

Алгебры

Харитонцев-Беглов Сергей

4 октября 2021 г.

Содержание

1. Теория чисел	1
1.1 НОД, делимость, линейные диофантовы уравнения	1
2. Продолжение теории чисел	4
2.1 Пара комментариев про предыдущую лекцию	4
2.2 Основная теорема арифметики	4
3. Кольца вычета и их друзья	6
3.1 Группы	6
3.2 Кольца	7
3.3 Построение кольца вычетов	7
3.4 Квадратное уравнение	9
3.5 Китайская теорема об остатках	9

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 уравнение

$$ax + by = c.$$

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 ($a:b, b|a$), если $\exists c \in \mathbb{Z} : a = bc$.

Простые свойства:

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

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

$$4. \forall k \neq 0, k \in \mathbb{Z} : a:b \iff ak:bk.$$

$$5. a:b \iff a^2:b^2.$$

$$6. a:b \Rightarrow \begin{cases} |a| > |b| \\ a = 0 \end{cases}.$$

$$7. a:b, b:c \Rightarrow a:c.$$

$$8. a:a.$$

$$9. a:b, b:a \Rightarrow a = \pm b.$$

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

Доказательство. • Единственность. Пусть есть два результата: $a = b \cdot q_1 + r_1$ и $a = b \cdot q_2 + r_2$.

Тогда приравняем: $b \cdot q_1 + r_1 = b \cdot q_2 + r_2 \iff b(q_1 - q_2) = r_2 - r_1 \xrightarrow{r_1, r_2 \in [0; |b|-1]} [|r_1 - r_2| <$

$$|b|] r_2 - r_1 : b \Rightarrow r_2 - r_1 = 0 \iff r_1 = r_2 \Rightarrow b(q_1 - q_2) = 0 \iff q_1 = q_2$$

• Существование.

I. $a \geq 0, b \geq 0$.

– База: $a = 0$. $0 = b \cdot 0 + 0$. $(0, 0)$ – подходит.

– Переход: $a \rightarrow a + 1$.

$a = b \cdot q + r$, где $0 \leq r < b$.

$a + 1 = b \cdot q + (r + 1)$.

* $r < b - 1$. 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 $0 \leq r < b$. Соответственно $a = -bq - r$.

– $r = 0$. $a = b \cdot q + 0 \Rightarrow (-q, 0)$ – подходит.

– $r > 0 \Rightarrow r \in [1; b - 1]$. $a = -bq - b + b - r = b \cdot (-q - 1) + b - r \Rightarrow (-q - 1, b - r) \dots$

III. $b < 0 \iff -b > 0$. $\exists q, r : a = (-b) \cdot q + r$, где $0 \leq r < |b|$, 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 $\{ax + by \mid x, y \in \mathbb{Z}\} =: \langle a, b \rangle$

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

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

Заметим:

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

$$2. m \in \langle a, b \rangle \Rightarrow km \in \langle a, b \rangle \forall k$$

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

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

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 $I \cap \mathbb{N} \neq \emptyset$. 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: $a = r \cdot q + r_1$, $0 \leq r_1 < r$, 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 $I \subset \langle r \rangle$.

□

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

Докажем единственность. $\begin{cases} a:d, b:d \\ a:d_1, b:d_1 \end{cases} \iff d:d_1$. Тогда $d:d_1 \wedge d_1:d$, 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 $\iff c:d$.

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 $a:d$. Аналогично $b:d$.

С другой стороны пусть $a:d, b:d$, тогда $d = \underbrace{ax}_{:d} + \underbrace{by}_{:d} :d$.

- $ax + by = c$ имеет решение $\iff c \in \langle a, b \rangle = \langle d \rangle$. А $c \in \langle d \rangle \iff c:d$.

□

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

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

Доказательство. По условию $ab:c$, 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 $\begin{cases} aby:c \\ czb:c \end{cases} \Rightarrow b:c$

□

2. Продолжение теории чисел

2.1. Пара комментариев про предыдущую лекцию

1. Для любого набора $a_1, \dots, a_n \in \mathbb{Z}$ $\exists \gcd(a_1, \dots, a_n)$ и $\exists x_1, \dots, x_n : \text{НОД} = x_1 a_1 + \dots + x_n a_n$.
НОД - такое d , что $\langle a_1, \dots, a_n \rangle = \langle d \rangle$.
2. Алгоритм Евклида.
 - $(a, b) = (a, b - a)$, но и $b = a \cdot q + r$, тогда $(a, b) = (a, r)$.
 - Пусть $r = b \bmod a$, $x_1, x_2 \in \mathbb{N}$. Сделаем последовательность $x_{n+1} = x_{n-1} \bmod x_n$. Тогда $(x_1, x_2) = (x_3, x_4) = \dots$. 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 $x = x_1 x_2 \iff \begin{cases} x_1 = \pm 1 \\ x_2 = \pm 1 \end{cases} \quad \forall x_1, x_2$

Свойство *. x — обладает свойством *, $\iff x \neq \pm 1 \wedge ab : x \Rightarrow \begin{bmatrix} a : x \\ b : x \end{bmatrix}$

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

Доказательство. • \Leftarrow Пусть p — простое и $p = x_1 x_2$. Тогда $x_1 x_2 : p$ по *, $\begin{bmatrix} x_1 : p \\ x_2 : p \end{bmatrix}$. Пусть $x_1 = py$. $p = x_1 x_2 = pyx_2$. $1 = yx_2 \Rightarrow x_2 = \pm 1$.

• \Rightarrow . Пусть p — простое и $ab : p$. $d = (a, p)$, $d = d \cdot d_1$, p — простое $\Rightarrow d = p \vee d = 1$.

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

□

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

$$n = \epsilon p_1 p_2 \dots p_n, \epsilon = \pm 1 = \text{sign}(n), p_1 < p_2 < \dots < p_n.$$

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.
- $x = x_1 x_2$. $x_1, x_2 = \pm 1 \Rightarrow x_1, x_2 < X \Rightarrow x_1, x_2$ — раскладываемые. Или $x_1 = p_1 p_2 \dots p_n, x_2 = q_1 q_2 \dots q_m \Rightarrow x = p_1 p_2 \dots p_n q_1 q_2 \dots q_m$.

2. Единственность. Пусть есть плохие числа. X — минимальное из них. $q_1 q_2 \dots q_n = X = p_1 p_2 \dots p_m$. Значит $p_1 p_2 \dots p_m : q_1 \Rightarrow p_1 : q_1 \vee p_2 \dots p_m : q_1$. Тогда $\exists p_i : q_1$. Тогда можно поделить на q_1 , но p_i — простое, тогда $p_i =$. Рассмотрим $X' = \frac{X}{q_1}$. $q_2 q_3 \dots q_n = X' = p_1 p_2 \dots p_k$. $X' < X$, значит $q = p$. А значит противоречие.

□

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 — $\max\{k \mid n : p^k\}$

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: $V_p(n)$

- $V_p(xy) = V_p(x) + V_p(y)$
- $V_p(x + y) = \min(V_p(x), V_p(y))$, и если $V_p(x) \neq V_p(y)$

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

Не умаляя общности: $a \geq b$. Тогда $x + y = p^a \tilde{x} + p^b \tilde{y} = p^b (p^{a-b} \tilde{x} + \tilde{y})$. Если $a > b$, то $\underbrace{p^{a-b} \tilde{x} + \tilde{y}}_{:p}$

не делится на p . А значит $V_p(x + y) = \min(V_p(x), V_p(y))$.

□

Еще следствия из О. Т. А.

- $x : y \Rightarrow V_p(x) \geq V_p(y) \forall$ простого p
- $x = p_1^{a_1} \dots p_n^{a_n}, y = p_1^{b_1} \dots p_n^{b_n} \Rightarrow (x, y) = p_1^{\min(a_1, b_1)} \dots p_n^{\min(a_n, b_n)}$
- $x = z^k \iff \forall$ простого $p \ V_p(x) : k$
- Количество натуральных делителей $x = \prod x_i^{a_i}$ равно $\tau(x) = \prod (a_i + 1)$

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

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

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

- 6.

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

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

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 $a^2 - 2b^2 = 15^{2021} \iff (a - \sqrt{2}b)(a + \sqrt{2}b) = 3^{2021}5^{2021}$ 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: $a^2, b^2 \pmod 4 \in \{0, 1\}, 15^{2021} \pmod 4 = 3$. 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 $*$: $G \rightarrow G$ — 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. $(2^M, \triangle)$ $e = \emptyset, A^{-1} = A$.

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

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

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

Получили группы по композиции.

Пример. $M = \{1, 2, 3\}$. $f_1, f_2 : M \rightarrow M$ — биекция. f_1 — меняет местами 1 и 2: $1 \rightarrow 2, 2 \rightarrow 1, 3 \rightarrow 3$, f_2 переставляет по циклу: $1 \rightarrow 2, 2 \rightarrow 3, 3 \rightarrow 1$. $f_2 \circ f_1 : 1 \rightarrow 3, 2 \rightarrow 2, 3 \rightarrow 1$. $f_1 \circ f_2 : 1 \rightarrow 1, 2 \rightarrow 3, 3 \rightarrow 2$. 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, $+, \cdot : R \times R \rightarrow R$), 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. $\forall a \in R \setminus \{0\} \exists b \in R \ ab = 1 \wedge 1 \neq 0$

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.

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

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

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

$\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$. Элементы $\mathbb{Z}/n\mathbb{Z}$ называются классами вычетов по модулю.

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

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

$$\text{Доказательство } ac - bd = ac - bc + bc - bd = c(a - b) + b(c - d) : n.$$

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 $\bar{a} + \bar{b} = \overline{a + b} \wedge \bar{a} \cdot \bar{b} = \overline{a \cdot b}$ — ассоциативное коммутативное кольцо с единицей.

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

Закон сокращения не очень работает в кольце вычетов по модулю: $2 \cdot 1 = 2 \cdot 4 \pmod{6}$, но $1 \not\equiv 4 \pmod{6}$.

Определение 3.10. Пусть R — коммутативное ассоциативное кольцо с единицей. Тогда $\forall a \in R : a$ — делитель $\Rightarrow \exists b \neq 0 : ab = 0$.

Пример. n — составное $n = p_1 p_2$ в $\mathbb{Z}/n\mathbb{Z} \overline{p_1 p_2} = \bar{n} = 0$. Значит p_1, p_2 — делители числа.

Лемма. $\forall a, b, c \in R ab = ac \wedge a$ — не делитель $0 \Rightarrow b = c$.

Доказательство. $ab = ac : ab - ac = 0 \iff a(b - c) = 0$. a — не делитель $0 \Rightarrow b - c = 0 \iff b = c$. \square

Лемма. $a \in Ra$ — обратим $\Rightarrow a$ — не делитель 0 .

Доказательство. Пусть $ab = 0 \Rightarrow a^{-1}(ab) = a^{-1} \cdot 0 = (a^{-1}a)b = 0 \Rightarrow b = 0$. \square

Замечание. Обратное неверно: в \mathbb{Z} 2 — не делитель нуля, но $\frac{1}{2} \notin \mathbb{Z}$.

Теорема 3.2. $\forall a \in \mathbb{Z} : \bar{a} \in \mathbb{Z}/n\mathbb{Z}$. Тогда:

1. \bar{a} — обратим $\iff (a, n) = 1$
2. \bar{a} — делитель нуля $\iff (a, n) \neq 1$.

Доказательство. \bar{a} — обратим $\iff \exists \bar{b} : \bar{a} - \bar{b} = \bar{1} \iff \exists b : ab = 1 \pmod{n} \iff \exists b : ab - 1 : n \iff \exists b, k : ab - 1 = nk \iff \exists b, k : ab - nk = 1 \iff (a, n) = 1$.

$(a, n) = 1 \Rightarrow \bar{a}$ — обратим \Rightarrow не делитель нуля.

$(a, n) = d > 1, a = dx$. Тогда $\bar{a} \cdot \frac{\bar{n}}{d} = \bar{d}x\frac{\bar{n}}{d} = \bar{n}x = 0$ и $\frac{\bar{n}}{d} \neq 0$. Значит $9 < |\frac{n}{d}| < n$. \square

Следствие. n — простое $\Rightarrow \mathbb{Z}/n\mathbb{Z}$ — поле.

Доказательство. Достаточно проверить существование обратного. $\bar{a} \neq \bar{0} \iff a \not: n \iff (a, n) = 1 \iff a$ — обратим. \square

Определение 3.11. \forall ассоциативного кольца с 1 R : R — называется кольцом без делителей 0 (область целостности), если делитель 0 только 0. $ab = 0 \iff a = 0 \vee b = 0$.

Замечание. R — область $\Rightarrow ax_1 = ax_2 \Rightarrow x_1 = x_2$ ($a \neq 0$).

Вернемся к диофантову уравнению $ax + by = 1, (a, b) = 1$. Тогда $ax = c \pmod{b}$ и $by = c \pmod{a}$. Тогда $\bar{a}x = \bar{c}$ в $\mathbb{Z}/n\mathbb{Z} \xrightarrow{(a,b)=1} \bar{x} = \bar{a}^{-1}\bar{c} \pmod{b}$. Тогда $x = x_0 + kb$.

3.4. Квадратное уравнение

Посмотрим на $x^2 + px + q = 0$ в $\mathbb{Z}/n\mathbb{Z}$. Работает ли $x_{1,2} = \frac{-p \pm \sqrt{p^2 - 4q}}{2}$. Есть проблемки:

1. $p^2 - 4q$ — не квадрат в $\mathbb{Z}/n\mathbb{Z}$ (не решений).
2. $2 = 0$. Или $\nexists 2^{-1}$ (нельзя поделить на два).
3. n — не простое. Тогда $(x - x_1)(x - x_2) \dots = 0$. Тогда не следует, что $x = x_1 \vee x = x_2$. Пример: $x^2 - 1 = 0 \pmod{8}$

3.5. Китайская теорема об остатках

Чтобы решать такие уравнения можно свести к простым модулям при помощи китайской теоремы об остатках.

Вопрос такой: как связаны $\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/mn\mathbb{Z}$. Пусть $P_m : \mathbb{Z} \mapsto \mathbb{Z}/m\mathbb{Z}$, а $P_m n\mathbb{Z} \mapsto \mathbb{Z}/mn\mathbb{Z}$.

Определение 3.12. Гомоморфизмом колец $f : R_1 \mapsto R_2$ называется такое отображение, что $\forall r_1, r_2 \in R_1 : f(r_1 + r_2) = f(r_1) + f(r_2), f(r_1 r_2) = f(r_1) \cdot f(r_2), f(1) = 1$.

Определение 3.13. Гомоморфизмом группы $f : G_1 \mapsto G_2$ называется такое отображение, что $\forall g_1, g_2 : f(g_1 g_2) = f(g_1) \cdot f(g_2)$.

Замечание. f — гомоморфизм групп $G_1, G_2 \Rightarrow f(e_{G_1}) = e_{G_2}$. В частности f — гомоморфизм колец $R_1, R_2 \Rightarrow f(0_{R_1}) = 0_{R_2}$.

Доказательство. $f(e_{G_1}) = f(e_{G_1} \cdot e_{G_1}) = f(e_{G_1}) \cdot f(e_{G_1})$. Дальше сокращаем. □

Существует $P_{mn,m} : P_{mn,m} \cdot P_{mn} = P_m$.

Доказательство. $P_{mn,m}(\overline{a_{mn}}) = \overline{a_m}$. □

Корректность. $\overline{a_m} = \overline{b_m} \iff a \equiv b \pmod{mn} \iff a - b : mn \Rightarrow a - b : m \Rightarrow \overline{a_m} = \overline{b_m}$ □

Аналогично существует гомоморфизм $P_{mn,n}$. То есть $\overline{a_{mn}} \mapsto (\overline{a_m}, \overline{a_n})$ — отображение. То есть $\mathbb{Z}/mn\mathbb{Z} \mapsto \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Отступление.

Определение 3.14. R_1, R_2 — кольца. Рассмотрим $(R_1 \times R_2, +, \cdot) : (r_1, r_2) +_{R_1 \times R_2} (r'_1, r'_2) := (r_1 +_{R_1} r'_1, r_2 +_{R_2} r'_2)$. То же самое для умножения. Тогда $R_1 \times R_2$ — тоже кольцо.

Итак мы построили гомоморфизм $\mathbb{Z}/mn\mathbb{Z} \mapsto \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Подумаем про его свойства. Во-первых заметим, что слева mn элементов, но и справа mn элементов!

Определение 3.15. Биективный гомоморфизм (групп, колец, ...) (называется изоморфизмом, \cong) если каждому a_i задано ровно одно b_j и наоборот.

Теорема 3.3 (Китайская теорема об остатках). Пусть $(m, n) = 1$, тогда $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

Доказательство.

1. $i_{m,n}$ — инъективно. Пусть $i_{m,n}(\overline{a_{m,n}}) = (\overline{a_m}, \overline{a_n}), i_{m,n}(\overline{b_{n,m}}) = (\overline{b_m}, \overline{b_n}) \Rightarrow a - b : m \wedge a - b : n \xrightarrow{(m,n)=1} a - b : mn$.

2. $i_{m,n} : a \mapsto B$ инъективно: $|A| = |B| \Rightarrow i_{m,n}$ — сюръективно.

□

Теорема 3.4 (КТО 2). $m_1, m_2, m_3, \dots, m_n \in \mathbb{Z} \wedge (m_i, m_j) = 1 \Rightarrow \mathbb{Z}/m_1, m_2, \dots, m_n \mathbb{Z} \mapsto \mathbb{Z}/m_1 \mathbb{Z} \times \mathbb{Z}/m_2 \mathbb{Z} \dots$ — изоморфизм колец.

Теорема 3.5 (КТО без колец). $\forall m_1, \dots, m_n \in \mathbb{Z}, \forall a_1, \dots, a_n (m_i, m_j) = 1 \Rightarrow \exists x_0 \in \mathbb{Z} x \equiv a_1 \pmod{m_1} \wedge \dots \wedge x \equiv a_n \pmod{m_n} \iff x \equiv x_0 \pmod{\prod_i m_i}$

То есть по факту мы хотим получить обратную функцию к $f_{m_1, m_2, \dots} : \overline{a_{m_1 m_2 m_3}} \mapsto (\overline{a_{m_1}}, \overline{a_{m_2}}, \overline{a_{m_3}})$. Пусть тогда $g = f^{-1}$. Заметим, что g — гомоморфизм колец. Раз g сохраняет операции, то $g(\overline{x}, \overline{y}, \overline{z}) = g(\overline{x}, 0, 0) + g(0, \overline{y}, 0) + g(0, 0, \overline{z}) = \overline{x}g(1, 0, 0) + \overline{y}g(0, 1, 0) + \overline{z}g(0, 0, 1)$.

$$\text{Пусть } x = g(1, 0, 0) \iff \begin{cases} x \equiv 1 \pmod{m_1} \\ x \equiv 0 \pmod{m_2} \\ x \equiv 0 \pmod{m_3} \end{cases} \iff \begin{cases} x \equiv 1 \pmod{m_1} \\ x \equiv 0 \pmod{m_1 m_2} \end{cases}.$$

В группе $\forall a \neq e \forall x : ax \neq x$. Тогда посмотрим группу $(\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}) \supset \{(a, 0) \mid a \in \mathbb{Z}/m\mathbb{Z}\} \cong \mathbb{Z}/m\mathbb{Z}$.

Тогда для любого $n \in \mathbb{N} : n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n} \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{\alpha_1} \mathbb{Z} \times \dots \times \mathbb{Z}/p_n^{\alpha_n} \mathbb{Z}$.

Пример. Для того, чтобы решить $b^2 = a$ надо решить $b_i^2 = a$ для все составляющих.

Определение 3.16. Пусть C — группа ($a \in C$), тогда порядок элемента a : $\text{ord}(a) = \{\min k \in \mathbb{N} \mid a^k = 1\}$. А если такого k нет, то $\text{ord}(a) = \infty$

Лемма. Пусть G — группа ($a \in G$). $\langle a \rangle = \{a, a^2, \dots; a^{-1}, (a^{-1})^2, \dots, e\} = \{a^k \mid k \in \mathbb{Z}\}$. Тогда $(\langle a \rangle, *)$ — группа.

Доказательство. Проверим замкнутость относительно операций: 0-рной ($\{\} \rightarrow e$), унарной $a \rightarrow a^{-1}$, бинарной $(a, b) \rightarrow a * b$.

- $e = a^0 \in \langle a \rangle$
- $b \in \langle a \rangle. b = a^k \Rightarrow b^{-1} = a^{-k} \in \langle a \rangle$.
- $b, c \in \langle a \rangle. b = a^k, c = a^l \Rightarrow bc = a^{k+l} \in \langle a \rangle$.

□

Определение 3.17. $\langle a \rangle$ называется циклической группой, порожденной a . G — циклическая группа $\iff \exists a \in G G \cong \langle a \rangle$

Теорема 3.6. $\text{ord } a = \infty \Rightarrow \langle a \rangle \cong (\mathbb{Z}, +)$. $\text{ord } a = k \in \mathbb{N} \Rightarrow \langle a \rangle \cong (\mathbb{Z}/k\mathbb{Z}, +)$

Доказательство. $f : (\mathbb{Z}, +) \rightarrow \langle a \rangle$. То есть $k \mapsto a^k$. $f(k+l) = a^{k+l} = a^k \cdot a^l = f(k) + f(l)$. Тогда f — сюръекция по определению циклической группы.

Докажем инъективность. Пусть $a^k = a^l \iff a^{k-l} \cdot a^l = ea^l \iff a^{k-l} = e$. Но $\text{ord } a = \infty!$ Значит $k-l=0$.

Теперь $\text{ord } a \neq \infty$. Тогда построим $f : \mathbb{Z}/k\mathbb{Z} \rightarrow \langle a \rangle$, то есть $\overline{m_k} \mapsto a^m$.

Корректность: $\overline{m_k} = \overline{n_k} \Rightarrow (m-n):k$. То есть $m = n + k \cdot l$. Значит $a^m = a^{n+k \cdot l} \iff a^m = a^n \cdot a^{kl} = a^m$.

Сюръективность/инъективность: смотри выше. Или ниже, ну тут бан короче.

□

Простыми словами, если $\text{ord } a = \infty \Rightarrow$ в последовательности $\{a^i\}$ - элементы не повторяются. А если $\text{ord } a \neq \infty$, то элементы повторяются с периодом k , а внутри элементы не повторяются.

Теорема 3.7 (Теорема Лангранжа). Пусть G — группа. $\forall G$ — n -элементная группа, тогда $\forall a \in G : n \mid \text{ord } a$

Доказательство. Пусть $\text{ord } a = k$. Рассмотрим отображение $m_a(x) = ax$. $m_a G \rightarrow G$. Нарисуем граф отображений (вершины — элементы G , ребра (стрелки) — $x \rightarrow a_x$). $x \rightarrow ax \rightarrow a^2x \rightarrow a^3x \rightarrow \dots \rightarrow a^kx \rightarrow x$, так как для $\forall i, j \leq k : a^i x = a^j x \Rightarrow a^i = a^j$.

Значит все элементы G разбиваются на циклы длины k . Следовательно $n \mid k$. \square

Следствие. G — конечная группа ($a \in G$) $\Rightarrow a^{|G|} = e$

Доказательство. $\text{ord } a = k$. $n = k \cdot l$ по теореме Лагранжа. Тогда $a^n = a^{k \cdot l} = (a^k)^l = e^l = e$ \square

Пример. $(\mathbb{Z}/p\mathbb{Z}, +)$. $\bar{a}^x = \underbrace{\bar{a} + \bar{a} + \bar{a} + \bar{a}}_{x \text{ раз}} = \overline{xa}$.

Пример. p — простое.

$G := (\mathbb{Z}/p\mathbb{Z} \setminus \{0\}, \cdot)$. $|G| = p - 1$. Тогда $a^{p-1} = 1$. Малая теорема Ферма.

На языке сравнений: $a \in \mathbb{Z}, a \not\equiv 0 \pmod p \Rightarrow a^{p-1} \equiv 1 \pmod p \iff a^{p-1} \equiv 1 \pmod p$.

Пример. $(\mathbb{Z}/p\mathbb{Z}, +)$ — циклическая группа. А вот с G из предыдущего пункта — тоже, если p — простое. Но не очев.

Утверждение 3.8. G — группа ($|G| = n$). G — циклическая $\iff \exists a \in G : \text{ord } a = n$. МТФ: $\bar{a}, \bar{a}^2, \dots$ — периодична с периодом $p - 1$. Утверждение: $\exists \bar{a} : p - 1$ — наименьший период этой последовательности.

Определение 3.18. R — кольцо, тогда $R^* = \{a \in R \mid \exists a^{-1}\}$ — группа обратимых элементов.

Замечание. $a^n = 1 \Rightarrow a \in R^*$. Т.к. тут записано, что $a \cdot a^{n-1} = 1$ — то есть он обратим.

R — конечное кольцо. $a \in R^* \Rightarrow a^{|R^*|} = 1$. Следствие из теоремы Лагранжа. Посчитаем $|R^*|$. Это $\varphi(n)$ — функция Эйлера.

Замечание. Пусть G — группа, $|G| = p$ — простое. Тогда $G \cong (\mathbb{Z}/p\mathbb{Z}, +)$. G — циклическая.

Доказательство. Возьмем $a \neq e$. Тогда $p \mid \text{ord } a \Rightarrow \text{ord}(a) = 1 \vee \text{ord}(a) = p \Rightarrow a = e \vee \langle a \rangle = G \Rightarrow G$ — циклическая $\Rightarrow G \cong (\mathbb{Z}/p\mathbb{Z}, +)$. \square