6. Алгоритм Евклида

Однозначность разложения на множители (основную теорему арифметики) можно доказывать разными способами. Мы получим её как следствие *алгоритма Евклида вычисления наибольшего общего делителя* двух целых чисел.

▷ Это, пожалуй, не самый короткий, но самый естественный путь. Евклид — это тот самый древнегреческий Евклид, который написал первый в мире учебник геометрии, *Начала* — и там была не только геометрия. В частности, этот алгоритм (конечно, не называемый «алгоритмом» — это гораздо более позднее слово в часть арабского математика аль-Хорезми) там тоже был (для отрезков). ◁

Слова «наибольший общий делитель» (в применении к двум целым числам) надо понимать буквально. У каждого числа есть делители, и некоторые делители будут общими для двух чисел. Из них нужно выбрать самый большой.

Наибольший общий делитель чисел a, b обычно обозначают $\gcd(a, b)$ (от слов “greatest common divisor”), или по-русски НОД(a, b).

6.1 А почему самый большой вообще есть? Не может ли так случиться, что какой общий делитель ни возьми, есть ещё больший?

▷ Да, такое тоже может быть: если оба числа равны нулю, то любое число будет делителем, а среди всех чисел нет наибольшего. Поэтому мы не определяем НОД $(0, 0)$. Но в остальных случаях — если одно из двух чисел ненулевое — все делители не превосходят модуля этого числа, так что среди них есть и наибольший. ◁

• В принципе можно искать наибольший общий делитель двух чисел перебором — взять ненулевое (выгодно взять меньшее по модулю) число и пробовать все делители от 1 до этого числа (точнее, его модуля). Но иногда можно обойтись и без этого.

Числа a и b называют *взаимно простыми*, если НОД $(a, b) = 1$.

6.2 С какими числами взаимно просто простое число p?

▷ Если p — простое число, то у него только два делителя 1 и p. Значит, и общими делителями могут быть только 1 и p. При этом 1 (который всегда общий делитель) будет наибольшим, когда p не является общим делителем. Отсюда ответ: со всеми, которые не делятся на p. ◁

6.3 Чему, согласно нашему определению, равно НОД $(a, 0)$ при $a \neq 0$?

▷ Нуль делится на что угодно, поэтому общими делителями будут все делители a, и наибольший из них будет a (точнее, $|a|$, поскольку a может быть отрицательным). ◁

6.4 Найдите НОД $(1230, 1231)$ и НОД $(123, 1231)$

▷ У чисел 1230 и 1231 нет никаких общих делителей, кроме 1 (и -1, если считать и отрицательные). Почему? Если оба числа 1230 и 1231 делятся на какое-то d, то и их разность должна делиться на d, а она равна 1, так что остаётся только $d = \pm 1$.

Про вторую пару: НОД $(123, 1231) = 1$, потому что все делители 123 являются также и делителями 1230, значит общих делителей у 123 и 1231 может быть только меньше, чем у 1230 и 1231. ◁

6.5 Какие значения может принимать НОД $(n, n + 6)$ при разных n? Как это значение зависит от n? [Указание: важен остаток от деления n на 6.]

▷ Ключевое наблюдение (в продолжение решения предыдущей задачи): *у пары* $(n, n + 6)$ *те же общие делители, что и у пары* $(n, 6)$. (Речь только об об *общих* делителях: у числа $n + 6$ самого по себе могут быть и другие делители, которых нет ни у n, ни у 6.) Почему? Если какое-то число d делит и n, и $n + 6$, то оно делит и разность $(n + 6) - n = 6$, так что общие делители первой пары будут общими делителями второй. Напротив, если d делит и n, и 6, то d делит и их сумму $n + 6$, так что общие делители второй пары будут общими делителями первой. Значит, множество общих делителей не изменится, когда мы перейдём от первой пары ко второй.

Теперь про НОД $(n, 6)$: у 6 есть делители 1, 2, 3, 6 если n делится на 6, то 6, если n делится на 3, но не на 6, то НОД $(n, 6) = 3$ (это бывает, когда $n \equiv 3 \pmod 6$), если n делится на 2, но не на 3 и 6, то 2 (это бывает, когда $n \equiv 2 \pmod 6$ или $n \equiv 4 \pmod 6$), в остальных случаях 1.

$n \bmod 6$	0	1	2	3	4	5
НОД $(n, n + 6)$	6	1	2	3	2	1

◁

6.6 Докажите, что для любых целых a, b выполнено равенство

$$\text{НОД}(a, b) = \text{НОД}(a - b, b).$$

▷ В решении предыдущей задачи мы видели, что множество общих делителей у пар (a, b) и $(a - b, b)$ одно и тоже. В самом деле, если d делит a и b, то делит и разность $a - b$; если d делит $a - b$ и b, то делит и сумму $(a - b) + b = a$. ◁

6.7 Докажите, что $\text{НОД}(a, b) = \text{НОД}(a - 2b, b) = \text{НОД}(a + b, b) = \text{НОД}(a + b, 2a + 3b)$.

▷ Мы уже знаем из предыдущей задачи, что можно из одного элемента пары вычесть второй, и наибольший общий делитель не изменится. Значит, можно это сделать и дважды: переходя от a, b к $a - b, b$, а потом к $a - 2b, b$, мы не меняем наибольший общий делитель. Если смотреть на вычитание в обратном направлении, то будет прибавление к одному члены пары второго — и оно тоже не меняет наибольший общий делитель: $\text{НОД}(a, b) = \text{НОД}(a + b, b)$. Чтобы перейти от $(a + b, 2a + 3b)$ к (a, b), нужно нескольких шагов:

$$(a + b, 2a + 3b) \to (a + b, a + 2b) \to (a + b, b) \to (a, b)$$

(вычитание первого члена пары из второго, ещё одно, потом вычитание второго из первого) ◁

6.8 Докажите, что для любого целого a и любого положительного целого b выполнено равенство $\text{НОД}(a, b) = \text{НОД}(a \bmod b, b)$.

▷ Мы уже видели, что при вычитании второго члена пары из первого наибольший общий делитель не меняется. Значит, он не изменится, и если мы вычтем несколько раз — столько, сколько нужно, чтобы из a вышло $a \bmod b$. (Если a отрицательно, то надо не вычитать, а прибавлять, но это тоже можно.) ◁

6.9 Найдите $\text{НОД}(123456789, 987654321)$.

▷ Применяя предыдущую задачу, разделим второе число на первое с остатком:

$$987654321 = 8 \cdot 123456789 + 9$$

(как ни странно, остаток очень небольшой), поэтому надо найти наибольший общий делитель пары $(123456789, 9)$, а это будет 9 (по признаку делимости первый член пары делится на 9). ◁

Задача 8 позволяет довольно быстро искать наибольшие общие делители. Скажем,

$$\begin{aligned}\text{НОД}(34,157) = \text{НОД}(34, 157 \bmod 34) = \text{НОД}(34,21) = \\ = \text{НОД}(34 \bmod 21, 21) = \text{НОД}(13,21) = \text{НОД}(13, 21 \bmod 13) = \\ = \text{НОД}(13,8) = \text{НОД}(13 \bmod 8, 8) = \text{НОД}(5,8) = \\ = \text{НОД}(5, 8 \bmod 5) = \text{НОД}(5,3) = \text{НОД}(5 \bmod 3, 3) = \\ = \text{НОД}(2,3) = \text{НОД}(2, 3 \bmod 2) = \text{НОД}(2,1) = 1.\end{aligned}$$

Этот способ и называется *алгоритмом Евклида*.

• Мы довели вычисление до $\text{НОД}(2,1)$, хотя уже задолго до этого легко было сообразить, что общих делителей нет, — просто чтобы «следовать букве алгоритма». Кстати, можно было бы сделать и ещё один шаг:

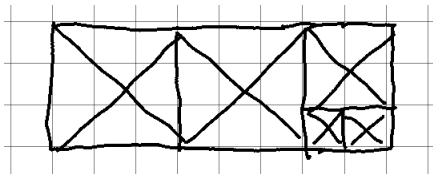
$$\text{НОД}(2,1) = \text{НОД}(2 \bmod 1, 1) = \text{НОД}(0,1) = 1.$$

В нашем примере почти всё время (кроме первого шага) деление с остатком сводится к однократному вычитанию, но так бывает не всегда. Может случиться, что числа (с самого начала или в середине вычислений) сильно различаются (одно много больше другого), и тогда деление с остатком заменяет большое число вычитаний.

▷ Программисты бы описали алгоритм Евклида как-нибудь так:

```
пока в паре большее число не делится на меньшее:
   заменить большее число остатком от деления на меньшее
ответ: меньшее число
```

(Точнее говоря, надо было бы написать «большее или равное» вместо «большее».) ◁



Алгоритм Евклида на квадратах

6.10 Машина действует так: получив прямоугольник размером $a \times b$ при $a < b$, она отрезает от него квадрат $a \times a$ — и остаётся прямоугольник $a \times (b - a)$, который снова засовывают в машину, если он не квадратный.

На какие квадраты будет разрезан прямоугольник 34×157? Как этот процесс связан с алгоритмом Евклида?

• Для произвольного прямоугольника никто не обещает, что процесс рано или поздно закончится (может быть, будут оставаться меньшие и меньшие прямоугольники, но не квадраты).

▷ Для этого конкретного прямоугольника: 4 квадрата 34×34 и останется прямоугольник 34×21, потом квадрат 21×21, останется 13×21, потом 13×13, останется 8×13, потом 8×8, останется 5×8, потом 5×5, останется 3×5, потом 3×3, останется 2×3, потом 2×2, останется 1×2, и наконец мы этот последний прямоугольник разрежем на квадраты 1×1.

сторона квадрата	34	21	13	8	5	3	2	1
сколько квадратов	4	1	1	1	1	1	1	2

Прямоугольник соответствует паре чисел (стороны прямоугольника). При отрезании квадрата из большего числа вычитается меньшее. Если оно после этого остаётся бóльшим, то отрезается ещё один такой же квадрат, и так далее — пока мы не получаем деление с остатком, разбитое в последовательность вычитаний. Так что получается, так сказать, «алгоритм Евклида в замедленной съёмке». ◁

6.11 При разрезании на квадраты описанным способом получились квадраты трёх размеров: 3 больших квадрата, 2 квадрата поменьше и 5 совсем маленьких. Найдите отношение сторон исходного прямоугольника.

▷ Будем смотреть с конца. Примем сторону совсем маленького квадрата за единицу. Раз их пять, то разрезали 1×5, значит, квадрат поменьше был 5×5 и на предыдущем шаге был прямоугольник 11×5 (ведь $1 + 2 \cdot 5 = 11$), и большой квадрат 11×11, их было 3, то есть изначально было 38×11 (ведь $5 + 3 \cdot 11 = 38$). Отношение сторон исходного прямоугольника: $38 : 11$. ◁

6.12 Найдите значение «непрерывной» (или, как ещё говорят, «цепной») дроби

$$3 + \cfrac{1}{2 + \cfrac{1}{5}}$$

(и сравните с предыдущей задачей).

▷ Такую дробь можно вычислять снизу вверх (= изнутри наружу) — а как ещё? получится $2 + 1/5 = 11/5$, потом $3 + 5/11 = 38/11$. Так что происходит всё то же самое, что в предыдущей задаче, но в обратном порядке (выделение целой части и перестановка числителя со знаменателем — это и есть один шаг алгоритма Евклида). ◁

6.13 Найдите целые положительные числа x, y, z, при которых

$$\frac{38}{11} = x + \cfrac{1}{y + \cfrac{1}{z}}$$

(укажите все возможные варианты).

▷ Тут один возможный ответ даёт предыдущая задача. Но единственный ли он? Да, и рассуждать можно так: число $y + \frac{1}{z}$ не меньше 1, поэтому дробь $\cfrac{1}{y + \cfrac{1}{z}}$ находится между 0 и 1, так что x определяется однозначно как целая часть 38/11. По тем же причинам однозначно определяется y, и тем самым z. ◁

6.14 Докажите, что $\text{НОД}\,(2a, 2b) = 2\,\text{НОД}\,(a, b)$ и вообще

$$\text{НОД}\,(ca, cb) = c \cdot \text{НОД}\,(a, b)$$

при любых целых $a, b, c \neq 0$.

▷ Будем параллельно применять алгоритм Евклида к обеим парам чисел — или, если угодно, к обоим прямоугольникам, их изображающим. Тогда один прямоугольник будет вдвое (или в c раз) больше другого, если единица измерения общая, и процесс разрезания будет происходить синхронно. Значит, и результирующие маленькие квадраты будут отличаться в c раз. (А если выбрать единицы отличающимися в c раз, можно прямоугольники вообще сделать численно одинаковыми.) ◁

• Без алгоритма Евклида тут обойтись не так просто. Понятно, что если d — общий делитель a и b, то $2d$ — общий делитель $2a$ и $2b$, так что $\text{НОД}\,(2a, 2b) \geqslant 2\,\text{НОД}\,(a, b)$. Но как доказать обратное неравенство? Тут достаточно было бы доказать, что если d' — общий делитель $2a$ и $2b$, то либо d' чётный, либо d' — общий делитель a и b (и это верно, но надо использовать, что если нечётное число делит $2a$, то оно делит и a — что тоже обычно доказывается с помощью алгоритма Евклида, как мы вскоре и сделаем).

6.15* Докажите, что разрезание прямоугольника $a \times b$ на квадраты закончится в том и только том случае, если у его сторон есть *общая мера*. Здесь общей мерой называется отрезок, который укладывается и в a, и в b целое число раз.

• Именно в такой ситуации алгоритм Евклида (без такого названия, естественно) описан в «Началах» Евклида — только там не прямоугольник разрезается, а просто два отрезка, и меньший откладывается на большем.

▷ Если у сторон прямоугольника есть общая мера, примем её за единицу измерения. Тогда все квадраты, на которые мы разрезаем, будут с целыми сторонами, и прямоугольники будут уменьшаться (точнее можно сказать так: меньшая сторона прямоугольника будет уменьшаться), так что рано или поздно всё должно кончиться.

Напротив, если всё разрежется на конечное число квадратов, то идя с конца, видим, что сторона самого маленького квадрата целое число раз укладывается во всех сторонах ◁

6.16* Говорят, что стороны прямогольника находятся в отношении «золотого сечения», если после отрезания от него квадрата остаётся прямоугольник с тем же отношением сторон, что у исходного. Закончится ли алгоритм Евклида, если применить его к такому прямоугольнику? А если применить к прямоугольнику с отношением сторон $\sqrt{2} : 1$ (как у диагонали квадрата к его стороне)?

▷ Для золотого сечения — очевидно, нет, потому что новый прямоугольник будет с тем же отношением сторон, что и старый, поэтому и второй будет с тем же отношением сторон, и так далее.

Про прямоугольник с отношением $\sqrt{2}$: мы видели, что $\sqrt{2}$ иррациональный, поэтому общей меры нет, так что процесс будет бесконечным. Можно и более конкретно описать, что будет происходить: отношение после первого шага (отрезали один квадрат) будет $1/(\sqrt{2}-1) = \sqrt{2}+1$ (проверяется умножением), потом после отрезания одного квадрата будет снова $\sqrt{2}$, и так далее. Вообще для любого квадратного корня всё зациклится аналогичным образом (но это надо доказывать, так сразу это не ясно). ◁

6.17* Начав разрезать описанным способом прямоугольник на квадраты, мы получили два квадрата побольше, один поменьше и остался прямоугольник с тем же отношением сторон, что исходный (то есть дальше будет снова два квадрата, потом один ещё меньше, потом два ещё меньше и т.п.). Каково было отношение сторон исходного прямоугольника?

• Иногда эту задачу формулируют так: чему равна бесконечная периодическая цепная дробь

$$2+\cfrac{1}{1+\cfrac{1}{2+\cfrac{1}{1+\cfrac{1}{2+\ldots}}}}$$

▷ Если отношение большей стороны к меньшей равно x, то

$$x = 2 + \cfrac{1}{1+\cfrac{1}{x}}$$

Свёртывая дробь, получаем $x = 2 + x/(x+1)$, или $x^2 + x = 2x + 2 + x$, то есть $x^2 - 2x - 2 = 0$, или $(x-1)^2 - 3 = 0$, единственный положительный корень $1+\sqrt{3}$. Проверим на всякий случай: сначала два квадрата и отношение $1 : (\sqrt{3}-1) = \frac{1}{2} + \frac{\sqrt{3}}{2}$, целая часть 1, остаётся $1 : \frac{\sqrt{3}-1}{2} = \sqrt{3}+1$, как и требовалось. ◁

6.18 Докажите, что числа n^2 и $n-1$ взаимно просты при любом целом $n > 1$.

▷ Можно вспомнить, что $n^2 - 1 = (n-1)(n+1)$, так что при делении n^2 на $n-1$ с остатком получится 1 (и частное $n+1$). Можно просто повторить рассуждения для этого случая, не ссылаясь на алгоритм Евклида: если d — общий делитель n^2, и $n-1$, то он делит и $n(n-1) = n^2 - n$, а значит, и n (как разность с n^2), а значит и 1 (как разность n и $n-1$). ◁

• Второе рассуждение лучше первого, потому что нет вопросов про то, с чего это мы позволяем себе применять алгоритм Евклида к отрицательным числам.

6.19* Докажите, что в последовательности

$$2+1, 2^2+1, 2^4+1, 2^8+1, 2^{16}+1, 2^{32}+1, \ldots$$

любые два числа (не обязательно соседние) взаимно просты. Как из этого вывести, что простых чисел бесконечно много?

▷ Произведение чисел этой последовательности до 2^n+1 равно $2^{2n}-1$ (удобно домножить формально на $(2-1)$ и потом применять формулу $(a-b)(a+b) = a^2 - b^2$ много раз), то есть на 2 меньше следующего члена $2^{2n}+1$. Значит, если бы этот следующий член имел общий делитель с одним из предыдущих, то и

разница 2 должна была бы на него делиться, а делителя 2 нет, потому что все числа нечётны).

Раз числа взаимно просты, то их разложения на простые множители не пересекаются (нет общих простых множителей), так что всего простых чисел должно быть бесконечно много. ◁

• Ещё одно доказательство получается из рассуждения с оценкой гармонического ряда, которое мы обсуждали в связи с плотностью простых чисел. Повторим его применительно к нашему случаю. Пусть есть всего k простых чисел $p_1, \ldots, p_k$. Каждая из k сумм

$$1+\frac{1}{p_1}+\frac{1}{p_1^2}+\frac{1}{p_1^3}+\ldots,\quad 1+\frac{1}{p_2}+\frac{1}{p_2^2}+\frac{1}{p_2^3}+\ldots,\quad \ldots,\quad 1+\frac{1}{p_k}+\frac{1}{p_k^2}+\frac{1}{p_k^3}+\ldots,$$

сколько слагаемых в ней ни бери, будет не больше такой суммы для наименьшего простого числа 2, то есть $1+\frac{1}{2}+\frac{1}{4}+\ldots$, а эта сумма при любом количестве слагаемых остаётся меньше 2 (сделаем шаг, потом полшага, останется полшага, потом четверть шага, останется четверть шага, и так далее). Поэтому произведение k таких сумм (при любом количестве слагаемых) будет не больше 2^k. С другой стороны, при раскрытии скобок и достаточно большом количестве слагаемых мы получим (среди прочего) все слагаемые в сумме

$$1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\ldots\frac{1}{N},$$

даже и для больши́х N (надо просто взять побольше слагаемых). В самом деле, любое m можно разложить как произведение степеней простых, и найдя эти степени в знаменателях, перемножить, получится $1/m$. (Мы не пользуемся однозначностью — если бы даже её и не было, то $1/m$ появилось бы несколько раз.) Поэтому в наших предположениях (все простые среди $p_1, \ldots, p_m$) мы получаем, что

$$1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\ldots\frac{1}{N}\leqslant 2^k$$

при любом k. Но если левую часть разбивать на скобки вида

$$\frac{1}{n+1}+\frac{1}{n+2}+\ldots+\frac{1}{2n},$$

то каждая скобка не меньше $1/2$ (в ней n членов, каждый не меньше $1/2n$), и потому при большом числе скобок получается противоречие.