1. Отношение делимости целых чисел

ОПРЕДЕЛЕНИЕ. Множество $\mathbb{N}$ *натуральных чисел* определяется с использованием *аксиом Пеано*:

1) $1 \in \mathbb{N}$ (единица – натуральное число);

2) Для любого $a \in \mathbb{N}$ существует единственное последующее $a^+ \in \mathbb{N}$;

3) Для любого $a \in \mathbb{N}$ выполняется неравенство $a^+ \neq 1$ (единица наименьшее натуральное число);

4) Если $a^+ = b^+$, то $a = b$ (каждое последующее число обладает единственным предыдущим);

5) Если некоторое подмножество $N \subseteq \mathbb{N}$ содержит единицу и для каждого натурального числа $a \in \mathbb{N}$ выполняется $a^+ \in \mathbb{N}$, то $N = \mathbb{N}$ (принцип индукции).

Таким образом, $\mathbb{N} = \{1, 2, 3, \dots\}$.

В арифметику натуральных чисел включены операции сложения и умножения.

ОПРЕДЕЛЕНИЕ. Каждой паре натуральных чисел a, b можно единственным образом поставить их *сумму* – натуральное число $a + b = \underbrace{(\dots (a^+)^+ \dots)^+}_{b \text{ раз}}$ так, чтобы выполнялись условия для любых натуральных чисел a, b, c:

1) $a + 1 = a^+$;

2) $(a + b) + c = a + (b + c)$ (ассоциативность сложения);

3) $a + b = b + a$ (коммутативность сложения);

4) если $a + b = a + c$, то $b = c$.

ОПРЕДЕЛЕНИЕ. Каждой паре натуральных чисел a, b можно единственным образом поставить их произведение – натуральное число $a \cdot b = \underbrace{(\dots (a + a) + \dots + a)}_{b \text{ раз}}$ так, чтобы выполнялись условия для любых натуральных чисел a, b, c:

1) $a \cdot 1 = a$;

2) $a \cdot b^+ = a \cdot b + a$;

3) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ (ассоциативность умножения);

4) $a \cdot b = b \cdot a$ (коммутативность умножения);

5) $a \cdot (b + c) = a \cdot b + a \cdot c, \quad (a + b) \cdot c = a \cdot c + b \cdot c$ (дистрибутивность умножения относительно сложения);

6) если $a \cdot c = a \cdot b$, то $b = c$.

ОПРЕДЕЛЕНИЕ. Множество натуральных чисел *линейно упорядоченно*, т.е. $\forall a, b \in \mathbb{N}$ выполняется ровно одно из трех условий: $a < b, a > b, a = b$.

ОПРЕДЕЛЕНИЕ. Отношение «меньше» ($<$) (как и отношение «больше» ($>$)) *транзитивно*, то есть из неравенств $a < b$ и $b < c$ следует, что $a < c$ ($a > b, b > c \implies a > c$).

ОПРЕДЕЛЕНИЕ. Множество *целых чисел* $\mathbb{Z}$ определяется как объединение множеств натуральных чисел, им противоположных и нуля:

$\mathbb{Z} = \mathbb{N} \cup (-\mathbb{N}) \cup \{0\}$.

Таким образом, $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$.

На множестве целых чисел $\mathbb{Z}$ операции сложения и умножения задаются теми же правилами, что и для натуральных чисел.

ОПРЕДЕЛЕНИЕ. Пусть a и b некоторые целые числа, $b \neq 0$. Число b называется *делителем* числа a, если существует такое целое число q, что выполняется равенство $a = bq$. При этом a называется *кратным* числа b, а q – *частным* от деления a на b. Делитель называется *собственным*, если он отличен от самого числа.

Если число b является делителем числа a, то для краткости будем писать $b|a$. Если же b не является делителем числа a, то будем писать $b \nmid a$.

СВОЙСТВА ОТНОШЕНИЯ ДЕЛИМОСТИ

1) Для любого $a \in \mathbb{Z}, a \neq 0$ справедливо $a|a$ (рефлексивность);

2) Для любого $a \in \mathbb{Z}$ справедливо $1|a$;

3) Если $b|a$, то при любом сочетании знаков $\pm b| \pm a$;

4) Если $c|b$ и $b|a$, то $c|a$ (транзитивность);

5) Если $b|a$, то $\forall\, k \in \mathbb{Z}, k \neq 0$ справедливо $kb|ka$;

6) Если $kb|ka$, причем $k \neq 0$, то $b|a$;

7) Если $b|a$, то $\forall\, c \in \mathbb{Z}$ справедливо $b|ca$;

8) Если $c|a$ и $c|b$, тогда $c|(a+b)$ и $c|(a-b)$;

9) Если $c|a_1, c|a_2, \ldots, c|a_n$ и $b_1, b_2, \ldots, b_n$ – произвольные целые числа, тогда $c|(a_1b_1 + a_2b_2 + \cdots + a_nb_n)$;

10) Если $b_1|a_1, b_2|a_2, \ldots, b_n|a_n$, тогда $b_1 \cdot b_2 \cdot \ldots \cdot b_n | a_1 \cdot a_2 \cdot \ldots \cdot a_n$;

11) Если $b|a$ и $a \neq 0$, то $|a| \geq |b|$;

12) Если $b|a$ и $a|b$, то $|a| = |b|$.

ОПРЕДЕЛЕНИЕ. Пусть a и b целые и $b \neq 0$. *Разделить a на b* с остатком – значит представить a в виде $a = qb + r$, где $q, r \in \mathbb{Z}$ и $0 \leq r < |b|$. Число q называется неполным частным, число r – остатком от деления a на b.

ПРИМЕР.

1) Для $b = 15$ имеем:

$$45 = 3 \cdot 15 + 0, \quad 0 \leq 0 < 15;$$

$$123 = 8 \cdot 15 + 3, \quad 0 \leq 3 < 15;$$

$$-105 = (-7) \cdot 15 + 0, \quad 0 \leq 0 < 15;$$

$$-169 = (-12) \cdot 15 + 11, \quad 0 \leq 11 < 15;$$

…

2) Для $b = -11$ имеем:

$$44 = (-4) \cdot (-11) + 0, \quad 0 \leq 0 < 11;$$

$$119 = (-10) \cdot (-11) + 9, \quad 0 \leq 9 < 11;$$

$$-253 = 23 \cdot (-11) + 9, \quad 0 \leq 0 < 11;$$

$$-288 = 21 \cdot (-11) + 3, \quad 0 \leq 3 < 11;$$

…

ТЕОРЕМА (о делении с остатком). Для любых $a, b \in \mathbb{Z}, b \neq 0$, существует единственная пара таких чисел $q, r \in \mathbb{Z}$, что $a = qb + r, 0 \leq r < |b|$.

ТЕОРЕМА. Для любых $a, b \in \mathbb{Z}, a > 0, b \geq 2$, существует, и при том единственное разложение вида: $a = a_n b^n + \cdots + a_1 b + a_0, 0 \leq a_i < b, i = \overline{1, n}, 0 < a_n < b$.

Представление числа a в виде $a = a_n b^n + \cdots + a_1 b + a_0$ называется *представлением числа в b – ичной системе счисления* и записывается в виде $a = (a_n \ldots a_0)_b$.

УТВЕРЖДЕНИЕ. Пусть $a, b \in \mathbb{Z}, b \neq 0$. Число b является делителем числа a тогда и только тогда, когда остаток от деления a на b равен нулю.

2. Простые числа.

ОПРЕДЕЛЕНИЕ. Пусть a – целое число. Числа $1, -1, a, -a$ называются *тривиальными делителями* числа a.

ОПРЕДЕЛЕНИЕ. Целое число $p \in \mathbb{Z}/\{-1, 0, 1\}$ называется *простым*, если не имеет других делителей, кроме тривиальных. В противном случае число $p \in \mathbb{Z}/\{-1, 0, 1\}$ называется *составным*.

ПРИМЕР. Числа $\pm 2, \pm 3, \pm 5, \pm 7, \pm 11, \pm 13, \pm 17, \pm 19, \pm 23, \pm 29, \ldots$ являются простыми.

Числа: $4 = 2 \cdot 2,\ 6 = 2 \cdot 3,\ 8 = 2 \cdot 4,\ 9 = 3 \cdot 3,\ 10 = 2 \cdot 5, \ldots$ являются составными.

СВОЙСТВА ПРОСТЫХ ЧИСЕЛ:

1) Если p и q простые и p делится на q, то $p \sim q$ (ассоциированные, т.е. $p = \pm q$).

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

3) 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.

ТЕОРЕМА (первая теорема Евклида о простых числах). Простых чисел бесконечно много.

ТЕОРЕМА (вторая теорема Евклида о простых числах). Существуют сколь угодно длинные отрезки натурального ряда, не содержащие простых чисел.

(Если выписать подряд все простые числа, то можно заметить, что относительная плотность их убывает: от 1 до 10 – четыре простых числа, т.е. 40% целых чисел являются простыми, от1 до 100 – 25 простых чисел (25%), от 1 до 1000 – 168 простых чисел (17%), от 1 до 10^5 – 9592 простых числа (менее 10%)).

ТЕОРЕМА (основная теорема арифметики). Всякое число $n \in \mathbb{Z}/\{-1, 0, 1\}$ можно представить в виде $n = \varepsilon \cdot p_1 \cdot p_2 \cdot \ldots \cdot p_r$, где $\varepsilon = \pm 1$ и $p_1, p_2, \ldots, p_r$ – простые числа (не обязательно различные), $r \geq 1$.

ОПРЕДЕЛЕНИЕ. Представление числа $n \in \mathbb{Z}/\{-1, 0, 1\}$ в виде $n = \varepsilon \cdot p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_s}$, где $\varepsilon = \pm 1$ и $p_1, p_2, \ldots, p_s$ – простые числа, $\alpha_i \geq 1$ для $i = \overline{1, s}$ $(s \geq 1)$, называется *каноническим разложением* числа n.

ПРИМЕР. Записать каноническое разложение числа: а) 12345876; б) -2345679.

а)	б)
12345876 | 2 6172938 | 2 3086469 | 3 1028823 | 3 342941 | 17 20173 | 20173 1	2345679 | 3 781893 | 3 260631 | 3 86877 | 3 28959 | 3 9653 | 7 1379 | 7 197 | 197 1
$12345876 = 2^2 \cdot 3^2 \cdot 17 \cdot 20173$	$-2345679 = (-1) \cdot 3^5 \cdot 7^2 \cdot 197$

УТВЕРЖДЕНИЕ 1. Для любого натурального числа $n > 1$ наименьший отличный от единицы делитель всегда есть простое число.

УТВЕРЖДЕНИЕ 2. Наименьший отличный от единицы делитель составного числа n не превосходит $\sqrt{n}$.

УТВЕРЖДЕНИЕ 3. Если натуральное число $n > 1$ не делится ни на одно простое число, не превосходящее $\sqrt{n}$, то оно простое.

На данном утверждении основан *метод пробных делений* проверки числа a на простоту. При этом перебираются все числа $d = 2,3, \ldots, [\sqrt{a}]$ ([] – целая часть без округления) и проверяется, делится ли число a на d. Если среди данного набора делитель не будет найден, то число a является простым.

Например, $a = 17 \Rightarrow \left[\sqrt{17}\right] = 4 \Rightarrow d = 2, 3, 4 \Rightarrow 2 \nmid 17, 3 \nmid 17, 4 \nmid 17 \Rightarrow 17 -$ простое.

3. Решето Эратосфена.

Алгоритм Эратосфена (III век до н.э.) или *решето Эратосфена* – древний и один из самых эффективных алгоритмов для нахождения простых чисел до определенного предела.

АЛГОРИТМ ЭРАТОСФЕНА:

1) Создать список чисел от 2 до заданного предела N.

2) Определить первое число в списке (в начале это будет 2) и удалить (просеять) все его кратные, кроме самого числа.

3) Перейти к следующему числу в списке и повторить шаг2.

4) Продолжать процесс, пока не дойдет до конца списка.

5) По завершении алгоритма, все оставшиеся числа в списке будут простыми.

ПРИМЕР. (любой)

Алгоритм Эратосфена можно оптимизировать для улучшения его производительности и снижения потребления памяти:

1. Исключить четные числа, чтобы сократить объем проверяемых чисел вдвое.

2. Ограничить проверку до $\sqrt{N}$, поскольку все простые числа, большие $\sqrt{N}$, не могут быть делителями составных чисел, меньших или равных N.

3. Провести сегментацию, которая позволяет сократить объем используемой память и обрабатывать большие интервалы чисел.

Проблемы и ограничения алгоритма Эратосфена:

1. Потребление памяти. Алгоритм требует большого объема памяти для хранения списка чисел, особенно при обработке больших диапазонов.

2. Время выполнения. С увеличение числового диапазона время выполнения алгоритма растет, что может стать проблемой в реальных приложениях, где требуется быстрый поиск простых чисел.

3. Параллелизация. Параллельная реализация алгоритма может быть сложной и не всегда обеспечивать значительное увеличение производительности.