# К линейному представлению НОД

1. Деление с остатком...

   ... в $\mathbb{Z}$ $\quad \forall a, b \in \mathbb{Z},\ b \neq 0 \quad \exists (!) q, r \in \mathbb{Z}: \quad a = bq + r$ и $0 \leq r < |b|$.

   ... в $\mathbb{Z}[\mathrm{i}]$ $\quad \forall a, b \in \mathbb{Z}[\mathrm{i}],\ b \neq 0 \quad \exists q, r \in \mathbb{Z}[\mathrm{i}]: \quad a = bq + r$ и $|r| < |b|$.

   ... в $\mathbb{F}[t]$ $\quad \forall a, b \in \mathbb{F}[t],\ b \neq 0 \quad \exists q, r \in \mathbb{F}[t]: \quad a = bq + r$ и $\left[\begin{array}{c} r = 0 \\ \deg r < \deg b \end{array}\right.$.

2. Евклидово кольцо

   $\mathcal{R}$ — ассоциативное коммутативное кольцо без делителей нуля.

   Норма $|\cdot| : \mathcal{R} \backslash \{0\} \to \mathbb{N}_0$, $\forall x, y\ |xy| \geq |x|$.

   $\forall a, b \in \mathcal{R},\ b \neq 0 \quad \exists q, r \in \mathcal{R}: \quad a = bq + r$ и $\left[\begin{array}{c} r = 0 \\ |r| < |b| \end{array}\right.$.

3. Алгоритм Евклида

$$\begin{array}{rcrcrcrl}
a & = & b & \cdot & q_1 & + & r_1, & |r_1| < |b|, \\
b & = & r_1 & \cdot & q_2 & + & r_2, & |r_2| < |r_1|, \\
r_1 & = & r_2 & \cdot & q_3 & + & r_3, & |r_3| < |r_2|, \\
 & \ldots & & & & & & \\
r_{k-2} & = & r_{k-1} & \cdot & q_k & + & r_k, & |r_k| < |r_{k-1}|, \\
r_{k-1} & = & r_k & \cdot & q_{k+1} & + & r_{k+1}, & r_{k+1} = 0.
\end{array}$$

   $(a, b) = (b, r_1) = (r_1, r_2) = \ldots = (r_{k-1}, r_k) = r_k$.

4. Линейное представление НОД.

   $\forall a, b \in \mathcal{R} \quad \exists x, y \in \mathcal{R} \quad (a, b) = ax + by$

5. Линейное представление НОД из алгоритма Евклида

   □ Каждое из $r_m$ представимо в виде $ax + by$ $(x, y \in \mathcal{R})$. ■

6. Линейное представление НОД методом крайнего

   □ Первое. Пусть $M = \{ax + by :\ x, y \in \mathbb{R}, ax + by \neq 0\}$, $m = \min\{|c| :\ c \in \mathcal{M}\}$.

   Второе. Пусть $d \in \mathcal{M}$ (т.е. $d = ax_0 + by_0$), $|d| = m$.

   Третье. $a \vdots z$, $b \vdots z \Rightarrow d \vdots z \Rightarrow |d| \geq |z|$ (т.е. $d$ не меньше любого общего делителя).

   Четвёртое. Если $a = dq + r$, $0 < r < d$, то $r = a(1 - qx_0) + b(-qy_0)$ ↯

   Пятое. $a \vdots d$, $b \vdots d$ (т.е. $d$ является общим делителем). ■

7. Разрешимость линейных диофантовых уравнений

   Уравнение $ax + by = c$ $(a, b, c \in \mathbb{Z})$ имеет решение $x, y \in \mathbb{Z} \iff c \vdots (a, b)$.