5. Простые и составные числа

Целое число $p > 1$ называется *простым*, если оно не имеет делителей, кроме 1 и самого себя. Если же такие делители есть, то число называется *составным*.

• Мы использовали здесь букву p, её часто используют для простых (английское prime) чисел. Но, конечно, в математике такого жёсткого правила нет (это в физике m почти всегда масса, а g — ускорение свободного падения).

Напомним кстати, что по нашим соглашениям делители должны быть целыми положительными числами, так что -1 или $-p$ делителем не будет.

5.1 Докажите, что целое число $n > 1$ является составным тогда и только тогда, когда его можно представить в виде произведения двух меньших положительных целых чисел.

• Странное выражение «тогда и только тогда» означает, что надо доказать две вещи: (1) если число n составное (не является простым, то есть имеет делитель помимо 1 и n), то его можно представить в виде произведения двух меньших положительных целых чисел и (2) если число n можно представить в виде произведения двух меньших положительных целых чисел, то оно не является простым (имеет делитель помимо 1 и n).

Оговорка про положительность сомножителей нужна: число 3 простое, но равно произведению $(-3) \cdot (-1)$.

▷ Оба утверждения по существу очевидны, тем не менее скажем подробно.

Если n составное, то оно имеет некоторый делитель m, отличный от 1 и n. Делимость n на m значит, что $n = mk$ для некоторого k. Оба числа m, k целые и положительные, не совпадают с 1 и n (про m это мы знаем; если k равно 1 или n, то m равно n или 1 соответственно), их произведение равно n, поэтому оба меньше n.

Напротив, если $n = ab$, где $0 < a, b < n$, то a является (по определению) делителем n. По предположению $a < n$ и потому a не совпадает с n. Если же $a = 1$, то $b = n$, что противоречит предположению $b < n$. Поэтому n имеет делитель a, помимо 1 и n, и потому не простое (составное). ◁

• Будет ли число 1 простым или составным? Обычно его не считают ни таким, ни сяким (как и, скажем, 0, или $1/3$, или -5, или π), в нашем определении *классифицируются на простые и составные только целые числа, большие* 1. Это удобно в некоторых формулировках.

5.2 Покажите, что *минимальный* делитель любого числа n (не считая 1) всегда простой. (Если n простое, то этот минимальный делитель совпадает с самим n.)

▷ Если какой-то делитель не простой, то множители, на которые он разлагается, будут меньшими делителями — значит, делитель этот не минимальный. ◁

5.3 Покажите, что любое составное число n имеет делитель, больший 1, но не превосходящий $\sqrt{n}$. Как этот факт можно использовать при проверке простоты?

▷ Делители числа n группируются в пары (произведение в каждой паре равно n): если a делит n, то по определению $n = ab$, и b тоже делит n. Ясно, что в паре оба члена не могут быть больше $\sqrt{n}$, иначе их произведение будет больше n.

Отсюда следует, что при проверки простоты достаточно проверить делители до $\sqrt{n}$ включительно. Если их нет, то и дальше уже не будет — вплоть до самого n. ◁

5.4 Покажите, что количество делителей у любого положительного целого n не превышает $2\sqrt{n}$.

▷ В предыдущей задаче мы видели, что делители группируются в пары, и меньшие члены пар не больше $\sqrt{n}$. Значит, и самих пар не больше $\sqrt{n}$. (Может быть делитель, парный самому себе, но тогда в этой «паре» только одно число, и делителей только меньше.) ◁

5.5* Покажите, что число $2^{128} - 1$ — составное. Найдите его разложение в произведение семи целых чисел, больших 1.

▷ Можно последовательно применять формулу $n^2 - 1 = (n + 1)(n - 1)$ к $n = 2^{64}$, $n = 2^{32}$ и так далее, получится

$$2^{128} - 1 = (2^{64} + 1)(2^{32} + 1)(2^{16} + 1)(2^8 + 1)(2^4 + 1)(2^2 + 1)(2 + 1)(2 - 1)$$

(восьмая скобка, равная единице, написана для красоты, она в число семи множителей не входит). ◁

• На самом деле два первых сомножителя можно разложить дальше, но это сразу не видно. (Числа такого вида называются *числами Ферма*.)

5.6* Покажите, что число 999 991 составное, разложив его в произведение меньших. (Это можно сделать в уме, почти без вычислений.)

▷ Заметим, что $999\,991 = 1\,000\,000 - 9 = 1000^2 = 3^2 = 997 \cdot 1003$. (Можно и дальше разложить, но это уже не так сразу видно: 1003 делится на 17.) ◁

5.7 Число 2 простое и чётное. Бывают ли другие такие числа?

▷ Нет, конечно: у чётного числа есть делитель 2, и если само число не 2, то простым оно не будет. ◁

5.8 Числа 2 и 3 — соседние простые числа (отличающиеся на 1). Бывают ли другие такие пары?

▷ Нет: из двух соседних чисел одно должно быть чётным, и если оно просто, то это должно быть 2 (см. предыдущую задачу). ◁

5.9 Три простых числа $3, 5, 7$ идут через одно (следующее больше предыдущего на 2). Бывают ли другие такие тройки?

▷ Нет — это следует из того, что из трёх чисел, идущих через одно, всегда одно делится на 3. В самом деле, пусть это числа n, $n+2$, $n+4$. Посмотрим, какой остаток даёт при делении на 3. Если 0, то первое из трёх делится на 3, если 1, то второе, если 2, то третье. А простое число, делящееся на 3, может быть только 3. ◁

• Простые числа, отличающиеся на 2, называют «близнецами»: таковы, например, 9 и 11, 137 и 139, и так далее. Известны очень большие пары простых близнецов, с сотнями тысяч цифр — но пока никто не может доказать, что их бесконечно много. (Опровергнуть тоже не могут.)

Самих по себе простых чисел, как мы увидим скоро, бесконечно много.

5.10 Числа $8, 9, 10$ — три подряд идущих составных числа. Найдите 5 подряд идущих составных чисел. Найдите 7 подряд идущих составных чисел.

▷ Искомые примеры небольшие, и их можно найти, просто смотря на все числа по порядку: $24, 25, 26, 27, 28$ — пять идущих подряд составных чисел. А $90 = 9 \cdot 10, 91 = 7 \cdot 13, 92 = 46 \cdot 2, 93 = 31 \cdot 3, 94 = 47 \cdot 2, 95 = 19 \cdot 5, 96 = 48 \cdot 2$ — семь подряд идущих составных чисел. ◁

5.11* Докажите, что можно найти и 100 подряд идущих составных чисел, и вообще любое количество подряд идущих составных чисел.

▷ Если какое-то число a делится на 2, 3, 4, 5, 6,..., 101, то все числа $a+2$, $a+3$, $a+4$, $a+5$, $a+6$,..., $a+101$ будут составными: скажем, $a+47$ делится на 47. А их как раз 100 подряд. Остаётся подобрать такое a. Можно просто взять произведение

всех этих чисел $2 \cdot 3 \cdot 4 \cdot \ldots \cdot 101$ в качестве a, потому что произведение делится на все свои множители. ◁

• Бывают и меньшие — скажем, незачем умножать на 2, если мы умножаем на 4. Математики бы сказали, что вместо 101! можно взять наименьшее общее кратное чисел от 2 до 101.

5.12* Выпишем в порядке возрастания нечётные простые числа: 3, 5, 7, 11, 13, 17, 19, 23,.... Докажите, что среднее арифметическое двух соседних чисел в этой последовательности — всегда составное число.

▷ Эта задача сильно проще, чем кажется на первый взгляд: среднее арифметическое двух соседних чисел лежит между ними, а там простых чисел нет, потому что они были соседними. (Поскольку соседи были простыми нечётными, то сумма их чётна, и среднее арифметическое целое. Надо ещё заметить, что оно не может быть 2.) ◁

• Почему простые числа называют простыми, не очень понятно (по-английски, кстати, они prime, а не simple). Легче объяснить, почему составные называют составными (по-английски composite): их можно *составить* (compose) из меньших множителей, скажем, 6 состоит из 2 и 3 ($6 = 2 \cdot 3$, 30 состоит из 2, 3 и 5, и так далее.

5.13 Докажите, что любое целое число, большее 1, можно *разложить на простые множители*, то есть представить в виде произведения простых сомножителей. (Одно и то же простое число может входить в произведение несколько раз. Допускаются и «произведения», состоящие из одного сомножителя.)

▷ Если число $n > 1$ простое, его мы считаем произведением из одного сомножителя. Если оно составное, то по определению его можно представить в виде произведения ab двух меньших чисел, которые сами могут быть простыми или составными. Если они простые, то разложение уже получено, если составные, то повторим рассуждение и разложим их на меньшие, и так далее. (Процесс закончится, потому что на каждом шаге числа уменьшаются.) ◁

▷ Это называют «рассуждением по индукции»: мы доказываем, что n можно разложить на множители, предполагая, что для меньших чисел (в нашем случае a и b) это утверждение уже известно. ◁

5.14 Разложите на простые множители числа 1000 и 1001.

▷ Про 1000 сразу ясно: $1000 = 10^3 = 2\cdot5\cdot2\cdot5\cdot2\cdot5 = 2^3\cdot5^3$. Про 1001 надо пробовать разные делители, но (к счастью для нас) они оказываются небольшими: $7 \cdot 11 \cdot 13$. ◁

Составное число можно по-разному разбить на сомножители: скажем, $30 = 2 \cdot 15 = 3 \cdot 10$. Но если разлагать дальше, пока части не станут простыми ($15 = 3 \cdot 5$, $10 = 2 \cdot 5$), то получится в итоге одно и то же разложение $2 \cdot 3 \cdot 5$. Это не случайно — можно доказать, что *любые два разложения на множители данного числа по существу одинаковы — отличаются лишь порядком множителей*. Это утверждение называется *теоремой об однозначности разложения на простые множители* (а иногда торжественно объявляется «основной теоремой арифметики»). Может показаться странным, но это не само собой разумеется и даже не так просто доказать (нам потребуется некоторая подготовка).

5.15 Дотошный ученик считает, что опроверг теорему об единственности разложения, обнаружив пример двух разложений.

$$78227 \cdot 244999 = 19165536773 = 99599 \cdot 192427$$

Прав ли он — и если неправ, то в чём его ошибка?

▷ Разложения правильные (проверьте!) — но вот только множители в них не простые, и на самом деле

$$\begin{aligned} 78227 &= 137 \cdot 571, \\ 244999 &= 337 \cdot 727, \\ 99599 &= 137 \cdot 727, \\ 192427 &= 337 \cdot 571. \end{aligned}$$

Если продолжить разложение, то получатся одни и те же четыре простых множителя. ◁

- «Задача нечестная — как можно найти эти множители, не зная их заранее?» Действительно, так сразу их не угадаешь, а проверять все довольно долго. Можно написать программу (или просто указать запрос типа `factor(78827)` на сайте `wolframalpha.com`), а можно воспользоваться алгоритмом Евклида для поиска общих множителей, о котором мы расскажем дальше.

5.16 Дано положительное целое число n (можно взять, скажем, 1000). (а) Докажите, что есть число, которое делится на все числа от 2

до n. (б) Докажите, что есть число, большее 1, которое даёт остаток 1 при делении на все числа от 2 до n. (в) Докажите, что есть число, большее 1, которое не делится ни на одно из чисел от 2 до n.

▷ Если перемножить все числа от 2 до n, получится число, которое на все эти числа (от 2 до n) делится. Если теперь прибавить единицу, то получится число, которое даёт при делении на все эти числа остаток 1 — и, значит, на них не делится. ◁

5.17 Докажите, что простых чисел бесконечно много. (Можно переформулировать это так: простые числа нигде не кончаются, для любого n есть простое число, большее n.)

• Это — одна из самых первых теорем теории чисел, она есть в знаменитых «Началах» Евклида. В книжке «Математическая смесь» Дж. Литлвуда (М.:Наука, 1990) автор спрашивает себя, какие настоящие математические результаты можно объяснить «с минимумом сырого материала», и пишет, что «“Общеизвестное” евклидово доказательство бесконечности множества простых чисел может, конечно, претендовать на первое место».

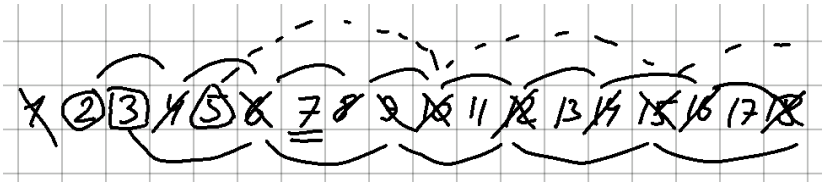
▷ Если бы все простые числа были меньше n, то какие были бы простые делители у числа из предыдущей задачи, которое не делится ни на одно из них? А хоть один-то простой делитель должен быть (само число, если нет других). ◁

• Вот как это излагает Литлвуд: «Евклидово доказательство бесконечности множества простых чисел может быть для профессионала сжато в одну строчку: если $p_1, \dots, p_n$ простые, то $1 + p_1 p_2 \dots p_n$ не делится ни на одно p_n».

5.18* Докажите, что остаток от деления любого простого числа на 30 будет либо 1, либо простое число.

▷ Если исходное простое число меньше 30, то оно и будет остатком. Пусть теперь оно больше 30. Тогда оно не делится ни на 2, ни на 3, ни на 5. Значит, и остаток не делится ни на 2, ни на 3, ни на 5. Какие есть составные числа до 30, которые не делятся ни на 2, ни на 3, ни на 5? Никаких (если наименьший простой делитель 7, то число будет минимум 49, так как должен быть ещё один простой делитель, не меньший 7). ◁

Как составить таблицу простых чисел? Можно написать все числа $1, 2, 3, 4, 5, 6, \dots$ подряд и выбросить составные (и единицу). Сначала выбросим все чётные, кроме 2. Потом — все кратные 3, кроме 3. Потом — кратные 5, кроме 5, и так далее. (Понятно, почему можно пропустить кратные четырём? потому что они уже учтены среди кратных двум.)



Такой процесс называют «решетом Эратосфена» (того самого, про которого рассказывают, что он первым измерил размер Земли, сравнивая тени в Александрии и Сиене). «Решетом» — потому что мы «просеиваем» простые числа. Один этап просеивания можно описать так: у нас уже найдены несколько первых простых чисел и вычеркнуты все их кратные. Берём наименьшее невычеркнутое число (не считая уже найденных простых), оно будет следующим простым, и вычёркиваем все его кратные.

5.19* (а) Почему наименьшее невычеркнутое число будет простым? (б) Как долго нужно продолжать этот процесс, если мы хотим составить таблицу простых чисел до 1000?

▷ (а) Если бы оно было составным, то имело бы *простой* делитель, меньший его самого, а меньшие простые числа уже найдены и все их кратные вычеркнуты. (б) Достаточно остановиться, вычеркнув все кратные 31. В самом деле, следующее простое число будет 37 и его квадрат больше 1000 — поэтому любое составное число до 1000 имеет простой делитель, меньший 37. ◁

5.20* Докажите, что при достаточно больши́х n (достаточно взять $n \geqslant 100$, например), простые числа составляют не больше трети от всех чисел 1 до n. Можно ли найти такое n, чтобы среди чисел от 1 до n не меньше 90% были бы составными? Тот же вопрос для 99%.

• Простые числа — дело тонкое, и на самые невинно звучащие вопросы ответ может оказаться неизвестным. Скажем, никто не знает, всякое ли чётное число, начиная с 4, представляется в виде суммы двух простых чисел (ни одного контрпримера не известно, но и не доказано, что их нет). Это утверждение называют *гипотезой Гольдбаха* (она сформулирована в 1742 году в переписке Христиана Гольдбаха и знаменитого Леонарда Эйлера).

▷ Первую часть легко проверить: в каждой шестёрке $6k, 6k+1, 6k+2, 6k+3, 6k+4, 6k+5$ при $n \geqslant 1$ четыре числа из шести заведомо составные (кроме второго и последнего), потому что делятся на 2 или на 3. Остаются неучтённые: 1, 2, 3, 4, 5 (здесь три простых числа из пяти) и сколько-то в последней шестёрке (если она неполная, то там может быть максимум одно простое число). Чтобы скомпенсировать это, достаточно найти шесть неучтённых составных чисел, скажем 25, 35, 49, 55, 65, 75 (и есть ещё, скажем, 95).

Вторая часть: на самом деле можно найти любую долю, сколь угодно близкую к единице. Но доказать это не так просто. Подсчитаем долю чисел, которые останутся после k этапов просеивания в решете, то есть не делятся на первые k простых чисел $p_1, \ldots, p_k$ (как мы это делали для 2 и 3). Эти числа идут по циклу с периодом $p_1 \cdot \ldots \cdot p_k$, и доля их в этом периоде равна

$$\left(1-\frac{1}{2}\right)\cdot\left(1-\frac{1}{3}\right)\cdot\ldots\cdot\left(1-\frac{1}{p_k}\right)$$

($p_1 = 2$, $p_2 = 3$, так что мы написали их явно). Это следует из «китайской теоремы об остатках», которую мы потом докажем. Надо показать, что при больши́х k это произведение может быть сильно меньше 1%, тогда числа в неполном последнем периоде и в первом периоде сильно дела не изменят.

Это доказывается с помощью такого удивительного приёма: умножим обе части на

$$B = \left(1+\frac{1}{2}+\frac{1}{2^2}+\ldots\right)\cdot\left(1+\frac{1}{3}+\frac{1}{3^2}+\ldots\right)\cdot\left(1+\frac{1}{p_k}+\frac{1}{p_k^2}+\ldots\right)$$

(сколько членов написать в каждой скобке, мы выберем потом). В левой части получится не больше 1, потому что

$$(1-x)(1+x+x^2+\ldots+x^m) = 1-x^{m+1} \leqslant 1$$

поэтому левая часть не больше $1/B$. А число B можно сделать сколь угодно большим, если взять достаточно много простых чисел и достаточно много слагаемых в каждой скобке в B. В самом деле, в произведении будут члены вида $1/m$ при любом m, которое разлагается на простые множители до p_k, и выбирая достаточно большое k и достаточно много членов внутри скобок, можно получить

$$B \geqslant 1+\frac{1}{2}+\ldots+\frac{1}{N}+\text{ещё что-то}$$

для любого N, и остаётся доказать, что гармонический ряд расходится, то есть сумма справа может быть сколь угодно большой. Это следует из того, что

$$\frac{1}{k+1}+\frac{1}{k+2}+\ldots+\frac{1}{2k} \geqslant \frac{1}{2k}+\frac{1}{2k}+\ldots+\frac{1}{2k} \geqslant \frac{1}{2}.$$

(В этом рассуждение даже не важно, что всякое число единственным образом разлагается на простые множители, если бы это вдруг было не так, то было бы только больше членов в правой части.) $\triangleleft$