Алгебра и теория чисел

Курс Жукова И. Б.

Осень 2021 г.

Примечание

Конспекты написаны полностью, но (скорее всего) с большим числом опечаток!

Оглавление

Часть I

Алгебраические структуры

ГЛАВА 1

Множества

1.1. Нотация

Стандартная запись:

$$A' = \{1, 3, 5, 7\}$$
$$A = \{1, 3, 5, ..., 99\}$$

Общий вид:

$$B = \{2, 4, 6, ...\} = \{2n : n \in \mathbb{N}\}$$

Стандартные числовые множества:

$$\mathbb{N} = \{1, 2, 3, ...\} \qquad \mathbb{Z} = \{..., -1, 0, 1, 2, ...\}$$
$$\mathbb{Q} = \left\{\frac{p}{q} : p, q \in \mathbb{Z}, q \neq 0\right\} \qquad \mathbb{R}, \mathbb{C}$$

Подмножества:

$$A' \subset A \subset \mathbb{N}, A' \not\subset B$$
$$C = \{1, 2, 3\} \quad \varnothing, \{1\}, \{2\}, \{3\}$$
$$\{1, 2\}, \{1, 3\}, \{2, 3\}$$
$$\{1, 2, 3\} = C$$

Предикат для подмножеств: $\{n \in \mathbb{N} : n < 5\} = \{1, 2, 3, 4\}$

1.2. Операции на множествах

Пусть A, B — множества

$$A \cap B = \{a \in A \wedge a \in B\}$$
$$A \cup B = \{a : a \in A \vee a \in B\}$$
$$A \setminus B = \{a \in A \wedge a \notin B\}$$
$$A \triangle B = (A \setminus B) \cup (B \setminus A)$$
$$A \times B = \{(a, b) : a \in A, b \in B\}$$
$$\bigcap_{i=1}^{n} A_i \quad \bigcup_{i=1}^{n} A_i$$
$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$
$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

Пример.

$$A = \{1, 2, 3\} \quad B = \{-1, 1\}$$
$$A \times B = \{(1, -1), (1, 1), (2, -1), (2, 1), (3, -1), (3, 1)\}$$

1.3. Отображение

A, B — множества

Определение 1.1. Задать отображение A в B, значит для каждого $a \in A$ задать некоторый элемент B (т.н. образ элемента A)

$$A = \{1, 2, 3, 4\}$$
$$B = \mathbb{R}$$

a	$f(a)$
1	$\sqrt{2}$
2	0
3	7^5
4	0

$$f : \mathbb{R} \to \mathbb{R}$$
$$f(a) = a - 3$$
$$\Leftrightarrow$$
$$f : \mathbb{R} \to \mathbb{R}$$
$$a \mapsto a - 3$$

a	$f(a)$
1	-2
2	-1
3	0
4	1

$$f : \mathbb{R} \to \mathbb{Z}$$
$$a \mapsto \begin{cases} 1, & a > 0 \\ 0, & a = 0 \\ -1, & a < 0 \end{cases}$$
$$\varphi : \mathbb{N} \to \mathbb{N}$$
$$n \mapsto |\{m \in \mathbb{N} : m \leqslant n \,\&\, (m, n) = 1\}|$$

Определение 1.2. $|M| = \#M = \text{Card } M$ — мощность множества

Определение 1.3. 2^M — множество всех подмножеств M, его мощность $|2^M| = 2^{|M|}$

Свойства

Свойство 1.1. $f : A \to B$ называется инъекцией, если

$$\forall a_1, a_2 \in A : a_1 \neq a_2 \implies f(a_1) \neq f(a_2)$$

Свойство 1.2. $f : A \to B$ называется сюръекцией, если

$$\forall b \in B, \exists a \in A : f(a) = b$$

Свойство 1.3. $f : A \to B$ называется биекцией, если оно одновременно инъекция и сюръекция

Определение 1.4. Пусть $f : A \to B$, тогда $b \in B$ – полный прообраз b относительно f, если

$$f^{-1}(b) = \{a \in A : f(a) = b\}$$

Следствие 1.1.

- f – *инъекция* $\Leftrightarrow \forall b \in B : |f^{-1}(b)| \leqslant 1$
- f – *сюръекция* $\Leftrightarrow \forall b \in B : |f^{-1}(b)| \geqslant 1$
- f – *биекция* $\Leftrightarrow \forall b \in B : |f^{-1}(b)| = 1$

Определение 1.5 (Сужение отображения)**.** Пусть $f : A \to B$ и $A' \subset A$, тогда

$$f|_{A'} : A' \to B$$
$$a \mapsto f(a)$$

Определение 1.6 (Образ подмножества)**.** Пусть $f : A \to B$ и $M \subset A$, тогда

$$f(M) = \{f(m) : m \in M\}$$
$$f(A) = \operatorname{Im} A$$

1.4. Композиция

Определение 1.7. Пусть $f : A \to B$ и $g : B \to C$, тогда

$$g \circ f : A \to C$$
$$a \mapsto g(f(a))$$

— композиция f и g

Пример.

$$f, g : \mathbb{R} \to \mathbb{R}$$
$$f(x) = x + 1$$
$$g(x) = 2x$$
$$g \circ f : \mathbb{R} \to \mathbb{R} \qquad f \circ g : \mathbb{R} \to \mathbb{R}$$
$$x \mapsto 2x + 2 \qquad x \mapsto 2x + 1$$

1.5. Тождественное отображение

Определение 1.8 (Тождественное отображение)**.** Пусть M – множество

$$\mathrm{id}_M : M \to M$$
$$m \mapsto m$$

Определение 1.9 (Обратное отображение)**.** Пусть $f : X \to Y$, тогда отображение $g : Y \to X$ называется обратным, если $g \circ f = \mathrm{id}_X, f \circ g = \mathrm{id}_Y$

Теорема 1.1. *У $f : X \to Y$ есть обратное $\Leftrightarrow$ f – биекция*

Доказательство. Прямое доказательство: Зададим обратное отображение $g : Y \to X$, так что $g \circ f = \mathrm{id}_X$ и $f \circ g = \mathrm{id}_Y$. Тогда $\forall y \in Y$ верно

следующее:

$$g(y) = x \qquad f^{-1}(y) = \{x\}$$
$$(g \circ f)(x) = g(f(x)) = x$$
$$(f \circ g)(y) = f(g(y)) = y$$

Обратное доказательство: Если $g \circ f = \mathrm{id}_X$ верно, то и f – инъекция

$$f(x_1) = f(x_2) \implies g(f(x_1)) = g(f(x_2)) \implies x_1 = x_2$$

Если $f \circ g = \mathrm{id}_Y$ верно, то и f – сюръекция

$$y \in Y \implies \exists x \in X : f(x) = y \implies f(g(y)) = y$$

■

ГЛАВА 2

Группы

2.1. Введение

Определение 2.1. Бинарная операция на множестве M – отображение из $M \times M \to M$

Примеры

1. $+, -, \cdot$ на $\mathbb{Z}$
2. $+$ на векторном пространстве
3. $M = X^X = \{f : X \to X\}$
   $(f, g) \mapsto f \circ g$
   $M \times M \mapsto M$

Свойства

Есть операция $M \times M \to M$, обозначим ее $(a, b) \mapsto a * b$

1. Если $\forall a, b \in M : a * b = b * a$, то $*$ коммутативна
2. $*$ ассоциативна, если $\forall a, b, c \in M : (a * b) * c = a * (b * c)$
3. $e \in M$ называется левым нейтральным, если $\forall a \in M : e * a = a$
   $e \in M$ называется правым[1] нейтральным, если $\forall a \in M : a * e = a$
   $e \in M$ называется нейтральным, если он и левый, и правый нейтральный

[1] В вычитании целых чисел ноль нейтрален справа

Лемма 2.1. *Пусть $*$ – операция, e_L, e_R – нейтральные слева и справа относительно $*$, тогда $e_L = e_R$.*

Доказательство.

$$e_R = e_L * e_R = e_L$$

■

4. Пусть e нейтральный относительно $*$, $a \in M$. Элемент $b \in M$ называется обратным к a[2], если $b * a = a * b = e$
Если $b * a = e \implies b$ обратный слева
Если $a * b = e \implies b$ обратный справа

Лемма 2.2. *Если $*$ ассоциативна и у a если левый и правый обратный, тогда они равны. $b * a = e, a * c = e$*

Доказательство.

$$(b * a) * c = b * (c * a)$$
$$e * c = b * e$$
$$c = b$$

■

Если $*$ – ассоциативная операция, $m \in \mathbb{Z}$:

$$a^m = \begin{cases} a_1 * a_2 * ... * a_m & m > 0 \\ e & m = 0 \\ a_1^{-1} * a_2^{-1} * ... * a_{-m}^{-1} & m < 0 \end{cases}$$

$$a^m * a^n = a^{m+n} \qquad (a^m)^n = a^{mn}$$

2.2. Определение группы

Определение 2.2. Группой называется множества G с операцией $*$, такие что:

1. $*$ ассоциативна
2. У $*$ есть нейтральный элемент
3. У любого $g \in G$ есть обратный

Группа G называется абелевой (коммутативной), если $*$ коммутативна

[2]Обратное к a обозначается a^{-1}

Примеры

1. $(\mathbb{Z}, +)$
2. $(\mathbb{Q}, +), (\mathbb{R}, +)$
3. $(\mathbb{Q} \setminus \{0\}, \cdot), (\mathbb{R} \setminus \{0\}, \cdot)$
4. $(\{1, -1\}, \cdot)$[3]
5. $(X^X, \cdot)$ – не группа, при $|X| > 1$
6. $(S(X), \cdot)$, что $S(x) = \{f : x \to x : x$ - биекция$\}$ – группа, не абелева при $|X| = 2$

2.3. Подгруппы

Пример. $(\mathbb{Z}, +)$ – группа, $2\mathbb{Z} = \{2n : n \in \mathbb{Z}\}$ – подгруппа

Определение 2.3. G – группа, $H \subset G$ называется подгруппой, если:

1. H замкнуто относительно умножения, т.е. $\forall h_1, h_2 \in H : h_1 h_2 \in H$
2. $e \in H$
3. H замкнуто относительно обратного, т.е. $\forall h \in H : h^{-1} \in H$

Примеры

- $2\mathbb{Z} < \mathbb{Z}$[4]
- $\{0\} < \mathbb{Z}$
- $\mathbb{Z} \in \mathbb{Q}$
- $(\{-1, 1\}, \cdot) < \mathbb{Q}^*$
- $\{2^n : n \in \mathbb{Z}\} < \mathbb{Q}^*$
- Группы самосовмещений (симметрий) фигур, Π - плоскость, $S(\Pi)$, $T(\Pi) < S(\Pi)$ – перемещения плоскости (движения)

[3] 1–4 абелевы группы

[4] В данном контексте $\subset$ и $<$ означают одно и то же

Законы сокращения

Лемма 2.3. *Пусть G - группа, $g, h_1, h_2 \in G$*

1. $gh_1 = gh_2 \implies h_1 = h_2$
2. $h_1 g = h_2 g \implies h_1 = h_2$

Доказательство.

$$g^{-1}gh_1 = g^{-1}gh_2 \implies h_1 = h_2$$

■

2.4. Таблицы Кэли

Дана группа $G = \{g_1, g_2, \dots g_n\}$:

	g_1	g_2	$\cdots$	g_n
g_1	g_1g_1	g_1g_2	$\cdots$	g_1g_n
g_2	g_2g_1	g_2g_2	$\cdots$	g_2g_n
$\vdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
g_n	$\cdots$	$\cdots$	$\cdots$	$\cdots$

Дана группа $\mathbb{Z}^* = (\{\pm 1\}, \cdot)$:

	1	-1
1	1	-1
-1	-1	1

Дана группа самосовмещений правильного прямоугольника[5]:

$\square$	e	S_1	S_2	R_π
e	e	S_1	S_2	R_π
S_1	S_1	e	R_π	S_2
S_2	S_2	R_π	e	S_1
R_π	R_π	S_2	S_1	e

Группа абелева, т.к. симметрична относительно диагонали

Рассмотрим $\mathbb{Z}^* \times \mathbb{Z}^* = \{(1,1), (1,-1), (-1,1), (-1,-1)\}$. Операции будем производить покомпонентно: $(a,b)(a',b') = (aa', bb')$.

[5]Таблица Кэли является латинским квадратом

	e	$(1,-1)$	$(-1,1)$	$(-1,-1)$
e	e	$(1,-1)$	$(-1,1)$	$(-1,-1)$
$(1,-1)$	$(1,-1)$	e	$(-1,-1)$	$(-1,1)$
$(-1,1)$	$(-1,1)$	$(-1,-1)$	e	$(1,-1)$
$(-1,-1)$	$(-1,-1)$	$(-1,1)$	$(1,-1)$	e

Последние 2 группы изоморфны (если заменить все элементы, например, буквами, то они и их таблицы Кэли будут идентичны)

Теория групп изучает группы с точностью до изомфорфизма

Аксиома 2.1. Любые группы третьего порядка изоморфны.

С группами порядка 4 это уже не выполняется

ГЛАВА 3

Отношения на множестве

Определение 3.1. Отношения на множестве M – это подмножество в $M \times M$

Пример. $\leqslant$ на $\{1, 2, 3\}$ – $\{(1, 1), (1, 2), (1, 3), (2, 2), (2, 3), (3, 3)\}$

Определение 3.2. R на M называется рефлексивным, если

$$\forall m \in M : (m, m) \in R$$

Определение 3.3. R на M называется симметричным, если

$$\forall m, n \in M : (m, n) \in R \implies (n, m) \in R$$

Определение 3.4. R на M называется антисимметричным, если

$$\forall m, n \in M : (m, n) \in R, (n, m) \in R \implies m = n$$

Определение 3.5. R на M называется транзитивным, если

$$\forall a, b \in M : (a, b) \in R, (b, c) \in R \implies (a, c) \in R$$

Определение 3.6. R называется отношением эквивалентности, если оно рефлексивно, симметрично и транзитивно.

Определение 3.7 (Класс эквивалентности)**.** Пусть R – отношения эквивалентности на M, $a \in M$. Класс $[a] = \{b \in M : bRa\}$[1]

[1]Будем использовать запись $(a, b) \in R = aRb$

Лемма 3.1.

$$\forall m, n \in M : [m] = [n] \text{ или } [m] \cap [n] = \varnothing$$

Доказательство.

$$[m] \cap [n] \neq \varnothing$$
$$\exists l \in [m] \cap [n] \implies lRm, lRn \implies mRl \implies mRn$$
$$a \in [m] \implies aRm \implies aRn \implies a \in [n]$$
Таким образом $[m] \subset [n]$. Аналогично $[n] \subset [m] \implies [m] = [n]$

■

Теорема 3.1. *Пусть R отношение эквивалентности на множестве M, тогда $M = \bigcup_{i \in I} C_i$, т.ч. $C_i \cap C_j = \varnothing (i \neq j)$ и $mRn \Leftrightarrow m, n \in C_i$ для некоторого i.*

Доказательство.

$$C_i\text{– всевозможные } [m] \in R$$
$$M = \bigcup_{m \in M} [m] \text{ т.к. } m \in [m]$$
$$a, b \in [m] \implies \begin{cases} aRm \\ bRm \end{cases} \implies aRb$$
$$\left.\begin{array}{l} a \in [m] \\ b \in [n] \\ aRb \end{array}\right\} \implies [m] = [n]$$
$$\left.\begin{array}{l} bRn \\ aRb \end{array}\right\} \implies aRn \implies a \in [m] \cap [n] \implies [m] \cap [n] \neq \varnothing \implies [m] = [n]$$

■

Определение 3.8. Если $\sim$ – отношение эквивалентности на M, то множество классов эквивалентности: $M/\sim$ – фактормножество M относительно $\sim$

Часть II

Основы теории чисел

ГЛАВА 4

Делимость

$a \mid b$ или $b \vdots a$ читается как a делит b или b делится на a, если $\exists q \in \mathbb{Z} : b = aq$

Пример. Делители $4 : -4, -2, -1, 1, 2, 4$
Делители 0: все элементы $\mathbb{Z}$

4.1. Свойства

1. Рефлексивность
2. $\left.\begin{matrix} a \mid b \\ b \mid a \end{matrix}\right\} \implies a = \pm b$
3. Транзитивность
4. $a \mid b \implies \forall c \in Z : a \mid bc$
5. $a \mid b, a \mid c \implies a \mid (b \pm c)$
6. $a \mid b \implies \forall k \in \mathbb{Z} : ka \mid kb \qquad b = aq \implies kb = kaq \implies ka \mid kb$
7. $ka \mid kb, k \neq 0 \implies a \mid b \qquad kb = kaq \Leftrightarrow k(b - aq) = 0 \implies b - aq = 0 \implies b = aq$

Теорема 4.1 (О делении с остатком)**.** $\forall a \in \mathbb{Z} \forall b \in \mathbb{N} \exists! q, r \in \mathbb{Z}$

1. $a = bq + r$

2. $0 \leqslant r < b$

Доказательство. Выберем q, т.ч. $a - bq \geqslant 0$ наименьшая возможная разность

$$r = a - bq$$
$$r = a - bq \implies a = bq + r$$
$$r \geqslant 0, \text{ предположим, что } r \geqslant b$$
$$a - bq - b = r - b \geqslant 0 \implies a - b(q+1) < a - bq$$
$$\text{противоречие с выбором } q$$

Пусть $a = bq_1 + r_1 = bq_2 + r_2$

$$0 \leqslant r_1, r_2 < b$$
$$b(q_1 - q_2) = r_2 - r_1$$
$$-(b-1) \leqslant r_2 - r_1 \leqslant b - 1$$
$$b \mid b(q_1 - q_2) \implies q_1 - q_2 = 0 \implies r_2 - r_1 = 0$$

■

ГЛАВА 5

Простые числа

Определение 5.1. $p \in \mathbb{Z}$ называется простым, если $p \neq 0, \pm 1$ и $\{a : a \mid p\} = \{\pm 1, \pm p\}$. Простые числа могут быть отрицательными.

$$\mathbb{Z} = \{0, \pm 1\} \cup \{\text{простые}\} \cup \{\text{составные}\}$$

Утверждение 5.1. *Пусть $a > 1$, тогда наименьший натуральный делитель a, отличный от 1 – простое число.*

Доказательство. p – наименьший натуральный делитель n. Если p составное, то $\exists q : 1 < q < p, q \mid p$

$$\left.\begin{matrix} q \mid p \\ p \mid n \end{matrix}\right\} \implies q \mid n, q < p \qquad ※$$

■

Следствие 5.1. *Любое целое число, кроме ± 1 делится на простое*

Следствие 5.2. *Наименьший натуральный делитель, $\neq 1$, составного числа n не больше $\sqrt{n}$.*

Доказательство. [1] p – наименьший натуральный делитель n, $p \neq 1$, тогда

$$n = pb$$

[1] Здесь и далее ※ означает противоречие

Предположим, что $p > \sqrt{n}$, n – составное $\implies b \neq 1 \implies b \geqslant p > \sqrt{n}$

$$n = pb > \sqrt{n}\sqrt{n} = n \qquad ※$$

■

Теорема 5.1 (Евклида)**.** *Простых бесконечно много.*

Доказательство. Пусть это не так, $p_1, p_2, ..., p_k$ – все положительные простые.

$$n = p_1 p_2 ... p_k + 1$$

$$n > 1 \implies \text{составное} \implies \exists \text{ простое } p \mid n, p > 0$$

$$\implies p \in \{p_1, ..., p_k\} \implies p \mid (n-1)$$

$$\left.\begin{array}{l} p \mid n \\ p \mid (n-1) \end{array}\right\} \implies p \mid 1 \implies p = \pm 1 \qquad ※$$

■

ГЛАВА 6

Наибольший общий делитель

Определение 6.1. $a_1, ..., a_n \in \mathbb{Z}$ не все 0, $d \geqslant 0$ называется наибольшим общим делителем $a_1, ..., a_n$ если:

1. $d \mid a_1, ..., d \mid a_n$
2. $\forall d' \geqslant 0 : d' \mid a_1, ..., d' \mid a_n \implies d' \mid d$

Предложение 6.1. *НОД существует и единственный*

Доказательство.

$$I = \{a_1c_1 + ... + a_nc_n : c_1, ..., c_n \in \mathbb{Z}\}$$

d – наименьший положительный элемент I

$$c_i \neq 0 \implies c_i \cdot 1 > 0 \text{ или } c_i \cdot (-1) > 0$$

Доказать: d – НОД $a_1, ..., a_n$

Предположим, что $d \nmid a_j$

$$a_j = dq + r, 0 < r < d$$
$$r = a_j - dq = a_j - (a_1c_1 + ... + a_nc_n)q =$$
$$= a_1(-c_1)q + ... + a_j(1 - c_1q) + a_n(-c_nq) \in I \qquad ※$$

Пусть $d' \mid a_1, ..., d' \mid a_n \implies d' \mid a_1c_1, ..., d' \mid a_nc_n \implies d' \mid (a_1c_1 + ... + a_nc_n) \implies d' \mid d$

Единственность. Пусть d_1, d_2 – НОД $a_1, ..., a_n \implies d_2 \mid d_1$, аналогично $d_1 \mid d_2 \implies d_1 = d_2$ ■

6.1. Свойства

Обозначения: НОД$(a_1, ..., a_n)$ или $\gcd(a_1, ..., a_n)$ или $(a_1, ..., a_n)$

1. $b \mid a \implies (a, b) = b$
2. $a = bl + a' \implies (a, b) = (a', b)$

   Доказательство.

   $$\{\text{делители } a \text{ и } b\} = \{\text{делители } a' \text{ и } b\}$$

   Включение левого множества в правое:

   $$\left.\begin{matrix} d \mid a \\ d \mid b \end{matrix}\right\} \implies d \mid (a - bl) \implies d \mid a'$$

   Включение правого в левое доказывается аналогично, следовательно множества равны ■

3. $\forall m > 0 : (am, bm) = m(a, b)$
4. $d \mid a, d \mid b \implies \left(\frac{a}{d}, \frac{b}{d}\right) = \frac{(a,b)}{d}$
5. Линейное представление НОД: $a, b \in \mathbb{N} \implies \exists u, v \in \mathbb{Z} : au + bv = (a, b)$

   Доказательство.

   $r_1 = a - bq = a \cdot 1 + b \cdot (-q_1)$
   $r_2 = b - r_1 q_2 = b - (a \cdot 1 + b \cdot (-q_1))q_2 = a \cdot (-q_2) + b(1 + q_1 q_2)$
   $r_3 = r_1 - r_2 q_3 = a \cdot (...) + b \cdot (...)$ ■

6.2. Алгоритм Евклида

$$\text{Даны } a, b \in \mathbb{N}, a > b$$

$$\begin{array}{lll} & a = bq_1 + r_1 & 0 \leqslant r_1 < b \\ r_1 \neq 0 & b = r_1 q_2 + r_2 & 0 \leqslant r_2 < r_1 \\ r_2 \neq 0 & r_1 = r_2 q_3 + r_3 & 0 \leqslant r_3 < r_2 \\ & \vdots & \\ r_{n-2} \neq 0 & r_{n-3} = r_{n-2} q_{n-1} + r_{n-1} & 0 \leqslant r_{n-1} < r_{n-2} \\ r_{n-1} \neq 0 & r_{n-2} = r_{n-1} q_n + 0 & \end{array}$$

Теорема 6.1. $r_{n-1} = (a, b)$

Доказательство.

$$(a, b) = (b_1, r_1) = (r_1, r_2) = (r_2, r_3) = ... = (r_{n-2}, r_{n-1}) = r_{n-1}$$

■

6.3. Взаимно простые числа

Определение 6.2. $a, b \in \mathbb{Z}$ называются взаимно простыми, если $(a, b) = 1$.

Свойства

1. $(a, b) = 1 \Leftrightarrow \exists u, v \in \mathbb{Z} : au + bv = 1$

   Доказательство.

   $$\left.\begin{array}{l} \Longleftarrow \begin{array}{l} d \mid a \\ d \mid b \end{array} \end{array}\right\} \Longrightarrow d \mid (au + bv) \overset{\text{знаем}}{\Longrightarrow} d = \pm 1$$

   ■

2. $(a, b) = 1 \implies \forall c \in \mathbb{Z} : (a, bc) = (a, c)$

   Доказательство.

   $$\left.\begin{array}{l} (a, c) \mid a \\ (a, c) \mid bc \end{array}\right\} \Longrightarrow (a, c) \mid (a, bc)$$

   $$d = (a, bc)$$

   $$\left.\begin{array}{l} \left.\begin{array}{l} d \mid a \\ (a, b) = 1 \end{array}\right\} \Longrightarrow (d, b) = 1 \\ \left.\begin{array}{l} d \mid bc \\ (d, b) = 1 \end{array}\right\} \Longrightarrow d \mid c \end{array}\right\} \Longrightarrow d \mid (a, c) \Longrightarrow (a, c) = (a, bc)$$

   ■

3. $a \mid bc, (a, b) = 1 \implies a \mid c$

Доказательство.

$$\exists u, v \in \mathbb{Z} : au + bv = 1 \qquad | \cdot c$$
$$\underbrace{auc}_{a|...} + \underbrace{bvc}_{a|...} = c \implies c \mid a$$

■

4. $(a, b_1) = (a, b_2) = 1 \implies (a, b_1 b_2) = 1$

Доказательство.

$$au_1 + b_1 v_1 = 1$$
$$au_2 + b_2 v_2 = 1$$
$$1 = a^2 u_1 u_2 + a u_1 b v_2 + b_1 v_1 a u_2 + b_1 b_2 v_1 v_2 =$$
$$a \underbrace{(...)}_{u} + b_1 b_2 \underbrace{v_1 v_2}_{v} \implies (a, b_1 b_2) = 1$$

■

5. Пусть $a_1, ..., a_m, b_1, ..., b_n \in \mathbb{Z}$ и $(a_i, b_j) = 1 (1 \leqslant i \leqslant m; 1 \leqslant j \leqslant n)$

$$\implies (a_1 \cdot ... \cdot a_m, b_1 \cdot ... \cdot b_n) = 1$$

Доказательство. Возьмем $(a_i, b_1 \cdot ... \cdot b_n) = 1$. Через индукцию по k докажем $(a_i, b_1 \cdot ... \cdot b_k) = 1$. База:

$$(a_1, b_1) = 1$$

Переход:

$$\left.\begin{array}{l}(a_i, b_1 \cdot ... \cdot b_k) = 1 \\ (a_i, b_{k+1})\end{array}\right\} \implies (a_i, b_1 \cdot ... \cdot b_k b_{k+1}) = 1$$

Проведя аналогичную индукцию с b_i получим:

$$(a_1 \cdot ... \cdot a_m, b_1 \cdot ... \cdot b_n) = 1$$

■

ГЛАВА 7

НОК

Определение 7.1. Пусть $a_1, ..., a_n \in \mathbb{Z}$, их наименьшее общее кратное – наименьшее натуральное c, т.ч. $a_1 \mid c, ..., a_m \mid c$.

Обозначение: НОК$(a_1, ..., a_n)$.

Теорема 7.1. *Пусть $a, b \in \mathbb{N}$, тогда*

$$\text{НОК}(a, b) = \frac{ab}{(a, b)}$$

Доказательство. Пусть $(a, b) = d, a = da_1, b = db_1$

$$\frac{ab}{d} = a_1 b = ab_1$$

то есть $\frac{ab}{d}$ – общее кратное a, b

Пусть M – какое-либо общее кратное a, b

$$M = dM_1$$

$$a \mid M \implies da_1 \mid dM1 \implies a_1 \mid M_1$$

Аналогично $b_1 \mid M_1$

$$M_1 = a_1 c$$

$$b_1 \mid M_1 \qquad (b_1, a_1) = 1 \implies b_1 \mid c$$

$$a_1 b_1 \mid M_1 \qquad a_1 b_1 d \mid M, \text{ где } a_1 b_1 d = \frac{ab}{(a, b)}$$

■

Замечание. При этом проверили: любое общее кратное a, b, кратно НОК(a, b)

ГЛАВА 8

Основная теорема арифметики

Лемма 8.1. *Пусть p – простое число $a \in \mathbb{Z}$, тогда либо $p \mid a$, либо $(p, a) = 1$.*

Доказательство.

$$(p,a) \mid p \implies \left[\begin{array}{l} (p,a) = 1 \\ (p,a) = p \implies p \mid a \end{array} \right.$$

■

Лемма 8.2. *Пусть p – простое и $p \mid (a_1 \cdot ... \cdot a_n) \implies \exists i : p \mid a_i$*

Доказательство. Индукция по n. База: $n = 1$ – тривиально. Переход:

$$p \mid (a_1 ... a_n)$$

По лемме 8.1

$$\left[\begin{array}{l} (p, a_n) = 1 \implies p \mid (a_1 ... a_{n-1}) \\ p \mid a_n \implies \text{ок} \end{array} \right.$$

По идукционному предположению

$$p \mid a_i (1 \leqslant i \leqslant n-1)$$

■

Теорема 8.1 (Основная теорема арифметики)**.** *Любое натуральное число раскладывается в произведение положительных простых чисел, так что это разложение единственно с точностью до порядка множителей.*

Доказательство. Докажем существование: для натурального числа $n \geqslant 2$ проведем индукцию по n.

База:

$$2 = 2$$

Переход:

$$n \text{ – простое, то доказывать нечего}$$
$$n \text{ – составное, то } n = ab, 1 < a, b < n$$

Тогда a, b раскладываются на простые множители и, соответственно, их произведение тоже раскладывается

Докажем единственность: проведем индукцию по n.

$$n = p_1 ... p_r = q_1 ... q_s$$
$$q_s \mid n \implies \exists j : \underbrace{q_s \mid p_j}_{>0} \implies q_s = p_j \implies p_1 ... \hat{p_j} ... p_r = \underbrace{q_1 ... q_{s-1}}_{<n}$$

$(q_1, ..., q_{s-1})$ отличается от $(p_1, ..., \hat{p_j}, ..., p_r)$ только порядком (т.к. $s = r$), это означает единственность для n. ■

Определение 8.1. Представление числа $a > 1$ в виде $p_1^{\alpha_1} ... p_n^{\alpha_n}$, где p_i попарно различны, а $\alpha_i \in \mathbb{N}$ называется каноническим разложением (или факторизацией) числа a.

Следствие 8.1. *Пусть $a = p_1^{\alpha_1} ... p_n^{\alpha_n}$ – каноническое разложение, тогда множество положительных делителей a:*

$$\{p_1^{\beta_1} ... p_n^{\beta_n} : 0 \leqslant \beta_i \leqslant \alpha_i, i = 1, ..., n\}$$

Доказательство. Очевидно, что $p_1^{\beta_1} ... p_n^{\beta_n} \mid a$. Обратно: пусть $d \mid a, a = dc$. Из единственности разложения можно утверждать в d входят только $p_1, ..., p_n$ и показатель p_i не больше α_i. ■

Следствие 8.2. *Число натуральных делителей $a = p_1^{\alpha_1} ... p_n^{\alpha_n}$ – это*

$$(\alpha_1 + 1) ... (\alpha_n + 1)$$

Предложение 8.1. *Пусть* $m = \pm p_1^{l_1}...p_s^{l_s}; n = \pm p_1^{r_1}...p_s^{r_s}$, *тогда*

$$\text{НОД}(m,n) = p_1^{\min(l_1,r_1)}...p_s^{\min(l_s,r_s)}$$

$$\text{НОК}(m,n) = p_1^{\max(l_1,r_1)}...p_s^{\max(l_s,r_s)}$$

Доказательство.

$$\begin{aligned}
d \mid m \Leftrightarrow d = p_1^{\alpha_1}...p_s^{\alpha_s} \qquad & \alpha_j \leqslant l_j \\
d \mid n \Leftrightarrow ... \qquad & \alpha_j \leqslant r_j \\
\begin{cases} d \mid m \\ d \mid n \end{cases} \Leftrightarrow ... \qquad & \alpha_j \leqslant \min(l_j, r_j) \\
d = \text{НОД}(n,m) \Leftrightarrow ... \qquad & \alpha_j = \min(l_j, r_j)
\end{aligned}$$

$$m \mid c, n \mid c \Leftrightarrow c = p_1^{\beta_1}...p_s^{\beta_s} q_1^{\gamma_1}...q_h^{\gamma_h}$$
$$l_j \leqslant \beta_j, r_j \leqslant \beta_j, j = 1...s \implies \beta_j \geqslant \max(l_j, r_j)$$
$$\text{НОК}(m,n) = p_1^{\beta_1}...p_s^{\beta_s}, \beta_j = \max(l_j, r_j)$$

■

Следствие 8.3.

$$\text{НОД}(m,n) \cdot \text{НОК}(m,n) = mn \qquad m, n > 0$$

ГЛАВА 9

Сравнения по модулю

Определение 9.1. $a, b \in \mathbb{Z}$ сравнимы по модулю m, если $m \mid (a - b)$

Пример. Если $m = 5$, то 13 и 28 сравнимы по модулю 5, а 17 и 26 не сравнимы по модулю 5.

Обозначение:

$$13 \equiv 28 \pmod 5 \qquad -7 \equiv 3 \pmod 5$$

9.1. Свойства

1. Рефлексивность: $a \equiv a \pmod m$
2. Симметричность: $a \equiv b \pmod m \implies b \equiv a \pmod m$

   Доказательство.

   $$m \mid (b - a) = m \mid -(a - b)$$

   ■

3. Транзитивность:

   $$\left.\begin{array}{ll} a \equiv b & \pmod m \\ b \equiv c & \pmod m \end{array}\right\} \implies a \equiv c \pmod m$$

Доказательство.

$$m \mid (a-c) = m \mid (a-b) + m \mid (b-c)$$

■

4. $\left.\begin{array}{l} a \equiv b \pmod{m} \\ a' \equiv b' \pmod{m} \end{array}\right\} \implies a + a' \equiv b + b' \pmod{m}$

Доказательство.

$$m \mid ((a+a') - (b+b')) = m \mid (a-b) + m \mid (a'-b')$$

■

5. $\left.\begin{array}{l} a \equiv b \pmod{m} \\ d \in Z \end{array}\right\} \implies da \equiv db \pmod{dm}$

Доказательство.

$$m \mid (a-b) \implies dm \mid d(a-b)$$

■

6. $\left.\begin{array}{l} a \equiv b \pmod{m} \\ k \mid m \end{array}\right\} \implies a \equiv b \pmod{k}$

7. $\left.\begin{array}{l} a \equiv b \pmod{m} \\ a' \equiv b' \pmod{m} \end{array}\right\} \implies aa' \equiv bb' \pmod{m}$

Доказательство.

$$\begin{gathered} aa' \equiv ba' \pmod{m} \\ (aa' \equiv ba' \pmod{ma'} \text{ по свойству 5} \\ \implies aa' \equiv ba' \pmod{m} \text{ по свойству 6}) \\ ba' = bb' \pmod{m} \\ \text{По транзитивности: } aa' \equiv bb' \pmod{m} \end{gathered}$$

■

8. $a \equiv b \pmod{m > 0} \Leftrightarrow$ остатки a и b при делении на m совпадают

Доказательство.

$$
\begin{gathered}
\Longleftarrow a = mq_1 + r \\
b = mq_2 + r \\
a - b = m(q_1 - q_2) \\
m \mid m(q_1 - q_2) \\
\Longrightarrow \; a = mq + r \qquad 0 \leqslant r < m \\
b = a = mt \qquad t \in \mathbb{Z} \\
\Longrightarrow \; b = mq + mt + r = m(q + t) + r \qquad 0 \leqslant r < m \\
\Longrightarrow \quad \text{остаток при делении } b \text{ на } m \text{ равен } r
\end{gathered}
$$

■

9. $a \equiv b \pmod{m} \implies (a, m) = (b, m)$

ГЛАВА 10

Кольцо классов вычетов

Определение 10.1. Класс эквивалентности относительно сравнимости по модулю m называется классом вычетов по модулю m. Класс числа a обозначается: $[a]_m = \overline{a} = \{..., a-2m, a-m, a, a+m, a+2m, ...\}$

Пример. Разбиение на классы при $m = 3$

$$M_0 = \{..., -3, 0, 3, 6, 9, ...\}$$
$$M_1 = \{..., -5, -2, 1, 4, 7, 10, ...\}$$
$$M_2 = \{..., -4, -1, 2, 5, 8, 11, ...\}$$
$$\mathbb{Z} = M_0 \cup M_1 \cup M_2$$

Определение 10.2. Фактор-множество относительно сравнимости по модулю обозначают $\mathbb{Z}/m\mathbb{Z}$, читают как «зет по эм зет», и называют множеством классов вычетов по модулю m

Предложение 10.1. *Пусть $m \in N$, тогда $|\mathbb{Z}/m\mathbb{Z}| = m$*

Доказательство. Пусть r – остаток от a при делении на m, тогда

$$[a]_m = [r]_m \implies \mathbb{Z}/m\mathbb{Z} = \{[0]_m, [1]_m, ..., [m-1]_m\}, \text{ т.е. } |\mathbb{Z}/m\mathbb{Z}| \leqslant m$$

осталось проверить, что $[i]_m \neq [j]_m, 0 \leqslant i < j \leqslant m-1$

$$i \not\equiv j, \pmod m \text{ т.к. } 0 < j - i < m$$

■

Определение 10.3. Набор чисел $a_1, ..., a_m$ называется полной системой вычетов по модулю m, если $\forall i \neq j : a_i \not\equiv a_j \pmod m$ (при этом: $\{[a_1], ..., [a_m]\} = \mathbb{Z}/m\mathbb{Z}$)

Предложение 10.2. *Пусть $a_1, ..., a_m$ – полная система вычетов по модулю m, пусть $(c, m) = 1, b \in \mathbb{Z}$, тогда $\{ca_j + b : j = 1, ..., m\}$ тоже ПСВ по модулю m*

Доказательство.

$$\begin{gathered} ca_i + b \equiv ca_j + b \pmod{m} \\ -b \equiv -b \pmod{m} \\ \Longrightarrow ca_i \equiv ca_j \pmod{m} \\ \left.\begin{array}{l} m \mid c(a_i - a_j) \\ (c, m) = 1 \end{array}\right\} \Longrightarrow m \mid (a_i - a_j) \\ \Longrightarrow a_j \equiv a_i \pmod{m} \Longrightarrow i = j \end{gathered}$$

■

Введем операции на $\mathbb{Z}/m\mathbb{Z}$

$$\overline{a} + \overline{b} := \overline{a + b}$$
$$\overline{a} \cdot \overline{b} := \overline{ab}$$

Предложение 10.3. *Сложение и умножение на этом множестве корректно определены.*

Доказательство. Нужно проверить: если $\overline{a} = \overline{a'}, \overline{b} = \overline{b'}$, то $\overline{a' + b'} = \overline{a + b}$ и $\overline{a'b'} = \overline{ab}$

Имеем

$$\begin{gathered} a \equiv a' \pmod{m} \qquad b \equiv b' \pmod{m} \\ \Longrightarrow a' + b' \equiv a + b \pmod{m} \\ a'b' \equiv ab \pmod{m} \\ \Longrightarrow \overline{a' + b'} = \overline{a + b} \qquad \overline{a'b'} = \overline{ab} \end{gathered}$$

■

Теорема 10.1. $(\mathbb{Z}/m\mathbb{Z}, +, *)$ – *коммутативное ассоциативное кольцо с единицей.*

Доказательство. 1. $\overline{a} + \overline{b} = \overline{a + b} = \overline{b + a} = \overline{b} + \overline{a}$

2. Ассоциативность аналогично.

3. $\overline{0}$ – нейтральный

4. $\overline{-a}$ обратный к $\overline{a}$
5. Коммутативность и ассоциативность умножения аналогично сложению
6. $\overline{a}(\overline{b}+\overline{c}) = \overline{a}\cdot\overline{(b+c)} = \overline{a(b+c)} = \overline{ab+ac} = \overline{ab}+\overline{ac} = \overline{a}\cdot\overline{b}+\overline{a}\cdot\overline{c}$ – дистрибутивность умножения
7. $\overline{1}$ – нейтральный по умножению

■

Определение 10.4. Областью целостности называется коммутативное ассоциативное кольцо с $1 \neq 0$, т.ч. если $a, b \neq 0$, то $ab \neq 0$

Предложение 10.4. *$\mathbb{Z}/m\mathbb{Z}$ – область целостности только если m простое.*

Доказательство. Пусть $m = 1 \implies \mathbb{Z}/m\mathbb{Z} = \{\overline{0}\}; 1 = 0$ – не ОЦ.

Пусть m – составное, тогда

$$\begin{gathered} m = ab \qquad 1 < a, b < m \\ \implies \overline{a}\cdot\overline{b} = \overline{ab} = \overline{m} = \overline{0} \\ \overline{a}, \overline{b} \neq \overline{0} \implies \text{ делители нуля} \end{gathered}$$

Пусть m – простое, тогда $\overline{1} \neq \overline{0}$, т.к. $m > 1$. Предположим, что $\overline{a}\cdot\overline{b} = \overline{0}$, но, если $\overline{ab} = \overline{0}$, то

$$\left.\begin{array}{l} m \mid ab \\ m \text{ простое} \end{array}\right\} \implies \left[\begin{array}{l} m \mid a \\ m \mid b \end{array}\right. \implies \left[\begin{array}{l} \overline{a} = \overline{0} \\ \overline{b} = \overline{0} \end{array}\right.$$

■

10.1. Обратимые классы

Определение 10.5. Если A – ассоциативное кольцо с 1, то $A^* = \{a \in A : \exists a^{-1}\}$ – множество обратимых элементов A, а так же группа по умножению.

Пример.

$$\mathbb{Z}^* = \{\pm 1\}, \mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$$

Теорема 10.2. *Пусть $m \in \mathbb{N}, a \in \mathbb{Z}$. Тогда $\overline{a} \in (\mathbb{Z}/m\mathbb{Z})^* \Leftrightarrow (a, m) = 1$*

Доказательство.

$$\begin{gathered}\overline{a} \in (\mathbb{Z}/m\mathbb{Z})^* \Leftrightarrow \exists \overline{c} \in \mathbb{Z}/m\mathbb{Z} : \overline{a} \cdot \overline{c} = \overline{1} \\ \Leftrightarrow \exists c \in \mathbb{Z} : ac \equiv 1 \pmod{m} \\ \Leftrightarrow \exists c, t \in \mathbb{Z} : ac = 1 + mt \\ \Leftrightarrow \exists c, t \in \mathbb{Z} : ac - mt = 1 \\ \Leftrightarrow (a, m) = 1\end{gathered}$$

■

Следствие 10.1. *$\mathbb{Z}/m\mathbb{Z}$ – поле, только если m – простое.*

Доказательство. Пусть m – составное $\implies$ $\mathbb{Z}/m\mathbb{Z}$ – не ОЦ $\implies$ не поле.

Пусть $p = m$ – простое

$$\begin{gathered}\implies (\mathbb{Z}/p\mathbb{Z})^* = \{\overline{a} : 0 \leqslant a < p - 1, (a, p) = 1\} = \\ \{\overline{1}, \overline{2}, \overline{3}, ..., \overline{p-1}\} = (\mathbb{Z}/p\mathbb{Z}) \setminus \{\overline{0}\}\end{gathered}$$

т.е. $\mathbb{Z}/p\mathbb{Z}$ – конечное поле ■

Мы обнаружили поля из конечного числа элементов. Что мы о них знаем:

1. Поле вида $\mathbb{Z}/p\mathbb{Z}$ единственное вплоть до изоморфизма.
2. Если в поле $m = p^l$ количество элементов, то оно существует и единственно.
3. Если в поле $m \neq p^l$ элементов, то такое поле не существует.

Теорема 10.3 (Вильсона)**.** *Пусть p – простое число, тогда*

$$(p-1)! \equiv -1 \pmod{p}$$

Пример.

$$4! = 1 \cdot 2 \cdot 3 \cdot 4 = 24 \equiv -1 \pmod{5}$$

Доказательство.

$$\prod_{n=1}^{p-1} \overline{n} = \overline{-1} \text{ в } \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$$

$$\overline{a}, \overline{b} : \overline{a} \cdot \overline{b} = \overline{1}$$

$$\overline{a'}, \overline{b'} : \overline{a'} \cdot \overline{b'} = \overline{1}$$

...

В итоге весь класс разобьется на пары: x, x^{-1}, но некоторые числа будут выписаны дважды, нужно выяснить когда

$$x \cdot x = \overline{1}?$$

Для этого решим уравнение:

$$x^2 = \overline{1}$$
$$x = \overline{c}$$
$$\overline{c} \cdot \overline{c} = \overline{1}$$
$$c^2 \equiv 1 \pmod{p}$$
$$(c-1)(c+1) \equiv 0 \pmod{p}$$
$$\left[\begin{array}{l} c \equiv 1 \pmod{p} \\ c \equiv -1 \pmod{p} \end{array} \right.$$
$$x = \overline{1} \qquad x = \overline{-1}$$
$$\prod_{n=1}^{p-1} \overline{n} = \overline{1} \cdot \ldots \cdot \overline{1} \cdot \overline{1} \cdot \overline{-1} = \overline{-1}$$

■

ГЛАВА 11

Китайская теорема об остатках

Теорема 11.1. *Пусть* $m, n \in \mathbb{N}, (m,n) = 1, a, b \in \mathbb{Z}$, *тогда*

$$\exists x \in \mathbb{Z} : \begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$$

Далее, если

$$x' \in \mathbb{Z}, \begin{cases} x' \equiv a \pmod{m} \\ x' \equiv b \pmod{n} \end{cases} \Leftrightarrow x' \equiv x \pmod{mn}$$

Доказательство.

$$x' \equiv x \pmod{mn} \Leftrightarrow \begin{cases} x' \equiv x \pmod{m} \\ x' \equiv x \pmod{n} \end{cases} \Leftrightarrow \begin{cases} x' \equiv a \pmod{m} \\ x' \equiv b \pmod{n} \end{cases}$$

$$(m,n) = 1 \implies \overline{m} \in (\mathbb{Z}/n\mathbb{Z})^*$$

$$\implies \exists x_1 \in \mathbb{Z} : \overline{mx_1} = \overline{1} \in (\mathbb{Z}/m\mathbb{Z})^* \implies mx_1 \equiv 1 \pmod{n}$$

Аналогично

$$\exists x_2 \in \mathbb{Z} : nx_2 \equiv 1 \pmod{m}$$

$$\begin{cases} mx_1 \equiv 0 \pmod{m} \\ mx_1 \equiv 1 \pmod{n} \end{cases} \qquad \begin{cases} nx_2 \equiv 1 \pmod{m} \\ nx_2 \equiv 0 \pmod{n} \end{cases}$$

$$\begin{matrix} b(mx_1) + a(nx_2) \equiv b \cdot 0 + a \cdot 1 \pmod{m} \\ b(mx_1) + a(nx_2) \equiv b \cdot 1 + a \cdot 0 \pmod{n} \end{matrix} \implies \begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$$

■

Доказательство.

$$\mathbb{Z}/mn\mathbb{Z} \xrightarrow{\text{инъ.}} (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$$
$$[a]_{mn} \mapsto ([a]_m, [a]_n)$$
$$|\mathbb{Z}/mn\mathbb{Z}| = mn = |(\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})| \implies \text{отображение биекция}$$

■

Пример. Сколько решением имеет уравнение $x^2 \equiv 1 \pmod{77}$

$$x^2 \equiv 1 \pmod{77} \Leftrightarrow \begin{cases} x^2 \equiv 1 \pmod{7} \\ x^2 \equiv 1 \pmod{11} \end{cases}$$

$$\Leftrightarrow \begin{cases} \left[\begin{array}{l} x \equiv 1 \pmod{7} \\ x \equiv -1 \pmod{7} \end{array}\right. \\ \left[\begin{array}{l} x \equiv 1 \pmod{11} \\ x \equiv -1 \pmod{11} \end{array}\right. \end{cases} \Leftrightarrow \left[\begin{array}{l} \begin{cases} x \equiv 1 \pmod{7} \\ x \equiv 1 \pmod{11} \end{cases} \\ \begin{cases} x \equiv 1 \pmod{7} \\ x \equiv -1 \pmod{11} \end{cases} \\ \begin{cases} x \equiv -1 \pmod{7} \\ x \equiv 1 \pmod{11} \end{cases} \\ \begin{cases} x \equiv -1 \pmod{7} \\ x \equiv -1 \pmod{11} \end{cases} \end{array}\right.$$

$$\Leftrightarrow \left[\begin{array}{l} x \equiv 1 \pmod{77} \\ x \equiv 43 \pmod{77} \\ x \equiv -43 \pmod{77} \\ x \equiv -1 \pmod{77} \end{array}\right.$$

ГЛАВА 12

Функция Эйлера

Определение 12.1. Функция Эйлера – это количество обратимых классов по модулю n:

$$n \in \mathbb{N}$$
$$\varphi = |(\mathbb{Z}/n\mathbb{Z})^*| = \{a : 0 \leqslant a < n, (a, n) = 1\}$$
$$\varphi : \mathbb{N} \to \mathbb{N}$$

Пример.

$$|(\mathbb{Z}/5\mathbb{Z})^*| = 4 \qquad \varphi(5) = 4$$
$$|(\mathbb{Z}/6\mathbb{Z})^*| = 2 \qquad \varphi(6) = 2$$

Предложение 12.1. *Пусть p – простое, $n \in \mathbb{N}$, тогда*

$$\varphi(p^n) = p^n - p^{n-1} = p^{n-1}(p-1)$$

Доказательство.

$$(a, p^n) = 1 \Leftrightarrow p \nmid a$$
$$|\{a : 0 \leqslant a < p^n - 1, (a, p) = 1\}| =$$
$$= p^n - |\{a : 0 \leqslant a \leqslant p^n - 1, p \mid a\}| = p^n - p^{n-1}$$

■

Предложение 12.2. *Пусть $m, n \in \mathbb{N}, (m, n) = 1$, тогда*

$$\varphi(mn) = \varphi(m)\varphi(n)$$

Доказательство.

$$\mathbb{Z}/mn\mathbb{Z} \xrightarrow{\lambda} (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$$
$$[a]_{mn} \mapsto ([a]_m, [a]_n)$$

По КТО λ – биекция

$$(a, mn) \Leftrightarrow \begin{cases} (a, m) = 1 \\ (a, n) = 1 \end{cases}$$
$$\lambda((\mathbb{Z}/mn\mathbb{Z})^*) = (\mathbb{Z}/n\mathbb{Z})^* \times (\mathbb{Z}/m\mathbb{Z})^*$$
$$[a]_{mn} \in (\mathbb{Z}/mn\mathbb{Z})^* \Leftrightarrow (a, mn) = 1 \Leftrightarrow \begin{cases} (a, m) = 1 \\ (a, n) = 1 \end{cases}$$
$$\Leftrightarrow \begin{cases} [a]_m \in (\mathbb{Z}/m\mathbb{Z})^* \\ [a]_n \in (\mathbb{Z}/n\mathbb{Z})^* \end{cases} \quad \Leftrightarrow \lambda([a]_{mn}) \in (\mathbb{Z}/n\mathbb{Z})^* \times (\mathbb{Z}/m\mathbb{Z})^*$$
$$\Longrightarrow \underbrace{|\mathbb{Z}/mn\mathbb{Z}|}_{\varphi(mn)} = \underbrace{|(\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})|}_{\varphi(m)\varphi(n)}$$

■

Таким образом $a = p_1^{r_1} ... p_s^{r_s}$, где $p_1 ... p_s$ – различные простые.

$$\varphi(a) = \varphi(p_1^{r_1}) ... \varphi(p_s^{r_s}) = p_1^{r_1 - 1}(p_1 - 1) ... p_s^{r_s - 1}(p_s - 1)$$

ГЛАВА 13

Теорема Эйлера

Теорема 13.1. *Пусть* $n \in \mathbb{N}, a \in \mathbb{Z}, (a,n) = 1$, *тогда*

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

Пример.

$$5^{301} \equiv ? \pmod{101}$$

$$5^{100} \equiv 1 \pmod{101}$$
$$5^{300} \equiv 1 \pmod{101}$$
$$5^{301} \equiv 5 \pmod{101}$$

Доказательство. Рассмотрим все обратимые классы $X_1, ..., X_{\varphi(n)}$

$$(\mathbb{Z}/n\mathbb{Z})^* = \{X_1, ..., X_{\varphi(n)}\}$$
$$\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^*$$
$$\overline{a}X_1, ..., \overline{a}X_{\varphi(n)} \in (\mathbb{Z}/n\mathbb{Z})^* \qquad (\overline{a}X_i \neq \overline{a}X_j, i \neq j)$$
$$\Longrightarrow (\mathbb{Z}/n\mathbb{Z})^* = \{\overline{a}X_1, ..., \overline{a}X_{\varphi(n)}\}$$
$$\Longrightarrow \prod_{i=1}^{\varphi(n)} (\overline{a}X_i) = \prod_{X \in (\mathbb{Z}/n\mathbb{Z})^*} X = \prod_{i=1}^{\varphi(a)} X_i$$
$$\prod_{i=1}^{\varphi(n)} (\overline{a}X_i) = (\overline{a})^{\varphi(n)} \prod_{i=1}^{\varphi(n)} X_i$$
$$(\overline{a})^{\varphi(n)} = \overline{1}$$
$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

■

Следствие 13.1 (Малая теорема Ферма)**.** *Пусть p – простое, $a \in \mathbb{Z}$, тогда*

$$a^p \equiv a \pmod{p}$$

Доказательство.

$$\begin{array}{ll} (a,p)=1 & a^{p-1} \equiv 1 \pmod{p} \\ & a^p \equiv a \pmod{p} \\ p \mid a & a^p \equiv 0 \equiv a \pmod{p} \end{array}$$

■

13.1. Алгоритм RSA

1. Создание пары ключей
   a) Выберем $p \neq q$ – большие числа простые числа
   b) $n = pq \qquad \varphi(n) = (p-1)(q-1)$
   c) Выбрать $1 < e < \varphi(n) \qquad (e, \varphi(n)) = 1$
   d) Вычислить $1 < d < \varphi(n) \qquad ed \equiv 1 \pmod{\varphi(n)}$

   Теперь пара (e, n) – открытый ключ, а пара (d, n) закрытый.

2. Шифрование
   a) $0 \leqslant m < n$ – сообщение
   b) $m^e \equiv r \pmod{n}, r < n$

3. Дешифрование
   a) $r^d \equiv r' \pmod{n}, r' < n$
   b) $r' \equiv r^d \equiv (m^e)^d \pmod{n} = m^{ed} \equiv m \pmod{n}$
   c) $\begin{cases} 0 \leqslant r' < n \\ 0 \leqslant m < n \end{cases} \implies r' = m$

Часть III

Комплексные числа

ГЛАВА 14

Определение

Комплексные числа — это числа вида $a + bi$, где $i^2 = -1$ и $a, b \in \mathbb{R}$. Тогда определим комплексные числа таким образом:

$$\mathbb{C} = \mathbb{R} \times \mathbb{R} \qquad (a, b)$$
$$(a, b) + (a', b') = (a + a', b + b')$$
$$(a, b) \cdot (a', b') = (aa' - bb', ab' + a'b)$$

Теорема 14.1. $(\mathbb{C}, +, \cdot)$ – *коммутативное ассоциативное кольцо с 1.*

Доказательство. 1. Коммутативность сложения очевидна

2. Ассоциативность сложения очевидна

3. $(0, 0)$ – нейтральный по сложению

4. $(-a, -b) = -(a, b)$

5. Коммутативность умножения очевидна

6. Ассоциативность – непосредственная проверка

7. Дистрибутивность – непосредственная проверка

8. $(1, 0)$ – нейтральный элемент

$$(a, b) \cdot (1, 0) = (a \cdot 1 - b \cdot 0, a \cdot 0 + 1 \cdot b) = (a, b)$$

■

Элементы $\mathbb{C}$ – комплексные числа
Если бы берем пару $(a, 0)$:

$$(a,0) + (b,0) = (a+b,0)$$
$$(a,0)(b,0) = (ab - 0c \cdot 0, a \cdot 0 + 0 \cdot b) = (ab,0)$$

Тогда $\{(a,0) : a \in \mathbb{R}\}$ – подкольцо. Будем отождествлять $(a,0)$ с a.

$$(0,b) = (0,1)(b,0)$$
$$(a,b) = (a,0) + (0,b) = a(0,1)b$$

Обозначим пару $(0,1)$ за i и получим запись

$$(a,b) = a + ib$$

Теперь справедливо следующее

$$i^2 = (0,1)(0,1) = (-1,0) = -1$$
$$(a+ib) + (a'+ib') = a + a' + i(b+b')$$

Обозначения

Задано

$$z = a + ib, a, b \in \mathbb{R}$$

тогда:

- a – вещественная часть $z \Leftrightarrow \operatorname{Re} z = a$
- b – мнимая часть $z \Leftrightarrow \operatorname{Im} z = b$
- i – мнимая единица

Из такого отождествления следует, что $\mathbb{R} \subset \mathbb{C}$
$\mathbb{C} \setminus \mathbb{R}$ – мнимые числа, т.е. числа вида $ib (b \in \mathbb{R})$

ГЛАВА 15

Комплексное сопряжение и модуль

Рассмотрим отображение:

$$\begin{gathered}\mathbb{C} \to \mathbb{C} \\ a + bi \mapsto a - bi \\ z \mapsto \overline{z}\end{gathered}$$

Оно называется комплексным сопряжением

Предложение 15.1. *1.* $\overline{z + w} = \overline{z} + \overline{w}$

2. $\overline{zw} = \overline{z} \cdot \overline{w}$

3. $\overline{\overline{z}} = z$

4. $z = \overline{z} \Leftrightarrow z \in \mathbb{R}$

5. $z \cdot \overline{z} \in \mathbb{R}_{\geqslant 0}; z \cdot \overline{z} = 0 \Leftrightarrow z = 0$

Доказательство.

$$z = a + bi \qquad w = c + di$$

Докажем 1:

$$\overline{(a + bi) + (c + di)} = \overline{(a + c) + (b + d)i} = (a + c) - (b + d)i = \\ (a - bi) + (c - di) = \overline{a + bi} + \overline{c + di}$$

Докажем 2:

$$\overline{(a+bi)(c+di)} = \overline{(ac-bd)+(ad+bc)i} = (ac-bd)-(ad+bc)i = (a-bi)(c-di) = \overline{a+bi}\cdot\overline{c+di}$$

Доказательство 3 очевидно, докажем 4:

$$z = \overline{z} \Leftrightarrow \operatorname{Im} z = 0 \Leftrightarrow z \in \mathbb{R}$$

Докажем 5:

$$z\cdot\overline{z} = (a+bi)(a-bi) = a^2-(bi)^2 = a^2+b^2 \in \mathbb{R}_{\geqslant 0}$$
$$a^2+b^2 = 0 \Leftrightarrow a = b = 0$$

■

Определение 15.1. Пусть $z \in \mathbb{C}$. Его модулем называется:

$$|z| = \sqrt{z\cdot\overline{z}} \qquad |a+bi| = \sqrt{a^2+b^2}$$

Замечание. Для числа $a \in \mathbb{R}$ новый модуль совпадает со старым.

Предложение 15.2. $\mathbb{C}$ – *поле*

Доказательство.

$$z \in \mathbb{C}, z \neq 0$$
$$z\cdot\overline{z} = |z|^2 \neq 0 \implies z\cdot\frac{1}{|z|^2}\overline{z} = 1$$

■

Теперь мы можем использовать деление:

$$\frac{z}{w} = z\cdot w^{-1} = w^{-1}z$$

а также возведение в степень и соответствующие свойства:

$$z^m = \begin{cases} \overbrace{z\cdot\ldots\cdot z}^{m} & m > 0 \\ 1 & m = 0 \\ \underbrace{z^{-1}\cdot\ldots\cdot z^{-1}}_{-m} & m < 0 \end{cases} \qquad m \in \mathbb{Z}$$

$$z^{m+n} = z^m + z^n$$
$$z^{mn} = (z^m)^n$$
$$(zw)^n = z^n w^n$$

Предложение 15.3 (Свойства модуля). *1.* $|zw| = |z||w|$

2. Если $w \neq 0$, *то* $\left|\frac{z}{w}\right| = \frac{|z|}{|w|}$

Доказательство. Докажем 1:

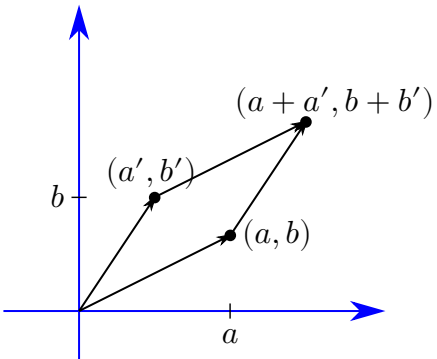
$$|zw|^2 = (zw)\overline{(zw)} = zw\overline{z} \cdot \overline{w} = z\overline{z}w\overline{w} = |z|^2|w|^2$$

Докажем 2:

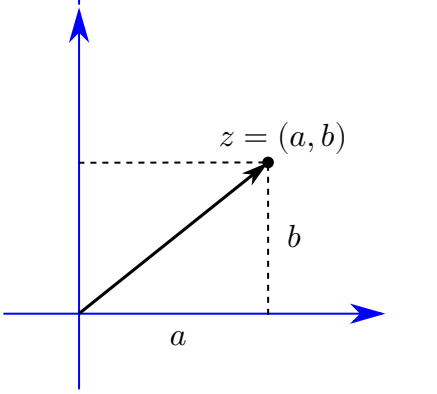
$$z = \frac{z}{w}w \implies |z| = \left|\frac{z}{w}\right| \cdot |w|$$

■

15.1. Геометрическое представление комплексного числа



$$z = a + bi$$
$$z' = a' + b'i$$
$$(a + bi) + (a' + b'i) =$$
$$(a + a') + (b + b')i$$



$$\sqrt{a^2 + b^2} = |z|$$

Таким образом $|z|$ – расстояние от точки изображающей число z до начала координат.

Замечание.

$$|\overline{z}| = |z|$$

Предложение 15.4 (Неравенство треугольника)**.** *Для $z, w \in \mathbb{C}$:*

$$||z| - |w|| \leqslant |z + w| \leqslant |z| + |w|$$

Доказательство. Докажем правое неравенство:

$$z + w = 0 \implies |z + w| \leqslant |z| + |w| \text{ очевидно верно}$$
$$z + w \neq 0 \qquad 1 = \frac{z}{z+w} + \frac{w}{z+w}$$
$$1 = \operatorname{Re} 1 = \operatorname{Re}\left(\frac{z}{z+w}\right) + \operatorname{Re}\left(\frac{w}{r+w}\right)$$
$$\sqrt{a^2 + b^2} \geqslant \sqrt{a^2} = |a| \geqslant a$$
$$\operatorname{Re}\left(\frac{z}{z+w}\right) + \operatorname{Re}\left(\frac{w}{r+w}\right) \leqslant \left|\frac{z}{z+w}\right| + \left|\frac{w}{z+w}\right|$$
$$|z + w| \leqslant |z| + |w|$$

Докажем левое неравенство:

$$z = (z + w) + (-w) \implies$$
$$|z| \leqslant |z + w| + |-w| \implies |z + w| \geqslant |z| - |w|$$
$$\text{Аналогично } |z + w| \geqslant |w| - |z|$$
$$\implies |z + w| \geqslant ||z| - |w||$$

■

ГЛАВА 16

Тригонометрическая форма комплексного числа

Дано $z = a + bi \in \mathbb{C}^*(\mathbb{C}^* = \mathbb{C} \setminus \{0\})$, тогда:

$$r = |z|$$

$$z = r\left(\frac{a}{r} + \frac{b}{r}i\right)$$

$$\left(\frac{a}{r}\right)^2 + \left(\frac{b}{r}\right)^2 = \frac{a^2 + b^2}{r^2} = 1$$

$$\implies \exists\varphi \in \mathbb{R} : \frac{a}{r} = \cos\varphi, \frac{b}{r} = \sin\varphi$$

$$\left[\frac{a}{r} = \cos\varphi \implies \left(\frac{b}{r}\right)^2 = 1 - \cos^2\varphi = \sin^2\varphi; \qquad \varphi = \pm\varphi\right]$$

$$z = |z|(\cos\varphi + i\sin\varphi)$$

– тригонометрическая форма z

$$\operatorname{Re} z = |z|\cos\varphi$$
$$\operatorname{Im} z = |z|\sin\varphi$$

φ называется аргументом z, φ определено с точностью до кратных 2π, т.е. φ – аргумент z, то и $\varphi + 2\pi k$ – аргумент $z \forall k \in \mathbb{Z}$. Если $\varphi \in [0, 2\pi)$, то такой φ называется главное значение аргумента z.

Замечание. Верно и обратное:

$$\cos\varphi' = \cos\varphi \qquad \sin\varphi' = \sin\varphi$$
$$\implies \varphi' = \varphi + 2\pi k, k \in \mathbb{Z}$$

Теорема 16.1. *1. Пусть $z, w \in \mathbb{C}^*$, тогда*

$$\arg(zw) = \arg z + \arg w$$

2. Пусть $z, w \in \mathbb{C}^*$, тогда

$$\arg\left(\frac{z}{w}\right) = \arg z - \arg w$$

3. Пусть $z \in \mathbb{C}^*$, тогда

$$\arg \overline{z} = -\arg z$$

Доказательство.

$$\varphi = \arg z \qquad \psi = \arg w$$

Докажем 1:

$$\begin{aligned} zw &= |z||w|(\cos\varphi + i\sin\varphi)(\cos\psi + i\sin\psi) = \\ &= |zw|\left((\cos\varphi\cos\psi - \sin\varphi\sin\psi) + (\cos\varphi\sin\psi + \sin\varphi\cos\psi)i\right) = \\ &= |zw|(\cos(\varphi+\psi) + i\sin(\varphi+\psi)) \\ &\Longrightarrow\ \varphi + \psi = \arg|zw| \end{aligned}$$

Докажем 2:

$$z = \frac{z}{w}w$$

$$\Longrightarrow\ \arg z = \arg\frac{z}{w} + \arg w\ \Longrightarrow\ \arg\frac{z}{w} = \arg z - \arg w$$

Докажем 3:

$$\begin{gathered} \arg z = \varphi \\ z = |z|(\cos\varphi + i\sin\varphi) \\ \overline{z} = |z|(\cos\varphi - i\sin\varphi) = |z|(\cos(-\varphi) + i\sin(-\varphi)) \\ \Longrightarrow\ -\varphi = \arg\overline{z} \end{gathered}$$

■

Следствие 16.1 (Формула Муавра)**.** *Пусть $z = r(\cos\varphi + i\sin\varphi), r = |z|$, тогда*

$$\forall n \in \mathbb{Z} : z^n = r^n(\cos(n\varphi) + i\sin(n\varphi))$$

Доказательство.

$$\arg z = \varphi$$

$$n > 0 \qquad z^n = r^n(\cos(n\varphi) + i\sin(n\varphi))$$

$$n = 0 \qquad 1 = 1$$

$$n < 0 \qquad n = -m, m \in \mathbb{N}$$

$$z^n = \frac{1}{z^m} = r^{-m}(\cos(0 - m\varphi) + i\sin(0 - m\varphi)) = r^n(\cos(n\varphi) + i\sin(n\varphi))$$

■

ГЛАВА 17

Корни из комплексных чисел

Теорема 17.1. *Пусть* $w = r(\cos\varphi + i\sin\varphi), r > 0, \varphi \in \mathbb{R}, n \in \mathbb{N}$. *Тогда существует ровно* n *таких* $z \in \mathbb{C}$, *что* $z^n = w$, *а именно,* $z_0, z_1, ..., z_{n-1}$, *где*

$$z_j = \sqrt[n]{r}\left(\cos\frac{\varphi + 2\pi j}{n} + i\sin\frac{\varphi + 2\pi j}{n}\right)$$

Доказательство. Решим уравнение $z^n = w, w \in \mathbb{C}, n \in \mathbb{N}$, относительно z. Если $w = 0 \implies z = 0$. Иначе пусть $r = |w|, \varphi = \arg w$. Будем искать z в тригонометрическом виде:

$$\rho(\cos\psi + i\sin\psi), \rho > 0, \psi \in \mathbb{R}$$

$$z^n = w \Leftrightarrow \rho^n(\cos n\psi + i\sin n\psi) = r(\cos\varphi + i\sin\varphi)$$

$$\Leftrightarrow \begin{cases} \rho^n = r \\ n\psi = \varphi + 2\pi j, j \in \mathbb{Z} \end{cases} \Leftrightarrow \begin{cases} \rho = \sqrt[n]{r} \\ \psi = \frac{\varphi + 2\pi j}{n}, j \in \mathbb{Z} \end{cases}$$

$$\Leftrightarrow z = \sqrt[n]{r}\left(\cos\frac{\varphi + 2\pi j}{n} + i\sin\frac{\varphi + 2\pi j}{n}\right), j \in \mathbb{Z}$$

$$\{z : z^n = w\} = \{z_j : j \in \mathbb{Z}\}$$

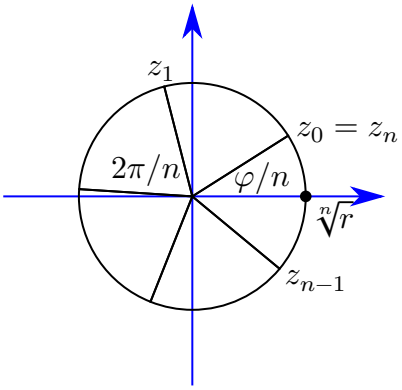
Выясним при каких $j, k : z_j = z_k$

$$z_j = z_k \Leftrightarrow \frac{\varphi + 2\pi j}{n} = \frac{\varphi + 2\pi k}{n} + 2\pi t, t \in \mathbb{Z}$$

$$\Leftrightarrow \frac{2\pi j}{n} = \frac{2\pi k}{n} + 2\pi t, t \in \mathbb{Z} \Leftrightarrow j = k + tn, t \in \mathbb{Z} \Leftrightarrow j \equiv k \pmod{n}$$

$$\implies \{z : z^n = w\} = \{z_j : j = 0, 1, ..., n-1\}$$

$z_0, ..., z_{n-1}$ – различны ■



$$z_n = z_0$$

Тогда $z_0, z_1, ..., z_{n-1}$ – вершины правильного n-угольника

$$z_j = z_0 \cdot \underbrace{\left(\cos\frac{2\pi j}{n} + i\sin\frac{2\pi j}{n}\right)}_{\zeta_j}$$

$$\zeta_j = \zeta_1^j \qquad \zeta_1 = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$$

$$z_0, z_0\zeta_1^1, z_0\zeta_1^2, ..., z_0\zeta_1^{n-1}$$

Следствие 17.1. *При $n > 1$:*

$$\sum_{z^n=w} z = \sum_{j=0}^{n-1} z_0\zeta_1^j = z_0\zeta_1^n - z_0 = 0$$

Предложение 17.1. *Пусть $n \in \mathbb{N}$, Тогда*

$$\mu_n = \{\zeta \in \mathbb{C} : \zeta^n = 1\}$$

– подгруппа в $\mathbb{C}^*$

Доказательство. 1. Множество не пустое ($1 \in \mu_n, |\mu_n| = n$)

2. Замкнуто по умножению ($\zeta, \zeta' \in \mu_n \implies \zeta\zeta' \in \mu_n$)

3. Существует обратный по умножению ($\zeta \in \mu_n \implies \zeta^{-1} \in \mu_n$)

■

Замечание. μ_n – циклическая группа порожденная элементом ζ_1

$$\mu_n = \langle\zeta_1\rangle = \langle\zeta_{-1}\rangle$$

$$g \in G \qquad \langle g\rangle = \{g^n : n \in \mathbb{Z}\}$$