§ 9. ПРОСТЫЕ И СОСТАВНЫЕ ЧИСЛА

В этом разделе нас будут интересовать делители натуральных чисел. Их помогает находить следующая теорема.

Теорема 11. Всякий натуральный делитель b натурального числа a не превосходит a.

Поскольку b – натуральный делитель натурального числа a, то для некоторого натурального c справедливо равенство $a = bc$. Предположим, что $a < b$. Умножая это неравенство на c, получим $ac < bc = a = a \cdot 1$. Согласно теореме 6.2 из неравенства $a \cdot c < a \cdot 1$ следует неравенство $c < 1$, противоречащее тому, что 1 – наименьшее натуральное число.

Значит из трех возможных случаев расположения чисел a, b на числовом луче $a < b$, $a = b$, $a > b$ первый случай невозможен, а второй и третий можно объединить записью $a \geq b$.

Теорема 11 показывает, что все натуральные делители числа a надо искать среди чисел $1, 2, \ldots, a$. В частности, все натуральные делители числа 1 не превосходят 1. Поэтому число 1 имеет только один натуральный делитель – самого себя.

Если натуральное число a больше 1, то равенство $a = 1 \cdot a$ показывает, что число a имеет по крайней мере два различных натуральных делителя: 1 и a. Это простое замечание служит исходным пунктом для двух важнейших в теории чисел определений.

*Отличное от 1 натуральное число a называется **простым**, если оно не имеет натуральных делителей отличных от 1 и a.*

*Отличное от 1 натуральное число a, называется **составным**, если оно имеет хотя бы один натуральный делитель, отличный и от 1, и от a.*

Поскольку всякое натуральное число, большее 1, имеет, по крайней мере, два различных натуральных делителя, то оно является либо простым, либо составным.

Например, натуральное число 2 является простым, поскольку равенство $2 = 2 \cdot 1$ показывает, что числа $1, 2$ являются делителями числа 2, а теорема 11 утверждает, что у двойки других претендентов на делители нет.

Число 3 тоже является простым, поскольку согласно теореме 11 его делителями могут быть лишь числа $1, 2, 3$. Равенство $3 = 2 \cdot 1 + 1$ показывает, что число 3 при делении на 2 дает остаток 1 и, по теореме 10, не делится нацело на 2. Равенство $3 = 3 \cdot 1$ показывает, что числа 1 и 3 являются делителями числа 3 и, значит, число 3 является простым.

Равенство $4 = 2 \cdot 2$ показывает, число 4 имеет натуральный делитель 2, отличный и от 1, и от 4, поэтому оно является составным.

Следующая теорема говорит о простых делителях натуральных чисел.

Теорема 12. Всякое отличное от $\mathbf{1}$ натуральное число $\boldsymbol{a}$ имеет простой делитель. Более точно, наименьший, отличный от $\mathbf{1}$, делитель $\boldsymbol{p}$ этого числа $\boldsymbol{a}$ является простым числом.

Среди чисел $1, 2, \ldots, a$ найдем наименьший делитель p числа a, отличный от 1. Такой делитель существует, поскольку $a \vdots a$ и $a \neq 1$. Если число p составное, то оно имеет делитель q, отличный и от 1, и от p. Тогда с учетом теоремы 11 получаем, что $1 < q < p$. Поскольку $a \vdots p$, $p \vdots q$, то $a \vdots q$ и q – отличный от 1 делитель числа a, меньший p, что противоречит выбору делителя p. Значит число p простое и теорема доказана.

Следующая теорема дошла до нас из трудов древнегреческого математика Евклида. Она имеет большое значение как для самой математики, так и для ее приложений, например, в вопросах цифровизации.

Теорема 13. Существует бесконечно много простых чисел.

Допустим, что существует лишь конечное число простых чисел. Тогда мы можем взять самое большое простое число p и вычислить выражение $a = 1 \cdot 2 \cdot 3 \cdot 4 \cdot \ldots \cdot p + 1$.

Поскольку $a > 1$, то по теореме 12 у числа a есть простой делитель q. Ясно, что $q > 1$. Так как p – самое большое простое число, то $p \geq q$. Значит, в произведении $1 \cdot 2 \cdot 3 \cdot 4 \cdot \ldots \cdot p$ встречается множитель q и произведение делится на q. Выше мы отмечали, что у числа 1 нет делителей, отличных от 1, поэтому $1 \not\vdots\, q$ и по теореме 10.4 число q не является делителем числа a, что противоречит выбору q.

Предположение о конечности количества простых чисел привело нас к противоречию. Следовательно, существует бесконечно много простых чисел.