Алгебры

Харитонцев-Беглов Сергей

20 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. $a, b \vdots c \Rightarrow \exists d, e : \begin{array}{c} a = c \cdot l \\ b = c \cdot e \end{array}$. 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

□

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. $r \in I \Rightarrow (-q) \cdot r \in I \land q \in I \Rightarrow a + (-q) \cdot r \in I$, 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 $d \vdots d_1 \land d_1 \vdots d$, 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 $\begin{cases} aby \vdots c \\ czb \vdots c \end{cases} \Rightarrow b \vdots c$ $\square$

2. Продолжение теории чисел

2.1. Пара комментариев про предыдущую лекцию

1. Для любого набора $a_1, \ldots, a_n \in \mathbb{Z}\ \exists \gcd(a_1, \ldots, a_n)$ и $\exists x_1, \ldots, x_n :$ НОД $= x_1a_1 + \ldots + x_na_n$. НОД - такое d, что $\langle a_1, \ldots, a_n \rangle = \langle d \rangle$.
2. Алгоритм Евклида.
   - $(a, b) = (a, b - a)$, но и $b = a \cdot q + r$, тогда $(a, b) = (a, r)$.
   - Пусть $r = b \mod a$, $x_1, x_2 \in \mathbb{N}$. Сделаем последовательность $x_{n+1} = x_{n-1} \mod x_n$. Тогда $(x_1, x_2) = (x_3, x_4) = \ldots$. Заметим, что x_n — убывает.
   - Тогда существует такое x_n, что $(x_1, x_2) = (x_n, 0) = x_n$.

2.2. Основная теорема арифметики

***Определение* 2.1.** $x \in \mathbb{Z}, x \neq 1$, тогда x — простое число, если $x = x_1x_2 \iff \begin{cases} x_1 = \pm 1 \\ x_2 = \pm 1 \end{cases} \quad \forall x_1, x_2$

Свойство *. x — обладает свойством *, $\iff x \neq \pm 1 \wedge ab \vdots x \Rightarrow \left[\begin{array}{l} a \vdots x \\ b \vdots x \end{array} \right.$

Утверждение 2.1. p — простое $\iff$ p — обладает свойством *.

Доказательство.
- $\Leftarrow$ Пусть p — простое и $p = x_1x_2$. Тогда $x_1x_2 \vdots p$ по *, $\left[\begin{array}{l} x_1 \vdots p \\ x_2 \vdots p \end{array} \right.$. Пусть $x_1 = py$. $p = x_1x_2 = pyx_2$. $1 = yx_2 \Rightarrow x_2 = \pm 1$.
- $\Rightarrow$. Пусть p — простое и $ab \vdots p$. $d = (a, p)$, $d = d \cdot d_1$, p — простое $\Rightarrow d = p \vee d = 1$.

  $d = p \Rightarrow a \vdots p$. $d = 1 \wedge (a, p) = 1$, по лемме $ab \vdots p \wedge (a, p) = 1 \Rightarrow b \vdots p$.

□

Теорема 2.2 (Основная теорема арифмктики)**.** Пусть $n \in \mathbb{Z}, n \neq 0$. Тогда n единственным образом с точностью до перестановки сомножителей, представимо в виде(p_i — простые)

$$n = \epsilon p_1p_2 \ldots p_n, \epsilon \pm 1 = \operatorname{sign}(n), p_1 < p_2 < \ldots < p_n.$$

Доказательство. 1. Существование. От противного. Пусть $\exists$ нераскладываемое число. Рассмотрим минимальное такое число.
- $x = 1$ — пустое произведение. Противоречие.
- $x = p$ — произведение из 1 члена. Противоречие.
- $x = x_1x_2$. $x_1, x_2 = \pm 1 \Rightarrow x_1, x_2 < X \Rightarrow x_1, x_2$ — раскладываемые. Или $x_1 = p_1p_2 \ldots p_n, x_2 = q_1q_2 \ldots q_m \Rightarrow x = p_1p_2 \ldots p_nq_1q_2 \ldots q_m$.

2. Единственность. Пусть есть плохие числа. X — минимальное из них. $q_1q_2\dots q_n = X = p_1p_2\dots p_m$. Значит $p_1p_2\dots p_m\vdots q_1 \Rightarrow p_1\vdots q_1 \vee p_2\dots p_m\vdots q_1$. Тогда $\exists p_i\vdots q_1$. Тогда можно поделить на q_1, но p_i — простое, тогда $p_i =$. Рассмотрим $X' = \frac{X}{q_1}$. $q_2q_3\dots q_n = X' = p_1p_2\dots p_k$. $X' < X$, значит $q = p$. А значит противоречие.

$\square$

Контр-примеры для О. Т. А:

1. Рассмотрим $2\mathbb{Z}$ — множество четных чисел. Теперь 6 — простое. и все $(4k+2)$.

   Теперь как разложить на простые 60? $60 = 2\cdot 30$, а также $60 = 6 \cdot 10$.

2. $\mathbb{Z}\cup\{\sqrt{5}\} = \{a + b\sqrt{5} \mid a, b \in \mathbb{Z}\}$. Заметим, что $\mathbb{Z} \subset \mathbb{Z}\{\sqrt{5}\}$

   $4 = 2\cdot 2 = \overbrace{(\sqrt{5}-1)}^{\text{простое}}\overbrace{(\sqrt{5}+1)}^{\text{простое}}$

***Определение* 2.2.** $n \in \mathbb{Z}, n \neq 0, p$ — простое, тогда степень вхождения $(V_p(n) = k)$ p в n — $\max\{k \mid n\vdots p^k\}$

В терминах разложения: $n = p_1^{a_1}p_2^{a_2}\dots p_k^{a_k}$. $V_p(n) = a_i$, а если p нет в разложении, то $V_p(n) = 0$.

Свойства: $V_p(n)$

1. $V_p(xy) = V_p(x) + V_p(y)$
2. $V_p(x+y) = \min(V_p(x), V_p(y))$, и если $V_p(x) \neq V_p(y)$

   Доказательство. $V_p(x) = a, V_p(y) = b$ и $x = p^a\cdot\widetilde{x}, y = p^b\cdot\widetilde{y}$.

   Не умаляя общности: $a \geqslant b$. Тогда $x + y = p^a\widetilde{x} + p^b\widetilde{y} = p^b(p^{a-b}\widetilde{x} + \widetilde{y})$. Если $a > b$, то $\underbrace{p^{a-b}\widetilde{x}}_{\vdots p} + \widetilde{y}$ не делится на p. А значит $V_p(x+y) = \min(V_p(x), V_p(y))$. $\square$

Еще следствия из О. Т. А.

1. $x\vdots y \Rightarrow V_p(x) \geqslant V_p(y)\ \forall$ простого p
2. $x = p_1^{a_1}\dots p_n^{a_n}, y = p_1^{b_1}\dots p_n^{b_n} \Rightarrow (x, y) = p_1^{\min(a_1,b_2)}\dots p_n^{\min(a_n,b_n)}$
3. $x = z^k \iff \forall$ простого p $V_p(x)\vdots k$
4. Количество натуральных делителей $x = \prod x_i^{a_i}$ равно $\tau(x) = \prod(a_i + 1)$

   Доказательство. Делители X однозначно соотносятся с $\{(b_1, b_2, \dots, b_n) \mid 0 \leqslant b_i \leqslant a_i$ $\square$

5. $\sigma(x)$ — сумма натуральных делителей x. Тогда $\sigma(x) = \frac{\prod(p_i^{a_i+1}-1)}{\prod(p_i-1)}$.

   Доказательство. $\frac{\prod(p_i^{a_i+1}-1)}{\prod(p_i-1)} = \prod\frac{p_i^{a_i+1}-1}{p_i-1} = \prod(1 + p_i + \ldots + p_i^{a_i}) =$ раскроем скобки. $=$ сумма делителей. $\square$

6.

   ***Определение* 2.3.** m — НОК (LCM, $[a, b]$), если $m\vdots a, m\vdots b$ и $\forall n\ n\vdots a \wedge n\vdots b \Rightarrow n\vdots m$

   $[a, b] = \prod p_i^{\max(a_i,b_i)}$

7. $a, b \in \mathbb{Z}$ $(a, b) = 1$ $ab = c^k \Rightarrow \exists c_1, c_2$ $a = c_1^k, b = c_2^k$

3. Кольца вычета и их друзья

Рассмотрим $a^2 - b^2 = 15^{2021} \iff (a-b)(a+b) = 3^{2021} \cdot 5^{2021} \Rightarrow \begin{cases} a+b = 3^k \cdot 5^l \\ a-b = 3^{2021-k} \cdot 5^{2021-l} \end{cases} \Rightarrow$ $a = \frac{3^k \cdot 5^l + 3^{2021-k} \cdot 5^{2021-l}}{2}$.

Уравнение $81a^2 - 169b^2 = 15^{2021}$ — тоже решается. А вот $a^2 - 2b^2 = 15^{2021} \iff (a - \sqrt{2}b)(s + \sqrt{2}b) = 3^{2021}5^{2021}$ уже не решается в целых чисел. Если вылезать, то надо расписывать разложение $a + \sqrt{2}b$, "3", "5" и единственность разложения на множители.

Еще один пример: $a^2 + b^2 = 15^{2021}$. Посмотрим на остатки от деления на 4: $a^2, b^2 \mod 4 \in \{0, 1\}, 15^{2021} \mod 4 = 3$. Но для этого нам нужно понимать что-то по кольцо вычетов по модулю.

3.1. Группы

***Определение* 3.1.** Группой называется пара $(G, *)$, где G — множество, а $* : G \to G$ — бинарная операция, так что выполнены свойства:

1. $\forall a, b, c \in G : (a * b) * c = a * (b * c)$. Ассоциативность.
2. $\exists e \in G : a * e = e * a = a$. Существование нейтрального элемента.
3. $\exists a^{-1} : a * a^{-1} = a^{-1} * a = e$. Существование обратного элемента.

Несколько примеров:

1. $(\mathbb{Z}, +)$. $e = 0, a^{-1} = -a$.
2. $(\mathbb{Q} \setminus 0, \cdot)$, $e = 1, a^{-1} = \frac{1}{a}$.
3. $(2^M, \triangle)$ $e = \varnothing, A^{-1} = A$.

***Определение* 3.2.** Группа G называется абелевой, если $\forall x, y \in G : x * y = y * x$.

Пример Главный пример группы. Пусть $G = S(M) = \{f : M \to M \mid f \text{ — биекция}\}$

- Ассоциативность — упражнение.
- Нейтральный элемент — $f(x) = x$, тождественное отображение.
- f^{-1} = обратная функция. Она существует, так как f — биекция.

Получили группы по композиции.

Пример. $M = \{1, 2, 3\}$. $f_1, f_2 : M \to M$ — биекция. f_1 — меняет местами 1 и 2: $1 \to 2, 2 \to 1, 3 \to 3$, f_2 переставляет по циклу: $1 \to 2, 2 \to 3, 3 \to 1$. $f_2 \circ f_1 : 1 \to 3, 2 \to 2, 3 \to 1$. $f_1 \circ f_2 : 1 \to 1, 2 \to 3, 3 \to 2$. Ну значит группа не абелева.

Докажем простейшие свойства групп:

1. $\exists!$ нейтральный элемент.

   Доказательство: заметим, что $e_1 = e_1 * e_2 = e_2$

2. $\exists!$ обратный элемент.

   Доказательство: пусть b, c — обратные к a. Тогда $(b * a) * c = e * c = c$, но при этом $b * (a * c) = b * e = b$. Значит $b = c$.

3. $a * b = b * c \iff a = c$

   Доказательство: $a * b = a * c \iff (a^{-1} * a) * b = (a^{-1} * a) * c \iff e * b = e * c \iff b = c$

3.2. Кольца

***Определение* 3.3.** Кольцо — тройка $(R, +, \cdot)$ (R — множество, $+, \cdot : R \times R \to R$), такая что:

1–4. $(R, +)$ — абелева группа. Нейтральный элемент обозначается 0, обратный к a — $-a$.

5. $a \cdot (b + c) = a \cdot b + a \cdot c$ и $(b + c) \cdot a = b \cdot a + b \cdot c$. Дистрибутивность.

***Определение* 3.4.** Кольцо R называется ассоциативным, если выполнено

6. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

***Определение* 3.5.** Кольцо R называется коммутативным, если

6. $a \cdot b = b \cdot a$

***Определение* 3.6.** Кольцо R называется кольцом с 1, если

7. $\exists 1 \in R : 1 \cdot a = a \cdot 1 = a$

Пример. $(\mathbb{Z}, +, \cdot)$ — коммутативное ассоциативное кольцо с 1.

***Определение* 3.7.** Коммутативное ассоциативное кольцо с 1 называется полем, если выполнена

8. $\forall a \in R \ \{0\} \ \exists b \in R \ ab = 1 \wedge 1 \neq 0$

Пример. $(\mathbb{Q}, +, \cdot)$ — поле, а вот $(\mathbb{Z}, +, \cdot)$ — не поле.

3.3. Построение кольца вычетов

***Определение* 3.8.** Пусть $a, b \in \mathbb{Z}$, говорят, что a сравнимо с b по модулю n ($a \equiv b \pmod n$), если $n \mid a - b$. Эквивалентное определение: a и b имеют одинаковые остатки по модулю n.

Докажем, что сравнимость по модулю — отношение эквивалентности.

- $a \equiv a \pmod n \iff n \mid 0$
- $n|a - b \iff n|b - a \Rightarrow a \equiv b \pmod n \iff b \equiv a \pmod n$.
- Транзитивность...

Наблюдение. $a \in \mathbb{Z} \to \overline{a} = \{b \mid a \equiv b\} = \{a + kn \mid k \in \mathbb{Z}\}$. $\mathbb{Z} = \overline{0} \cup \overline{1} \dots$

***Определение* 3.9.** Фактор множества по отношению $\equiv$ обозначается $\mathbb{Z}/n\mathbb{Z}$.

$\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$.Элементы $\mathbb{Z}/n\mathbb{Z}$ называются классами вычетами по модулю.

1. $a \equiv b \pmod n \wedge c \equiv d \pmod n \iff a + c \equiv b + d \pmod n \wedge ac \equiv bd \pmod n$.

   Доказательство $(a + c) - (b + d) = \underbrace{(a - b)}_{\vdots n} - \underbrace{(b + d)}_{\vdots n} \vdots n$.

   Доказательство $ac - bd = ac - bc + bc - bd = c(a - b) + b(c - d) \vdots n$.

   Значит класс суммы и произведения зависит только от классов множителей и слагаемых.

Теорема 3.1. Пусть $n \in \mathbb{N}$. Тогда класс $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$, где $\overline{a}+\overline{b} = \overline{a + b} \wedge \overline{a}\cdot\overline{b} = \overline{a \cdot b}$ — ассоциативное коммутативное кольцо с единицей.

Доказательство. Все аксиомы — следствия из $\mathbb{Z}$. Докажем для примера $(\overline{a}+\overline{b})+\overline{c} = \overline{a}+(\overline{b}+\overline{c}) = \overline{a + b} + \overline{c} = \overline{(a + b) + c} = \overline{a + (b + c)} = \overline{a} + \overline{(b + c)} = \overline{a} + (\overline{b} + \overline{c})$. □