Алгебры

Харитонцев-Беглов Сергей

6 сентября 2021 г.

Содержание

1. Теория чисел

1.1. НОД, делимость, линейные диофантовы уравнения

***Определение* 1.1.** Диофантовым уравнение называется уравнение, которое можно решить $\mathbb{Z}$.

Рассмотрим линейное диофантово уравнене

$$ax + by = c..$$

Если бы мы были в $\mathbb{R}$, то решение быстро бы нашлось: $y = \frac{c-ax}{b}$. Но в целых штуках такая штука не всегда будет решением, т.к. b не всегда делит $c - ax$.

***Определение* 1.2.** a делится на b ($a\vdots b, b|a$), если $\exists c \in \mathbb{Z} : a = bc$.

Простые свойства:

1. $\forall a : 1|a$.
2. $\forall a : a|a$.
3. $\forall a, b\vdots c, k, l \in \mathbb{Z} \Rightarrow (ka + lb)\vdots c$.

   Доказательство. $a, b\vdots c \Rightarrow \exists d, e : \begin{matrix} a = c \cdot l \\ b = c \cdot e \end{matrix}$. Тогда $ka + lb = k \cdot cd + l \cdot ce = c \cdot (kd + le) \Rightarrow (ka + lb)\vdots c$ □

4. $\forall k \neq 0, k \in \mathbb{Z} : a\vdots b \iff ak\vdots bk$.
5. $a\vdots b \iff a^2\vdots b^2$.
6. $a\vdots b \Rightarrow \left[\begin{array}{l} |a| > |b| \\ a = 0 \end{array} \right.$.
7. $a\vdots b, b\vdots c \Rightarrow a\vdots c$.
8. $a\vdots a$.
9. $a\vdots b, b\vdots a \Rightarrow a = \pm b$.

Теорема 1.1 (О делении с остатком). $a, b \in \mathbb{Z}\exists!(q, r) : \begin{cases} q, r \in \mathbb{Z} \\ a = b \cdot q + r \\ 0 \leqslant r < |b| \end{cases}$

Доказательство.

- Единственность. Пусть есть два результата: $a = b \cdot q_1 + r_1$ и $a = b \cdot q_2 + r_2$. Тогда приравняем: $b \cdot q_1 + r_1 = b \cdot q_2 + r_2 \iff b(q_1 - q_2) = r_2 - r_1 \xrightarrow{r_1, r_2 \in [0; |b|-1]} [|r_1 - r_2| < |b|] r_2 - r_1 \vdots b \Rightarrow r_2 - r_1 = 0 \iff r_1 = r_2 \Rightarrow b(q_1 - q_2) = 0 \iff q_1 = q_2$
- Существование.

I. $a \geqslant 0, b \geqslant 0$.
   - База: $a = 0$. $0 = b \cdot 0 + 0$. $(0, 0)$ – подходит.
   - Переход: $a \to a + 1$.
     $a = b \cdot q + r$, где $0 \leqslant r < b$.
     $a + 1 = b \cdot q + (r + 1)$.
     * $r < b - 1$. Тогда $r + 1 < b \Rightarrow (q, r + 1)$ — подходит.
     * $r = b - 1$. Тогда $a + 1 = b \cdot q + b = b \cdot (q + 1) \Rightarrow (q + 1, 0)$ — подходит.

II. $a < 0, b > 0$. $a < 0 \Rightarrow -a > 0$.
   Из I: $\exists (q, r) : -a = b \cdot q + r$, где $0 \leqslant r < b$. Соответственно $a = -bq - r$.
   - $r = 0$. $a = b \cdot q + 0 \Rightarrow (-q, 0)$ — подходит.
   - $r > 0 \Rightarrow r \in [1; b - 1]$. $a = -bq - b + b - r = b \cdot (-q - 1) + b - r \Rightarrow (-q - 1, b - r) - - -$

III. $b < 0 \iff -b > 0$. $\exists q, r : a = (-b) \cdot q + r$, где $0 \leqslant r < |b|$, тогда $a = b(-q) + r \Rightarrow (-q, r)$ — подходит

$\square$

Вернемся к диофантову уравнению $ax + by = c$, где a, b, c фиксированы, а x, y — переменные. Пусть только a, b — фиксированы. Тогда подумаем, когда же $ax + by = c$ имеет решения. Тогда решим задачу: описать $\{ax + by \mid x, y \in \mathbb{Z}\} =: < a, b >$

Пример. $\langle 1, b \rangle = \mathbb{Z}$

Пример. $\langle 4, 6 \rangle =$ четные числа

Заметим:

1. $\forall m, n \in \langle a, b \rangle \; m + n \in \langle a, b \rangle$

2. $m \in < a, b > \Rightarrow km \in < a, b > \forall k$

***Определение* 1.3.** Пусть $I \subset \mathbb{Z}$. I называется идеалом, если

$$\begin{cases} m, n \in I \Rightarrow m + n \in I \text{ (замкнутость по сложению)} \\ m \in I \Rightarrow \forall k \in \mathbb{Z} k \cdot m \in I \text{ (замкнутость по домножению)} \\ I \neq \varnothing \end{cases}$$

Пример. $\{0\}$ — идеал.

Пример. $\mathbb{Z}$ — идеал (собственный).

Пример. $\langle a, b \rangle$ — идеал, порожденный a и b.

$\forall a \in \mathbb{Z} \, \langle a \rangle = \{ax \mid x \in \mathbb{Z}\}$ — главный идеал (порожденный a).

Пример. $\{0\} = \langle 0 \rangle, \mathbb{Z} = \langle 1 \rangle, \langle 4, 6 \rangle = \langle 2 \rangle$

Теорема 1.2. В $\mathbb{Z}$ любой идеал главный.

Доказательство. $I = \{0\}$ — ок. Тогда пусть $I \neq \{0\}$. Пусть $a \in I \wedge a < 0 \Rightarrow -a = (-1)a \in I \wedge -a \in \mathbb{N}$. То есть $I \cap \mathbb{N} \neq \varnothing$. Найдем наименьшее $r \in I \cap \mathbb{N}$. Проверим, что $I = \langle r \rangle$ (тогда I — главный). Надо проверить $\langle r \rangle \subset I \wedge I \subset \langle r \rangle$.

- $x \in \langle r \rangle$. То есть $x = r \cdot z$. Т.к. $r \in I$, то $r \cdot z \in I$ (по определению идеала), т.е. $\langle r \rangle \subset I$.
- Пусть $a \in I$. Поделим с остатком: $a = r \cdot q + r_1$, $0 \leqslant r_1 < r$, то есть $r_1 = a - r \cdot q = a + (-q) \cdot r$. Т.к. $r \in I \Rightarrow (-q) \cdot r \in I \wedge q \in I \Rightarrow a + (-q) \cdot r \in I$, т.е. $r_1 \in I$. Но! $0 < r_1 < r$, а r — минимальное натуральное из I. Тогда $r_1 = 0 \Rightarrow a = r \cdot q$, т.е. $a \in \langle r \rangle$, а значит $I \subset \langle r \rangle$.

$\square$

***Определение* 1.4.** Пусть $a, b \in \mathbb{Z}$. Тогда d — НОД$(a, b) = \gcd(a, b) = (a, b)$

Докажем единственность. $\begin{cases} a \vdots d, b \vdots d \\ a \vdots d_1, b \vdots d_1 \end{cases} \iff d \vdots d_1$. Тогда $d \vdots d_1 \wedge d_1 \vdots d$, а значит $d = \pm d_1$.

Теорема 1.3.

1. $\forall a, b \; \exists d = (a, b)$
2. $\exists x, y \in \mathbb{Z} : \; d = ax + by$
3. $ax + by = c$ имеет решение $\iff c \vdots d$.

Доказательство. Докажем каждый пункт отдельно:

- Рассмотрим $\langle a, b \rangle$ — идеал. Он главный по предыдущей теореме: $\exists d \; \langle a, b \rangle = \langle d \rangle$.
- $d \in \langle d \rangle = \langle a, b \rangle$. А значит $\exists x, y : d = ax + by$.
  $a = a \cdot 1 + b \cdot 0 \in \langle a, b \rangle = \langle d \rangle$, значит $a \vdots d$. Аналогично $b \vdots d$.
  С другой стороны пусть $a \vdots d, b \vdots d$, тогда $d = \underbrace{ax}_{\vdots d} + \underbrace{by}_{\vdots d} \vdots d$.
- $ax + by = c$ имеет решение $\iff c \in \langle a, b \rangle = \langle d \rangle$. А $c \in \langle d \rangle \iff c \vdots d$.

$\square$

***Определение* 1.5.** a, b — взаимно просты, если $(a, b) = 1$, то есть $\langle a, b \rangle = \mathbb{Z}$

Лемма. $\begin{cases} ab \vdots c \\ (a, c) = 1 \end{cases} \Rightarrow b \vdots c$.

Доказательство. По условию $ab \vdots c$, значит $\exists x \in \mathbb{Z} : ab = c \cdot x$.

Так как $(a, c) = 1$, то $\exists y, z \in \mathbb{Z} : ay + cz = 1$. Тогда домножим все на b и получим $aby + czb = b$.

А значит $\begin{cases} aby \vdots c \\ czb \vdots c \end{cases} \Rightarrow b \vdots c$ $\square$