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.)

▷ Будем постепенно добавлять сомножители в произведение, сохраняя не-делимость на p. Вообще если известно, что произведение двух «хороших» чисел «хорошее» — что бы ни называлось «хорошим» — то и произведение любого количества хороших чисел будет хорошим (домножение произведения на хорошее число сохраняет хорошесть). ◁

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.

▷ Пусть есть два разложения целого положительного числа на простые множители. Если входящие в них простые числа пересекаются (есть простое число, входящее в оба), то сократим на все такие множители. Если после сокращения вообще ничего не останется (с обеих сторон будет 1), то, значит, разложения были одинаковые, только порядок разный (потому что состояли из тех самых множителей, на которые мы сократили). Может ли быть иначе? В этом случае получится два разложения одного числа, в которых нет общих множителей:

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

(мы написали снова a, но это может быть уже меньшее число после сокращения). Теперь это очевидно противоречит доказанному: левая часть делится на p_1, а правая часть (ей равная) состоит из простых чисел, не равных p_1 и потому не делящихся на p_1 — и, значит, их произведение не делится на p_1 (как говорит предыдущая задача). ◁

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.

▷ Общее число имело бы два разных разложения. ◁

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.

▷ Можно считать (как говорят, *не ограничивая общности* — это значит, что всегда можно свести дело к этому случаю), что m и n взаимно просты. (Иначе можно взять наибольший общий делитель и извлечь корень). Посмотрим теперь на разложение числа $u = a^n = b^m$. Поскольку разложение u единственно, то одно и то же разложение получится, если начать с a и если начать с b. Какова кратность какого-то простого числа p в этом разложении? она должна делиться на m, и одновременно на n, то есть должна делиться на mn (взаимная простота), поэтому из u можно извлечь нацело корень степени mn, и этот корень $x = \sqrt[mn]{u}$ будет давать $x^m = a$ и $x^n = b$. ◁

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?

▷ Чтобы убедиться, что a делится на b, надо проверить, что все числа, входящие в разложение b, входят и в a, причём не меньшее число раз (с не меньшей кратностью). Это почти очевидно, но скажем подробно. Надо проверить две вещи.

Пусть a делится на b. Покажем, что кратности простых чисел в a не меньше, чем в b. Раз a делится на b, то $a = bc$ для некоторого целого c (тоже положительного). Разложим b и c на простые множители. Соединяя эти разложения, получим разложение для a, в котором кратности не меньше, чем в разложении для b. Но поскольку разложение единственно, это и будет данное нам разложение на a.

Наоборот, пусть в a кратности не меньше, чем в b. Тогда излишек (множители из a, которые не попали в b) образует c, и $a = bc$. ◁

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

▷ Из предыдущей задачи видно, что они все имеют вид $2^a 3^b$, где $0 \leqslant a \leqslant 5$, $0 \leqslant b \leqslant 1$. Таким образом, для 2^a есть шесть вариантов $2^0, 2^1, \ldots, 2^5$, и каждый из них можно умножать на 3, а можно и не умножать, всего 12 вариантов. ◁

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

▷ Делители имеют вид $2^{n_1} 3^{m_1} 5^{k_1}$, где $0 \leqslant n_1 \leqslant n$, $0 \leqslant m_1 \leqslant m$ и $0 \leqslant k_1 \leqslant k$. Для n_1 есть $n+1$ вариантов, затем $m+1$ и $k+1$, всего комбинаций $(n+1)(m+1)(k+1)$. ◁

8.8* Найдите наименьшее число, имеющее ровно 18 делителей.

▷ Вспоминая разложение $18 = 3 \cdot 3 \cdot 2$, видим, что годится любое число $p^2 q^2 r$, где p, q, r — простые числа. Наименьшее будет при $p = 2$, $q = 3$, $r = 5$, то есть 180. Ещё есть разложение 18 (то есть числа вида p^{19}, а также $2 \cdot 9$, то есть числа pq^8, или $3 \cdot 6$, то есть числа $p^2 q^5$. Но в каждом из трёх вариантов наименьшее число будет больше. (Для последнего: $3^2 \cdot 2^5 = 9 \cdot 32 = 288$, для остальных ещё больше.) ◁

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

▷ Все простые множители должны входить в него чётное число раз. ◁

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.

▷ В задаче 7 мы видели, что число делителей равно произведению кратностей в разложении, увеличенных на 1. Чтобы это произведение было нечётным, необходимо и достаточно, чтобы все кратности были чётны. ◁

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

▷ Посмотреть, есть ли у них общие простые делители в разложениях: если есть, то они явно не взаимно просты, если нет, то простых общих делителей нет (здесь используется однозначность разложения!), поэтому и никаких нет (любой общий делитель можно разложить на простые). ◁

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

▷ Что такое число нулей на конце? это максимальная степень $10^n = 2^n 5^n$, на которую число делится. Значит, надо посмотреть, сколько в разложении двоек и сколько пятёрок, и взять минимум из этих двух кратностей. ◁

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?

▷ В общий делитель каждое простое число должно входить с кратностью не больше чем в a и не больше чем в b. Делитель будет наибольшим, если эта кратность максимальна.

Другими словами, общие делители чисел

$$N = 2^{n_2} 3^{n_3} 5^{n_5} \quad \text{и} \quad M = 2^{m_1} 3^{m_2} 5^{m_5}$$

имеют вид $2^{k_2} 3^{k_3} 5^{k_5} \ldots$, где k_p не превосходит n_p и m_p. Наибольший общий делитель получится, если $k_p = \min(n_p, m_p)$. (Через $\min(u, v)$ обозначается минимум из двух чисел u и v — то из них, которое меньше, или любое, если они равны.) ◁

• 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.)

▷ Кратность какого-то простого p в ka и kb получается из кратностей в a и b добавлением кратности в k, поэтому и минимум тоже увеличится на кратность p в k. Что соответствует умножению $\text{НОД}(a, b)$ на k. ◁

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

▷ Если m — общее кратное a и b, то любое простое p входит в разложение m не меньше раз, чем в a и чем в b, и наоборот. Поэтому надо взять максимум из кратностей p в сомножителях. ◁

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

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

▷ Это следует из сказанного выше про кратности и очевидного соотношения $\min(u, v) + \max(u, v) = u + v$. ◁

• 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?

▷ Если числа взаимно просты (это следует, например, из предыдущей задачи). ◁

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: $|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$.

▷ Достаточно проверить, что для любого простого p кратности в левой и правой части одинаковы. Это сводится к проверке тождества

$$\max(u,v,w) = u + v + w + \min(u,v,w) - \min(u,v) - \min(u,w) - \min(v,w).$$

От перестановок это тождество не меняется, поэтому достаточно его проверить для $u \leqslant v \leqslant w$, а тогда это будет

$$w = u + v + w + u - u - u - v,$$

и всё сокращается. ◁

• В этом решении есть пробел: а почему дробь в правой части целая и вообще можно считать кратности? Можно заметить, что сомножители в знаменателе делят a, c и b соответственно и потому числитель их сокращает. А можно перенести знаменатель в левую часть, тогда вопрос отпадает и рассуждение действует, а потом поделить.

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.

▷ (а) Если ab делится на k, то разложение ab содержит разложение k, но в a нет тех множителей, которые есть в k, так что все они приходятся на b. (б) В разложении a есть разложение b и есть разложение c, при этом они не пересекаются, так как b и c не имеют общих множителей. ◁

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.

▷ Пусть $(u/v)^n = a$ для целых u и $v \neq 0$. Можно считать $v > 0$ (изменим знак у u и v, если нужно). Можно считать также, что $u > 0$. В самом деле, если n нечётно, то это автоматически так, а если чётно, то знак можно поменять. Теперь разложим u и v на множители (и сократим общие, если они есть). Если в знаменателе что-то останется, то оно никуда не денется и после возведения в степень, так что u^n/v^n — тоже несократимая дробь. Получаем два разных разложения $u^n = av^n$, что противоречит теореме о единственности разложения на множители. ◁

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).

▷ Множители p в разложении для $n!$ появляются, когда сомножитель в $1 \cdot 2 \cdot \ldots \cdot n$ кратен p. Таких кратных сомножителей как раз $\lfloor n/p \rfloor$ (а именно, p, $2p$,...kp, где k — максимальное целое, меньшее или равное n/p). Но могут быть и сомножители, в которых p входит несколько раз: $p^2, 2p^2, \ldots, kp^2$ при $k = \lfloor n/p^2 \rfloor$. Как подсчитать общий вклад? Есть такой способ считать сумму нескольких целых положительных чисел: подсчитать все числа по разу, потом ещё раз пересчитать числа, большие или равные 2, потом ещё добавить числа, большие или равные 3, и так далее. Тогда число, равное u, будет как раз u раз и посчитано. Этот способ подсчёта и даёт утверждение задачи. ◁

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 $n!$).

▷ В соответствии с методом подсчёта в предущей задачи достаточно убедиться, что среди $1, 2, \ldots, n$ не больше кратных p^k, чем в любых подряд идущих

n чисел. Количество кратных зависит от того места натурального ряда, с которого мы начинаем считать, то меньше всего их будет в том случае, когда мы начинаем точно сразу после очередного кратного (как с $1, 2, 3, \dots, n$, которые сразу следуют за 0). ◁

8.23* Покажите, что среди степеней двойки $1, 2, 4, 8, \dots$ и степеней тройки $1, 3, 9, 27, \dots$ 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.

▷ Надо искать решения уравнений $2^m = 3^n + 1$ и $3^m = 2^n + 1$. Начнём с первого. Начиная с 8. левая часть делится на 8, значит, и правая часть должна делиться, то есть $3^n \equiv 7 \pmod 8$, а так не бывает (остатки у степеней 3 по модулю 8 чередуются: $1, 3, 1, 3, \dots$. Среди меньших 8 (кроме указанных вариантов) решений очевидно нет.

Второе: $3^m = 2^n + 1$. Снова рассуждая по модулю 8, видим, что m должно быть чётно, так что достаточно доказать, что непредвиденных решений у уравнение $3^{2k} = 2^n + 1$ нет. Переписав его как $3^{2k} - 1 = 2^n$ и разложив левую часть как $(3^k - 1)(3^k + 1)$, видим, что обе скобки должны быть степенями двойки, и отличаться на 2, так что это может быть только 2 и 4, снова ничего непредвиденного не получается. ◁

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 σ и τ иногда называют *мультипликативностью*. Оно останется верным, если мы рассмотрим сумму любых степеней делителей, скажем, сумму их квадратов. (Для степени 0 получается τ, для степени 1 получается σ.)

▷

Выпишем все делители чисел a и b: пусть это будут $u_1, \dots, u_k$ и $v_1, \dots, v_l$ соответственно. Если перемножить какие-то u_i и v_j, то произведение $u_i v_j$ будет делителем числа ab. Поскольку a и b взаимно просты, так получатся все делители ab, и каждый по одному разу. В самом деле, любой делитель ab разлагается на простые множители, и можно разделить эти множители на те, которые встречаются в a, и те, которые встречаются в b. Отсюда сразу следует, что $t(ab)$ (число делителей ab) равно числу пар (делитель a, делитель b), то есть $\tau(a)\tau(b)$.

Для σ: раскроем скобки в произведение $\sigma(a)\sigma(b) = (u_1 + \dots + u_k)(v_1 + \dots + v_l)$, получится сумма kl слагаемых вида $u_i v_j$, то есть как раз сумма всех делителей числа ab.

То же рассуждение годится и для суммы s-х степеней делителей при любом s.

Теперь легко посчитать ответ для нашего примера:

$$\tau(2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11) = \tau(2^2)\tau(3)\tau(5)\tau(7)\tau(11) = 3 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 48$$

(это мы уже обсуждали). Для суммы:

$$\sigma(2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11) = \sigma(2^2)\sigma(3)\sigma(5)\sigma(7)\sigma(11) = \\ = (1 + 2 + 4)(1 + 3)(1 + 5)(1 + 7)(1 + 11) = 7 \cdot 4 \cdot 6 \cdot 8 \cdot 12 = 16\,128.$$

$\triangleleft$

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).

$\triangleright$ В бесконечной последовательности $1, 11, 111, 1111, \dots$ есть два числа, дающие одинаковые остатки при делении на n, поэтому их разница делится на n. Если n взаимно просто с 10, то нули на конце можно убирать без нарушения делимости. $\triangleleft$