1. Ряд простых чисел

Число 6 равно произведению двух чисел: 2 и 3. Число 7 нельзя разложить подобным образом на два сомножителя. Поэтому 7 называют *простым* числом. Вообще простым числом называется целое положительное число, которое нельзя разложить на два меньших сомножителя. 5 и 3 тоже простые числа; напротив, число 4 не простое, так как $4 = 2 \cdot 2$. Сама двойка также является простым числом. Число 1 составным не является, но оно ведет себя настолько отлично от остальных, что простым его также не считают. Таким образом, 2 — наименьшее простое число; первые несколько простых чисел суть

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, \ldots$$

С первого же взгляда видно, что эта последовательность не подчиняется никакой простой закономерности; и действительно, структура последовательности простых чисел весьма сложна.

Любое число можно разлагать на сомножители до тех пор, пока оно не будет представлено в виде произведения простых. Представив 6 в виде $2 \cdot 3$, мы убеждаемся в этом для 6 непосредственно; $30 = 5 \cdot 6$, но в свою очередь $6 = 2 \cdot 3$, поэтому $30 = 2 \cdot 3 \cdot 5$ является произведением трех простых сомножителей; $24 = 3 \cdot 8 = 3 \cdot 2 \cdot 4 = 3 \cdot 2 \cdot 2 \cdot 2$ разлагается на четыре сомножителя, из которых один, именно 2, повторяется трижды. Если число — скажем, 5, — само является простым, то нам остается только написать $5 = 5$ («произведение одного простого числа»). Такое последовательное разложение позволяет представить любое целое положительное число, кроме 1, в виде произведения простых. Поэтому простые числа являются как бы основными элементами, из которых построен весь числовой ряд.

В IX книге «Начал» Евклида ставится вопрос: *имеет ли последовательность простых чисел конец?* И там же дается ответ на этот вопрос: конца у этой последовательности нет, *за каждым простым числом может быть указано еще одно, большее простое число* [I]*.

---

*Напомним, что цифрами обозначаются ссылки на раздел «Дополнения и примечания» в конце книги.

Доказательство Евклида необычайно остроумно. Оно основывается на следующем простом замечании. Таблица, получающаяся при умножении последовательных чисел на 3:

$$3, 6, 9, 12, 15, 18, 21, 24, \ldots$$

содержит все числа, в которые входит множителем число 3; ни в какое другое число 3 не входит, в частности, оно не входит ни в одно из тех чисел, которые следуют непосредственно за числами этой последовательности, т. е. за кратными числа 3; таковы, например, $19 = 6 \cdot 3 + 1$, $22 = 7 \cdot 3 + 1$ и т. д.

Подобным же образом число 5 не может быть множителем числа, следующего непосредственно за числами, кратными 5, например числа $21 = 4 \cdot 5 + 1$; то же самое будет верно по отношению к 7, 11 и т. д.

Евклид строит числа

$$\begin{aligned} 2 \cdot 3 + 1 &= 7 \\ 2 \cdot 3 \cdot 5 + 1 &= 31 \\ 2 \cdot 3 \cdot 5 \cdot 7 + 1 &= 211 \\ 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 + 1 &= 2311 \\ 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 &= 30\,031 \quad \text{и т. д.,} \end{aligned}$$

которые получаются перемножением нескольких первых простых чисел и прибавлением единицы к полученному произведению.

Получающиеся таким образом числа не могут содержать в качестве множителей тех простых чисел, с помощью которых они сами были построены. Например, 31 не делится на 2, так как оно на 1 больше числа, кратного 2; оно же на 1 больше числа, кратного 3, так что оно не делится на 3, а так как оно на 1 больше числа, кратного 5, то оно не делится на 5. Число 31 оказывается простым, и оно бесспорно больше, чем 5. 211 и 2311 — также новые простые числа, а вот число 30 031 простым не является. Но тем не менее оно не делится на 2, 3, 5, 7, 11, 13, так что все его простые делители больше, чем 13. И действительно, путем нескольких проб можно обнаружить, что $30\,031 = 59 \cdot 509$; оба эти числа — и 59 и 509 — простые числа, бóльшие 13.

Это рассуждение будет справедливо и в том случае, если мы продолжим процесс образования таких чисел сколь угодно далеко.

Пусть p — какое-либо простое число; образуем из всех простых чисел от 2 до p число

$$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot \ldots \cdot p + 1 = N;$$

тогда ни одно из использованных здесь простых чисел 2, 3, 5, 7, …, p не войдет множителем в N. В таком случае либо само N будет простым числом, и притом значительно превышающим p, либо N будет разлагаться на простые множители, заведомо отличные от чисел 2, 3, 5, …, p, т. е. бо́льшие чем p. И в том и в другом случае должны существовать простые числа, бо́льшие p. За каждым простым числом следует, таким образом, еще одно большее. А это и требовалось доказать.

Неизвестно, что должно нас больше всего удивлять в этом тексте Евклида: то ли, что греческие математики вообще могли поставить подобный вопрос ради него самого, из внутреннего влечения к математическому мышлению, т. е. по мотивам, не свойственным ни одному из более древних народов и переданным в наследство позднейшим культурам лишь греческой традицией [2], или то, что они поставили именно этот вопрос, столь легко ускользающий от наивного наблюдателя, кажущийся ему праздным и тривиальным, вопрос, подлинная трудность которого не лежит на поверхности. Нельзя, наконец, не восхититься тем, как просто и красиво Евклид доказывает свою теорему. Было бы естественно пытаться доказать ее не так, как это сделал Евклид, но пытаясь найти простое число, непосредственно следующее за данным. Такие попытки действительно были, но они неизменно оканчивались неудачей, причина которой в том, что последовательность простых чисел устроена чрезвычайно нерегулярно.

Доказательство Евклида обходит трудность, вызываемую этой нерегулярностью: в нем строится не *ближайшее* следующее за p простое число, но *какое-то* простое число, большее p. Например, в качестве простого числа, заведомо превышающего 11, доказательство дает не 13, а 2311, а за 13 оно дает простое число 59. Обычно между тем простым числом, которое дает нам доказательство Евклида, и ближайшим простым числом находится много других простых чисел. Это свидетельствует не о слабости евклидовского рассуждения, а об изобретательности древних греков, умело ограничившихся в доказательстве ровно тем, что требовалось.

Чтобы дать представление о сложности последовательности простых чисел, мы покажем, что в *ряду простых чисел могут быть сколь угодно большие пробелы* [3]; так, например, мы покажем, что среди тысячи следующих друг за другом чисел может не оказаться ни одного простого числа. Мы исходим при этом из соображений, весьма близких к евклидовым.

Выше мы заметили, что число $2 \cdot 3 \cdot 5 + 1 = 31$ не делится ни на одно из простых чисел 2, 3, 5. Если два числа делятся на 2, то и их сумма делится на 2, и то же верно для 3, 5, 7 и т. д. Заметим теперь, что $2 \cdot 3 \cdot 5$ делится на 2, на 3 и на 5, так что $2 \cdot 3 \cdot 5 + 2 = 32$ делится на 2, $2 \cdot 3 \cdot 5 + 3 = 33$ делится на 3, $2 \cdot 3 \cdot 5 + 4 = 34$ делится на 2, $2 \cdot 3 \cdot 5 + 5 = 35$ делится на 5 и $2 \cdot 3 \cdot 5 + 6 = 36$ делится на 2. Стало быть, ни одно из чисел 32, 33, 34, 35 и 36 не является простым; эта последовательность прерывается на числе $2 \cdot 3 \cdot 5 + 7 = 37$, которое ни на 2, ни на 3, ни на 5 не делится.

Точно так же можно найти и 1000 последовательных составных чисел. Обозначим первое простое четырехзначное число (именно 1009) через p и построим тысячу последовательных чисел

$$2 \cdot 3 \cdot \ldots \cdot p + 2,\ \ 2 \cdot 3 \cdot \ldots \cdot p + 3,\ \ \ldots,\ \ 2 \cdot 3 \cdot \ldots \cdot p + 1001.$$

Применим к ним только что проиллюстрированный метод рассуждения. Каждое из чисел 2, 3, …, 1001 делится по крайней мере на одно из простых чисел 2, 3, …, p, произведение же $2 \cdot 3 \cdot \ldots \cdot p$ делится на все эти числа. Значит, каждая из вышенаписанных сумм делится по крайней мере на одно из этих простых чисел, так что ни одна из них не может быть простым числом. Итак, мы нашли *тысячу последовательных чисел, среди которых нет ни одного простого*.

Конечно, нужно зайти довольно далеко в ряду простых чисел, прежде чем встретится такого рода пробел. Но если пойти достаточно далеко, то можно, следуя тому же принципу, найти пробел, охватывающий миллион последовательных чисел, и вообще сколь угодно большой величины.

Эта вторая проблема, сколь ни близка она к первой как по характеру постановки вопроса, так и по методу доказательства, не встречается ни у кого из греческих математиков. Ее выдвинула новая математика, связав с нею целый круг дальнейших задач. Большинство этих новых задач уже далеко не столь просты. Некоторые из них и сегодня остаются нерешенными, работа над другими привела к созданию совершенно новых разделов математики.

Мы остановимся здесь на одном небольшом примере, который поддается анализу методом Евклида и позволяет составить некоторое представление о том, в каком именно направлении современная математика расширяет исследования, начатые древними греками. Выше мы рассматривали сначала числа 3, 6, 9, …, получающиеся от умножения последовательности чисел натурального ряда на 3, а затем последовательность следующих за ними чисел 4, 7, 10, …; теперь рассмотрим еще оставшиеся после этого числа

$$2, 5, 8, 11, 14, 17, 20, 23, \ldots,$$

т. е. числа, которые при делении на 3 дают в остатке 2. Верно ли, что и среди одних только этих чисел содержится уже бесчисленное множество простых чисел? Правда ли, что последовательность простых чисел

$$2, 5, 11, 17, 23, \ldots$$

также не имеет конца?

Для начала заметим, что если перемножить между собой два каких-либо числа последовательности

$$1, 4, 7, 10, 13, \ldots,$$

то получается число, принадлежащее к этой же последовательности. Действительно, каждое из этих чисел есть кратное 3, увеличенное на единицу, так что оно имеет вид $3x+1$. Если второе такое число равно $3y+1$, то в их произведении получим

$$(3x+1)(3y+1) = 9xy + 3y + 3x + 1 = 3(3xy + y + x) + 1,$$

т. е. опять число, на единицу большее кратного трем.

Из этого следует, что среди простых множителей любого из чисел последовательности 2, 5, 8, 11, … всегда найдется по крайней мере один, принадлежащий к этой же последовательности. Так, например, для $14 = 2 \cdot 7$ таковым является множитель 2, а для $35 = 5 \cdot 7$ — множитель 5. Действительно, ни один из таких простых множителей не может принадлежать к ряду 3, 6, 9, …, в котором имеется лишь одно-единственное простое число 3. С другой стороны, если бы рассматриваемое число состояло из одних только простых множителей, принадлежащих к последовательности 4, 7, 10, 13, ..., то, согласно предыдущему замечанию, оно само должно было бы принадлежать к этой же последовательности. Таким образом, чтобы число принадлежало к последовательности 2, 5, 8, 11, ..., оно должно содержать по меньшей мере один простой множитель, принадлежащий к этой же самой последовательности.

Теперь мы можем действовать аналогично евклидовскому доказательству, с тем отличием, что мы рассмотрим число

$$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot \ldots \cdot p - 1 = M$$

вместо

$$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot \ldots \cdot p + 1 = N.$$

Число M, будучи на единицу *меньше* кратного 3, принадлежит к последовательности 2, 5, 8, 11, ... Число M, так же как и N, не делится ни на одно из простых чисел 2, 3, 5, 7, 11, ..., p. Является ли само M простым числом или оно разлагается на несколько простых множителей — в обоих случаях эти простые числа будут больше p. Среди этих множителей должен быть по крайней мере один, принадлежащий к последовательности 2, 5, 8, 11, ... Таким образом, в этой последовательности заведомо имеются простые числа, превышающие сколь угодно большое простое число p и расположенные, следовательно, сколь угодно далеко.

Теперь остается открытым вопрос о том, содержит ли также и последовательность 1, 4, 7, 10, 13, ... бесконечно много простых чисел; нет ничего невозможного в предположении, что из всей совокупности простых чисел бесконечно много их приходится на последовательность 2, 5, 8, ... и только конечное число — на последовательность 1, 4, 7, ... Доказательство того, что и вторая последовательность содержит также бесконечно много простых чисел, требует уже совершенно других методов, представление о которых мы попытаемся дать в одном из следующих этюдов [4].

Нам хотелось лишь показать здесь, что современная математика не только в отдельных частных случаях, но и в проблемах кардинальной важности — как в постановке вопросов, так и в методах их решения — примыкает к греческой. Это относится не только к отдельным задачам, но и к целым разделам науки, исследования в которых продолжаются и сегодня.