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?

• 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?

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

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

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.]

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

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

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

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

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

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:

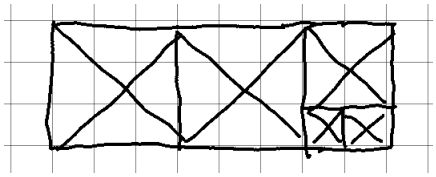
$$\text{НОД}(2, 1) = \text{НОД}(2 \bmod 1, 1) = \text{НОД}(0, 1) = 1.$$

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).

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.

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

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

(и сравните с предыдущей задачей).

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).

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 $a, b, c \neq 0$.

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.

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)?

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

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

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

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?

• 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 $1 + \frac{1}{2} + \frac{1}{4} + ...$, 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

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

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 $p_1, ..., p_m$) мы получаем, что

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

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

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

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