# 8. Однозначность разложения и её следствия

Сейчас уже всё готово для доказательства теоремы об единственности разложения на простые множители. Основная лемма тут (уже доказанная): *произведение двух чисел, не делящихся на простое $p$, тоже не делится на $p$*. То же самое верно и для большего числа сомножителей.

**8.1** Докажите, что это верно для любого числа сомножителей: если число $p$ простое ни один из сомножителей в произведении не делится на $p$, то и всё произведение не делится на $p$.

• Другими словами, если произведение делится на $p$, то хотя бы один сомножитель делится на $p$. Или так: не может быть, чтобы все сомножители не делились, а произведение делилось. (Речь везде идёт, конечно, о произведении целых чисел.)

Мы уже говорили про однозначность разложения на простые множители: если какое-то положительное целое число двумя способами представлено в виде произведения простых множителей, то есть

$$a = p_1 \cdot p_2 \cdot \ldots \cdot p_k = q_1 \cdot q_2 \cdot \ldots \cdot q_l,$$

то эти разложения отличаются лишь перестановкой множителей (в них входят одни и те же множители в разном порядке; в частности, $k = l$.

**8.2** Докажите это утверждение, пользуясь предыдущей задачей.

**8.3** Пусть $p, q$ — два различных простых числа. Покажите, что в последовательностях $1, p, p^2, p^3, \ldots$ и $1, q, q^2, q^3, \ldots$ нет общих чисел, кроме 1.

**8.4*** Пусть $a$ и $b$ — два целых положительных (не обязательно простых) числа. Покажите, что если $a^n = b^m$ при некоторых целых $m, n > 0$, то оба числа $a$ и $b$ являются степенями некоторого одного числа $x$.

Если какой-то множитель повторяется в разложении несколько раз, его можно написать в соответствующей степени, если он совсем не входит, его можно написать в нулевой степени ($p^0 = 1$). Поэтому теорему о разложении на множители можно пересказать так: всякое число $n$ однозначно представляется в виде

$$N = 2^{n_2} \cdot 3^{n_3} \cdot 5^{n_5} \cdot \ldots$$

где $k_2, k_3, k_5, \ldots$ — неотрицательные целые числа, среди которых лишь конечное число ненулевых (так что реально в произведении конечное число множителей). Для случая $N = 1$ можно считать, что все $n_i$ равны нулю (все сомножители единицы).

Глядя на степени простых чисел в разложении (другими словами, их *кратности* — сколько раз они входят в разложение), можно многое сказать о делимости, наибольшем общем делителе и так далее. В следующих задачи сформулированы такие утверждения.

**8.5** Два положительных целых числа $a$ и $b$ разложены в произведение простых. Как, глядя на эти разложения, определить, делится ли $a$ на $b$?

**8.6** Сколько делителей у числа $2^5 \cdot 3$?

**8.7*** Сколько делителей у целого числа $2^n 3^m 5^k$?

**8.8*** Найдите наименьшее число, имеющее ровно 18 делителей.

**8.9** Как определить по разложению числа на множители, будет ли оно точным квадратом?

**8.10*** Докажите с помощью предыдущих задач (если вы этого еще не сделали другим способом раньше), что целое положительное число $n$ имеет нечётное число делителей тогда и только тогда, когда оно является точным квадратом.

**8.11** Как, глядя на разложение на множители двух целых положительных чисел, узнать, будут ли они взаимно простыми?

**8.12** Как, глядя на разложение на множители целого положительного числа, определить, сколько у него на конце нулей в десятичной записи?

**8.13** Как, глядя на разложение на множители двух целых положительных чисел $a$ и $b$, найти их наибольший общий делитель? Почему сразу ясно, что он делится на любой другой общий делитель?

• Глядя на эту задачу, можно было бы подумать, что алгоритм Евклида не особо и нужен: можно разложить числа на множители и потом найти их наибольший общий делитель описанным способом. С точки зрения практики это совсем не так: раскладывать на множители большие числа гораздо сложнее. Число из нескольких тысяч цифр на современных компьютерах разложить часто не удаётся — а найти наибольший общий делитель двух чисел такого размера с помощью алгоритма Евклида можно практически мгновенно.

**8.14** Используя предыдущую задачу, покажите, что для целых положительных $a, b, k$ выполняется равенство $\text{НОД}(ka, kb) = \text{НОД}(a, b)$.

(Раньше мы видели другое доказательство, с помощью алгоритма Евклида.)

**8.15** Как найти наименьшее общее кратное двух чисел, зная их разложение на множители? Почему любое общее кратное делится на наименьшее общее кратное?

Будем обозначать наименьшее общее кратное двух целых положительных чисел $a$ и $b$ через $\text{НОК}(a, b)$. (В английских текстах иногда используют обозначение $\text{lcm}(a, b)$, сокращение от least common multiple.)

**8.16** Докажите, что для любых целых положительных $a$ и $b$ выполняется равенство

$$\text{НОД}(a, b) \cdot \text{НОК}(a, b) = ab$$

• Когда складывают две простые дроби, часто ищут наименьшее кратное их знаменателей (чтобы привести дроби к общему знаменателю).

**8.17** В каких случаях наибольшее кратное двух чисел равно их произведению?

Наибольший общий делитель и наименьшее общее кратное можно определить не только для двух, но и для трёх (и более) чисел (посмотрев на все общие делители, то есть числа, являющиеся делителями всех трёх, и выбрав наибольший, и т.п.).

**8.18*** Докажите, что для любых целых положительных $a$, $b$ и $c$ выполняется равенство

$$\text{НОК}(a, b, c) = \frac{a \cdot b \cdot c \cdot \text{НОД}(a, b, c)}{\text{НОД}(a, b) \cdot \text{НОД}(a, c) \cdot \text{НОД}(b, c)}.$$

• Эта формула аналогична так называемой *формуле включений и исключений* для числа элементов в множествах: $|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$.

**8.19** Используя теорему об однозначности разложения на множители (и уже выведенные из неё следствия), докажите заново уже встречавшиеся нам утверждения: (а) если $ab$ делится на $k$ и $a$ взаимно просто с $k$, то $b$ делится на $k$; (б) если $a$ делится на каждое из двух взаимно простых чисел $b$ и $c$, то $a$ делится на их произведение $bc$.

**8.20** Докажите, что если для некоторого целых положительных $a$ и $n$ уравнение $x^n = a$ имеет рациональное решение (найдётся рациональное $x$, для которого $x^n = a$), то найдётся и целое решение этого уравнения.

**8.21*** Покажите, что кратность любого простого множителя $p$ в разложении на множители числа $n! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot n$ равна

$$\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \ldots$$

Здесь $\lfloor u \rfloor$ обозначает целую часть (наибольшее целое, не превосходящее $u$); сумма в правой части обрывается, когда все дальнейшие слагаемые становятся равны нулю (потому что очередные степени $p$ все больше $n$).

**8.22*** Следуя предыдущей задаче, покажите, что для любого целого $n \geqslant 2$ произведение любых последовательных $n$ чисел делится на $n!$ (сравнив кратного произвольного простого $p$ в этом произведении и в $n!$).

**8.23*** Покажите, что среди степеней двойки $1, 2, 4, 8, \ldots$ и степеней тройки $1, 3, 9, 27, \ldots$ не только нет общих чисел, кроме 1, но нет и соседних чисел, кроме четырёх пар: $(1, 2)$, $(2, 3)$, $(3, 4)$ и $(8, 9)$. (Это установил ещё в XIV веке Леви бен Гершон — который помимо математики занимался талмудом, астрономией и многим другим.)

• Верно гораздо более сильное утверждение: если рассматривать степени целых чисел (кроме первой, то есть квадраты, кубы и т.д.), то среди них не найдётся двух идущих подряд чисел, кроме 8 и 9. Эта *гипотеза Каталана*, сформулированная аж в 1844 году, была доказана только сравнительно недавно (2002, Михайлеску), и доказательство сложное.

**8.24*** Для целого положительного числа $n$ можно подсчитать количество его делителей, которое мы обозначим $\tau(n)$, и сумму всех его делителей, которую мы обозначим $\sigma(n)$. Покажите, что если (целые положительные) числа $a$ и $b$ взаимно просты, то $\tau(ab) = \tau(a)\tau(b)$ и $\sigma(ab) = \sigma(a)\sigma(b)$. Найдите $\tau(4620)$ и $\sigma(4620)$, используя разложение $4620 = 2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11$.

• Указанное в этой задаче свойство функций $\sigma$ и $\tau$ иногда называют *мультипликативностью*. Оно останется верным, если мы рассмотрим сумму любых степеней делителей, скажем, сумму их квадратов. (Для степени 0 получается $\tau$, для степени 1 получается $\sigma$.)

**8.25*** Пусть $n$ — целое положительное число, которое не делится ни на 2, ни на 5. Докажите, что существует число вида 111 ... 111 (несколько единиц подряд в десятичной записи), которое делится на $n$.

- В качестве первого шага можно доказать, что некоторое число вида 1111 ... 111000 ... 000 делится на $n$ (тут даже не важно, на что $n$ не делится).