Конспект лекций по алгебре

Лектор: Игорь Борисович Жуков

Оглавление

Элементы теории чисел

1 Делимость

Определение. $a, b \in \mathbb{Z}, a \mid b \iff \exists c \in \mathbb{Z} : b = ac$

Свойства:

1. $a \mid a$ — рефлексивность
2. $a \mid b, b \mid c \implies \exists c \in \mathbb{Z} : b = ac$ — транзитивность
3. $a \mid b, k \in \mathbb{Z} \implies ka \mid kb$
4. $a \mid b_1, a \mid b_2 \implies a \mid (b_1 \pm b_2)$
5. $\pm 1 \mid a$
6. a и b ассоциированны, если $a \mid b,\ b \mid a \implies a = \pm b$
7. a, a' и b, b' — ассоциированны, тогда $a \mid b \iff a' \mid b'$
8. $k \neq 0, ka \mid kb \iff a \mid b$

2 Отношение эквивалентности и разбиение на классы

Определение. Отношение эквивалентности — бинарное отношение, удовлетворяющее следующим свойствам: рефлексивность, симметричность, транзитивность.

Определение. Разбиение на классы множества M — это представление M в виде $M = \bigcup\limits_{i \in I} M_i$, где M_i — классы, I — индексное множество, $M_i \cap M_j = \emptyset$ при $i \neq j$.

Теорема. *Пусть* $M = \bigcup\limits_{i \in I} M_i$ *— разбиение на классы, тогда* $a \sim b \iff \exists i : a, b \in M_i$.

Доказательство. рефлексивность, симметричность — очевидны
транзитивность: $a \sim b, b \sim c \implies \exists i, j : a, b \in M_i$ и $b, c \in M_j$
$b \in M_i \cap M_j \iff M_i \cap M_j \neq \emptyset \implies i = j \implies a, c \in M_i \implies a \sim c$

Теорема. $\exists \sim$ — *отношение эквивалентности на* M. *Значит* $\exists$ *разбиение на классы* $M = \bigcup\limits_{i \in I} M_i$ *такое, что* $\forall a, b \in M : a \sim b \iff \exists i : a, b \in M_i$.

Доказательство.
$[a] = \{b \in M \mid a \sim b\}$ — класс, $a \in M$
$\forall a_1, a_2 \in M : [a_1] \cap [a_2] = \emptyset$ или $[a_1] = [a_2]$ $\exists [a_1] \cap [a_2] \neq \emptyset \implies \exists x \in [a_1] \cap [a_2]$
$x \in [a_1], x \in [a_2] \implies x \sim a_1, x \sim a_2 \implies a_2 \sim a_1$
$[a_2] \subset [a_1], c \in [a_2] \implies c \sim a_2 \implies c \sim a_1 \implies c \in [a_1]$
$[a_1] \subset [a_2], c \in [a_1] \implies c \sim a_1 \implies c \sim a_2 \implies c \in [a_2]$
Значит $[a_1] = [a_2]$

$I = \{[a] \mid a \in M\}$
$\forall \mathfrak{A}, \mathfrak{B} \in I : \mathfrak{A} \cap \mathfrak{B} = \emptyset$
$a_1, a_2 \in \mathfrak{A} \implies [a_1] = \mathfrak{A} = [a_2] \implies a_2 \in [a_1] \implies a_2 \sim a_1$
$a_1 \in \mathfrak{A}, a_2 \in \mathfrak{B} \implies \neg(a_1 \sim a_2)$, так как иначе $a_1 \in [a_2] \implies \mathfrak{B} \in \mathfrak{A} \implies \mathfrak{A} \cap \mathfrak{B} \neq \emptyset$

Определение. Фактор-множество по отношению эквивалентности $\sim$ — множество I, обозначим его как $M/\sim$

Пример: $\mathbb{Z}/\sim = \{[z] \mid z \in \mathbb{Z}\} = \{[0], [1], [2], \dots\}$

3 Сравнение по модулю

Определение. $\exists a, b, m \in \mathbb{Z}$. Говорят, что $m \mid (a - b)$.

Свойства:

1. $\underset{m}{\equiv}$ — рефлексивно
2. $\underset{m}{\equiv}$ — симметрично
3. $\underset{m}{\equiv}$ — транзитивно
4. $a \underset{m}{\equiv} b, d \mid m \implies a^d \underset{m}{\equiv} b$
5. $a \underset{m}{\equiv} b, k \in \mathbb{Z} \implies ka \underset{km}{\equiv} kb$
6. $a \underset{m}{\equiv} b, k \in \mathbb{Z} \implies ka \underset{m}{\equiv} kb$
7. $a_1 \underset{m}{\equiv} b_1, a_2 \underset{m}{\equiv} b_2 \implies a_1 \pm a_2 \underset{m}{\equiv} b_1 \pm b_2$
8. $a_1 \underset{m}{\equiv} b_1, a_2 \underset{m}{\equiv} b_2 \implies a_1 a_2 \underset{m}{\equiv} b_1 b_2$

4 Кольцо классов вычетов

Определение. Множество классов вычетов по модулю m — это множество всех вычетов по модулю m.
Обозначается как $\mathbb{Z}/m\mathbb{Z} \iff \mathbb{Z}/m \iff \mathbb{Z}/\underset{m}{\equiv}$

Теорема. $\exists m \in \mathbb{N}$. *Тогда*

1. $\mathbb{Z}/m\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}$

2. $|\mathbb{Z}/m\mathbb{Z}| = m$

Доказательство.

1. $a \in \mathbb{Z}$ $(!)\overline{a} = \overline{r},\ 0 \leqslant r < m$

   a) $a \geqslant 0$, $\exists r$ — наименьшее число, такое что $r \geqslant 0, a \underset{m}{\equiv} r$
   $r \geqslant m \implies r - m \underset{m}{\equiv} a, r - m \geqslant 0, r - m < r$. Противоречие с выбором r.
   Значит $r < m$, тоесть r — искомое.

   b) $a < 0,\ a' = a \pm (-a)m = a(1-m) \geqslant 0$
   $\overline{a} = \overline{a'} = \overline{r},\ 0 \leqslant r < m$

2. предположим $\overline{r} = \overline{r'},\ 0 \leqslant r, r' < m$.
   $|r' - r| < m \implies m \mid (r - r') \implies r' - r = 0$

Следствие: Теорема о делениии с остатком — $\exists a \in \mathbb{Z}, b \in \mathbb{N} \implies \exists! q, r \in \mathbb{Z}$

1. $a = bq + r,\ 0 \leqslant r < b$

2. $0 \leqslant r < b$

Доказательство.
Существование:
В $\mathbb{Z}/b\mathbb{Z}$ рассмотрим $\overline{a} \in \{\overline{0}, \overline{1}, \ldots, \overline{b-1}\}$, тогда если $\overline{a} = \overline{r},\ 0 \leqslant r < b$
$a \underset{b}{\equiv} r \iff a = bq + r,\ q \in \mathbb{Z}$
Единственность:
$\exists a = bq + r = bq' + r',\ 0 \leqslant r, r' < b \iff \overline{bq + r} = \overline{bq' + r'} \iff \overline{r} = \overline{r'} \iff r = r' \implies bq = bq' \implies q = q'$

Определение. q — неполное частное при делении a на b, r — остаток при делении a на b

Определение. Операция на множестве M — бинарная операция $M \times M \to M$

На $\mathbb{Z}/m\mathbb{Z}$ определим операцию сложения и умножения по модулю m:

- $\overline{a} + \overline{b} = \overline{a+b}$
- $\overline{a} \cdot \overline{b} = \overline{a \cdot b}$

(!) $\overline{a} = \overline{a'},\ \overline{b} = \overline{b'} \implies \overline{a+b} = \overline{a'+b'},\ \overline{a \cdot b} = \overline{a' \cdot b'}$
$\overline{a} = \overline{a'},\ \overline{b} = \overline{b'} \implies a \underset{m}{\equiv} a',\ \implies b \underset{m}{\equiv} b' \implies a+b \underset{m}{\equiv} a'+b',\ a \cdot b \underset{m}{\equiv} a' \cdot b' \implies$
$\overline{a+b} = \overline{a'+b'},\ \overline{a \cdot b} = \overline{a' \cdot b'}$

Пример:
$m = 4, \mathbb{Z}/4\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Определение. $e \in M$ — нейтральный элемент относительно операции(*) на M, если $\forall a \in M$ справедливо $a * e = e * a = a$

Предложение. *Операции сложения и умножения на $\mathbb{Z}/m\mathbb{Z}$ обладают следующими свойствами:*

1. $A + B = B + A$ — коммутативность сложения
2. $(A + B) + C = A + (B + C)$ — ассоциативность сложения
3. $A + \overline{0} = A$— существование нейтрального элемента относительно сложения
4. $A + A' = \overline{0}$ — существование обратного элемента относительно сложения
5. $AB = BA$ — коммутативность умножения
6. $(AB)C = A(BC)$ — ассоциативность умножения
7. $A \cdot \overline{1} = A$ — существование нейтрального элемента относительно умножения
8. $A \cdot (B + C) = A \cdot B + A \cdot C$ — дистрибутивность умножения относительно сложения.
9. $(B + C) \cdot A = B \cdot A + C \cdot A$ — дистрибутивность сложения относительно умножения.

Определение. Кольцом называется множество M с операциями сложения и умножения, для которых выполнены аналоги свойств 1-4 и 8-9.

Определение. Кольцо коммутативное, если выполнены свойство 5.

Определение. Колько ассоциативное, если выполнено свойство 6.

Определение. Кольцо с единицей, если выполнено свойство 7.

Определение. $\forall x \in \mathbb{R} \exists y \in \mathbb{R} : x + y = n \implies n$ — нейтральный элемент относительно сложения.

<u>*Замечание:*</u> Если (*) — операция на M, то существует единственный нейтральный элемент относительно (*).
Доказательство. e, e' — нейтральные элементы относительно (*), тогда $e = e * e' = e'$.

Предложение. ***В нашем курсе все кольца будут ассоциативные с единицей.***

Лемма. *В любом кольце* $0 \cdot a = 0$.

Доказательство. $0 + 0 = 0 \implies (0 + 0) \cdot a = 0 \cdot a \implies 0 \cdot a + 0 \cdot a = 0 \cdot a$
$\neg 0 \cdot A \neq 0 \implies \exists b : b + 0 \cdot A = 0$
$0 = b + 0 \cdot a = b + (0 \cdot a + 0 \cdot a) = (b + 0 \cdot a) + (0 \cdot a) = 0 + (0 \cdot a) = (0 \cdot a)$

Определение. A^* — множество обратимых элементов A.

<u>Примеры:</u>

- $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$
- $\mathbb{Z}^* = \{-1, 1\}$
- $(\mathbb{Z}/4\mathbb{Z})^* = \{\overline{1}, \overline{3}\}$
- $(\mathbb{Z}/5\mathbb{Z})^* = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}\}$

Определение. Полем называется коммутативное кольцо F, такое что $F^* = F \setminus \{0\}$.

5 Наибольший общий делитель

Определение. R — коммутативное кольцо, $a, b \in R$.
Элемент d называется наибольшим общим делителем, если:

1. $d \mid a, d \mid b$
2. $d' \mid a, d' \mid b \implies d' \mid d$

Предложение.

1. *d_1, d_2 — наибольшие общие делители, тогда d_1, d_2 — ассоциированны.*

2. *$\exists d_1$ — наибольший общий делитель, d_2 ассоциированн с d_1, тогда d_2 — тоже наибольший общий делитель.*

Доказательство.

1. По свойству 2. $d_1 \mid d_2,\ d_2 \mid d_1 \implies d_1,\ d_2$ — ассоциированны.

2. $d_2 \mid d_1,\ d_1 \mid a,\ d_1 \mid b \implies d_2 \mid a,\ d_2 \mid b$
   Пусть d_2 не наибольший, тогда $\exists d' > d_2$.
   $d' \mid a,\ d' \mid b \implies d' \mid d_1$
   $d' \mid d_1,\ d_1 \mid d_2 \implies d' \mid d_2$
   Противоречие

Предложение. $\exists a, b \in \mathbb{Z} \implies$

1. *$\exists d \in \mathbb{Z} :\ a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$*

2. *при этом d — наибольший общий делитель a, b.*

Доказательство.

1. $I = a\mathbb{Z} + b\mathbb{Z}$, заметим что $0 \in I$, так как $0a + 0b = 0$.
   $I = \{0\} \implies I = 0\mathbb{Z}$
   $I \neq \{0\} \implies c \in I \implies -c \in I$, так как $-(ax + by) = a \cdot -x + b \cdot -y$
   То есть в I есть положительные числа.
   $d = \min\{c \mid c \in I, c > 0\}$, докажем что $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$
   "$\subset$":
   $d \in I \implies d = ax_0 + by_0, x_0, y_0 \in \mathbb{Z} \implies$
   $\forall z \in \mathbb{Z} : dz = a(x_0 z) + b(y_0 z) \in I$
   "$\supset$":
   $\exists c \in I, d \in \mathbb{N} \implies \exists q, r \in \mathbb{Z} : c = dq + r, 0 \leqslant r < d$
   $c = ax_1 + by_1, x_1, y_1 \in \mathbb{Z}$
   $d = ax_0 + by_0, x_0, y_0 \in \mathbb{Z}$
   $r = c - dq = a(x_1 - x_0 q) + b(y_1 - y_0 q) \in I$
   Но $r < d \overset{defn(d)}{\implies} r = 0 \implies c \in d\mathbb{Z}$

2. $a = a1 + b0 \in I = d\mathbb{Z} \implies d \mid a$
   $b = a0 + b1 \in I = d\mathbb{Z} \implies d \mid b$
   $\exists d' \mid a,\ d' \mid b,\ d = ax_0 + by_0$
   $d' \mid ax_0,\ d' \mid by_0 \implies d' \mid d$

Следствие:

1. $a, b \in \mathbb{Z}$: Тогда наибольший общий делитель a, b существует.

2. Если d — наибольший общий делитель a, b, то $\exists x, y \in \mathbb{Z} :\ d = ax + by$(Линейное представление наибольшего общего делителя).

Доказательство.

1. Доказали в двух частях предложения.

2. $\exists d_0$ — наибольший общий делитель a, b, то есть $d_0 = ax_0 + by_0$
   d ассоциирован с $d_0 \implies d = d_0\mathbb{Z}, z \in \mathbb{Z} \implies d = a(x_0z) + b(y_0z)$

Определение. НОД$(a, b) = \gcd(a, b)$ — неотрицательный наибольший общий делитель a, b.

Предложение. $\exists a_1, a_2, b \in \mathbb{Z} : a_1 \underset{b}{\equiv} a_2$
Тогда $\gcd(a_1, b) = \gcd(a_2, b)$.

Доказательство. (!) $\{c : c \mid a_1, c \mid b\} = \{c : c \mid a_2, c \mid b\}$
"$\subset$":
$a_2 - a_1 = bm \implies a_2 = a_1 + bm$
$c \mid a_1, c \mid b \implies c \mid a_2$
"$\supset$":
$a_1 - a_2 = bm \implies a_1 = a_2 + bm$
$c \mid a_2, c \mid b \implies c \mid a_1$
$\forall x \in \{c : c \mid a_1, c \mid b\} : x \mid \gcd(a_1, b)$
$\forall x \in \{c : c \mid a_2, c \mid b\} : x \mid \gcd(a_2, b)$
$\gcd(a_1, b) = \gcd(a_2, b)$

Определение. Алгоритм Евклида
$\gcd(a, b) = \gcd(b, a \mod b)$, если $b \neq 0$

6 Взаимно простые числа

Определение. Числа a и b называются взаимно простыми, если $\gcd(a, b) = 1$.

Предложение.

1. *$\exists a, b \in \mathbb{Z}$, тогда $a \perp b \iff \exists m, n \in \mathbb{Z} : am + bn = 1$.*

2. *$a_1 \perp b, a_2 \perp b \implies a_1a_2 \perp b$.*

3. *$a_1, \ldots, a_m, b_1, \ldots, b_n \in \mathbb{Z}$ и $\forall i, j : a_i \perp b_j \implies a_1 \ldots a_m \perp b_1 \ldots b_n$.*

4. *$a \mid bc,\ a \perp b \implies a \mid c$.*

5. *$ax \underset{m}{\equiv} ay,\ a \perp m \implies x \underset{m}{\equiv} y$.*

6. *$\gcd(a, b) = d \implies a = da',\ b = db', a' \perp b'$.*

Доказательство.

1. m и n существуют согласно линейному представлению НОД.
$d = \gcd(a,b), d \mid a, d \mid b \implies d \mid (am+bn) = 1 \implies d \mid 1 \implies d = 1.$

2. $1 = a_1m_1+bn_1, 1 = a_2m_2+bn_2 \implies 1 = a_1a_2(m_1m_2)+b(a_1m_1n_2+a_2m_2n_1+bn_1n_2) \implies a_1a_2 \perp b.$

3. $a_1 \perp b, \ldots,\ a_n \perp b \implies a_1 \ldots a_n \perp b$
$a_1 \ldots a_n \perp b_1, \ldots,\ a_1 \ldots a_n \perp b_n \implies a_1 \ldots a_n \perp b_1 \ldots b_n$

4. $1 = am+bn, c = acm+bcn$
$a \mid acm,\ a \mid bcn \implies a \mid c.$

5. $m \mid (ax-ay), a \perp m \implies m \mid (x-y) \implies x \underset{m}{\equiv} y.$

6. $d \mid a, d \mid b \implies a = da',\ b = db' : a', b' \in \mathbb{Z}$
$d = am+bn,\ m, n \in \mathbb{Z}$
$d = 0 \implies a' = b' = 1 = da'm + db'm$
$d \neq 0 \implies 1 = a'm + b'n \implies a' \perp b'.$

7 Линейные диофантовы уравнения

Определение. Линейным диофантовым уравнением с двумя неизвестными называется уравнение вида $ax+by=c$, где $a, b, c \in \mathbb{Z}$.

Для решения нужно найти пару $(x, y) \in \mathbb{Z}^2 : ax+by=c$.
Пример: $12x+21y=5$ — уравнение не имеет решений.
Если $\gcd(a,b) \mid c$, то решение существует, иначе — нет.
нужно доделать параграф

8 Простые числа

Определение. Число $p \in \mathbb{Z}$ называется простым, если $p \notin \{-1, 0, 1\}$ и все делители p — это ± 1 и p.

Свойства:

1. p — простое $\iff -p$ — простое.

2. p — простое, $a \in \mathbb{Z} \implies p|a$ или $p \perp a$.

3. p, q — простые $\implies p, q$ — ассоциированны или $p \perp q$.

4. $p \mid ab \implies p \mid a$ или $p \mid b$.

Предложение. $\exists a \neq \pm 1$, *тогда существует простое число* $p : p \mid a$.

Доказательство. $a = 0 \implies p = 239$
$a = 1 \implies a > 0$
Индукция по a:
a — простое $\implies p = a, p \mid a$
a — не простое, $\exists d : 1 < d < a, d \mid a$
$a = dd'$, тогда по индукционному переходу существует простое число $p : p \mid d$
$p \mid d, d \mid a \implies p \mid a$

Определение. Составное число — это число отличное от 0, и не являющееся простым.

Решето Эратосфена

2, 3, 4, 5, 6, 7, 8, 9, ..., 100

- 2 — простое, вычеркиваем все числа кратные 2
- 3 — простое, вычеркиваем все числа кратные 3
- 4 — составное, пропускаем
- и.т.д.

Теорема. *(Теорема Евклида) Существует бесконечно много простых чисел*

Доказательство. $\exists p_1, p_2, \ldots p_n$ — все простые числа
$N = p_1 p_2 \ldots p_n + 1 \implies$
$\exists$ простое число $p : p \mid N, p > 0 \implies \exists j : p = p_j \implies p \mid (N-1) \implies p \mid 1 \implies p = \pm 1$
Противоречие

9 Основная теорема арифметики

Теорема. $\exists n \geqslant 2$. *Тогда n можно представить в виде произведения простых чисел, и такое представление единственно с точностью до порядка сомножителей.*

Доказательство.
Существование:
$\exists n_0$ — наименьшее число ($\geqslant 2$), для которого такого представления нету.
n_0 — составное число $\implies n_0 = ab, 2 \leqslant a, b < n_0$
По минимальности $\implies a = p_1 \ldots p_k, b = q_1 \ldots q_l$, все p_i, q_j — простые.

$\implies n_0 = p_1 \dots p_k q_1 \dots q_l$ — Противоречие
Единственность:
$n = p_1 \dots p_k = q_1 \dots q_l$, p_i, q_j — простые.
Нудно доказать: $k = l$, $q_1, \dots, q_k$ совпадают с $p_1, \dots, p_k$ с точностью до порядка.
Не умаляя общности иожно считать: $k \leqslant l$.
Индукция по k:
$k = 1$: $p_1 = q_1 \dots q_l$, p_1 — простое $\implies l = 1, p_1 = q_1$
k > 1: $p_k \mid n \implies p_k \mid (q_1 \dots q_l) \implies \exists j : p_k \mid q_j \implies p_k \sim q_j \implies p_k = q_j \implies$
$p_1 \dots p_{k-1} = q_1 \dots \hat{q}_j \dots q_l, \ k-1 \leqslant l-1$
$k - 1 < k \implies$ применим индукционный переход:
$k - 1 = l - 1$ и $q_1, \dots, \hat{q}_j, \dots, q_k$ — это $p_1, \dots, p_{k-1}$ с точностью до порядка. $\implies$
$q_1, \dots, (q_j = p_k), \dots, q_k$ — это $p_1, \dots, p_k$ с точностью до порядка.

Определение. Каноническое разложение(факторизация) числа n — это представление n в виде $p_1^{r_1} \dots p_s^{r_s}$, где p_i — разложение n на простые множители, $r_i \in \mathbb{N}$

Примеры:

- $n = 112 = 2^4 \cdot 7$
- $n = 6006 = 2^1 \cdot 3^1 \cdot 7^1 \cdot 11^1 \cdot 13^1$

Предложение. $\exists a = p_1^{r_1} \dots p_s^{r_s}, b = p_1^{t_1} \dots p_s^{t_s}$
Тогда $a \mid b \iff r_i \leqslant t_i \ \forall i \in \{1, \dots, s\}$

Доказательство. "$\Rightarrow$":
$b = a \cdot p_1^{t_1 - r_1} \dots p_s^{t_s - r_s}$
"$\Leftarrow$":
$b = ac \ c = p_1^{m_1} \dots p_s^{m_s} p_{s+1}^{m_{s+1}} \dots p_n^{m_n}$
$p_1^{t_1} \dots p_s^{t_s} = p_1^{r_1 + m_1} \dots p_s^{r_s + m_s} p_{s+1}^{m_{s+1}} \dots p_n^{m_n} \implies$
$t_i = r_i + m_i \ \forall i \in \{1, \dots, s\}, m_{s+1} = \dots = m_n = 0 \implies t_i \geqslant r_i \ \forall i \in \{1, \dots, s\}$
Следствие: $\exists a = p_1^{r_1} \dots p_s^{r_s}$
Тогда $\{d > 0 : d \mid a\} = \{p_1^{t_1} \dots p_s^{t_s} \mid 0 \leqslant t_i \leqslant r_i, \ \forall i \in \{1, \dots, s\}\}$
Следствие: $\exists a = p_1^{r_1} \dots p_s^{r_s}, \ b = p_1^{t_1} \dots p_s^{t_s}$
Тогда $\gcd(a, b) = p_1^{min(r_1, t_1)} \dots p_s^{min(r_s, t_s)}$

Определение. $\exists a, b \in \mathbb{Z}$. Число $c \in \mathbb{Z}$ называется наименьшим общим кратным чисел a и b, если

1. $a \mid c, b \mid c$
2. Если $a \mid c', b \mid c'$, то $c \mid c'$

Предложение. $\exists a = p_1^{r_1} \dots p_s^{r_s}, b = p_1^{t_1} \dots p_s^{t_s}$
Тогда $c = p_1^{max(r_1, t_1)} \dots p_s^{max(r_s, t_s)}$ *— наименьшее общее кратное чисел* a *и* b

Доказательство. $a \mid c, b \mid c$ — очевидно
$\exists a \mid c', b \mid c', c' = p_1^{m_1} \dots p_s^{m_s} p_{s+1}^{m_{s+1}} \dots p_n^{m_n}$
$a \mid c',\ b \mid c' \implies r_i \leqslant m_i,\ t_i \leqslant m_i,\ \forall i \in \{1, \dots, s\} \implies$
$max(r_i, t_i) \leqslant m_i,\ \forall i \in \{1, \dots, s\} \implies c \mid c'$

Определение. НОК$(a, b) = lcm(a, b)$ — положительное значение наименьшего общего кратного чисел a и b.

Следствие: $\exists a, b \in \mathbb{N}$
Тогда $lcm(a, b) \cdot \gcd(a, b) = ab$
Доказательство. $min(r_i, t_i) + max(r_i, t_i) = r_i + t_i$

10 Китайская теорема об остатках

Теорема. *Пусть* $(m_1, m_2) = 1$*;* $a_1, a_2 \in \mathbb{Z}$*.*

1. $\exists x \in \mathbb{Z}$: $\begin{cases} x_0 \underset{m_1}{\equiv} a_1 \\ x_0 \underset{m_2}{\equiv} a_2 \end{cases}$

2. $\exists x_0$ *удовлетворяет системе выше*
Тогда для $x \in \mathbb{Z}$*:* x *удовлетворяет системе выше* $\iff x \underset{m_1 m_2}{\equiv} x_0$

Доказательство.

1. $x_0 = a_1 + km_1 = a_2 + lm_2 \implies km_1 - lm_2 = a_2 - a_1$ — линейное диофантово уравнение с дыумя неизвестными k, l
$(m_1, m_2) = 1 \implies$ у него есть решение (k_0, l_0)
$x_0 = a_1 + k_0 m_1$ — искомое

2. "$\Rightarrow$"
$x \underset{m_1 m_2}{\equiv} x_0 \implies \begin{cases} x \underset{m_1}{\equiv} x_0 \\ x \underset{m_2}{\equiv} x_0 \end{cases} \implies \begin{cases} x \underset{m_1}{\equiv} a_1 \\ x \underset{m_2}{\equiv} a_2 \end{cases}$
"$\Leftarrow$"
x удовлетворяет системе из теоремы $\implies \begin{cases} x \underset{m_1}{\equiv} x_0 \\ x \underset{m_2}{\equiv} x_0 \end{cases} \implies \begin{cases} m_1 \mid (x - x_0) \\ m_2 \mid (x - x_0) \end{cases} \implies$
$m_1 m_2 \mid (x - x_0)$

Определение. $\exists R, S$ — кольца с единицей. Отображение $\varphi : R \to S$ называется изоморфизмом колец, если: φ биекция.

1. $\forall r_1, r_2 : \varphi(r_1 + r_2) = \varphi(r_1) + \varphi(r_2)$

2. $\forall r_1, r_2 : \varphi(r_1 r_2) = \varphi(r_1)\varphi(r_2)$

Предложение. $\exists (m_1, m_2) = 1$
Тогда существует изоморфизм
$\mathbb{Z}/m_1m_2\mathbb{Z} \to \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z}$
$[a]_{m_1m_2} \mapsto ([a]_{m_1}, [a]_{m_2})$

Доказательство. Проверим корректность: $\exists [a]_{m_1m_2} = [a']_{m_1m_2} \implies$
$a \underset{m_1m_2}{\equiv} a' \implies$
$\begin{cases} a \underset{m_1}{\equiv} a' \\ a \underset{m_2}{\equiv} a' \end{cases} \implies ([a]_{m_1}, [a]_{m_2}) = ([a']_{m_1}, [a']_{m_2})$
$\varphi([a]_{m_1m_2} + [b]_{m_1m_2}) = \varphi([a+b]_{m_1m_2}) = \varphi([a+b]_{m_1}, [a+b]_{m_2}) =$
$\varphi([a]_{m_1} + [a]_{m_2}) + \varphi([b]_{m_1} + [b]_{m_2}) = \varphi([a]_{m_1m_2}) + \varphi([b]_{m_1m_2})$
Для умножения аналогично.
Проверим сюрьективность φ
$X = ([a_1]_{m_1}, [a_2]_{m_2})$
По китайской теореме об остатках $\exists a \in \mathbb{Z} : \begin{cases} a \underset{m_1}{\equiv} a_1 \\ a \underset{m_2}{\equiv} a_2 \end{cases}$
про сюръективность $\implies$ биекция:
$|Y| = |Z| < \infty$
$\varphi : Y \to Z$
Тогда φ инъективна $\iff$ φ сюръективна
что-то про принцип дирихле и готово)

11 Функция Эйлера

Предложение. $\exists m \in \mathbb{N};\ a \in \mathbb{Z}$
$[a]_m \in (\mathbb{Z}/m\mathbb{Z})^* \iff (a, m) = 1$

Доказательство. $[a]_m \in (\mathbb{Z}/m\mathbb{Z})^* \iff \exists [b]_m :\ [a]_m \cdot [b]_m = [1]_m \iff$
$\exists b \in \mathbb{Z} :\ ab \underset{m}{\equiv} 1 \iff$
$\exists b, c \in \mathbb{Z} :\ ab = 1 + mc \iff$
$\exists b, c \in \mathbb{Z} :\ ab - mc = 1 \iff (a, m) = 1$

Следствие: $\mathbb{Z}/m\mathbb{Z}$ - поле $\iff$ m — простое число.

Доказательство. считаем $m \geqslant 1$
$m = 1$: $\mathbb{Z}/1\mathbb{Z} = \{\overline{0}\}$

m — простое: $(a, m) = 1$ для $\forall a \in \{1, 2, \ldots, m-1\} \implies$
$(\mathbb{Z}/m\mathbb{Z})^* = \{\overline{1}, \overline{2}, \ldots, \overline{m-1}\}$
m — составное: $m = ab,\ 2 \leqslant a \leqslant m-1$
$(a, m) \neq 1 \implies \overline{a} \notin (\mathbb{Z}/m\mathbb{Z})^*$

Определение. $\mathbb{F}_{p^r}$ — поле из n элементов $\iff n = p^r,\ p \in \mathbb{P},\ r \in \mathbb{N}$
(хз что это)

Определение. $\exists m \in \mathbb{N} : \varphi(n) = |(\mathbb{Z}/m\mathbb{Z})^*|$
Функция $\varphi \times \mathbb{N} \to \mathbb{N}$ — функция Эйлера.

Предложение. $\exists p \in \mathbb{P},\ r \in \mathbb{N}$.
Тогда $\varphi(p^r) = p^r - p^{r-1}$.

Доказательство. $\varphi(p^r) = |\{a \mid 0 \leqslant a \leqslant p^r - 1,\ (a, p^r) = 1\}| =$
$p^r - |\{a \mid 0 \leqslant a \leqslant p^r - 1,\ (a, p) \neq 1\}| =$
$p^r - |\{a \mid 0 \leqslant a \leqslant p^r - 1,\ p \mid a\}| = p^r - p^{r-1}$

Предложение. $\exists m, n \in \mathbb{N},\ (m, n) = 1$.
Тогда $\varphi(mn) = \varphi(m) \cdot \varphi(n)$.*(Мультипликативность)*

Доказательство. Построим отображение $\lambda : (\mathbb{Z}/mn\mathbb{Z})^* \times (\mathbb{Z}/m\mathbb{Z})^* \to (\mathbb{Z}/n\mathbb{Z})^*$:
$[a]_{mn} = A \in (\mathbb{Z}/mn\mathbb{Z})^* \mapsto ([a]_m, [a]_n)$

$$[a]_{mn} \in (\mathbb{Z}/mn\mathbb{Z})^* \implies (a, mn) = 1 \implies \begin{cases} (a, m) = 1 \\ (a, n) = 1 \end{cases} \begin{cases} [a]_m \in (\mathbb{Z}/m\mathbb{Z})^* \\ [a]_n \in (\mathbb{Z}/n\mathbb{Z})^* \end{cases}$$

Проверка корректности:
$[a]_{mn} = [a']_{mn} \implies ([a]_m, [a]_n) = ([a']_m, [a']_n)$?

$$[a]_{mn} = [a']_{mn} \implies a \underset{mn}{\equiv} a' \implies \begin{cases} a \underset{m}{\equiv} a' \\ a \underset{n}{\equiv} a' \end{cases} \begin{cases} [a]_m = [a']_m \\ [a]_n = [a']_n \end{cases}$$

Проверим что λ — биекция:
Инъективность:

$$\lambda([a]_{mn}) = \lambda([b]_{mn}) \implies \begin{cases} [a]_m = [b]_m \\ [a]_n = [b]_n \end{cases} \overset{chineese\ theorem}{\implies} a \underset{mn}{\equiv} b \implies [a]_{mn} = [b]_{mn}$$

Сюръективность:
Рассмотрим $([b]_m, [c]_n) \in (\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*$.

$$(m, n) = 1 \overset{chineese\ theorem}{\implies} \exists a : \begin{cases} a \underset{m}{\equiv} b \\ a \underset{n}{\equiv} c \end{cases}$$

$$\begin{cases} (b, m) = 1 \implies (a, m) = 1 \\ (c, m) = 1 \implies (a, n) = 1 \end{cases} \implies (a, mn) = 1 \implies [a]_{mn} \in (\mathbb{Z}/mn\mathbb{Z})^*$$

$\lambda([a]_{mn}) = ([a]_m, [a]_n) = ([b]_m, [c]_n) \implies \lambda$ — биекция.
λ — биекция $\implies |(\mathbb{Z}/mn\mathbb{Z})^*| = |(\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*| \implies \varphi(mn) = \varphi(m) \cdot \varphi(n)$
Следствие: $\exists m_1, \ldots, m_k$ — попарно взаимно простые числа.
Тогда $\varphi(\prod\limits_{i=1}^{k} m_i) = \prod\limits_{i=1}^{k} \varphi(m_i)$.
Доказательство. Индукция по k.
База: $k = 1 \implies \varphi(m_1) = \varphi(m_1)$
Переход: $n - 1 \to n$
$(m_n, m_1) = \ldots = (m_n, m_{n-1}) = 1 \implies (m_1, \ldots, m_n) = 1 \implies$
$\varphi(m_1 \ldots m_n) = \varphi(m_1 \ldots m_{n-1})\varphi(m_n) = \varphi(m_1) \ldots \varphi(m_{n-1})\varphi(m_n)$
Следствие: $\exists n = p_1^{r_1}, \ldots, p_s^{r_s}$ — разложение числа n на простые множители.
$\implies \varphi(n) = \prod\limits_{i=1}^{s}(p_i^{r_i} - p_i^{r_i-1})$

Доказательство. По следствию: $\varphi(n) = \varphi(\prod\limits_{i=1}^{s} p_i^{r_i}) = \prod\limits_{i=1}^{s} \varphi(p_i^{r_i}) = \prod\limits_{i=1}^{s}(p_i^{r_i} - p_i^{r_i-1})$

Теорема. $\exists m \in \mathbb{N}, a \in \mathbb{Z}, (a, m) = 1 \implies a^{\varphi(m)} \underset{m}{\equiv} 1$ — *теорема Эйлера.*

Лемма. *Пусть R — ассоциативное кольцо с единицей.*

1. $a, b \in R^* \implies ab \in R^*$
2. $a \in R^*,\ x, y \in R \implies ax = ay \implies x = y,\ xa = ya \implies x = y$

Доказательство.

1. a' — обратный к a элемент, b' — обратный к b элемент.
   $(ab)(b'a') = a(bb')a' = aa' = 1$
   $(b'a)(ab) = b'(aa')b = bb' = 1$

2. a' — обратный к a элемент.
   $ax = ay \implies a'ax = a'ay \implies x = y$
   $xa = ya \implies xaa' = yaa' \implies x = y$

Доказательство. (теоремы Эйлера)
$(\mathbb{Z}/m\mathbb{Z})^* = \{A_1, A_2, \ldots, A_{\varphi(m)}\}$
$[a]_m, A_j \in (\mathbb{Z}/m\mathbb{Z})^* \overset{lemma-1}{\implies}$
$[a]_m A_1, \ldots, [a]_m A_{\varphi(m)}$ — различные элементы
$([a]_m A_j = [a]_m A_k \overset{lemma-2}{\implies} A_j = A_k) \implies$
$\{[a]_m A_1, \ldots, [a]_m A_{\varphi(m)}\} = (\mathbb{Z}/m\mathbb{Z})^* \implies$
$[a]_m A_1 \cdot \ldots \cdot [a]_m A_{\varphi(m)} = A_1 A_2 \ldots A_{\varphi(m)} \implies$
$[a]_m^{\varphi(m)} A_1 A_2 \ldots A_{\varphi(m)} = [1]_m A_1 A_2 \ldots A_{\varphi(m)} \overset{lemma-2}{\implies}$
$[a]_m^{\varphi(m)} = [1]_m \implies [a^{\varphi(m)}]_m = [1]_m \implies a^{\varphi(m)} \underset{m}{\equiv} 1$

Теорема. *(Малая теорема Ферма)*
$\exists p \in \mathbb{P}, a \in \mathbb{Z} \implies a^p \underset{p}{\equiv} a$

Доказательство.
$(a,p) = 1 \implies a^{p-1} \underset{p}{\equiv} 1 \implies a^{p-1}a \underset{p}{\equiv} 1a \implies a^p \underset{p}{\equiv} a$
$(a,p) \neq 1 \implies a \underset{p}{\equiv} 0 \implies a^p \underset{p}{\equiv} 0 \implies a^p \underset{p}{\equiv} a$

Теорема. *(Теорема Вильсона)*
$p \in \mathbb{P} \implies (p-1)! \underset{p}{\equiv} -1$

Доказательство. В $(\mathbb{Z}/m\mathbb{Z})^*$
$\overline{(p-1)!} = \overline{1} \cdot \overline{2} \cdot \ldots \cdot \overline{p-1} = \prod\limits_{A \in (\mathbb{Z}/m\mathbb{Z})^*} A = \prod\limits_{A^2 = \overline{1}} \cdot \prod\limits_{A^2 \neq \overline{1}} = \prod\limits_{A^2 = \overline{1}} \cdot (A_1 \cdot A_1' \cdot \ldots) = \prod\limits_{A^2 = \overline{1}} \cdot \overline{1} = \prod\limits_{A^2 = \overline{1}}$
$A^2 = \overline{1} \iff A^2 - \overline{1}^2 = \overline{0} \iff (A - \overline{1})(A + \overline{1}) = \overline{0} \overset{\mathbb{Z}/p\mathbb{Z}-field}{\iff} A - \overline{1} = \overline{0}, A + \overline{1} = \overline{0} = \prod\limits_{A^2 = \overline{1}}$
$p \neq 2 \implies \overline{1} \cdot \overline{-1} = \overline{-1}$
$p = 2 \implies \overline{1} = \overline{-1}$

12 Построение поля комплексных чисел

Определение. $\mathbb{C} = \mathbb{R} \times \mathbb{R} = \{(a,b) \mid a, b \in \mathbb{R}\}$

Определение.

- Сложение на $\mathbb{C}$: $(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$
- Умножение на $\mathbb{C}$: $(a_1, b_1) \cdot (a_2, b_2) = (a_1 a_2 - b_1 b_2, a_1 b_2 + a_2 b_1)$

Предложение. $(\mathbb{C}, +, \cdot)$ - *поле.*

Доказательство.

- Коммутативность сложения — очевидно.
- Ассоциативность сложения — очевидно.
- $(0,0)$ — нейтральный элемент сложения.
- $(-a, -b)$ — обратный элемент к (a,b).
- Коммутативность умножения — очевидно.
- Ассоциативность умножения — проверяется.

- Дистрибутивность — проверяется.
- $(1,0)$ — нейтральный элемент умножения.
- $(a,b)z_1z_2 = (1,0): \ z_1 = (a,-b), \ z_2 = \frac{1}{a^2+b^2}$

Определение. $\mathbb{C}$ — поле комплексных чисел.

Определение. $c \in \mathbb{C}$ — комплексное число.

Предложение. $\mathbb{R}' = \{(a,0) \mid a \in \mathbb{R}\}$
R' замкнуто относительно сложения, вычитания, умножения, содержит единицу, то есть является подкольцом поля $\mathbb{C}$.
$\implies$ *$\mathbb{R}'$ — само является кольцом относительно сложения, умножения, ограниченных на $\mathbb{R}'$.*
$\mathbb{R} \xrightarrow{\varphi} \mathbb{R}'(a \mapsto (a,0))$, *$\varphi(a)$ — изоморфизм колец, т.е. φ — биекция и $\varphi(a+b) = \varphi(a)+\varphi(b)$; $\varphi(ab) = \varphi(a)\varphi(b)$.*
Отождествим $(a,0)$ с вещественным числом a.
$(a,0) \cdot (0,1) = (0,a)$
$(a,b) = (a,0) + (0,b) = (a,0) + (b,0) \cdot (0,1) = a + b \cdot (0,1) = a + bi$

13 Temp

14 Temp

15 Temp