией по натуральному k. Учтем, что F_{n+1} — целое число, а числа $\Phi^{n+1}/\sqrt{5}$ и F_{n+1}, согласно формуле Бине, отличаются меньше чем на 1:

$$\left| F_{n+1} - \frac{\Phi^{n+1}}{\sqrt{5}} \right| < 1. \tag{16}$$

Покажем, что в таком случае выполнение неравенства (14) невозможно. Действительно: если выполнена формула (14), то

$$F_{n+1} \leqslant 10^v - 1 \quad \text{и} \quad \frac{\Phi^{n+1}}{\sqrt{5}} \geqslant 10^v,$$

поэтому

$$\frac{\Phi^{n+1}}{\sqrt{5}} - F_{n+1} \geqslant 10^v - (10^v - 1) = 1. \tag{17}$$

Однако неравенство (17) противоречит оценке (16), поэтому выполнение неравенства (14) невозможно.

Пусть теперь выполнено неравенство (15). Как мы видели выше, $F_{n+1} \neq 10^v$, поэтому

$$F_{n+1} \geqslant 10^v + 1 \quad \text{и} \quad \frac{\Phi^{n+1}}{\sqrt{5}} < 10^v,$$

откуда

$$F_{n+1} - \frac{\Phi^{n+1}}{\sqrt{5}} \geqslant 10^v + 1 - \frac{\Phi^{n+1}}{\sqrt{5}} \geqslant 10^v + 1 - 10^v = 1. \tag{18}$$

Оценка (18) снова противоречит неравенству (16), поэтому выполнение неравенства (15) также невозможно. Свойство доказано.

4. Доказательство первого утверждения теоремы 1

Докажем сначала следующую предварительную оценку:

$$n < \frac{v + \lg \frac{\sqrt{5}}{\Phi}}{\lg \Phi}. \tag{19}$$

Доказательство предварительной оценки (19). Пусть, согласно условию, число b записывается v десятичными цифрами

$$b = \left(\overline{b_1 b_2 \dots b_v}\right)_{10}, \tag{20}$$

где

$$b_1, b_2, \dots, b_v \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}, \quad b_1 \neq 0,$$

— десятичные цифры числа b. Рассмотрим алгоритм Евклида с аргументами a и b, описанный выше. Оценим с двух сторон число $b+1$.

С одной стороны, согласно (20), $b < 10^v$, поэтому

$$b + 1 \leqslant 10^v. \tag{21}$$

С другой стороны, в алгоритме Евклида число b — это первый остаток: согласно введенным выше обозначениям $b = r_1$. Поэтому для числа b имеет место неравенство (2). Точнее, если в формуле (2) положить $i = n-1$, то, согласно формуле Бине, получаем оценку

$$b = r_1 \geqslant F_{n+1} = \frac{\Phi^{n+1} - \overline{\Phi}^{n+1}}{\sqrt{5}}. \tag{22}$$

Но, поскольку $\left|\overline{\Phi}^{n+1}\right| < 1 < \sqrt{5}$, то из (22) следует, что

$$b+1 \geqslant \frac{\Phi^{n+1}-\overline{\Phi}^{n+1}}{\sqrt{5}}+1=\frac{\Phi^{n+1}+\left(\sqrt{5}-\overline{\Phi}^{n+1}\right)}{\sqrt{5}} > \frac{\Phi^{n+1}}{\sqrt{5}}. \tag{23}$$

Рассмотрев нижнюю оценку (23) вместе с верхней оценкой (21), получаем уже двустороннюю оценку величины $b+1$:

$$\frac{\Phi^{n+1}}{\sqrt{5}} < b+1 \leqslant 10^v. \tag{24}$$

Отбрасывая в неравенстве (24) среднюю часть (то есть выражение «$b+1\leqslant$») и умножая оставшееся неравенство на $\sqrt{5}$, получаем

$$\Phi^{n+1} < 10^v\sqrt{5}. \tag{25}$$

Логарифмируя неравенство (25) по основанию 10, получаем:

$$(n+1)\lg\Phi < v+\lg\sqrt{5},$$

или

$$n+1 < \frac{v+\lg\sqrt{5}}{\lg\Phi}. \tag{26}$$

Вычитая 1 из обеих частей равенства (26), получаем неравенство (19):

$$n < \frac{v+\lg\sqrt{5}}{\lg\Phi}-1=\frac{v+\lg\sqrt{5}-\lg\Phi}{\log_{10}\Phi}=\frac{v+\lg\frac{\sqrt{5}}{\Phi}}{\lg\Phi}.$$

Предварительная оценка доказана.

Теперь к результату неравенства (19) применим функцию целой части, из-за чего неравенство станет нестрогим:

$$n \leqslant \left[\frac{v+\lg\frac{\sqrt{5}}{\Phi}}{\lg\Phi}\right]. \tag{27}$$

Мы вывели неравенство (27), которое и представляет собой верхнюю оценку из первой части теоремы 1. Чтобы доказать равенство в (7), нужно показать также *достижимость* оценки (27) — то, что при каждом v для величины $n(v)$ существует то v-значное число b, для которого длина алгоритма Евклида совпадает с правой частью неравенства (27). Только тогда первая часть теоремы 1 будет полностью доказана.

Достижимость оценки (27). Для доказательства этого факта поступим следующим образом. Для каждого v определим число n двумя различными способами. В первом из них определим число n как максимальное из тех натуральных чисел, для которых выполняется неравенство

$$F_{n+1} < 10^v. \tag{28}$$

Тогда, полагая $a = F_{n+2}$, $b = F_{n+1}$, получаем, что алгоритм Евклида, примененный к этим a и b, содержит ровно n делений с остатком, которые приводят к таким остаткам:

$$F_n, F_{n-1}, F_{n-2}, \ldots, F_3, F_2, F_0 = 0.$$

Рассмотрим теперь ситуацию с другой стороны: определим число n вторым способом — формулой (7). Тогда это n равно максимуму из тех целых чисел, для которых выполняется неравенство

$$n \leqslant \frac{v + \lg \frac{\sqrt{5}}{\Phi}}{\lg \Phi}. \tag{29}$$

Покажем, что неравенство в (29) выполняется строго. Действительно: упрощая неравенство (29), его можно представить в виде

$$\Phi^{n+1} \leqslant 10^v \sqrt{5}. \tag{30}$$

Но равенство в неравенстве (30) невозможно в силу иррациональности числа $\sqrt{5}$. Таким образом, неравенство в (29) выполняется строго. Поэтому число n, определенное выше неравенством (29), или, что то же самое, неравенством (30), можно определить как максимальное целое, удовлетворяющее неравенству

$$\frac{\Phi^{n+1}}{\sqrt{5}} < 10^v.$$

Сравним это определение с (28). Чтобы доказать, что эти определения вводят для заданного v одно и то же значение n, нужно доказать, что число 10^v не может оказаться между числами $\Phi^{n+1}/\sqrt{5}$ и F_{n+1}. Но этот факт уже был обоснован выше в пункте “Расположение трех чисел на прямой”.

Первое утверждение теоремы 1 доказано.

5. Доказательство второго утверждения теоремы 1

Для всякого действительного x его целую часть $[x]$ можно представить в виде разности числа x и его дробной доли $\{x\}$:

$$[x] = x - \{x\}. \tag{31}$$

Пользуясь равенством (31), формулу (7) можно преобразовать к виду

$$n = \frac{v + \lg \frac{\sqrt{5}}{\Phi}}{\lg \Phi} - \left\{ \frac{v + \lg \frac{\sqrt{5}}{\Phi}}{\lg \Phi} \right\}. \tag{32}$$

Однако выражение в фигурных скобках в (32) представляет собой линейную функцию от параметра v. Ее дробные доли, согласно теореме Вейля [4] о дробных долях линейной функции, равномерно распределены в отрезке $[0,1]$. Это означает, что для любого ρ из интервала $(0,1)$ и для любого положительного числа ε в ε-окрестности числа ρ найдется бесконечно много значений дробной доли от этой линейной функции при различных v. Отсюда и следует неравенство (8). Поэтому второе утверждение теоремы 1 доказано.

6. Доказательство третьего утверждения теоремы 1

Сравнив между собой правые части формул (6) и (7), приходим к выводу, что эти целые части значений линейных функций от v тогда и только тогда дают один и тот же результат, когда выполнено неравенство

$$\left\{\frac{v+\lg\frac{\sqrt{5}}{\Phi}}{\lg\Phi}\right\}<1-\lg\frac{\Phi^2}{\sqrt{5}}. \tag{33}$$

Согласно упомянутой выше теореме Вейля, неравенство (33) выполняется для бесконечно многих значений v. Поэтому третье утверждение теоремы 1 доказано.

7. Доказательство четвертого утверждения теоремы 1

Доказательство достаточности. При v, равном 1, 2 или 3, первая оценка из теоремы Ламе достигается на парах аргументов (a,b) алгоритма Евклида, которые для этих случаев принимают значения

$$(13,\ 8),\quad (144,\ 89)\quad \text{или}\quad (1597,\ 987). \tag{34}$$

Алгоритм Евклида, примененный к парам (34), содержит 5, 10 или 15 делений с остатком, что согласуется с неравенством (1) (поскольку числа b, равные 8, 89 или 987, составлены из одной, двух или трех десятичных цифр, соответственно). Достаточность неравенства $v\leqslant 3$ доказана.

Доказательство необходимости. Чтобы доказать необходимость неравенства $v\leqslant 3$, воспользуемся предварительной оценкой (19). Предположим, что для некоторых v выполнено неравенство

$$\frac{\lg\frac{\sqrt{5}}{\Phi}+v}{\lg\Phi}<5v. \tag{35}$$

В этом случае число $5v$ уже не может быть длиной алгоритма Евклида (количеством делений с остатком в нем) ввиду неравенств (19) и (35): в противном случае из предположения $n=5v$ следовало бы тогда, что $5v<5v$. Другими словами, оценка $5v$ в этом случае недостижима.

Чтобы узнать, при каких v это случится, нужно решить неравенство (35) относительно v. В ответе получаем

$$v>\frac{\lg\frac{\sqrt{5}}{\Phi}}{5\lg\Phi-1}. \tag{36}$$

Вычисляя, находим, что правая часть неравенства (36) меньше четырех. Поэтому при $v\geqslant 4$ неравенство (36) выполнено. Это означает, что при $v\geqslant 4$ неравенство (35) также выполнено. Следовательно, согласно сказанному выше, при таких значениях v оценка $5v$ из неравенства (1) уже не может быть достигнута. Необходимость неравенства $v\leqslant 3$ доказана.

Список литературы

[1] Нестеренко Ю. В., *Теория чисел*, Издательский центр “Академия”, М., 2008.

[2] Кнут Д. Э., *Искусство программирования.* Т. 2, Издательство “Диалектика-Вильямс”, 1998.

[3] Воробьёв Н. Н., *Числа Фибоначчи*, Главная редакция физико-математической литературы издательства “Наука”, М., 1978.

[4] Вейль Г., “О равномерном распределении чисел по модулю”, *Избранные труды*, Наука, М., 1984, 58–93.

Поступила в редакцию
5 ноября 2023 г.

Kan I. D.[1] Reachability of inequalities from Lame’s theorem. *Far Eastern Mathematical Journal.* 2024. V. 24. No 1. P. 45–54.

[1] Moscow aviation institute (National Research University), Russia

ABSTRACT

In this paper, the following result is proved. The number of steps in Euclid’s algorithm for two natural arguments, the smaller of which has v digital digits in the decimal system, does not exceed the integer part of the fraction $(v + \lg(\sqrt{5}/\Phi))/\lg\Phi$, where $\Phi = (1 + \sqrt{5})/2$, and this estimate is achieved for every natural v. It is also proved that partial or asymptotic reachability is valid for the other two known upper bounds on the length of the Euclid algorithm.

Key words: *Lame’s theorem, Euclid’s algorithm.*