Дискретная математика

Лектор - Посов И.А.

1 Алгоритмы с целыми числами

Опр.: (Деление с остатком)

Поделить $a \in \mathbb{Z}$ на $b \in \mathbb{Z} \backslash \{0\}$ - это найти $q, r \in \mathbb{Z}$.

$$a = bq + r, \qquad 0 \le r < |b|$$

a - делимое, b - делитель, q - неполное частное, r - остаток

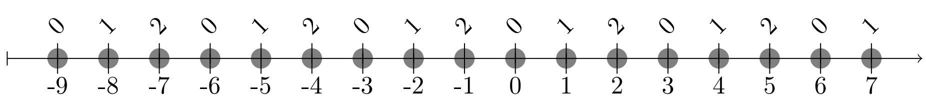
Примеры:

± 7 на 3

7 = 3 * 2 + 1, q = 2, r = 1 7 = 3 * 4 + (-5) т.к. -5<0, то $-5 \neq r$

-7 = 3 * (-3) + 2, 2 - остаток -7 = 3 * (-2) + (-1), т.к. -1<0, то $-1 \neq r$

Остатки при делении на 3:



Остатки циклически повторяются для $\mathbb{Z}$

Утв.: деление с остатком единственно.

Док-во:

$$\begin{cases} a = bq_1 + r_1 & 0 \le r_1 < |b| \\ a = bq_2 + r_2 & 0 \le r_2 < |b| \end{cases}$$

$$0 = b(q_1 - q_2) + (r_1 - r_2) \Leftrightarrow b(q_2 - q_1) = r_1 - r_2$$

$-|b| < r_1 - r_2 < |b|$

1)

$$\begin{cases} r_1 < |b| \\ r_2 \ge 0 \end{cases}$$

$r_1 - r_2 < |b| - 0$

2)

$$\begin{cases} r_2 < |b| \\ r_1 \ge 0 \end{cases}$$

$r_1 - r_2 < 0 - |b| \Rightarrow\ q_1 = q_2 \Rightarrow 0 = r_1 - r_2 \Rightarrow r_1 = r_2$

Опр.: $a \in \mathbb{Z}$ $b \in \mathbb{Z}$

$a \vdots b$ a кратно b, если остаток от деления a на b равен нулю.

Переформулировка:

$a \vdots b$, если $\exists q \in \mathbb{Z}$.

Примеры:

$9 \vdots 3, \quad 12 \vdots 4, \quad 0 \vdots 5$

Свойства делимости:

1) $\forall x \in \mathbb{Z}$ $x \vdots 1$;

2) $\forall x \in \mathbb{Z} \backslash \{0\}$ $x \vdots \pm x$;

3) $\forall x, y, z \in \mathbb{Z}$ $x \vdots y$ $y \vdots z \Rightarrow x \vdots z$;

4) Если $x \vdots y \Rightarrow \pm x \vdots \pm y$;

5) Если $x_i \vdots y$, $\lambda_i \in \mathbb{Z}$, то $\lambda_1 x_1 + \lambda_2 x_2 + \ldots + \lambda_n x_n \vdots y$

План д-ва 5)

I: $x \vdots y \Rightarrow \lambda x \vdots y$

$x = y * q; \lambda x = y * (\lambda q)$

II: $x_1 \vdots y$ и $x_2 \vdots y \Rightarrow x_1 + x_2 \vdots y$

$x_1 = yq_1, x_2 = yq_2 \Rightarrow (x_1 + x_2) = y(q_1 + q_2)$

Обозначим $a\ mod\ b$ - остаток от деления a на b.

Примеры:

$7\ mod\ 3 = 1 \qquad -7\ mod\ 3 = 2$

2 Системы счисления

$\mathbb{N}$ - множество натуральных чисел.

Опр.: "пэичная"система счисления - p с/сч.

Числа записываются цифрами, их p штук $(0, \ldots, p-1)$.

Пример: в 3-ой с/сч $0, 1, 2$.

Число $x \in \mathbb{N} \cup \{0\}$ $\qquad x = (\overline{c_n c_{n-1} \ldots c_0})_p$,

где c_i - цифры, p - основание с/сч.

$x = c_n p^n + c_{n-1} p^{n-1} + \ldots + c_1 p + c_0$

$\overline{57121}_{10} = 5 * 10^4 + 7 * 10^3 + 1 * 10^2 + 2 * 10^1 + 1$

Утв.: $\forall x \in \mathbb{N}$ и $p \in \mathbb{N}$ $(p \geq 2)$

1) $\exists$ представление в p с/сч.

2) Оно единственно (если запретить нулевые цифры в начале)

Д-во:

1) Поделим n с остатком на p.

$n = pn_1 + a_0$, pn_1 - частное, a_0 - остаток $\quad 0 \leq a_0 < p$

Далее делим n_1 на p: $n_1 = pn_2 + a_1$

Делаем, пока $n_i \neq 0$. Это произойдет, т.к. $n_k > n_{k+1}$.

Поймем, что a_i - цифры числа.

$n = pn_1 + a_0 = p(pn_2 + a_1) + a_0 = p^2 n_2 + pa_1 + a_0 = \ldots = p^n a_n + \ldots + pa_1 + a_0$ - это определение $(\overline{a_n a_{n-1} \ldots a_0})_p$.

2) [деление с остатком x на p]

x $= (\overline{c_n c_{n-1} \ldots c_0})_p = c_n p^n + c_{n-1} p^{n-1} + \ldots + c_1 p + c_0 = p(y_1) + c_0$

x $= (\overline{d_m d_{m-1} \ldots d_0})_p = d_m p^m + d_{m-1} p^{m-1} + \ldots + d_1 p + d_0 = p(y_2) + d_0$

$y_1 = \overline{c_n c_{n-1} \ldots c_1}, \quad y_2 = \overline{d_m d_{m-1} \ldots d_1}$

$0 \leq c_0, d_0 < p \Rightarrow c_0 = d_0 \Rightarrow y_1 = y_2$

Аналогично $c_1 = d_1$ и т.д. $\Rightarrow c_i = d_i$