

Элементы теории чисел

Лектор профессор Ю.В. Нестеренко
механико-математический факультет МГУ

1 поток 1 курса, осень 2026г.

Лекция 2: Алгоритм Евклида. Решение в целых числах
линейных уравнений. Простые и составные числа. Решето
Эратосфена. Бесконечность множества простых чисел.

§1.3. Алгоритм Евклида

Пусть $a \geq b$ - натуральные числа, требуется найти (a, b) - их наибольший общий делитель.

Придуманный в Древней Греции алгоритм, называемый алгоритмом Евклида, достаточно быстро находит наибольший общий делитель и при этом не разлагает числа на множители. В основе его лежит следующее утверждение.

Лемма 1

1. Если a – целое, b - натуральное и $b|a$, то $(a, b) = b$.
2. Если

$$a = bq + r, \quad 0 \leq r < b,$$

то $(a, b) = (b, r)$.

Доказательство вспомогательной леммы

Доказательство.

1. Пусть $b|a$. Множество общих делителей чисел a и b содержится среди делителей b . В то же время, каждый делитель числа b , в силу условия $b|a$ будет делителем числа a . Следовательно, множество общих делителей чисел a и b совпадает с множеством делителей b . Это доказывает, что $(a, b) = b$, т.е. первое утверждение леммы ??.
2. Пусть $a = bq + r$, $0 < r < b$,. Для доказательства леммы ?? в этом случае заметим, что по свойствам делимости каждый общий делитель чисел b и r делит число $bq + r = a$. Точно так же, каждый общий делитель чисел a и b делит число $a - bq = r$, так что является общим делителем чисел b и r . Отсюда следует совпадение наибольших общих делителей пар чисел a, b и b, r , т.е. второе утверждение леммы. □

Алгоритм Евклида (найти (a, b))

1. Положим $r_0 = a$, $r_1 = b$ и обозначим $r_2, \dots, r_n$ - последующие делители в алгоритме Евклида.
2. Таким образом, получаются следующие равенства

$$\begin{array}{ll} a = r_0 = bq_1 + r_2, & 0 < r_2 < b, \\ b = r_1 = r_2q_2 + r_3, & 0 < r_3 < r_2, \\ r_2 = r_3q_3 + r_4, & 0 < r_4 < r_3, \\ \dots\dots\dots & \dots\dots\dots \\ r_{n-2} = r_{n-1}q_{n-1} + r_n, & 0 < r_n < r_{n-1}, \\ r_{n-1} = r_nq_n. & \end{array} \quad (1)$$

3. В соответствии с леммой ?? находим равенства

$$(a, b) = (b, r_2) = (r_2, r_3) = (r_3, r_4) = \dots = (r_{n-1}, r_n) = (r_n, 0) = r_n.$$

Значит (a, b) есть последний ненулевой остаток в алгоритме Евклида.

Найти наибольший общий делитель чисел 81 и 48

Пользуясь алгоритмом Евклида, находим

$$\begin{aligned}81 &= 48 \cdot 1 + 33, \\48 &= 33 \cdot 1 + 15, \\33 &= 15 \cdot 2 + 3, \\15 &= 3 \cdot 5.\end{aligned}\tag{2}$$

Последний ненулевой остаток равен 3, поэтому $(81, 48) = 3$.

Алгоритм Евклида на компьютере

Для реализации алгоритма Евклида на компьютере больше подходит следующая его форма, в которой отсутствуют индексы у делителей и остатков.

Алгоритм 1

Даны: *Натуральные числа a и b ; $b < a$.*

Найти: *Наибольший общий делитель (a, b) .*

1. *Вычислить r - остаток от деления a на b , т.е. найти целое r , удовлетворяющее условиям $a = bq + r$, $0 \leq r < b$.*
2. *Если $r = 0$, то $(a, b) = b$, СТОП.*
3. *Если $r \neq 0$, то заменить пару $\{a, b\}$ парой $\{b, r\}$ и перейти в пункт 1 алгоритма.*

Примеры показывают, что алгоритм Евклида достаточно быстро находит наибольший общий делитель. Оценку количества делений в нем дает следующая теорема Г. Ламе, доказанная в 1845г. Доказательство её в лекциях мы не приводим.

Теорема 4 (Теорема Ламе)

Количество делений, необходимое для вычисления с помощью алгоритма Евклида наибольшего общего делителя двух положительных целых чисел, не превышает пятикратного количества цифр в десятичной записи меньшего из этих двух чисел.

§1.4. Решение в целых числах линейных уравнений.

Уравнения, в которых неизвестные величины принимают целые значения, называются диофантовыми по имени древнегреческого ученого Диофанта.

Пусть a, b, c – целые числа. Рассмотрим простейшее диофантово уравнение

$$ax + by = c. \quad (3)$$

Теорема 5

1. Уравнение $(??)$ разрешимо в целых числах x, y тогда и только тогда, когда $(a, b) | c$.
2. В случае разрешимости множество решений бесконечно. Все они имеют вид

$$x = x_0 + \frac{b}{(a, b)}t, \quad y = y_0 - \frac{a}{(a, b)}t, \quad (4)$$

где пара чисел x_0, y_0 есть какое-либо фиксированное решение, а t – произвольное целое число.

Доказательство.

- Предположим, что целые числа x_0, y_0 составляют решение уравнения (??). Так как $(a, b) | a$ и $(a, b) | b$ то из свойств делимости следует $(a, b) | ax_0 + by_0 = c$. Значит, условие $(a, b) | c$ необходимо для разрешимости уравнения (??).
- Утверждение теоремы в обратную сторону можно доказывать, считая коэффициенты уравнения a, b целыми неотрицательными числами. Общий случай всегда можно свести к этому, сменив, если потребуется, знак у неизвестной. Далее будем считать $a \geq 0, b \geq 0$.
- Докажем нужное утверждение методом математической индукции по величине суммы $a + b$. Пусть $a + b = 1$, скажем, $a = 1, b = 0$. Тогда $(a, b) = 1$ и условие $(a, b) | c$ выполняется при любом c . Уравнение также разрешимо при любом c . Решением является пара чисел $x = c, y = 0$. □

Продолжение доказательства теоремы ??.

- Предположим, что целое $n \geq 1$, и утверждение теоремы выполняется для уравнений вида (??) с неотрицательными коэффициентами, сумма которых положительна и не превосходит n . Пусть также a, b – неотрицательные числа $a + b = n + 1$. Не уменьшая общности можно считать, что $a \geq b$.
- В случае $b = 0$ имеем $(a, b) = a$ и условие $(a, b) | c$ равносильно делимости $a | c$, т.е. равенству $c = au$ с некоторым $u \in \mathbb{Z}$. Уравнение (??) имеет решением числа $x = u, y = 0$.



Продолжение доказательства теоремы ??.

- В случае $b \geq 1$ при любом $d \in \mathbb{Z}$ имеем

$$d|a, d|b \Leftrightarrow d|(a-b), d|b \Rightarrow (a-b, b) = (a, b)|c.$$

- Так как $b + (a - b) = n + 1 - b \leq n$, то существуют $u, v \in \mathbb{Z}$
 $(a - b)u + bv = c$, так что, $au + b(v - u) = c, x = u, y = v - u$.

Первое утверждение теоремы полностью доказано. □

Продолжение доказательства теоремы ??.

- Для доказательства второго утверждения заметим прежде всего, что числа (??) составляют решение уравнения (??).

Действительно,

$$a \left(x_0 + \frac{b}{(a, b)} t \right) + b \left(y_0 - \frac{a}{(a, b)} t \right) = ax_0 + by_0 = c.$$

- Осталось проверить, что каждое решение уравнения (??) представимо в виде (??). Если x_1, y_1 – некоторое решение, то из равенств $ax_1 + by_1 = c$, $ax_0 + by_0 = c$ следует

$$a(x_1 - x_0) = b(y_0 - y_1). \quad (5)$$

- Числа a, b могут быть представлены в виде $a = (a, b)r$, $b = (a, b)s$, где r, s – целые взаимно простые числа. Сократив равенство (??) на (a, b) получим $r(x_1 - x_0) = s(y_0 - y_1)$ и $s|r(x_1 - x_0)$. □

Продолжение доказательства теоремы ??.

$$s|r(x_1 - x_0).$$

- Воспользуемся следствием 2 из параграфа §1.2. С его помощью, учитывая $(r, s) = 1$, заключаем $s|(x_1 - x_0)$ или $x_1 - x_0 = st$ с некоторым целым t .
- Итак,

$$x_1 = x_0 + st = x_0 + \frac{b}{(a, b)}t.$$

- Подставляя это выражение в (??), находим $\frac{ab}{(a, b)}t = b(y_0 - y_1)$ и $y_1 = y_0 - \frac{a}{(a, b)}t$. Это завершает доказательство теоремы ??.



Теорема ?? сводит решение уравнения (??) к нахождению одного решения. Способ вычисления такого решения основан на алгоритме Евклида (расширенный алгоритм). Все вычисления удобно оформить в табличном виде.

Пример

Решить диофантово уравнение

$$81x + 48y = 3. \quad (6)$$

Рассмотрим следующую таблицу

81	48	33	15	3	0
1	0	1	-1	<u>3</u>	-
0	1	-1	2	<u>-5</u>	-

Решение. Сравнивая эту таблицу с вычислением НОД(81, 48), см. (??), нетрудно заметить, что в первой строке таблицы записаны коэффициенты уравнения (??), а также остатки, возникающие при работе алгоритма Евклида.

81	48	33	15	3	0
1	0	1	-1	<u>3</u>	-
0	1	-1	2	<u>-5</u>	-

В каждом из первых двух столбцов таблицы стоят числа 1 и 0, причём они образуют единичную матрицу размера 2×2 .

Остальные столбцы таблицы вычисляются по тому же правилу, что и элементы первой строки: нужно последний вычисленный столбец таблицы умножить на соответствующее неполное частное и вычесть из предшествующего столбца. Результат нужно записать в следующий столбец.

Координаты частного решения уравнения стоят во второй и третьей строках последнего столбца с ненулевым остатком. В нашем примере $x_0 = 3$, $y_0 = -5$.

Глава 2. Простые и составные числа

- Натуральное число называется *составным*, если его можно представить в виде произведения двух меньших натуральных чисел. Заметим, что оба множителя при этом отличны от 1.
- Можно сказать, что натуральное число – составное, если оно делится на некоторое меньшее число, отличное от 1. Все чётные числа, превосходящие 2, делятся на 2 и потому все они составные.
- Примеры составных чисел

$$1111111 = 239 \cdot 4649, \quad 11111111111 = 21649 \cdot 513239.$$

- Некоторые натуральные числа, отличные от 1, нельзя представить в виде произведения меньших множителей. Такие числа называются *простыми*.
- Сомножители в приведённых примерах – простые числа. Простое число p имеет лишь два натуральных делителя: 1 и p .

§2.1. Бесконечность множества простых чисел.

Чтобы построить составное число, достаточно перемножить два целых числа, больших 1. Строить примеры простых чисел намного сложнее. Следующая лемма сокращает перебор возможных делителей натурального числа N при проверке его простоты.

Лемма 2

Пусть N – составное число и p – наименьший из его делителей, с условием $p > 1$. Тогда p – простое число и $p^2 \leq N$.

Доказательство.

Так как N – составное число, то оно может быть представлено в виде $N = u \cdot v$, где $u, v \in \mathbb{Z}$, $1 < u < N$, $1 < v < N$. По условию имеем $p^2 \leq u \cdot v = N$.

Пусть d – какой-либо отличный от единицы делитель p , тогда $d \leq p$. Свойства $d|p, p|N$ означают, что d есть делитель N , и по определению p имеем $d \geq p$. Итак $d = p$. Натуральные делители числа p исчерпываются 1 и p , что доказывает его простоту.



Бесконечность множества простых чисел.

Следствие 1

Каждое целое число $N > 1$ имеет простой делитель.

Доказательство.

Если N – простое число, то утверждение, очевидно, выполняется. Если же N – составное число, утверждение имеет место согласно лемме ??.



Наибольшее из известных к настоящему времени простых чисел равно $2^{136279841} - 1$. Оно записывается с помощью 41024320 десятичных цифр и было найдено в 2024 году.

Существует ли самое большое простое число? Отрицательный ответ на этот вопрос был дан ещё в Древней Греции.

Бесконечность множества простых чисел.

Теорема 6 (Теорема Евклида)

Множество простых чисел бесконечно.

Доказательство.

Пусть n - натуральное число, $n! = 1 \cdot 2 \cdot \dots \cdot n$ и $N = n! + 1$. Согласно лемме ?? число N имеет простой делитель p , который, очевидно, больше n , ведь N делится на p , но при делении на каждое из чисел промежутка от 2 до n имеет остаток 1. Итак, для любого натурального числа n можно найти простое число $p > n$. □

Далее мы опишем алгоритм, позволяющий сравнительно легко определить список всех простых чисел, до заданной границы N . Этот алгоритм носит название *решето Эратосфена*.

Следующий алгоритм находит список всех простых чисел $p_1 < p_2 < \dots$ до заданной границы N .

Алгоритм 2 (Решето Эратосфена)

1. Выпишем все целые числа $2, 3, 4, 5, \dots, N - 1, N$. Положим $p_1 = 2$ и начиная с $4 = p_1^2$ будем вычеркивать числа, двигаясь с шагом 2. (Все числа, вычеркнутые на этом шаге алгоритма – чётны, т.е. делятся на 2.)
2. Пусть $k \geq 2$ и уже определены числа $p_1, \dots, p_{k-1}$. Обозначим p_k первое невычеркнутое число, следующее за p_{k-1} . Если $p_k^2 > N$, обозначаем $p_{k+1}, p_{k+2}, \dots$ все оставшиеся невычеркнутыми числа, следующие за p_k в порядке возрастания. На этом алгоритм завершает свою работу.
3. Если $p_k^2 \leq N$, вычеркиваем числа, начиная с p_k^2 и двигаясь до N с шагом p_k . Вычеркнутые ранее числа, также принимаются в учёт, но не вычеркиваются ещё раз. По завершении этой процедуры алгоритм увеличивает индекс k на единицу и переходит в шаг 2.

Обоснование решета Эратосфена.

- Для обоснования корректности алгоритма, заметим, что в процессе его работы вычеркиваются только составные, а все простые числа остаются невычеркнутыми.
- Предположим теперь, что среди невычеркнутых чисел осталось хотя бы одно составное, обозначим его буквой a , $2 \leq a \leq N$. По лемме ?? это число имеет простой делитель p , удовлетворяющий неравенствам $p^2 \leq a \leq N$.
- Как и всякое простое, число p осталось невычеркнутым по окончании работы алгоритма. Вместе с тем неравенство $p^2 \leq N$ означает, что в результате одного из проходов алгоритма по списку чисел от 2 до N были вычеркнуты, начиная с p^2 все числа, делящиеся на p . Но тогда и a должно содержаться среди вычеркнутых чисел.
- Получившееся противоречие доказывает, что алгоритм оставляет невычеркнутыми только простые числа. Это завершает обоснование алгоритма.

2, 3, 4, 5, 6, 7, 8, 9, 10,
11, 12, 13, 14, 15, 16, 17, 18, 19, 20,
21, 22, 23, 24, 25, 26, 27, 28, 29, 30,
31, 32, 33, 34, 35, 36, 37, 38, 39, 40

Простые числа:

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37

Основная теорема арифметики.

Пример:

$$6025729 = 2419 \cdot 2491 = 2173 \cdot 2773. \quad (7)$$

Сомножители не могут быть простыми числами. Должны существовать разложения на меньшие сомножители.

Теорема 7

Каждое целое число, большее единицы, раскладывается в произведение простых чисел и притом единственным способом, если не учитывать порядок сомножителей.

Теорема утверждает, что два произведения простых чисел могут быть равны друг другу лишь в случае, если они имеют одинаковые сомножители и, возможно, отличаются порядком их следования.

Доказательство основной теоремы арифметики (существование).

Воспользуемся методом математической индукции. Числа 2, 3, как мы в этом уже убедились, просты, и, значит, утверждение теоремы для них справедливо.

Пусть натуральное $n > 3$ и каждое целое число, меньшее n , единственным способом представимо в виде произведения простых.

Докажем сначала, что n может быть разложено в произведение простых чисел. По следствию ?? существует простое p_1 , делящее n . В случае $n = p_1$ искомое произведение состоит из одного множителя.

Если же $p_1 < n$, то $n = p_1 m$, где $1 < m < n$. Согласно индуктивному предположению найдутся простые числа $p_2, \dots, p_r$, для которых $m = p_2 \cdots p_r$. Тогда $n = p_1 p_2 \cdots p_r$.
Существование разложения доказано. □

Доказательство основной теоремы арифметики (единственность).

Предположим теперь, что возможны два не совпадающих разложения

$$n = p_1 \cdots p_r = q_1 \cdots q_s, \quad (8)$$

где p_i, q_j – простые числа.

Если p_1 совпадает с каким-либо из чисел q_j , то, сократив равенство (??) на этот общий множитель, получим два представления $m = p_2 \cdots p_r < n$ в виде произведения простых чисел. Эти представления не могут быть различными, тогда мы пришли бы к противоречию с индуктивным предположением. Если же получившиеся разложения для m совпадают друг с другом, то совпадающими будут и разложения (??), что противоречит их определению. Получившееся противоречие означает, что p_1 отлично от всех чисел q_j . □

Завершение доказательства основной теоремы арифметики.

Все положительные делители p_1 исчерпываются числами $1, p_1$, а все положительные делители q_1 исчерпываются числами $1, q_1$. Лишь единица присутствует в обоих множествах. Значит, $(p_1, q_1) = 1$. Согласно следствию 2 из первой лекции число $u = q_2 \cdots q_s < n$ делится на p_1 , т.е. $u = p_1 \cdot v$ с $v \in \mathbb{Z}$.

Число v согласно индуктивному предположению можно представить в виде произведения простых чисел. Это приводит к новому разложению u на простые сомножители, ведь все числа q_j отличны от p_1 . Итак, u допускает два различных представления в виде произведения простых чисел, вопреки индуктивному предположению. Получившееся противоречие завершает доказательство теоремы. □

Конец 2-й лекции