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 $(-3) \cdot (-1)$.

• 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.)

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?

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

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

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

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

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

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

• 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.

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

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.

• 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.)

▷ 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.

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?

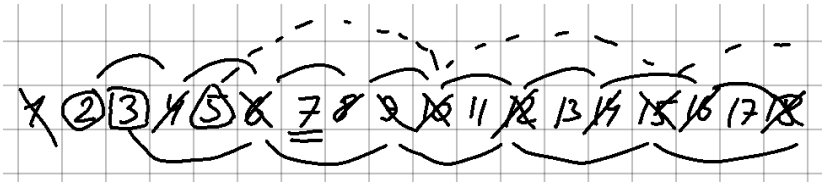
5.16 Дано положительное целое число n (можно взять, скажем, 1000). (а) Докажите, что есть число, которое делится на все числа от 2 до n. (б) Докажите, что есть число, большее 1, которое даёт остаток 1 при делении на все числа от 2 до n. (в) Докажите, что есть число, большее 1, которое не делится ни на одно из чисел от 2 до n.

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».

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

Как составить таблицу простых чисел? Можно написать все числа $1, 2, 3, 4, 5, 6, \ldots$ 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?

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).