Простые числа

Определение 1.10. Пусть a — целое число. Числа $1, -1, a, -a$ называются *тривиальными делителями* числа a.

Определение 1.11. Целое число $p \in \mathbb{Z} \setminus \{0\}$ называется *простым*, если оно не является делителем единицы и не имеет других делителей, кроме тривиальных. В противном случае число $p \in \mathbb{Z} \setminus \{-1, 0, 1\}$ называется *составным*.

Пример 1.21. Числа $\pm 2, \pm 3, \pm 5, \pm 7, \pm 11, \pm 13, \pm 17, \pm 19, \pm 23, \pm 29$, ± 7927, ± 7933, ± 7937, ± 7949, ± 7951, ± 7963, ± 7993, ± 8009, ± 8011, ± 8017, $\pm 8575773501597484328339530743573866684929048460408516782 09$ являются простыми. □

Пример 1.22. Числа

$$-17647 = -7 \cdot 2521,\ 1752458619827 = 4133 \cdot 5851 \cdot 72469,$$

$$916941942360412139468515338546876825319747546525 9 =$$

$$= 857577350158321091012200932964 3 \cdot 106922360086950931 3$$

являются составными. □

Свойства простых чисел

1. Если числа p и q простые и p делится на q, то $p \sim q$.

Доказательство. Из определения простого числа и того, что p делится на q, следует, что $q \in \{\pm 1, \pm p\}$.

Если $q = \pm 1$, то q не простое; если $q = \pm p$, то $p \sim q$. □

2. Если число p простое и число a целое, то либо a делится на p, либо НОД$(a, p) = 1$.

Доказательство. Пусть НОД$(a, p) = d > 1$. Тогда a делится на d и p делится на d, но так как число p простое, то либо $d = \pm 1$ (что противоречит предположению), либо $d = \pm p$. □

3. Если число p простое и произведение ab делится на p, то либо a делится на p, либо b делится на p.

Доказательство. Пусть a не делится на p. Тогда по предыдущему свойству НОД$(a, p) = 1$. Следовательно, по свойству 2 наибольшего общего делителя, b делится на p. □

4. Если число p простое и произведение $a_1 a_2 \ldots a_k$ делится на p, то хотя бы одно из чисел $a_1, a_2, \ldots, a_k$ делится на p.

5. Если числа $p_1, p_2, \ldots, p_k, q_1, q_2, \ldots, q_l$ простые и выполняется равенство для произведений $p_1 p_2 \ldots p_k = q_1 q_2 \ldots q_l$, то $l = k$ и числа $q_1, q_2, \ldots, q_l$ можно перенумеровать так, что $p_1 \sim q_1, p_2 \sim q_2, \ldots, p_k \sim q_k$.

Упражнение. Методом математической индукции доказать свойства 4, 5.

Пример 1.23. Найдем все простые числа p, для которых числа $p + 2$ и $p + 5$ одновременно являются простыми.

При $p = 2$ получаем $p + 2 = 4$ — составное число, при $p = -2$ получаем $p + 2 = 0$.

Все остальные простые числа — нечетные и имеют вид $p = 2k + 1$. Тогда $p + 5 = 2k + 1 + 5 = 2(k + 3)$. Это число четное и может быть простым лишь тогда, когда оно равно 2 или -2. В первом случае получаем $k + 3 = 1$, $k = -2$, $p = -3$. Но тогда $p + 2 = -1$ — не простое число.

Во втором случае получаем $k+3=-1$, $k=-4$, $p=-7$. Тогда $p+2=-5$ — простое число.

Таким образом, число $p=-7$ является единственным решением нашей задачи. □

Учитывая свойство 1 простых чисел, под простыми числами обычно понимают только положительные простые числа.

Теорема 1.11 (основная теорема арифметики). Всякое число $n \in \mathbb{Z} \setminus \{-1, 0, 1\}$ можно представить в виде $n = \varepsilon p_1 p_2 \ldots p_r$, где $\varepsilon = \pm 1$ и $p_1, p_2, \ldots, p_r$ — простые числа (не обязательно различные), $r \geq 1$. Это представление единственно с точностью до порядка сомножителей.

Представление числа $n \in \mathbb{Z} \setminus \{-1, 0, 1\}$ в виде $n = \varepsilon p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_s^{\alpha_s}$, где $\varepsilon = \pm 1$, $p_1, p_2, \ldots, p_s$ — различные простые числа, $\alpha_i \geq 1$ для $i = 1, 2, \ldots, s$, $s \geq 1$, называется *каноническим разложением* числа n.

Пример 1.24. Каноническое разложение числа 12345876 имеет вид $2^2 \cdot 3^2 \cdot 17 \cdot 20173$; каноническое разложение числа -2345679 имеет вид $(-1) \cdot 3^5 \cdot 7^2 \cdot 197$. □

Следующие две теоремы называются теоремами Евклида о простых числах.

Теорема 1.12. Простых чисел бесконечно много.

Теорема 1.13. Существуют сколь угодно длинные отрезки натурального ряда, не содержащие простых чисел, то есть для любого $k \geq 1$ существует такое $n \in \mathbb{N}$, что числа $n+1$, $n+2$, …, $n+k$ составные.