Содержание

1. Множества и операции над ними

Понятия “множество” и “элемент” считаем интуитивно понятными

Обозначение. Запись $x \in A$ означает, что элемент x принадлежит множеству A.
Используется также запись $x \notin A$, оначающая, что элемент x **не** принадлежит множеству A

Определение 1. Пустым множеством называется множество, не содержащее ни одного элемента

Обозначение. $\emptyset$

Определение 2. Множество B называется подмножеством множества A, если любой элемент множества B принадлежит множеству A

Обозначение. $B \subset A$

Подмножество B множества A называется собственным, если $B \neq A, B \neq \emptyset$

Операции над множествами.

1. **Пересечением** множеств A и B называется множество $\{\, x \mid x \in A \text{ и } x \in B \,\}$

Обозначение. $A \cap B$

2. **Объединением** множеств A и B называется множество $\{\, x \mid x \in A \text{ или } x \in B \,\}$

   Обозначение. $A \cup B$

3. **Разностью** множеств A и B называется множество $\{\, x \mid x \in A \text{ и } x \notin B \,\}$

   Обозначение. $A \setminus B$

4. Предположим, что все рассматриваемые множества являются подмножествами некоторого универсального множества $\mathbb{U}$. Тогда множество $\mathbb{U} \setminus A$ называется **дополнением** A

   Обозначение. $\overline{A}$

5. **Симметрической разностью** множеств A и B называется множество $(A \setminus B) \cup (B \setminus A)$

   Обозначение. $A \triangle B$

Порядок действий.

1. Дополнение
2. Пересечение
3. Объединение, разность, симметрическая разность

Свойства.

1. Дистрибутивность

   (a) $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$

   Доказательство.

   - Докажем, что $(A \cap B) \cup C \subset (A \cup C) \cap (B \cup C)$:
     Пусть $x \in (A \cap B) \cup C$. Тогда выполнено хотя бы одно из условий:
     i. $x \in A \cap B \implies \begin{Bmatrix} x \in A \\ x \in B \end{Bmatrix} \implies \begin{Bmatrix} x \in A \cup C \\ x \in B \cup C \end{Bmatrix} \implies x \in (A \cup C) \cap (B \cup C)$
     ii. $x \in C \implies \begin{Bmatrix} x \in A \cup C \\ x \in B \cup C \end{Bmatrix} \implies x \in (A \cup C) \cap (B \cup C)$
   - Докажем, что $(A \cup C) \cap (B \cup C) \subset (A \cap B) \cup C$:
     Пусть $x \in (A \cup C) \cap (B \cup C)$. Тогда $\begin{cases} x \in A \cup C \\ x \in B \cup C \end{cases}$
     Рассмотрим два случая:
     i. $x \in C \implies x \in (A \cap B) \cup C$
     ii. $x \notin C$:

$$\left.\begin{matrix} x \in A \cup C \implies x \in A \\ x \in B \cup C \implies x \in B \end{matrix}\right\} \implies x \in A \cap B \implies x \in (A \cap B) \cup C$$

$\square$

   (b) $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$

Доказательство.

- Докажем, что $(A \cup B) \cap C \subset (A \cap C) \cup (B \cap C)$:
  Пусть $x \in (A \cup B) \cap C$. Тогда $x \in C$ и выполнено хотя бы одно из условий:
  i. $x \in A \implies x \in A \cap C$
  ii. $x \in B \implies x \in B \cap C$
  В обоих случаях, $x \in (A \cap C) \cup (B \cap C)$
- Докажем, что $(A \cap C) \cup (B \cap C) \subset (A \cup B) \cap C$: Пусть $x \in (A \cap C) \cup (B \cap C)$. Тогда выполнено хотя бы одно из условий:
  i. $\begin{cases} x \in A \\ x \in C \end{cases}$
  ii. $\begin{cases} x \in B \\ x \in C \end{cases}$
  В обоих случаях, $x \in C$. Кроме того, выполнено $x \in A$ или $x \in B$, а значит, $x \in A \cup B \implies x \in (A \cup C) \cap (A \cup B)$

$\square$

2. Законы де-Моргана:
   (a) $\overline{A \cup B} = \overline{A} \cap \overline{B}$

   Доказательство. $x \in \overline{A \cup B} \iff x \notin (A \cup B) \iff \begin{Bmatrix} x \notin A \\ x \notin B \end{Bmatrix} \iff \begin{Bmatrix} x \in \overline{A} \\ x \in \overline{B} \end{Bmatrix} \iff x \in \overline{A} \cap \overline{B}$ $\square$

   (b) $\overline{A \cap B} = \overline{A} \cup \overline{B}$

   Доказательство. $x \in \overline{A \cap B} \iff x \in (A \cap B) \iff \begin{bmatrix} x \notin A \\ x \notin B \end{bmatrix}\} \iff [\begin{matrix} x \in \overline{A} \\ x \in \overline{B} \end{matrix}\} \iff x \in \overline{A} \cup \overline{B}$ $\square$

Определение 3. Прямым, или декартовым произведением множеств A и B называется множество, состоящее из всех упорядоченных пар (a, b), де $a \in A, b \in B$

Обозначение. $A \times B$

Обозначение. Между множествами $(A \times B) \times C$ и $A \times (B \times C)$ есть взаимно однозначное соответствие. Для таких множеств часто используется обозначение $A \times B \times C$

Обозначение. Множество $\underbrace{A \times A \times ... \times A}_{n}$ обозначается A^n

2. Отображения

Определение 4. Отображением, или функцией из множества X в множество Y называется правило, которое каждому элементу множества X сопоставляет ровно один элемент из множества Y
Множество X называется областью определения, множество Y – областью значений

Определение 5. Образом отображения f называется множество элементов вида $f(x)$

Обозначение. $\operatorname{Im} f, f(X)$

То есть, $\operatorname{Im} f = \{\, f(x) \mid x \in X \,\}$

Определение 6. Прообразом элемента $y \in Y$ называется множество элементов $x \in X$, которые при этом отображении переходят в y

Обозначение. $f^{-1}(y)$

То есть, $f^{-1}(y) = \{\, x \in X \mid f(x) = y \,\}$
Можно рассматривать прообраз любого подмножества образа: если $Y_1 \subset Y$, то

$$f^{-1}(y) = \{\, x \in X \mid \exists\, y \in Y_1 : f(x) = y \,\}$$

Определение 7. Отображение $f : X \to Y$ называется сюръективным, если прообраз любого элемента $y \in Y$ содержит хотя бы один элемент

Определение 8. Отображение $f : X \to Y$ называется инъективным, если прообраз любого элемента $y \in Y$ содержит не более одного элемента

Определение 9. Отображение $f : X \to Y$ называется биективным, если прообраз любого элемента $y \in Y$ содержит ровно один элемент

Примечание. Если отображение f биективно, то оно одновременно инъективно и сюръективно

Определение 10. Тождественным отображением называется такое отображение $e_X : X \to X$, что $e_X(x) = x$ для любого $x \in X$

Определение 11. Пусть для множеств X, Y, Z заданы отображения $f : Y \to Z, g : X \to Y$. Композицией отображений f и g называется отображение $f \circ g : X \to Z$, определённое условием:

$$(f \circ g)(x) = f(g(x))$$

Свойство. Операция композиции ассоциативна, то есть $(f \circ g) \circ h = f \circ (g \circ h)$
Отсюда следует, что можно использвать обозначение $f \circ g \circ h$

Доказательство. $\Big((f \circ g) \circ h\Big)(x) = f\Big(g\big(h(x)\big)\Big) = \Big(f \circ (g \circ h)\Big)(x)$ $\square$

Определение 12. Пусть заданы отображения $f : X \to Y$ и $g : Y \to X$. Отображение g называется обратным к отображению f, если $f \circ g = e_Y, g \circ f = e_X$

Обозначение. f^{-1}

Теорема 1 (существование обратного отображения)**.** Обратное отображение к отображению f существует тогда и только тогда, когда f является биекцией

Доказательство.

- Необходимость
  Докажем, что если $f : X \to Y$ является биекцией, то существует отображение $g : Y \to X$, для которого выполнено $f \circ g = e_Y, g \circ f = e_X$:
  Пусть $y \in Y$
  $$f \text{ – биекция} \implies \exists!\, x \in X : f(x) = y$$
  Положим $g(y) := x$
  Тогда $\begin{cases} \forall x \in X & g(f(x)) = x \\ \forall y \in Y & f(g(y)) = y \end{cases}$

- Достаточность
  Докажем, что если для некоторого отображения $g : Y \to X$ выполнено $f \circ g = e_Y, g \circ f = e_X$, то f является биекцией:
  - Проверим, что f – сюрьекция:
    Пусть $y \in Y$. Тогда $g(y)$ является прообразом y в X для отображения f
  - Проверим, что f – инъекция:
    Пусть $y \in Y$ и x_1, x_2 – различные прообразы y при отображении f. Тогда
    $$x_1 = g(f(x_1)) = f(y) = g(f(x_2)) = x_2 \text{ – } \lightning$$

□

Теорема 2 (единтсвенность обратного отображения). Пусть f – биекция из X в Y. Тогда отображение, обратное к f, единственно. То есть не существует различных отображений g_1 и g_2 из Y в X, таких, что:

$$f \circ g_1 = e_y, \quad g_1 \circ f = e_x, \qquad f \circ g_2 = e_Y, \quad g_2 \circ f = e_X$$

Доказательство. Предположим, что два таких отображения существуют. Тогда существует такой $y \in Y$, то $g_1(y) \neq g_2(y)$. Положим $x_1 := g_1(y), x_2 := g_2(y)$. Тогда:

$$f(x_1) = f(g_1(y)) = y, \qquad f(x_2) = f(g_2(y)) = y$$

Полчили, что у y есть два прообраза. $\lightning$ с инъективностью f □

Примечание. Из этой теоремы следует, что обозначение f^{-1} корректно

3. Отношения на множестве. Отношения эквивалентности и разбиение на классы

Определение 13. Бинарным отношением между X и Y называется подмножетво $X \times Y$

Обозначение. Пусть задано бинарное отношение $\omega \subset X \times Y$. Тогда условие $(x, y) \in \omega$ записывают как $x \; \omega \; y$

Обозначение. Если $Y = X$, то говорят, что задано отношение на X

Примечание. Любое отображение можно считать отношением

Определение 14. Бинарное отношение ω на множестве X называется:

1. Рефлексивным, если для любого x выполнено $x \; \omega \; x$
2. Антирефлексивным, если ни для какого x не выполнено $x \; \omega \; x$
3. Симметричным, если $x \; \omega \; y \implies y \; \omega \; x$
4. Ассиметичным, если ни для каких x, y не выполенено одновременно $x \; \omega \; y$ и $y \; \omega \; x$
5. Антисимметричным, если $x \; \omega \; y$ и $y \; \omega \; x$ выполнены одновременно только при $x = y$
6. Транзитивным, если $x \; \omega \; y, y \; \omega \; z \implies x \; \omega \; z$

Определение 15. Бинарное отношение на множестве X называется отношением эквивалентности, если оно рефлексивно, симметрично и транзитивно

Определение 16. Предположим, что на множестве X задано отношение эквивалентности $\sim$. Классом эквивалентности элемента a называется множество элементов, эквивалентных a, то есть $\{ x \in X \mid x \sim a \}$

Теорема 3 (разбиение на классы эквивалентности). Предположим, что на множестве X задано отношение эквивалентности $\sim$. Тогда множество X разбивается на классы эквивалентности.
То есть X является объединением непересекающихся подмножеств, каждое из которых является классом эквивалентности некоторого элемента

Доказательство. Требуется доказать, что:

1. любой элемент множества X принадлежит некоторому классу эквивалентности
   Доказательство. Элемент a принадлежит классу эквивалентности $\overline{a}$, так как по рефлексивности выполнено $a \sim a$ □

2. лобые два класса эквивалентности либо не пересекаются, либо совпадают

Доказательство. Предположим, что два класса эквивалентности $\overline{a}$ и $\overline{b}$ содержат хотя бы один общий элемент x. Докажем, что эти классы совпадают:
Требуется доказать, что $\overline{a} = \overline{b}$. Это равносильно тому, что $\overline{a} \subset \overline{b}$ и $\overline{b} \subset \overline{a}$. Докажем первое включение (второе доказывается аналогично):

$$\left.\begin{aligned} x \in \overline{a} \implies x \sim a \xRightarrow[\text{симметричность}]{} a \sim x \\ x \in \overline{b} \implies x \sim b \end{aligned}\right\} \xRightarrow[\text{транзитивность}]{} a \sim b$$

$$\left.\begin{aligned} y \in \overline{a} \implies y \sim a \\ a \sim b \end{aligned}\right\} \xRightarrow[\text{транзитивность}]{} y \sim b \implies y \in \overline{b}$$

□

□

4. Бинарные операции. Единственность единичного элемента. Определение моноида и полугруппы

Определение 17. Пусть X – множество. Бинарной алгебраической операцией на X называется отображение $X \times X \to X$

Обозначение. Множество X с операцией $*$ обозначается $(X, *)$

Примечание. Можно рассматривать n-арные оперции, то есть отображения $X^n \to X$

Определение 18. Бинарная операция на множестве X называется:

1. Ассоциативной, если $(a * b) * c = a * (b * c)$ для любых $a, b, c \in X$
2. Коммутативной, если $a * b = b * a$ для любых $a, b \in X$

Определение 19. Элемент $e \in X$ называется единичным (нейтральным), если для любого $a \in X$ выполнено $a * e = e * a = a$

Примечание. Если операция обозначена как $+$, нейтральный элемент обозначают как 0

Свойство (единственность единичного элемента)**.** Пусть на множестве X задана бинарная алгебраическая операция $*$. Тогда существует не более одного единичного элемента

Доказательство. Пусть элементы $e_1, e_2 \in X$ таковы, что $e_1 * a = a * e_1 = a$, $e_2 * a = a * e_2 = a$ для любого $a \in X$
Рассмотрим элемент $e_1 * e_2$. Из того, что e_1 – нейтральный, следует, что $e_2 = e_1 * e_2$. Из того, что e_2 – нейтральный, следует, что $e_1 = e_1 * e_2$. Таким образом,

$$e_2 = e_1 * e_2 = e_1$$

□

Определение 20. Полугруппой называется множество с заданной на нём бинарной ассоциативной операцией

Определение 21. Моноидом называется полугруппа, в которой существует нейтральный элемент

5. Группы: примеры, свойство сокращения, изоморфизм

Определение 22. Множество G с бинарной операцией $*$ называется группой, если:

1. операция $*$ ассоциативна
2. существует нейтральный элемент e
3. для любого $a \in G$ существует обратный элемент $a^{-1} \in G$ такой, что $a * a^{-1} = a^{-1} * a = e$

Обозначение. $(G, *)$

Определение 23. Группа $(G, *)$ называется абелевой (коммутативной), если операция $*$ коммутативна

Примеры.

1. $\mathbb{R}^*$: множество $\mathbb{R} \setminus \{0\}$, операция – умножение
   Нейтральный элемент: $e = 1$. Обратный: $a^{-1} = {}^1\!/_a$
2. Аналогично определяется $\mathbb{Q}^*$
   Эти группы абелевы
3. Абелевыми группами по умножению являются множества положительных чисел $\mathbb{R}^*_+$, $\mathbb{Q}^*_+$
4. $\mathbb{R}$ не группа по умножению, нет обратного у 0
5. $\mathbb{Z} \setminus \{0\}$ не группа по умножению, нет обратных (кроме 1)
6. $\mathbb{R}, \mathbb{Q}, \mathbb{Z}$, операция – сложение. Это абелевы группы
7. $\mathbb{N}$ не группа по сложению, нет нейтрального элемента
8. Группа биекций произвольного множества X в себя, операция – композиция
9. Группа движений плоскости, операция – композиция
10. Подмножества произвольного множества, операция – $\triangle$

Свойство (сокращение). Пусть G – группа, $a, b, c \in G$

- Если $ac = bc$, то $a = b$
  Доказательство. $ac = bc \implies (ac)c^{-1} = (bc)c^{-1} \implies a(cc^{-1}) = b(cc^{-1}) \implies ae = be \implies a = b$ □
- Если $ca = cb$, то $a = b$
  Доказательство. Аналогично □

Определение 24. Группы $(G, \cdot)$ и $(H, *)$ называются изоморфными, если существует биекция $f : G \to H$, такая что $\forall x, y \quad f(x \cdot y) = f(x) * f(y)$

Обозначение. $G \cong H$

6. Кольца и поля: определение и примеры

Определение 25. Кольцом называется множество R, на котором заданы операции $+$ и $\cdot$, и выполняются следующие свойства:

1. R – абелева группа по сложению
2. Дистрибутивность: $\forall a, b, c \in R \quad (a + b)c = ac + bc, \quad a(b + c) = ab + ac$

Примеры.

1. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ – кольца

2. $\mathbb{N}$ – не кольцо
3. $m\mathbb{Z}$ (множество целых чисел, делящихся на m) – кольцо
4. Множество многочленов с вещественными (целыми, рациональными) коэффициентами – кольцо

   Обозначение. $\mathbb{R}[x], \mathbb{Z}[x], \mathbb{Q}[x]$

5. Кольцо вычетов по модулю m

   Обозначение. $\mathbb{Z}_m$

Определение 26. Кольцо называется областью целостности, если оно коммутативно, ассоциативно и из равенства $ab = 0$ следует, что $a = 0$ или $b = 0$

Примеры.

1. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ – области целостности
2. $\mathbb{Z}_m$ – область целостности $\iff$ m простое

Определение 27. Кольцо называется полем, если для него выполняются свойства:

1. Ассоциативность умножения
2. Коммутативность умножения
3. Существование нейтрального по умножению
4. Существование обратного по умножению

Примеры.

1. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ – поля
2. $\mathbb{Z}$ – не поле (нет обратных)
3. $\mathbb{Z}_m$ – поле $\iff$ m простое

Примечание. Любое поле является областью целостности

7. Свойства делимости. Существование НОД и НОК

Определение 28. Говорят, что число a делится на число b, если существует такое число c, что $a = bc$

Обозначение. $a \,\vdots\, b$

Свойства.

1. Если a и b делятся на c, то $a + b$ и $a - b$ делятся на c

   Доказательство. Пусть d, e таковы, что $a = dc$, $b = ec$. Тогда $a + b = (d + e)c$, $a - b = (d - e)c$ $\square$

2. Если a делится на b, то ak делится на b для любого k

   Доказательство. Пусть c таково, что $a = bc$. Тогда $ak = (ck)b$ $\square$

3. Транзитивность: если $a \,\vdots\, b$, $b \,\vdots\, c$, то $a \,\vdots\, c$

   Доказательство. Пусть $a = db$, $b = ec$. Тогда $a = (de)c$ $\square$

4. Если a делится на b, то $|a| \geq |b|$ или $a = 0$

Доказательство. Пусть $a = bc$. Тогда $|a| = |b| \cdot |c|$. При этом $|c| \geq 1$ или $c = 0$ □

5. Число 1 является делителем любого числа
6. Число 0 является кратным любого числа

Определение 29. Наибольшим общим делителем чисел $a_1, ..., a_k$ называется наибольшее натуральное число, на которое делятся числа $a_1, ..., a_k$

Обозначение. $\text{НОК}(a_1, ..., a_k)$, $(a_1, ..., a_k)$

Определение 30. Наименьшим общим кратным чисел $a_1, ..., a_k$ называется наибольшее натуральное число, которое делится на числа $a_1, ..., a_k$

Обозначение. $\text{НОК}(a_1, ..., a_k)$, $[a_1, ..., a_k]$

Теорема 4.

1. Для любого набора чисел $a_1, ..., a_k$, в который входит хотя бы одно ненулевое число, существует $\text{НОД}(a_1, ..., a_k)$

   Доказательство. Множество общих натуральных делителей непусто, так как в него входит 1. Оно ограничено сверху числом $|a_i|$, где a_i – ненулевое число. В непустом ограниченном сверху множестве есть наибольший элемент □

2. Для любого набора чисел $a_1, ..., a_k$ в котором ни одно из чисел не равно 0, существует $\text{НОК}(a_1, ..., a_k)$

   Доказательство. Множество общих натуральных кратных непусто, так как в него входит модуль произведения всех чисел. Оно ограничено снизу числом 0. В непустом ограниченном снизу множестве есть наименьший элемент □

8. Теорема о делении с остатком для целых чисел

Теорема 5. Пусть $a \in \mathbb{Z}$, $b \in \mathbb{N}$. Тогда существуют единственные $q, r \in \mathbb{Z}$, такие что $a = bq + r$ и $0 \leq r \leq b - 1$

Доказательство.

- Существование
  Рассмотрим множество $A := \{ a - bx \mid x \in \mathbb{Z} \}$
  Среди его элементов есть неотрицательные: например, при $a \geq 0$ можно взять $a - b \cdot 0$, при $a < 0$ можно взять $a - ba$
  Обозначим через r наименьший неотрицательный элемент множества A, то есть наименьший элемент множества $B = A \cap (\mathbb{N} \cup \{ 0 \})$

  $$r \in A \implies \exists q \in \mathbb{Z} : r = a - bq$$

  Проверим, что эти r и q удовлетворяют условию:

  $$r \in \mathbb{N} \cup \{ 0 \} \implies r \geq 0$$

  Если бы выполнялось $r \geq b$, то элемент $r - b$ тоже принадлежал бы множеству B, однако, r минимальное, занчит $r \leq b - 1$

- Единственность
  Предположми, что $a = bq_1 + r_1 = bq_2 + r_2, \quad 0 \leq r_1, r_2 \leq b - 1$

  $$r_1 - r_2 = b(q_2 - q_1) \implies (r_1 - r_2) \,\vdots\, b \implies \left[\begin{aligned} |r_1 - r_2| &\geq b \\ r_1 - r_2 &= 0 \end{aligned}\right.$$

Первое неравенство не выполняется, так как из неравенств $0 \le r_1, r_2 \le b-1$ следует, что:

$$-(b-1) \le r_1 - r_2 \le b-1$$

□

9. Алгоритм Евклида

Алгоритм. Даны натуральные числа a и b, причём $a \ge b$

1. Если $a \vdots b$, то алгоритм заканчивается, его результат равен b
2. Если $a \not\vdots\, b$, то алгоритм применяется к паре b, r, где r – остаток от деления a на b

Лемма 1. Для любых a, b, k выполнено

$$\text{НОД}\,(a, b) = \text{НОД}\,(a + kb, b)$$

Доказательство. Обозначим через M_1 множество общих делителей a и b, обозначим через M_2 множество общих делителей $a + kb$ и b. Достаточно доказать, что $M_1 = M_2$

- $M_1 \subset M_2$

$$d \in M_1 \implies \left\{\begin{matrix} a \vdots d \\ b \vdots d \implies kb \vdots d \end{matrix}\right\} \implies a + kb \vdots d \implies d \in M_2$$

- $M_2 \subset M_1$

$$d \in M_2 \implies \left\{\begin{matrix} & b \vdots d & \\ a + kb \vdots d \implies \left\{\begin{matrix} kb \vdots d \\ a + kb \vdots d \end{matrix}\right\} \implies (a + kb) - kb \vdots d \implies a \vdots d \end{matrix}\right\} \implies d \in M_1$$

□

Теорема 6 (алгоритм Евклида)**.** Для любых чисел алгоритм Евклида заканчивается за конечное число шагов, и его результат равен НОД

Доказательство.

- Алгоритм заканчивается за конечное количество шагов, так как поледовательность получаемых остатков убывает и ограничена снизу числом 0:

$$b > r_1 > r_2 > \ldots > 0$$

- Шаг 2 алгоритма не меняет НОД:

$$a = bq + r \implies \text{НОД}\,(a, b) = \text{НОД}\,(r, b)$$

- Так как b является делителем a и b, и любой делитель числа b не превосходит b:

$$a \vdots b \implies b = \text{НОД}\,(a, b)$$

□

10. Теорема о линейном представлении НОД

Теорема 7 (линейное представление НОД)**.** Пусть $a, b \in \mathbb{N}$

1. $\exists x, y \in \mathbb{Z} : ax + by = \text{НОД}\,(a, b)$
2. Пусть k – общий делитель a и b. Тогда $\text{НОД}\,(a, b) \vdots k$

Доказательство. Положим $M := \{\, au + bv \mid u, v \in \mathbb{Z} \,\}$
Обозначим через d наименьший положительный элемент M
Обозначим $x, y : d = ax + by$
Докажем, что d – общий делитель a и b, и что для любого общего делителя k чисел a и b выполнено $d \vdots k$. Из этого следует утверждение теоремы

1. Докажем, что $a, b \vdots d$:
   Пусть $a \not\vdots d$. Разделим a на d с остатком:
   $$a = dq + r, \quad 0 < r < d$$
   Тогда:
   $$r = a - dq = a - (ax + by) = a(1 - x) + b(-y) \in M$$
   Получаем, что r – положительный элемент множества M, меньший, чем d – $\lightning$
2. $\left.\begin{matrix} a \vdots k \\ b \vdots k \end{matrix}\right\} \implies \begin{cases} ax \vdots k \\ by \vdots k \end{cases} \implies (ax + by) \vdots k$

□

11. Взаимная простота с произведением

Определение 31. Целые числа a и b называются взаимно простыми, если НОД $(a, b) = 1$

Определение 32. Целые числа $a_1, ..., a_k$ называются взаимно простыми в совокупности, если
$$\text{НОД}\,(a_1, ..., a_k) = 1$$

Определение 33. Целые числа $a_1, ..., a_k$ называются попарно взаимно простыми, если НОД $(a_i, a_j) = 1$ для любых различных i, j

Лемма 2 (линейное представление единицы)**.** Числа a и b взаимно просты $\iff \exists\, x, y : ax + by = 1$

Доказательство.

- $\implies$
  Из теоремы о линейном представлении НОД
- $\impliedby$
  Пусть $d =$ НОД (a, b). Тогда из свойств делимости получаем, что $(ax + by) \vdots d$
  Значит, $1 \vdots d \implies d = 1$

□

Свойство (взаимная простота с произведением)**.** Если каждое из чисел $a_1, ..., a_k$ взаимно просто с b, то $a_1 \cdot ... \cdot a_k$ взаимно просто с b

Доказательство. **Индукция** по k
База. $k = 2$:
Требуется доказать такое утверждение: если a_1 и b взаимно просты, a_2 и b взаимно просты, то $a_1 a_2$ и b взаимно просты
Пусть x_1, x_2, y_1, y_2 таковы, что:
$$a_1 x_1 + b_1 y = 1, \qquad a_2 x_2 + b y_2 = 1$$
Перемножим:
$$a_1 x_1 a_2 x_2 + a_1 x_1 b y_2 + b y_1 a_2 x_2 + b^2 y_1 y_2 = 1$$
$$(a_1 a_2)(x_1 x_2) + b(a_1 x_1 y_2 + y_1 a_2 x_2 + b y_1 y_2) = 1$$

Получили линейное представление единицы через $a_1 a_2$ и b. Значит, по лемме, $a_1 a_2$ и b взаимно просты
Переход. $k \to k+1$:
По индукционному предположению $a_1 \cdot \ldots \cdot a_k$ и b взаимно просты. Применяем утверждение для $k = 2$ к числам $a_1 \cdot \ldots \cdot a_k$ и a_{k+1} □

12. Взаимная простота: связь с делимостью

Свойство (взаимная простота и делимость).

1. Пусть $ab \vdots c$ и пусть числа a c взаимно просты. Тогда $b \vdots c$

   Доказательство. Запишем линейное представление единицы через a и c:

   $$ax + cy = 1$$

   Умножим на b:

   $$bax + bcy = b$$

   В левой части неравенства оба слагаемых делятся на c, значит b делится на c □

2. Пусть $a \vdots b,\ \ a \vdots c$, числа b и c взаимно просты. Тогда $a \vdots bc$

   Доказательство. Пусть $a = bk,\ \ a = cm$
   Запишем линейное представление единицы через b и c:

   $$bx + cy = 1$$

   Умножим на k:

   $$k = bkx + cyk = ax + cyk = cmx + cyk$$

   Подставим в формулу для a:

   $$a = bk = bc(mx + ky) \vdots bc$$

   □

13. Свойство составных чисел. Лемма о существовании простого делителя

Определение 34. Число p навывается простым, если $p > 1$, и у p нет натуральных делителей, кроме 1 и p
Число называется составным, если оно больше 1 и не простое

Обозначение. Будем обозначать множетсво простых чисел буквой $\mathbb{P}$

Свойство. Число a составное $\iff \exists b, c : a = bc, \quad 1 < b, c < a$

Доказательство.

- $\implies$
  Из того, что $a \notin \mathbb{P}$ следует, что у a есть делитель b, такой что $1 < b < a$
  По определению делимости сущетсвует такое c, что $a = bc$. Для $c = \frac{a}{b}$ выполнено $1 < c < a$

- $\impliedby$
  У a есть делитель $b \neq 1, \neq a$, значит, $a \notin \mathbb{P}$

□

Лемма 3 (о существовании простого делителя). У любого натурального числа, большего единицы, существует хотя бы один простой делитель

Доказательство. **Индукция** по n
База. $n = 2$. Простой делитель – 2
Переход. Предположим, что $n > 2$ и для любого k, такого что $1 < k < n$, у k есть простой делитель
Рассмотрим два случая:

- $n \in \mathbb{P}$
  У n есть простой делитель n

- $n \notin \mathbb{P}$
  У n есть делитель k, такой, что $1 < k < n$. По индукционному предположению, у k есть простой делитель p
  Получаем, что $n \mathrel{\vdots} k,\ k \mathrel{\vdots} p \implies n \mathrel{\vdots} p$

□

14. Бесконечность множества простых чисел

Теорема 8 (Евклида). Множество простых чисел бесокнечно

Доказательство. Пусть $p_1, ..., p_k$ – все простые числа
Положим $N = p_1 \cdot ... \cdot p_k + 1$
По лемме, у N есть простой делитель. То есть, $\exists\, i : N \mathrel{\vdots} p_i$. При этом:

$$N - 1 = p_i(p_1 \cdot ... \cdot p_{i-1} \cdot p_{i+1} \cdot ... \cdot p_k) \mathrel{\vdots} p_i$$

Тогда:

$$1 = N - (N - 1) \mathrel{\vdots} p_i$$

Противоречие □

15. Основная теорема арифметики

Теорема 9 (основная теорема арифметики). Любое натуральное число, большее 1, можно представить в виде произведения простых чисел. Такое представление единственно с точностью до порядка сомножиетелей

Доказательство.

- Существование
  Докажем по **индукции**
  База. $n = 2$. Разложение: $2 = 2$
  Переход. Предположим, что все числа, меньшие n, раскладываются на простые множтели. Докажем, что n тоже раскладывается:
  Рассмотим два случая:

  - $n \in \mathbb{P}$. Тогда $n = n$ – разложение на простые
  - $n \notin \mathbb{P}$
    У n есть простой делитель p, причём $p \neq n$
    Тогда $1 < p < n$
    По индукционному предположению, $\frac{n}{p}$ раскладывается на простые множители. Умножим разложение для $\frac{n}{p}$ на p, получим разложение для n

- Единственность
  Пусть n – наименьшее натуральное число, которое можно представить в виде произведения простых разными способами
  Пусть

  $$n = p_1 \cdot ... \cdot p_k, \qquad n = q_1 \cdot ... \cdot q_m$$

  Если $p_i = q_j$ для некоторых i, j, то $\frac{n}{p_i} = \frac{n}{q_j}$ тоже раскладывается на простые множители разными способами. Это противоречит минимальности n

Получаем, что $p_i \neq q_j$ для любых i, j
Рассмотрим p_1. Все числа $q_1, ..., q_m$ взаимно просты с p_1, так как делители любого q_j – это 1 и q_j, делители p_1 – это 1 и p_1, общий делитель – только 1
По свойству взаимно простых чисел, произведение $q_1 \cdot ... \cdot q_m$ взаимно просто с p_1. Но, при этом, оно равно n, и следовательно, делится на p_1

□

Следствие. Если произведение нескольких чисел делится на простое число p, то хотя бы один из сомножителей делится на p

16. Сравнения и их свойства

Определение 35. Пусть m – натуральное число. Числа a и b называются сравнимыми по модулю m, если $a - b \,\vdots\, m$

Обозначение. $a \equiv b(\mod m), \quad a \underset{m}{\equiv} b$

Теорема 10. Отношение $\underset{m}{\equiv}$ является отношением эквивалентности

Доказательство.

- Рефлексивность: $a - a = 0 \,\vdots\, m$
- Симметричность: $a - b \,\vdots\, m \implies b - a = -(a - b) \,\vdots\, m$
- Транзитивность: $a - b \,\vdots\, m,\ b - c \,\vdots\, m \implies a - c = (a - b) + (b - c) \,\vdots\, m$

□

Свойства (арифметические свойства сравнений)**.** Пусть $a \underset{m}{\equiv} b, \quad c \underset{m}{\equiv} d$

- $a + c \underset{m}{\equiv} b + d, \quad a - c \underset{m}{\equiv} b - d$

  Доказательство. $(a \pm c) - (b \pm d) = (a - b) \pm (c - d) \,\vdots\, m$ □

- $ac \underset{m}{\equiv} bd$

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

Свойство (решение линейного сравнения)**.** Пусть $a, b \in \mathbb{Z}, \quad m \in \mathbb{N} \quad (a, m) = 1$. Тогда:

- Сравнение $ax \underset{m}{\equiv} b$ имеет решение

  Доказательство. $(a, m) = 1 \implies \exists \widetilde{x}, \widetilde{y} : a\widetilde{x} + m\widetilde{y} = 1 \implies a\widetilde{x} \underset{m}{\equiv} 1 \underset{\cdot b}{\implies} a(b\widetilde{x}) \underset{m}{\equiv} b \implies x = b\widetilde{x}$ является решением сравнения □

- Если x_1, x_2 – решения, то $x_1 \underset{m}{\equiv} x_2$

  Доказательство.

$$\left.\begin{aligned} ax_1 \underset{m}{\equiv} b \\ ax_2 \underset{m}{\equiv} b \end{aligned}\right\} \implies ax_1 \underset{m}{\equiv} ax_2 \implies \underbrace{a}_{\not\vdots\, m}(x_1 - x_2) \,\vdots\, m \implies x_1 - x_2 \,\vdots\, m \implies x_1 \underset{m}{\equiv} x_2$$

  □

17. Кольцо вычетов

Определение 36. Классами вычетов по модулю m называются классы эквивалентности на $\mathbb{Z}$ по отношению $\underset{m}{\equiv}$

Определение 37. Набор чисел называется полной системой вычетов по модулю m, если в него входит по одному представителю из каждого класса вычетов

Определение 38. $\overline{a} + \overline{b} = \overline{a+b}, \qquad \overline{a}\overline{b} = \overline{ab}$

Теорема 11 (кольцо вычетов). Пусть $m \in \mathbb{N},\ m > 1$. Рассмотрим классы вычетов по модулю m

- Сумма и произведение классов вычетов определены корректно, то есть результат не зависит от выбора представителей классов

  Доказательство (для суммы). Пусть a_1, a_2 – представители одного класса, и b_1, b_2 – другого
  Нужно доказать, что $a_1 + b_1$ и $a_2 + b_2$ принадлежат одному классу
  Применим свойства сравнений:

  $$\left.\begin{array}{l} a_1 \underset{m}{\equiv} a_2 \\ b_1 \underset{m}{\equiv} b_2 \end{array}\right\} \implies a_1 + b_1 \underset{m}{\equiv} a_2 + b_2$$

  □

- Классы вычетов образуют ассоциативное коммутативное кольцо с единицей

  Доказательство.

  – Нейтральный по сложению – $\overline{0}$
  – Нейтральный по умножению – $\overline{1}$
  – Обратный по сложению к $\overline{a}$ – $\overline{(-a)}$

  Все свойства следуют из аналогичных свойств для чисел □

- Кольцо классов вычетов является полем тогда и только тогда, когда $m \in \mathbb{P}$

  Доказательство. Ассоциативное коммутативное кольцо с единицей является полем $\iff$ у любого ненулевого элемента есть обратный по умножению

  – $\Longleftarrow$
  Пусть a – такой элемент что $\overline{a} \neq \overline{0}$. Тогда $a \not\vdots\, m$

  $$\left.\begin{array}{l} m \in \mathbb{P} \\ a \not\vdots\, m \end{array}\right\} \implies (a, m) = 1$$

  По свойству о решении линейного сравнения, существует x, такой, что $ax \underset{m}{\equiv} 1$. Тогда $\overline{a} \cdot \overline{x} = 1$, класс $\overline{x}$ является обратным к $\overline{a}$ по умножению

  – $\implies$
  Пусть $m \notin \mathbb{P}$, $m = ab$, $a, b > 1$
  Докажем, что у класса $\overline{a}$ нет обратного. Пусть есть, $\overline{x} = (\overline{a})^{-1}$. Тогда

  $$\overline{b} = \overline{1} \cdot \overline{b} = \overline{xa} \cdot \overline{b} = \overline{xm} = \overline{0}$$

  Но $b \not\vdots\, m$ – $\lightning$

  □

18. Теорема Вильсона, малая теорема Ферма

Теорема 12 (Вильсона). $p \in \mathbb{P} \implies (p-1)! \underset{p}{\equiv} -1$

Доказательство.

- $p = 2$
  Подставим: $1! \underset{p}{\equiv} -1$, верно

- $p > 2$
  Докажем, что равенство $x = x^{-1}$ выполнено только для $x = 1$ и $x = p - 1$:
  Преобразуем формулы, и учтём, что поле является областью целостности:

$$x = x^{-1} \iff x \cdot x = x - 1 \cdot x \iff x^2 = 1 \iff x^2 - 1 = 0 \iff (x-1)(x+1) = 0 \iff \left[\begin{aligned} x - 1 = 0 \\ x + 1 = 0 \end{aligned}\right.$$

  Получили, что все элементы, кроме 1 и $p - 1$ разбиваются на пары обратных. Следовательно,

$$1 \cdot 2 \cdot \ldots \cdot (p-1) = 1 \cdot (p-1) \cdot (x_1 x_1^{-1}) \cdot (x_2 x_2^{-1}) \cdot \ldots = (p-1) \cdot 1 \cdot 1 \cdot \ldots = p - 1 \underset{p}{\equiv} -1$$

□

Лемма 4. Пусть $p \in \mathbb{P}$
Тогда для любого $a \in \mathbb{Z}_p, a \neq 0$ набор элементов $0 \cdot a, 1 \cdot a, \ldots, (p-1) \cdot a \in \mathbb{Z}_p$ является перестановкой элементов $0, 1, \ldots, (p-1) \in \mathbb{Z}_p$

Другая формулировка. Для любого $a \in \mathbb{Z}, a \not\vdots\, p$ набор чисел $0 \cdot a, 1 \cdot a, \ldots, (p-1) \cdot a \in \mathbb{Z}_p$ является полной системой вычетов по модулю p

Доказательство. Докажем, что все элементы $0 \cdot a, 1 \cdot 1, \ldots, (p-1) \cdot a \in \mathbb{Z}_p$ различны:
Пусть это не так, и $ax = ay$ для некоторых x, y
Тогда $a(x - y) = 0$
Из того, что $a \neq 0$ и $\mathbb{Z}_p$ – область целостности, следует, что $x - y = 0$, и таким образом, $x = y$
В наборе $0 \cdot a, 1 \cdot a, \ldots, (p-1) \cdot a$ все элементы различны, их количество равно p. Следовательно, это все элементы $\mathbb{Z}_p$ □

Теорема 13 (малая теорема Ферма)**.** $p \in \mathbb{P}, \quad a \not\vdots\, p \implies a^{p-1} \underset{p}{\equiv} 1$

Доказательство. Рассмотрим кольцо $\mathbb{Z}_p$
По лемме, совпадают наборы элементов $0 \cdot a, 1 \cdot a, \ldots, (p-1) \cdot a$ и $0, 1, \ldots, (p-1)$
Уберём из каждого набора 0 и перемножим
Получим, что в $\mathbb{Z}_p$ выполнено равенство

$$(1 \cdot a)(2 \cdot a)\ldots\Big((p-1) \cdot a\Big) = 1 \cdot 2 \cdot \ldots \cdot (p-1)$$

Поделим обе части на $1 \cdot 2 \cdot \ldots \cdot (p-1)$, получим, что $a^{p-1} = 1$ в $\mathbb{Z}_p$ □

19. Китайская теорема об остатках

Теорема 14 (китайская теорема об остатках для двух сравнений)**.** Пусть m и n взаимно просты
Тогда для любых a и b существует решение системы

$$\begin{cases} x \underset{m}{\equiv} a \\ x \underset{n}{\equiv} b \end{cases}$$

Если x_1, x_2 – два решения системы, то $x_1 \underset{mn}{\equiv} x_2$

Другая формулировка. Если a и b независимо друг от друга пробегают полные системы вычетов по модулям m и n, то x пробегает полную систему вычетов по модулю mn

Доказательство.

- Существование решения
  Положим $X = \{0, 1, ..., mn-1\}$, $M = \{0, 1, ..., m-1\}$, $N = \{0, 1, ..., n-1\}$, $Y = M \times N$
  Построим оотображение $f : X \to Y$ по правилу: $f(x) = (r_m, r_n)$, где r_m и r_n – остатки x от деления на m и n соответственно

  – Докажем, что f – инъекция:
    Пусть
    $$f(x) = (r_m, r_n), \qquad f(x') = (r_m, r_n)$$
    Тогда
    $$\left.\begin{array}{l} x \underset{m}{\equiv} r_m \underset{m}{\equiv} x' \\ x \underset{n}{\equiv} r_n \underset{n}{\equiv} x' \end{array}\right\} \implies \begin{Bmatrix} x - x' \vdots m \\ x - x' \vdots n \end{Bmatrix} \implies x - x' \vdots mn \implies x = x'$$
    Получили, что образы разных элементов не могут совпадать

  – Докажем, что f – биекция:
    Мощности множеств X и Y равны:
    $$|X| = mn, \qquad |Y| = |M| \cdot |N| = mn$$
    Мощность $\mathrm{Im}(f)$ равна мощности X, так как f – инъекция. Следовательно, $\mathrm{Im}(f) = Y$

  Из того, что f - биекция, следует, что существует обратное отображение f^{-1}
  Рассмотрим систему. Пусть r_m и r_n – остатки a и b от деления на m и n. Тогда $x = f^{-1}(r_m, r_n)$ – решение системы

- Пусть x_1, x_2 – решения. Тогда
  $$\left.\begin{array}{l} x_1 \underset{m}{\equiv} a \underset{m}{\equiv} x_2 \\ x_1 \underset{n}{\equiv} b \underset{n}{\equiv} x_2 \end{array}\right\} \implies \begin{Bmatrix} x_1 - x_2 \vdots m \\ x_1 - x_2 \vdots n \end{Bmatrix} \implies x_1 - x_2 \vdots mn$$

□

Теорема 15 (китайская теорема об остатках в общем виде)**.** Пусть $m_1, m_2, ..., m_k$ попарно взаимно просты. Тогда для любых $a_1, a_2, ..., a_k$ существует решение системы
$$\begin{cases} x \underset{m_1}{\equiv} a_1 \\ x \underset{m_2}{\equiv} a_2 \\ \cdots\cdots \\ x \underset{m_k}{\equiv} a_k \end{cases}$$
Если x_1, x_2 – два решения системы, то $x_1 - x_2 \vdots m_1 m_2 ... m_k$

Доказательство. **Индукция** по k
База. $k = 2$ – это предыдущая теорема
Переход. $k \to k+1$
Рассмотрим систему
$$\begin{cases} x \underset{m_1}{\equiv} a_1 \\ x \underset{m_2}{\equiv} a_2 \\ \cdots\cdots \\ x \underset{m_k}{\equiv} a_k \\ x \underset{n}{\equiv} b \end{cases}$$
где числа $m_1, ..., m_k, n$ попарно взаимно просты. Положим $m = m_1 \cdot ... \cdot m_k$. Тогда m и n взаимно просты по свойству о взаимной простоте с произведением
Применим индукционное предположение к системе из первых k сравнений. Система имеет решение x_0, и любое другое решение сравнимо с x_0 по модулю m. Следовательно, система из $k+1$ сравнений

равносильна системе
$$\begin{cases} x \underset{m}{\equiv} x_0 \\ x \underset{n}{\equiv} b \end{cases}$$
Применяя КТО для двух сравнений получаем, что эта система имеет решение, и для любых двух решений x_1, x_2 выполнено
$$x_1 - x_2 \vdots mn = m_1 m_2 ... m.n$$
$\square$

20. Группа обратимых элементов. Обратимые элементы в кольце вычетов. Теорема Эйлера

Определение 39. Пусть R – коммутативное кольцо с единицей. Элемент $x \in R$ называется обратимым, если существует x^{-1}, такой что $xx^{-1} = 1$. Элемент x^{-1} называется обратным к x

Обозначение. Множество обратимых элементов обозначается R^*

Примечание. В некоммутативном кольце можно рассматривать левые обратные и правые обратные

Свойство. Пусть R – коммутативное ассоциативное кольцо с единицей. Тогда R^* с операцией умножения является группой

Доказательство.

- Проверим, что R^* замкнуто относительно умножения, то есть
$$x, y \in R^* \implies xy \in R^*$$
Обратным к элементу xy является элемент $y^{-1}x^{-1}$, так как
$$(xy)(y^{-1}x^{-1}) = x(yy^{-1})x^{-1} = x \cdot q \cdot x^{-1} = xx^{-1} = 1$$
- Операция ассоциативна, так как кольцо ассоциативно
- $1 \in R^*$, так как $1 \cdot 1 = 1$, и, следовательно, $1 = q^{-1}$
- Проверим, что для любого $x \in R^*$ выполнено $x^{-1} \in R^*$:
Из равенства $xx^{-1} = 1$ следует, что x является обратным к x^{-1}. Следовательно, x^{-1} обратим

$\square$

Лемма 5 (НОД с вычетом)**.** Рассмотрим вычеты по модулю n. Пусть $a, x \in \mathbb{Z}$ таковы, что $x \in \overline{a}$. Тогда НОД$(x, n) =$ НОД(a, n)

Доказательство. Имеем $x = a + nq$ для некоторого q. По лемме из доказательства алгоритма Евклида выполнено
$$\text{НОД}(a, n) = \text{НОД}(a + qn, n) = \text{НОД}(x, n)$$
$\square$

Определение 40. Вычет $\overline{a}$ по модулю n называется примитивным, если НОД$(a, n) = 1$

Примечание. Из леммы следует, что определение корректно, то есть свойство примитивности не зависит от выбора представителя класса

Теорема 16 (обратимые элементы в кольце вычетов)**.** Множество обратимых элементов кольца $\mathbb{Z}_n$ совпадает с множеством примитивных вычетов

Доказательство. $\overline{a} \in \mathbb{Z}_n$ обратим $\iff \exists \overline{x} \in \mathbb{Z}_n : \overline{a}\overline{x} = \overline{1} \iff \exists x \in \mathbb{Z} : ax \underset{n}{\equiv} 1 \iff \exists x, q \in \mathbb{Z} :$

$ax - nq = 1$
По теореме о линейном представлении НОД последнее уравнение равносильно тому, что $1 \vdots \text{НОД}\,(a, n)$.
Это равносильно тому, что $\text{НОД}\,(a, n) = 1$ $\square$

Определение 41. Количество примитивных вычетов по модулю n обозначается $\varphi(n)$. Функция $\varphi(n)$ называется функцией Эйлера

Теорема 17 (Эйлера). $\text{НОД}\,(a, n) = 1 \implies a^{\varphi(n)} \underset{n}{\equiv} 1$

Доказательство. Положим $k := \varphi(n)$. Нужно доказать, что $\overline{a}^k = \overline{1}$ в $\mathbb{Z}_n$
Пусть $\mathbb{Z}_n^* = \{\,\overline{x_1}, ..., \overline{x_k}\,\}$
Из того, что $(a, n) = 1$ следует, что $\overline{a} \in \mathbb{Z}_n^*$
Элеенты $ax_1, ..., ax_k$ принадлежат $\mathbb{Z}_n^*$ и различны по свойству сокращения в группе. Следовательно, наборы $\overline{x_1}, ..., \overline{x_k}$ и $\overline{ax_1}, ..., \overline{ax_k}$ освпадают с точностью до перестановки
Перемножим и вынесесем из каждого сомножителя $\overline{a}$:

$$\overline{1} \cdot \overline{x_1} \cdot ... \cdot \overline{x_k} = \overline{a^k} \cdot \overline{x_1} ... \overline{x_k}$$

Сократим на $\overline{x_1} ... \overline{x_k}$ и получим, что $\overline{a^k} = \overline{1}$ в $\mathbb{Z}_n$ $\square$

21. Вычисление функции Эйлера

Теорема 18 (мультипликативность функции Эйлера). Если m и n взаимно просты, то

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

Доказательство.

- Пусть $x \in \mathbb{Z}$. Обозначим через r_m и r_n остатки x от деления на m и n соответственно. Докажем, что

$$\text{НОД}\,(x, mn) = 1 \iff \begin{cases} \text{НОД}\,(x, m) = 1 \\ \text{НОД}\,(x, n) = 1 \end{cases}$$

  Числа x и mn взамино просты $\iff$ у x нет общих простых делителей с mn $\iff$ у x нет общих простых делителей, ни с m, ни с n $\iff$ число x взаимно просто и с m, и с n
  По лемме про НОД с вычетом, из этого следует, что

$$\text{НОД}\,(x, mn) = 1 \iff \begin{cases} \text{НОД}\,(r_m, m) = 1 \\ \text{НОД}\,(r_n, n) = 1 \end{cases}$$

- Обозначим через X множество остатков от деления на mn, взаимно простых с mn, через M – множество остатков от деления на m, взаимно простых с m, через N – множество остатков от деления на n, и положим $Y = M \times N$. Тогда

$$|X| = \varphi(mn), \quad |M| = \varphi(m), \quad |N| = \varphi(n), \quad |Y| = \varphi(m) \cdot \varphi(n)$$

  Нужно доказать, что $|X| = |Y|$
  Построим отображение $f : X \to Y$. Пусть $x \in X$ и r_n, r_m – остатки от деления x на m, n. Тогда $(r_n, r_m) \in Y$. Положим $f(x) = (r_n, r_m)$

  – Проверим, что f – инъекция:
    Пусть

$$f(x_1) = \text{НОД}\,(r_n, r_m)\,, \qquad f(x_2) = \text{НОД}\,(r_n, r_n)$$

  Тогда

$$\left.\begin{matrix} x_1 \underset{m}{\equiv} r_m \underset{m}{\equiv} x_2 \\ x_1 \underset{n}{\equiv} r_n \underset{n}{\equiv} x_2 \end{matrix}\right\} \implies \left.\begin{matrix} x_1 - x_2 \vdots m \\ x_1 - x_2 \vdots n \end{matrix}\right\} \implies x_1 - x_2 \vdots mn \implies x_1 = x_2$$

- Проверим, что f – сюръекция:
  Пусть $y \in Y, y = \text{НОД}(r_n, r_m)$
  По КТО существует $x \in \mathbb{Z}$, такой, что $\begin{cases} x \underset{m}{\equiv} r_m \\ x \underset{n}{\equiv} r_n \end{cases}$
  Можно выбрать x так, что выполняется $0 \le x < mn$
  Из того, что r_m, r_n взаимно просты с m, n следует, что x взаимно прост с mn
  Получили, что $x \in X$. Элемент $x \in X$ является проообразом элемента $y \in Y$

Доказано, что f – биекция. Следовательно, $|X| = |Y|$ □

Следствие. Если числа $m_1, ..., m_k$ попарно взаимно просты, то

$$\varphi(m_1 \cdot ... \cdot m_k) = \varphi(m_1) \cdot ... \cdot \varphi(m_k)$$

Лемма 6. $p \in \mathbb{P} \implies \varphi(p^a) = p^a - p^{a-1}$

Доказательство. Множество чисел, взаимно простых с p^a совпадает с множеством чисел, не делящихся на p
Рассмотрим натуральные числа, не превосходящие p^a. Среди них $\frac{1}{p}p^a = p^{a-1}$ делятся на p, остальные $p^a - p^{a-1}$ не делятся на p □

Теорема 19 (формула для функции Эйлера)**.** Пусть $n = p_1^{a_1} \cdot ... \cdot p_k^{a_k}, \quad a_i > 0$. Тогда верны равенства:

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right) \cdot ... \cdot \left(1 - \frac{1}{p_k}\right)$$

$$\varphi(n) = (p_1^{a_1} - p_1^{a_1-1}) \cdot ... \cdot (p_k^{a_k} - p_k^{a_k-1})$$

Доказательство. Докажем вторую формулу (первая получается из неё вынесением всех множителей вида $p_i^{a_i}$):
Числа $p_1^{a_1}, ..., p_k^{a_k}$ попарно взаимно просты, следовательно,

$$\varphi(n) = \varphi(p_1^{a_1}) \cdot ... \cdot \varphi(p_k^{a_k})$$

Применим к каждому сомножителю лемму, получим нужное равенство □

22. Построение поля комплексных чисел. Комплексное сопряжение

Определение 42. Комплексными числами называются пары вещественных чисел
Если $z = (a, b)$, то a и b называются вещественной и мнимой частью z

Обозначение. $a = \operatorname{Re} z, \quad b = \operatorname{Im} z$

Число $(0, 1)$ называется мнимой единицей
Арифметические операции над комплексными числами определяются равенствами:

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$$

$$(a_1, b_1) \cdot (a_2, b_2) = (a_1a_2 - b_1b_2, a_1b_2 + b_1a_2)$$

Обозначение. Множество комплексных чисел обозначается $\mathbb{C}$

Вложение вещественных чисел в комплексные. Пара $(a, 0)$ отождествляется с вещественным числом a. Свойство равенства и арифметические операции для вещественных чисел и для пар $(a, 0)$ согласованы:

$$(a_1, 0) = (a_2, 0) \iff \begin{Bmatrix} a_1 = a_2 \\ 0 = 0 \end{Bmatrix} \iff a_1 = a_2$$

$$(a_1, 0) + (a_2, 0) = (a_1 + a_2, 0 + 0) = (a_1 + a_2, 0)$$

$$(a_1, 0) \cdot (a_2, 0) = (a_1 \cdot a_2 - 0 \cdot 0, a_1 \cdot 0 + 0 \cdot a_2) = (a_1 a_2, 0)$$

Теорема 20 (поле комплексных чисел). Множество $\mathbb{C}$ является полем
При этом, 0 и 1 явлются нейтральными элементами по сложению и умножению
Для $z = (a, b)$ выполнено:

- $-z = (-z, -b)$
- если $z \neq 0$, то $z^{-1} = \left(\frac{a}{a^2+b^2}, -\frac{b}{a^2+b^2}\right)$

То есть, выполнены следующие свойства:

1. Коммутативность сложения: $z_1 + z_2 = z_2 + z_1$

   Доказательство. $(a_1, b_1)+(a_2, b_2) = (a_1+a_2, b_1+b_2) = (a_2+a_1, b_2+b_1) = (a_2, b_2)+(a_1, b_1)$ □

2. Ассоциативность сложения: $(z_1 + z_2) + z_3 = z_1 + (z_2 + z_3)$
3. Нейтральный элемент по сложению: $z + 0 = z$
4. Обратный элемент по сложению: $(a, b) + (-a, -b) = 0$
5. Дистрибутивность: $z_1(z_2 + z_3) = z_1 z_2 + z_1 z_3, \quad (z_1 + z_2) z_3 = z_1 z_3 + z_2 z_3$
6. Коммутативность умножения: $z_1 z_2 = z_2 z_1$
7. Ассоциативность умножения: $(z_1 z_2) z_3 = z_1 (z_2 z_3)$
8. Нейтральный элемент по умножению: $z \cdot 1 = z$
9. Обратный элемент по умножению: $(a, b) \cdot \left(\frac{a}{a^2+b^2}, -\frac{b}{a^2+b^2}\right) = (1, 0)$

Алгебраическая запись комплексного числа. Комплексное число (a, b) записывается как $a + bi$.
В частности, $i = (0, 1)$
Знак "+" соответствует сложению в $\mathbb{C}$

Определение 43. Пусть $z = a + bi$. Число $a - bi$ называется сопряжённым к z

Обозначение. $\overline{z}$

Свойства.

1. (a) $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$

   Доказательство. Пусть $z_1 = a_1 + b_1 i, \quad z_2 + a2 + b_2 i$. Тогда

   $$\overline{z_1} = a_1 - b_1 i, \qquad \overline{z_2} = a_2 - b_2 i$$

   $$z_1 + z_2 = (a_1 + a_2) + (b_! + b_2)i, \qquad \overline{z_1 + z_2} = (a_1 + a_2) - (b_1 + b_2)i$$
   $$\overline{z_1} + \overline{z_2} = (a_1 + a_2) - (b_1 + b_2)i$$

   □

   (b) $\overline{z_1 z_2} = \overline{z_1} \cdot \overline{z_2}$

   Доказательство. Пусть $z_1 = a_1 + b_1 i, \quad z_2 + a2 + b_2 i$. Тогда

   $$\overline{z_1} = a_1 - b_1 i, \qquad \overline{z_2} = a_2 - b_2 i$$

   $$z_1 z_2 = (a_1 a_2 - b_1 b_2) + (a_1 b_2 + b_1 a_2)i, \qquad \overline{z_1 z_2} = (a_1 + a_2) - (b_1 + b_2)i$$
   $$\overline{z_1} \cdot \overline{z_2} = (a_1 a_2 - (-b_1)(-b_2)) + (a_1(-b_2) + (-b_1)a_2)i = (a_1 a_2 - b_1 b_2) - (a_1 b_2 + b_1 a_2)i$$

   □

2. $z + \overline{z} \in \mathbb{R}, \quad z \cdot \overline{z} \in \mathbb{R}$ для любого $z \in \mathbb{C}$

Причём, при $z \neq 0$ выполнено $z \cdot \overline{z} > 0$

Доказательство. Пусть $z = a + bi$. Тогда $z + \overline{z} = 2a, \quad z \cdot \overline{z} = a^2 - (bi)^2 = a^2 + b^2$ ☐

23. Комплексная плоскость. Свойства модуля

Изображение комплексных чисел на плоскости. На плоскости задана система координат, оси называются вещественной и мнимой, и обозначаются Re и Im
Комплексное число $z = a + bi$ изображается точкой с координатами (a, b)

Определение 44. Модулем комплексного числа называется расстояние от 0 до точки, изображающей это число

Обозначение. $|z|$

Определение 45. Аргументом ненулевого комплексного числа называется угол между направлением оси Re и направлением на точку, изображающую это комплексное число
Аргумент определён с точностью до 2π, то есть аргумент – это класс эквивалентности по отношению

$$x \sim y \iff x - y = 2\pi k, \quad k \in \mathbb{Z}$$

Обозначение. $\arg(z)$

Примечание. Модуль и аргумент – полярные координаты соответствующей точки

Свойства.

1. $|z|^2 = (\operatorname{Re} z)^2 + (\operatorname{Im} z)^2$

   Доказательство. Следует из формулы расстояния между точками на плоскости ☐

2. $|z| = |-z| = |\overline{z}|$

   Доказательство. Пусть $z = x + yi$. Тогда $-z = (-z) + (-y)i, \quad \overline{z} = x + (-y)i$. Подставим в предыдущий пункт, получим, что все три модуля равны $\sqrt{x^2 + y^2}$ ☐

24. Неравенство треугольника

Теорема 21 (неравенство треугольника)**.** Для любых комплексных чисел $z_1, \dots, z_n$ выполнено

$$|z_1 + \dots + z_n| \leq |z_1| + \dots + |z_n|$$

Доказательство. **Индукция** по n
База. $n = 2$
Пусть $z_1 = a + bi, \quad z_2 = c + di$. Тогда

$$z_1 + z_2 = (a + c) + (b + d)i, \qquad |z_1| = \sqrt{a^2 + b^2}, \qquad |z_2| = \sqrt{c^2 + d^2}, \qquad |z_1 + z_2| = \sqrt{(a + c)^2 + (b + d)^2}$$

Требуется доказать, что для любых вещественных чисел a, b, c, d выполнено неравенство

$$\sqrt{(a + c)^2 + (b + d)^2} \leq \sqrt{a^2 + b^2} + \sqrt{c^2 + d^2}$$

Возведём в квадрат:

$$(a + c)^2 + (b + d)^2 \leq a^2 + b^2 + 2\sqrt{a^2 + b^2}\sqrt{c^2 + d^2}$$

$$a^2 + 2ac + c^2 + b^2 + 2bd + d^2 \leq a^2 + b^2 + 2\sqrt{a^2 + b^2}\sqrt{c^2 + d^2}$$

$$2ac + 2bd \leq 2\sqrt{a^2 + b^2}\sqrt{c^2 + d^2}$$

$$ac + bd \leq \sqrt{a^2+b^2}\sqrt{c^2+d^2}$$

Возведём в квадрат:

$$a^2c^2 + 2abcd + b^2d^2 \leq (a^2+b^2)(c^2+d^2)$$
$$a^2c^2 + 2abcd + b^2d^2 \leq a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2$$
$$0 \leq a^2d^2 - 2abcd + b^2c^2$$
$$0 \leq (ad-bc)^2$$

Это верно всегда

Переход. $n \to n+1$

Положим $z' = z_1 + ... + z_n$. Тогда по индукционному предположению выполнено

$$|z'| \leq |z_1| + ... + |z_n|$$

$$|z_1 + ... + z_n + z_{n+1}| = |z' + z_{n+1}| \leq |z'| + |z_{n+1}| \leq |z_n| + ... + |z_n| + |z_{n+1}|$$

□

Следствие.

- $|z_1 - z_2| \leq |z_1| + |z_2|$

  Доказательство. Применим неравенство треугольника к z_1 и $-z_2$ и учтём, что $|-z_2| = |z_2|$ □

- $|z_1 - z_2| \leq |z_1| - |z_2|$

  Доказательство. Имеем $|z_1| = |(z_1 - z_2) + z_2| \leq |z_1 - z_2| + |z_2|$ □

- $|z_1 + z_2| \leq |z_1| - |z_2|$

  Доказательство. Получается из предыдущего пункта заменой z_2 на $-z_2$ □

25. Тригонометрическая форма комплексного числа. Умножение и деление

Теорема 22 (тригонометрическая форма)**.** Пусть $z \in \mathbb{C}, \quad z \neq 0$

1. Пусть $x = \operatorname{Re} z, \quad y = \operatorname{Im} z, \quad r = |z|, \quad \varphi = \arg(z)$. Тогда

$$r = \sqrt{x^2+y^2}, \qquad \cos\varphi = \frac{x}{r}, \qquad \sin\varphi = \frac{y}{r}$$

   Доказательство. Первая формула следует из формулы расстояния между точками на плоскости, вторая и третья – из определения синуса и косинуса и подобия треугольников □

2. Пусть $\varphi = \arg(z), \quad r = |z|$. Тогда

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

   Доказательство. Положим $x := \operatorname{Re} x, \quad y := \operatorname{Im} z$. Тогда из предыдущего пункта следует что $x = r\cos\varphi, \quad y = r\sin\varphi$. Подставим:

$$r(\cos\varphi + i\sin\varphi) = r\cos\varphi + ir\sin\varphi = x + iy = z$$

   □

3. Пусть для некоторых $r, \varphi \in \mathbb{R}, \quad r > 0$ выполнено

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

Тогда $r = |z|, \quad \varphi = \arg(z)$

Доказательство. Положим $x := \operatorname{Re} z, \quad y := \operatorname{Im} z$
Приравняем и раскроем скобки:

$$x + yi = z = r\cos\varphi + ir\sin\varphi \implies \begin{cases} x = r\cos\varphi \\ y = r\sin\varphi \end{cases}$$

Пусть $\rho = |z|, \quad \psi = \arg(z)$. Тогда из первого пункта следует, что $x = \rho\cos\psi, \quad y = \rho\sin\psi$
Проверим, что $r = \rho$:

$$r = \sqrt{r^2} = \sqrt{r^2\cos^2\varphi + r^2\sin^2\varphi} = \sqrt{x^2 + y^2} = \sqrt{\rho^2\cos^2\psi + \rho^2\sin^2\psi} = \sqrt{\rho^2} = \rho$$

Получили, что

$$\left.\begin{aligned} x = \rho\cos\varphi \\ x = \rho\cos\psi \end{aligned}\right\} \implies \cos\varphi = \cos\psi$$

Следовательно, φ и ψ совпадают с точностью до $2\pi k$ □

Определение 46. Тригонометрической формой числа $z \in \mathbb{C}, \quad z \neq 0$ называется запись

$$z = r(\cos\varphi + i\sin\varphi), \qquad r = |z|, \quad \varphi = \arg z$$

Теорема 23 (умножение комплексных чисел в тригонометрической форме)**.** При умножении комплексных чисел их модули перемножаются, аргументы – складываются
То есть для любых комплексных чисел $z_1, ..., z_n$, не равных 0, выполнено

$$|z_1 \cdot ... \cdot z_n| = |z_1| \cdot ... \cdot |z_n|$$

$$\arg(z_1 \cdot ... \cdot z_n) = \arg(z_1) + ... + \arg(z_n)$$

Доказательство. **Индукция** по n
База. $n = 2$
Пусть $z_1 = r_1(\cos\varphi_1 + i\sin\varphi_1), \quad z_2 = r_2(\cos\varphi_2 + i\sin\varphi_2)$. Тогда

$$\begin{aligned} z_1 z_2 &= r_1 r_2(\cos\varphi_1 + i\sin\varphi_1)(\cos\varphi_2 + i\sin\varphi_2) = \\ &= r_1 r_2\Big((\cos\varphi_1\cos\varphi_2 - \sin\varphi_1\sin\varphi_2) + i(\cos\varphi_1\sin\varphi_2 + \sin\varphi_1\cos\varphi_2)\Big) = \\ &= (r_1 r_2)\Big(\cos(\varphi_1 + \varphi_2) + i\sin(\varphi_1 + \varphi_2)\Big) \end{aligned}$$

Переход. $n \to n + 1$
Пусть $z' = z_1 z_2 ... z_n$
По индукционному предположению, выполнено

$$|z'| = |z_1| \cdot ... \cdot |z_n|, \qquad \arg z' = \arg(z_1) + ... + \arg(z_n)$$

Применяя утверждение для $n = 2$ к z' и z_n, получаем нужные равенства □

Следствие (тригонометрическая форма обратного числа)**.** Для любого $z \neq 0$ выполнено

$$|z^{-1}| = |z|^{-1}, \qquad \arg z^{-1} = -\arg z$$

26. Формула Муавра. Корни из комплексных чисел

Теорема 24 (возведение в степень комплексных чисел в тригонометрической форме)**.** Пусть $z \in \mathbb{C}, \quad r = |z|, \quad \varphi = \arg z, \quad n \in \mathbb{Z}$. Тогда

$$z^n = r^n\big(\cos(n\varphi) + i\sin(n\varphi)\big)$$

Доказательство.

- $n = 0$
$$z^0 = 1, \qquad r^0\big(\cos(0\varphi) + i\sin(0\varphi)\big) = 1(1 + i\cdot 0) = 1$$

- $n > 0$
Применим теорему о произведении в тригонометрической форме к $z_1 = z_2 = \ldots = z_n = z$

- $n < 0$
Положим $n_1 = -n, \quad z_1 = z^{-1}$, применим формулу для тригонометрической формы обратного числа и доказанное утверждение для $n_1 > 0$:
$$z^n = z_1^{n_1} = \left(\frac{1}{r}\big(\cos(-\varphi) + i\sin(-\varphi)\big)\right)^{n_1} = \frac{1}{r^{n_1}}\big(\cos(-n_1\varphi) + i\sin(-n_1\varphi)\big) = r^n\big(\cos(n\varphi) + i\sin(n\varphi)\big)$$

□

Следствие (формула Муавра)**.** Пусть $z = \cos\varphi + i\sin\varphi, \quad n \in \mathbb{Z}$. Тогда $z^n = \cos(n\varphi) + i\sin(n\varphi)$

Теорема 25 (извлечение корня в тригонометрической форме)**.** Пусть $a \in \mathbb{C}, \quad a \neq 0, \quad n \in \mathbb{N}$. Тогда уравнение $z^n = a$ имеет n решений
Если $a = r(\cos\varphi + i\sin\varphi)$, то решениями уравнения являются числа вида
$$z_k = r^{1/n}\left(\cos\frac{\varphi + 2\pi k}{n} + i\sin\frac{\varphi + 2\pi k}{n}\right), \qquad k = 0, 1, \ldots, (n-1)$$

Доказательство. Будем искать решение в виде $z = \rho(\cos\psi + i\sin\psi)$
Возведём z в n-ю степень в тригонометрической форме и приравняем к a:
$$\rho^n\big(\cos(n\psi) + i\sin(n\psi)\big) = r(\cos\varphi + i\sin\varphi)$$
Следовательно,
$$\rho^n = r, \qquad n\psi = \varphi + 2\pi k, \qquad k \in \mathbb{Z}$$
Получаем, что корни уравнения имеют вид
$$z_k = r^{1/n}\left(\cos\frac{\varphi + 2\pi k}{n} + i\sin\frac{\varphi + 2\pi k}{n}\right), \qquad k \in \mathbb{Z}$$
Проверим, что при $k = 0, 1, \ldots, (n-1)$ корни z_k различны, и любой другой корень совпадает с одним из этих корней
Модели всех чисел z_k равны. Следовательно,
$$z_k = z_l \iff \arg z_k = \arg z_l \iff \frac{\varphi + 2\pi k}{n} = \frac{\varphi + 2\pi l}{n} + 2\pi m, \quad m \in \mathbb{Z} \iff$$
$$\iff \varphi + 2\pi k = \varphi + 2\pi l + 2\pi mn, \quad m \in \mathbb{Z} \iff k \underset{n}{\equiv} l$$
Следовательно, z_k и z_l совпадают тогда и только тогда, когда k и l принадлежат одному классу вычетов по модулю n □

27. Комплексные корни из единицы. Первообразные корни

Определение 47. Число $\varepsilon \in \mathbb{C}$ называется корнем n-й степени из единицы, если $\varepsilon^n = 1$

Обозначение. Будем обозначать корни из единицы как
$$\varepsilon_k = \cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n}, \qquad k = 0, 1, \ldots, (n-1)$$

Свойства.

1. Корни n-й степени из 1 образуют группу с операцией умножения

   Доказательство.

   - Замкнутость относительно операции:
     Проверим, что если x, y – корни n-й степени из 1, то xy – корень n-й степени из 1:
     $$\left.\begin{matrix} x^n = 1 \\ y^n = 1 \end{matrix}\right\} \implies (xy)^n = x^n y^n = 1 \cdot 1 = 1$$
   - Ассоциативность следует из ассоциативности в $\mathbb{C}$
   - Существование единицы:
     Число 1 является корнем n-й степени из 1, так как $1^n = 1$
   - Существование обратного:
     Проверим, что если x – корень n-й степени из 1, то $\frac{1}{x}$ – корень n-й степени из 1:
     $$\left(\frac{1}{x}\right)^n = \frac{1}{x^n} = \frac{1}{1} = 1$$

   $\square$

2. Пусть $a \in \mathbb{C}, \quad a \neq 0, \quad x$ – некоторый корень n-й степени из a. Тогда $\varepsilon_0 x, ..., \varepsilon_{n-1} x$ – все корни n-й степени из a

   Доказательство.

   - Докажем, что если $y = \varepsilon_i x$, то y – корень n-й степени из a:
     $$y^n = x^n \varepsilon_i^n = a \cdot 1 = a$$
   - Докажем, что если y – корень n-й степени из 1, то $y = \varepsilon_i x$ для некоторого x, то есть $\frac{y}{x}$ является корнем n-й степени из 1:
     $$\left(\frac{y}{x}\right)^n = \frac{y^n}{x^n} = \frac{a}{a} = 1$$

   $\square$

Определение 48. Число $\varepsilon \in \mathbb{C}$ называется первообразным корнем n-й степени из единицы, если $\varepsilon^n = 1$, и $\varepsilon^k \neq 1$ при $1 \leq k < n$

Другое название. Корень, принадлежащий показателю n

Свойства. Рассмотрим корни n-й степени из единицы

1. Корень ε_k является первообразным тогда и только тогда, когда НОД$(k, n) = 1$

   Доказательство. Докажем, что $\varepsilon_k^m = 1 \iff km \,\vdots\, n$:
   Разделим km на n с остатком: пусть $km = nq + r, \quad 0 \leq r < n$. Тогда
   $$\varepsilon_k^m = \left(\cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n}\right)^m = \cos\frac{2\pi km}{n} + i\sin\frac{2\pi km}{n} = \cos\frac{2\pi r}{n} + i\sin\frac{2\pi r}{n}$$
   Правая часть равна 1 тогда и только тогда, когда $r = 0$

   - Пусть НОД$(k, n) = 1$. Тогда из условия $km \,\vdots\, n$ следует, что $m \,\vdots\, n$. Для $1 \leq m < n$ это не выполнено, корень является первообразным
   - Пусть НОД$(k, n) = d > 1$
     Тогда для $m = \frac{n}{d} < n$ выполнено $mk \,\vdots\, n$, корень не является первообразным

   $\square$

2. Пусть ε_k – первообразный корень. Тогда любой корень k-й степени из единицы равен ε_k^m для некоторого m

Доказательство. Числа $\varepsilon_k, \varepsilon_k^2, ..., \varepsilon_k^n$ являются корнями k-й степени из единицы
Докажем, что они различны:
Пусть $\varepsilon_k^m = \varepsilon_k^l, \quad 0 < m < l < k$
Тогда $\varepsilon_k^{l-m} = 1$. Это противоречит тому, что ε_k – первообразный корень □

28. Кольцо многочленов. Переход к стандартной записи

Определение 49. Пусть A – кольцо. Многочленом над кольцом A будем называть последовательность $(a_0, a_1, ...)$, в которой только конечное количество членов отлично от нуля
Пусть $P = (a_0, a_1, ...), Q = (b_0, b_1, ...)$. Суммой $P + Q$ называется многочлен $(c_0, c_1, ...)$, заданный условием $\forall k \quad c_k = a_k + b_k$
Произведением PQ называется многочлен $(d_0, d_1, ...)$, заданный условием

$$\forall k \quad d_k = a_0 b_k + a_1 b_{k-1} + ... + a_{k-1} b_1 + a_k b_0$$

Обозначение. Множество многочленов над кольцом A обозначается $A[x]$

Теорема 26 (кольцо многочленов).

1. Сумма и произведение многочленов определены корректно, то есть в последовательностях $(c_0, c_1, ...)$ и $(d_0, d_1, ...)$ только конечное число членов отлично от нуля

   Доказательство. Пусть N, M таковы, что $\begin{cases} \forall k > N \quad a_k = 0 \\ \forall k > M \quad b_k 0 \end{cases}$
   Тогда:

   - $\forall k > \max\{M, N\} \quad c_k = 0$
   - $\forall k > M + N \quad d_k = 0$, так как в сумме

   $$d_k = a_0 b_k + a_1 b_{k-1} + ... + a_{k-1} b_1 + a_k b_0 = \sum_{i+j=k} a_i b_j$$

   для каждой пары (i, j) выполнено $i > M$ или $j > N$, следовательно, в каждом слагаемом хотя бы один из сомножителей равен 0

   □

2. Множество $A[x]$ является кольцом

Доказательство. Нужно проверить свойства:

- Ассоциативность сложения – следует из ассоциативности в A
- Коммутативность сложения – следует из коммутативности в A
- Нейтральный по сложению:
  Положим $N = (0, 0, ...)$

$$P + N = (a_0, a_1, ...) + (0, 0, ...) = (a_0 + 0, a_1 + 0, ...) = (a_0, a_1, ...) = P$$

- Обратный по сложению – следует из существования обратного по сложению в A
- Дистрибутивность:
  Пусть $P = (a_0, a_1, ...)$, $\quad Q = (b_0, b_1, ...)$, $\quad R = (c_0, c_1, ...)$
  Докажем, что $(P + Q)R = PR + QR$, записав формулу для k-го элемента последовательности:

$$P + Q = (a_0 + b_0, a_1 + b_1, ...)$$

$$(P + Q)R = (..., (a_0 + b_0)c_k + (a_1 + b_1)c_{k-1} + ... + (a_{k-1}b_{k-1})c_1 + (a_k + b_k)c_0, ...)$$

$$PR = (..., a_0c_k + a_1c_{k-1} + ... + a - k - 1c_1 + a_kc_0, ...)$$

$$QR = (..., b_0c_k + b_1c_{k-1} + ... + b_{k-1}c_1 + b_kc_0, ...)$$

$$(P+Q)R = (..., (a_0c_k + a_1c_{k-1} + ... + a_{k-1}c_1 + a_kc_0) + (b_0c_k + b_1c_{k-1} + ... + b_{k-1}c_1 + b_kc_0), ...)$$

$\square$

Обозначение. Пусть $a \in A$. Элемент a отождествляется с многочленом $(a, 0, 0, ...)$

Корректность. Пусть $a, b \in A$. Тогда $a + b$ и ab определены в A и в $A[x]$ одинаково

Обозначение. Положим $x = (0, 1, 0, 0, ...)$

Свойства (переход к стандартной записи)**.** Пусть A – ассоциативное кольцо с единицей

1. Пусть $b \in A$. Тогда для любого $P = (a_0, a_1, ...)$ выполнено $bP = (a_0b, a_1b, ...)$

   Доказательство. Пусть $bP = (c_0, c_1, ...)$. Тогда

$$c_k = ba_k + 0b_{k-1} + 0a_{k-2} + ... = ba_k \quad \forall k$$

   $\square$

2. Для любого $P = (a_0, a_1, ...)$ выполнено $xP = (0, a_0, a_1, ...)$

   Доказательство. Пусть $xP = (c_0, c_1, ...)$. Тогда $c_0 = a_0 \cdot 0 = 0$

$$c_k = 0a_k + 1a_{k-1} + 0a_{k-2} + ... = a_{k-1} \quad \forall k \geq 1$$

   $\square$

3. $x^n = (0, 0, ..., 0, 1, 0, ...)$, где 1 записано на месте с номером n

   Доказательство. Следует из предыдущего пункта $\square$

4. Пусть $P = (a_0, a_1, a_2, ..., a_n, 0, 0, ...)$. Тогда $P = a_0 + a_1x + a_2x^2 + ... + a_nx^n$

   Доказательство. Из первого и третьего пункта слудет, что для $a \in A$ выполнено $ax^n = (0, 0, ..., 0, a, 0, ...)$, где a записано на месте с номером n
   Применим эту формулу к $a_0, a_1x, a_2x^2, ...$ и сложим $\square$

Обозначение. Будем использовать обозначение $P(x) = a_0 + a_1x + a_2x^2 + ... + a_nx^n$

29. Степень многочлена. Многочлены над областью целостности

Определение 50. Пусть $P = (a_0, a_1, ...)$ – многочлен, отличный от нуля. Степенью P называется $\max\{\, k \mid a_k \neq 0 \,\}$

Обозначение. $\deg P$

Если P – нулевой многочлен, полагаем $\deg P = -\infty$

Теорема 27 (многочлены над областью целостности)**.** Пусть A – область целостности. Тогда

1. Для любых многочленов P, Q выполнено $\deg(P+Q) \leq \max\{\, \deg P, \deg Q \,\}$

   Доказательство. Пусть $n = \max\{\, \deg P, \deg Q \,\}, \quad P = (a_0, a_1, ...), \quad Q = (b_0, b_1, ...)$
   При $i > n$ выполнено
   $$\left.\begin{aligned} a_i = 0 \\ b_i = 0 \end{aligned}\right\} \implies a_i + b_i = 0$$
   □

2. Для любых многочленов P, Q выполнено $\deg(PQ) = \deg P + \deg Q$

   Доказательство. Если $P = 0$ или $Q = 0$, то $PQ = 0$. Равенство $-\infty = -\infty + k$, где $k \in \mathbb{Z}$ или $k = -\infty$, верно
   Пусть $P \neq 0, \quad Q \neq 0, \quad \deg P = k, \quad \deg Q = m$
   Докажем, что $PQ \neq 0$ и $\deg(PQ) = k + m$:
   Пусть
   $$P = (a_0, a_1, ...), \qquad Q = (b_0, b_1, ...), \qquad PQ = (c_0, c_1, ...)$$
   Тогда
   $$\left.\begin{aligned} a_k \neq 0 \\ b_m \neq 0 \end{aligned}\right\} \implies a_k b_m \neq 0$$
   $a_i = 0$ при $i > k$, и $b_i = 0$ при $i > m$
   Докажем, что $c_{k+m} \neq 0$:
   $$c_{k+m} = a_0 b_{k+m} + ... + a_k b_m + ... + a_{k+m} b_0 = a_0 \cdot 0 + ... + a_k b_m + 0 \cdot b_0 = a_k b_m \neq 0$$
   Докажем, что $c_n = 0$ при $i > k + m$:
   $$c_n = \sum_{i+j=k+m} a_i b_j$$
   для каждой пары (i, j) выполнено $i > k$ или $j > m$, следовательно, в каждом слагаемом хотя бы один из сомножителей равен 0 □

3. $A[x]$ – область целостности

Доказательство.

- Коммутативность:
  Пусть $P = (a_0, a_1, ...)$, $\quad Q = (b_0, b_1, ...)$, $\quad PQ = (c_0, c_1, ...)$, $\quad QP = (d_0, d_1, ...)$
  $$c_k = \sum_{i+j=k} a_i b_j = \sum_{i+j=k} b_j a_i = d_k$$
- Ассоциативность:
  Пусть $P = (a_0, a_1, ...)$, $\quad Q = (b_0, b_1, ...)$, $\quad R = (c_0, c_1, ...)$
  Пусть $(PQ) = (d_0, d_1, ...)$, $\quad d_k = \sum_{i+j=k} a_i b_j$, и коэффициент многочлена $(PQ)R$ на n-м месте равен
  $$\sum_{k+l=n} d_k c_l = \sum_{k+l=n} \Big(\sum_{i+j=k} a_i b_j \Big) c_l = \sum_{i+j+l=n} a_i b_j c_l$$
  Аналогично доказывается, что соответствующий коэффициент многочлена $P(QR)$ равен этой же сумме
- Из второго пункта следует, что произведение ненулевых многочленов – ненулевой многочлен

□

30. Деление с остатком для многочленов. Теорема Безу

Определение 51. Пусть K – поле, $F(x), G(x) \in K[x]$, $\quad G(x) \neq 0$. Если для многочленов $Q(x)$ и $R(x)$ выполнено
$$F(x) = Q(x)G(x) + R(x), \qquad \deg R < \deg G$$
то $Q(x)$ и $R(x)$ называются неполным частным и остатком от деления $F(x)$ на $G(x)$

Теорема 28 (деление многочленов с остатком)**.** Пусть K – поле, $F(x), G(x) \in K[x]$, $\quad G(x) \neq 0$
Тогда существуют единственные многочлены $Q(x)$ и $R(x)$, для которых выполнено
$$F(x) = Q(x)G(x) + R(x), \qquad \deg R < \deg G$$

Доказательство.

- Существование
  Положим
  $$A = \{\, F(x) - T(x)G(x) \mid T(x) - \text{многочлен} \,\}$$
  В множестве A выберем многочлен наименьшей степени. Обозначим его через $R(x)$, и обозначим через $Q(x)$ таком многочлен, что $R(x) = F(x) - Q(x)G(x)$
  Докажем, что эти многочлены $Q(x)$ и $R(x)$ подходят:
  Равенство $F(x) = Q(x)G(x) + R(x)$ выполнено. Проверим, что $\deg R < \deg G$:
  Пусть это не так.
  Положим $G(x) \coloneqq a_n x^n + ... + a_0$, $\quad R(x) \coloneqq b_m x^m + ... + b_0$, $\quad a_n \neq 0$, $\quad b_m \neq 0$, $\quad m \geq n$
  Положим
  $$R_1(x) = R(x) - \frac{b_m}{a_n} x^{m-n} G(x)$$
  Тогда $R_1(x) \in A$, так как
  $$R_1(x) = F(x) - \left(T(x) + \frac{b_m}{a_n} x^{m-n} \right) G(x)$$
  При этом, $\deg R_1 < \deg R$
  Получили противоречие с тем, что $R(x)$ – многочлен наименьшей степени в множестве A
- Единственность
  Предположим, что
  $$F(x) = Q_1 G(x) + R_1(x), \qquad \deg R_1 < \deg G$$

$$F(x) = Q_2(x)G(x) + R_2(x), \qquad \deg R_2 < \deg G$$

$$Q_1(x) \neq Q_2(x), \qquad R_1(x) \neq R_2$$

Приравняем формулы для $F(x)$:

$$Q_1(x)G(x) + R_1(x) = Q_2(x)G(x) + R_2(x)$$

Преобразуем:

$$\Big(Q_1(x) - Q_2(x)\Big)G(x) = R_2(x) - R_1(x)$$

Степени многочленов в левой и правой части должны быть равны. Но, по свойствам степени суммы и произведения многочленов, выполнено

$$\deg\Big((Q_1 - Q_2)G\Big) = \deg(Q_1 - Q_2) + \deg G \geq \deg G$$

$$\deg(R_1 - R_2) \geq \max\{\deg R_1, \deg R_2\} < \deg G$$

Противоречие

□

Теорема 29 (Безу). Пусть K – поле, $F(x) \in K[x]$, и $c \in K$
Тогда остаток от деления многочлена $F(x)$ на $(x - c)$ равен $F(c)$

Доказательство. Остаток от деления – многочлен, степень которого не выше 0, следовательно, это константа
Обозначим остаток через r. Тогда

$$F(x) = Q(x)(x - c) + r$$

Подставив $x = c$, получаем

$$F(c) = Q(c)\underbrace{(c - c)}_{=0} + r$$

□

Следствие. Число c является корнем многочлена $F(x) \iff F(x) \,\vdots\, (x - c)$

Доказательство. Многочлен $F(x)$ делится на двучлен $(x - c)$ тогда и только тогда, когда остаток от деления $F(x)$ на $(x - c)$ равен 0. По теореме Безу, это равносильно тому, что $F(c) = 0$ □

31. Число корней многочлена. Формальное и функциональное равенство многочленов

Теорема 30 (о количестве корней многочлена). Пусть K – поле, $F(x) \in K[x]$, $F(x) \neq 0$. Тогда количество корней многочлена $F(x)$ не превосходит $\deg F$

Доказательство. Докажем, что многочлен $P(x)$ степени n имеет не более n корней:
Индукция по n
База. $n = 0$. Многочлен $P(x)$ – ненулевая константа. У него нет корней
Переход. $n \to n + 1$
Пусть $P(x)$ – многочлен степени $n + 1$
Если у $P(x)$ нет корней, то утверждение верно
Пусть у многочлена $P(x)$ есть корень c. Тогда, по следствию к теореме Безу, выполнено $P(x) = Q(x)(x - c)$ для некоторого многочлена $Q(x)$
По свойству степени произведения, выполнено

$$n + 1 = \deg P = \deg Q + \deg(x - c) = \deg Q + 1$$

следовательно, $\deg Q = n$

По индукционному предположению, у многочлена $Q(x)$ не более n корней
Для любого корня x_0 многочлена $P(x)$ выполнено

$$0 = P(x_0) = (x_0 - c)Q(x_0)$$

Следовательно, x_0 равно c или одному из корней многочлена $Q(x)$. Таким образом, у многочлена $P(x)$ не более $n+1$ корней $\square$

Следствие (формальное и функциональное равенство)**.** Пусть K – бесконечное поле, $F, G \in K[x]$
Если для любого $c \in K$ выполнено $F(c) = G(c)$, то $F = G$, то есть соответсвующие коэффициенты F и G совпадают

Доказательство. Пусть $F \neq G$
Положим $H = F - G$
Тогда H – ненулевой многочлен. Следовательно, H имеет не более $\deg H$ корней. Но $H(c) = 0 \quad \forall c \in k$ $\square$

32. Интерполяционная формула Лагранжа

Теорема 31 (интерполяционная формула Лагранжа)**.** Пусть K – поле
Для любых различных $x_1, ..., x_n \in K$ и любых чисел $y_1, ..., y_n$ существует единственный многочлен $F \in K[x]$, такой, что $\deg F \leq (n-1)$, и $F(x_i) = y_i$ для любого i
Многочлен можно найти по формуле

$$F(x) = L_1(x)y_1 + L_2(x)y_2 + ... + L_n(x)y_n$$

где

$$L_i(x) = \frac{(x - x_1)...(x - x_{i-1})(x - x_{i+1})...(x - x_n)}{(x_i - x_1)...(x_i - x_{i-1})(x_i - x_{i+1})...(x_i - x_n)}$$

Доказательство.

- Существование и формула
  Проверим, что многочлен, заданный формулой, подходит:
  - Оценим степень:
    Для любого i выполнено $\deg L_i(x) = (n-1)$, следовательно, $L_i(x)y_i$ – либо многочлен степени $(n-1)$, либо нулевой многочлен, следовательно

    $$\deg F \leq \max \{ \deg L_1, ..., \deg L_n \} \leq n - 1$$

  - Проверим, что $F(x)$ принимает нужные значения:
    Заметим, что $L_i(x_i) = 1, \quad L_i(x_j) = 0$ при $i \neq j$. Действительно,

    $$L_i(x_i) = \frac{(x_i - x_1)...(x_i - x_{i-1})(x_i - x_{i+1})...(x_i - x_n)}{(x_i - x_1)...(x_i - x_{i-1})(x_i - x_{i+1})...(x_i - x_n)} = 1$$

    а при $i \neq j$, в формуле для $L_i(x_j)$ в числителе есть нулевой сомножитель $(x_j - x_j)$
    Теперь найдём значения $F(x)$ в точках x_i:

    $$F(x_i) = L_1(x_i)y_1 + ... + L_i(x_i)y_i + ... + L_n(x_n) = 0y_1 + ... + 1y_i + ... + 0y_n = y_i$$

- Единтсвенность
  Прдеположим, что для различных многочленов $F(x)$ и $G(x)$ выполнено $\deg F, \deg G \leq (n-1), \quad F(x_i) = G(x_i) = y_i$
  Положим $R(x) = F(x) - G(x)$. Тогда

  $$\deg R \leq \max \{ \deg F, \deg G \} \leq n - 1$$

  и $R(x)$ имеет n корней $x_1, ..., x_n$ – $\lightning$

$\square$

33. Метод интерполяции Ньютона

Алгоритм (метод интерполяции Ньютона). Для данных различных $x_1, ..., x_n$ и произвольных $y_1, ..., y_n$ требуется построить многочлен $F(x)$, такой, что $\deg F \le n-1$ и $F(x_i) = y_i$
Построим последовательно многочлены $L_1(x), ..., L_n(x)$, такие, что $\deg L_k \le k-1, \quad L_k(x_i) = y_i$ при $i \le k$
В качетсве $F(x)$ подойдёт $L_n(x)$

- Многочлен $L_1(x)$ – это константа y_1
- Многочлен $L_k(x)$ определим по формуле

$$L_k(x) = L_{k-1}(x) + A_{k-1} g_{k-1}(x)$$

где

$$g_{k-1}(x) = (x - x_1)...(x - x_{k-1}), \qquad A_{k-1} = \frac{y_k - F_{k-1}(x_k)}{g_{k-1}(x_k)}$$

Теорема 32. Метод интерполяции Ньютона корректно определён, и результат его применения – требуемый многочлен

Доказательство.

- Число A_k корректно определено, так как $g(x_k) \ne 0$
- Неравенство $\deg F_k \le (k-1)$ доказывается по **индукции**:
База. $k = 1$: $\deg F_1 = 0$ или $\deg F_1 = -\infty$
Переход. Имеем $\deg g_{k-1} \le (k-1)$, следовательно, $\deg A_k g_{k-1} = k-1$ или $\deg A_k g_{k-1} = 0$

$$\left.\begin{aligned} &\deg F_{k-1} \le k-2 < k-1 \\ &\deg A_k g_{k-1} \le k-1 \end{aligned}\right\} \implies \deg F_{k-1} + a_k g_{k-1} \le k-2 < k-1$$

При $i < k$ выполнено $g(x_i) = 0$, следовательно,

$$F_k(x_i) = F_{k-1}(x_i) + a_k \cdot 0 = F_k(x_i) = y_i$$

- Равенство $F(x_k) = y_k$ проверяется подстановкой в формулу

□

34. Делимость в области целостности

Свойства.

1. Если a и b делятся на c, то $a+b$ и $a-b$ делятся на c
Доказательство. Пусть d, e таковы, что $a = dc, b = ec$. Тогда $a+b = (d+e)c, a-b = (d-e)c$ □
2. Если a делится на b, то ak делится на b для любого k
Доказательство. Пусть c таково, что $a = bc$. Тогда $ak = (ck)b$ □
3. Транзитивность: если $a \,\vdots\, b, b \,\vdots\, c$, то $a \,\vdots\, c$
Доказательство. Пусть $a = db, b = ec$. Тогда $a = (de)c$ □

Определение 52. Пусть A – область целостности, $a, b \in A$
Элементы $a, b \in A$ называются ассоциированными, если $a \,\vdots\, b$ и $b \,\vdots\, a$

Примеры.

1. Кольцо $\mathbb{Z}$. Числа, ассоциированные с a – это $\pm a$
2. Кольцо $\mathbb{R}[x]$. Многочлены, ассоциированные с $P(x)$ – это $cP(x)$, где c – ненулевое число

Свойства. Пусть A – область целостности с единицей

1. Элементы $a, b \in A$ ассоциированы $\iff \exists\, u : a = bu$ и u – обратимый элемент

   Доказательство.

   - $\implies$
     Пусть $a = bc, \quad b = ad$
     Тогда $ab = (cd)(ab)$, следовательно, $cd = 1$, и c обратим
   - $\impliedby$
     Пусть $a = bu$ и u обратим. Тогда $b = au^{-1}$

   $\square$

2. Пусть $a, b \in A, \quad a \vdots b$, элементы a_1, b_1 ассоциированы с a, b осстветственно. Тогда $a_1 \vdots b_1$

   Доказательство. Пусть $a = bc, \quad a = ua_1, \quad b = wb_1$, и u, w обратимы. Тогда $a_1 = b_1(u^{-1}wc)$ $\square$

Определение 53. Пусть A – область целостности с единицей. Элемент $p \in A$ называется неразложимым (простым), если он необратим, и его нельзя представить в виде $p = ab$, где a, b – необратимые элементы

Определение 54. Пусть K – поле, $A = K[x]$
Неразложимый в A многочлен называется неприводимым над K

Определение 55. Пусть A – область целостности, $a, b \in A$
Элемент $d \in A$ называется НОД(a, b), если $a, b \vdots d$ и для $x \in A$ выполнено $a, b \vdots x \implies d \vdots x$

Определение 56. Элементы a и b называются взаимно простыми, если 1 является НОД(a, b)

Свойства.

1. Если d является НОД(a, b), и d_1 ассоциирован с d, то d_1 является НОД(a, b)

   Доказательство. Свойство делимости сохраняется при замене элементов на ассоциированные. Если $a, b \vdots d$, то $a, b \vdots d_1$; если $d \vdots x$, то $d_1 \vdots x$ $\square$

2. Если d_1, d_2 являются НОД(a, b), то d_1 и d_2 ассоциированы

   Доказательство. Из того, что d_1 является общим делителем, и d_2 является НОД, следует, что $d_2 \vdots d_1$. Аналогично, $d_1 \vdots d_2$ $\square$

Определение 57. Кольцо A называется факториальным, если оно является областью целостности с единицей;
Любой элемент $a \in A \setminus \{0\}$ можно представить в виде произведения $a = up_1 ... p_r$, где u – обратим, p_i неразложимы;
Такое представление единственно с точностью до замены сомножитлей на ассоциированные и их перестановки

35. Евклидовы кольца. НОД в евклидовом кольце

Определение 58. Пусть A – область целостности с единицей. Кольцо A называется евклидовым, если существует отображение

$$\delta : A \setminus \{0\} \to \mathbb{N} \cup \{0\}$$

такое, что

1. $\delta(ab) \geq \delta(a) \quad \forall a, b \in K \setminus \{0\}$
2. для любых $a \in K, \quad b \in K \setminus \{0\}$ сущетсвуют $q, r \in K$, такие, что $a = bq + r$ и выполнено $\delta(r) < \delta(b)$ или $r = 0$

Отображение δ называется евклидовой нормой

Лемма 7. Пусть A – евклидово, δ – евклидова норма, и $a, b \in A \setminus \{0\}$. Тогда

1. если $a \vdots b$, то $\delta(a) \geq \delta(b)$

Доказательство. Существует c такое, что $a = bc$, следовательно,

$$\delta(a) = \delta(bc) \geq \delta(b)$$

□

2. если a и b ассоциированы, то $\delta(a) = \delta(b)$

Доказательство. Из предыдущего пункта следует, что $\delta(a) \geq \delta(b)$ и $\delta(b) \geq \delta(a)$ □

3. если $a = bc$ и c необратим, то $\delta(a) > \delta(b)$

Доказательство. Докажем, что $b \not\vdots a$. Пусть для некоторого d выполнено $b = ad$. Тогда

$$a = bc = (ad)c = a(dc) \implies dc = 1$$

Это противоречит тому, что c не обратим
"Разделим с остатком" b на a: пусть q, r таковы, что $a = bq + r$, и $\delta(r) < \delta(a)$ или $r = 0$
Из того, что $b \vdots a$, следует, что $r \neq 0$. Из того что $a \vdots b$, следует, что

$$r = a - bq \vdots b$$

Следовательно,

$$\delta(a) > \delta(r) \geq \delta(b)$$

□

Теорема 33 (НОД в евклидовом кольце)**.** Пусть A – евклидово кольцо, $a, b \in A$, и $(a, b) \neq (0, 0)$
Тогда

1. Существует НОД(a, b)
2. Пусть d явлется НОД(a, b). Тогда существуют $x, y \in A$, такие, что $ax + by = d$

Доказательство. Положим $M \coloneqq \{ au + bv \mid u, v \in A \}$
Пусть $m \coloneqq \min \{ \delta(c) \mid c \in M, c \neq 0 \}$
Пусть $d_0 \in M$ таков, что $\delta(d_0) = m$, и x_0, y_0 таковы, что $d_0 = ax_0 + by_0$
Докажем, что d_0 – общий делитель a и b
Пусть $a \not\vdots d_0$. Тогда существуют q, r, такие, что

$$a = d_0 q + r, \qquad r \neq 0, \qquad \delta(r) < \delta(d_0)$$

Тогда

$$r = a - d_0 q = a - (ax_0 + by_0) = a(1 - x_0) + b(-y_0) \in M, \qquad \delta(r) < m$$

Получаем противоречие
Докажем, что если k – общий делитель, то $d \vdots k$:

$$\left.\begin{matrix} a \vdots k \\ b \vdots k \end{matrix}\right\} \implies \left\{\begin{matrix} ax_0 \vdots k \\ by_0 \vdots k \end{matrix}\right\} \implies ax + by \vdots k$$

Получили, что d_0 является НОД(a, b), и для него существует линейное представление
Пусть d – произвольный НОД(a, b). Тогда $d = wd_0$ для некоторого обратимого w. Следовательно, $d = a(2x_0) + b(wy_0)$ □

36. Свойства взаимно простых элементов в евклидовом кольце

Свойство (взаимная простота с произведением). Пусть A – евклидово кольцо, $a_1, \ldots, a_k, \quad b \in A$, НОД $(a_i, b) = 1 \quad \forall i$
Тогда $(a_1 \cdot \ldots \cdot a_k, b) = 1$

Доказательство. **Индукция** по k
База. $k = 2$:
Требуется доказать такое утверждение: если a_1 и b взаимно просты, a_2 и b взаимно просты, то $a_1 a_2$ и b взаимно просты
Пусть x_1, x_2, y_1, y_2 таковы, что:

$$a_1 x_1 + b_1 y = 1, \qquad a_2 x_2 + b y_2 = 1$$

Перемножим:

$$a_1 x_1 a_2 x_2 + a_1 x_1 b y_2 + b y_1 a_2 x_2 + b^2 y_1 y_2 = 1$$

$$(a_1 a_2)(x_1 x_2) + b(a_1 x_1 y_2 + y_1 a_2 x_2 + b y_1 y_2) = 1$$

Получили линейное представление единицы через $a_1 a_2$ и b. Значит, по лемме, $a_1 a_2$ и b взаимно просты
Переход. $k \to k + 1$:
По индукционному предположению $a_1 \cdot \ldots \cdot a_k$ и b взаимно просты. Применяем утверждение для $k = 2$ к числам $a_1 \cdot \ldots \cdot a_k$ и a_{k+1} □

Свойство (взаимная простота и делимость). Пусть A – евклидово кольцо, $a, b, c \in A$

1. $\left.\begin{array}{l} ab \,\vdots\, c \\ \text{НОД}\,(a, c) = 1 \end{array}\right\} \implies b \,\vdots\, c$

   Доказательство. Запишем линейное представление единицы через a и c:

   $$ax + cy = 1$$

   Умножим на b:

   $$bax + bcy = b$$

   В левой части неравенства оба слагаемых делятся на c, значит b делится на c □

2. $\left.\begin{array}{l} a \,\vdots\, b \\ a \,\vdots\, c \\ \text{НОД}\,(b, c) = 1 \end{array}\right\} \implies a \,\vdots\, bc$

   Доказательство. Пусть $a = bk, \ \ a = cm$
   Запишем линейное представление единицы через b и c:

   $$bx + cy = 1$$

   Умножим на k:

   $$k = bkx + cyk = ax + cyk = cmx + cyk$$

   Подставим в формулу для a:

   $$a = bk = bc(mx + ky) \,\vdots\, bc$$

   □

37. Факториальность евклидова кольца

Теорема 34. Евклидово кольцо факториально

Доказательство.

- Докажем, что любой ненулевой элемент можно представить в виде произведения неразложимых

элементов и обратимого элемента:
Пусть сущетсвуют элементы, которые нельзя так представить. Выберем из них элемент a, на котором значение δ минимально
Элемент a не является обратимым и не является неразложимым, так как иначе $a = a$ было бы подходящим произведением
Следовательно, существуют такие b, c, что $a = bc$, и b, c не обратимы
Тогда $\delta(b) < \delta(a), \quad \delta(c) < \delta(a)$, и, следовательно, для b, c существуют представления нужного вида:

$$b = up_1 \cdot \ldots \cdot p_k, \qquad c = wq_1 \cdot \ldots \cdot q_m$$

Перемножив их, получим представление для a:

$$a = (uw)p_1 \cdot \ldots \cdot p_k \cdot q_1 \cdot \ldots \cdot q_m$$

Противоречие

- Докажем, что представление единственно с точностью до перестановки сомножителей и замены сомножителей на ассоциированные
Пусть для некоторых элементов представление не единственно, и a – такой элемент с минимальным значением δ. Пусть

$$a = up_1 \cdot \ldots \cdot p_k, \qquad a = wq_1 \cdot \ldots \cdot q_m$$

Из неразложимости p_1 следует, что среди сомножителей второго произведения есть элемент, делящийся на p_1
Это не элемент u, так как иначе оказалось бы, что $q = uu^{-1} \vdots p_1$, а p_1 – не делитель 1
Переставив сомножители, будем считать, что $q_1 \vdots p_1$
Из неразложимости q_1 следует, что q_1 и p_1 ассоциированы, пусть $q_1 = vp_1$. Тогда

$$up_1p_2 \cdot \ldots \cdot p_k = a = (wv)p_1 \cdot q_2 \cdot \ldots \cdot q_m \implies up_2 \cdot \ldots \cdot p_k = (wv) \cdot q_2 \cdot \ldots \cdot q_m$$

Обозначим элемент из последнего равенства через b. Тогда

$$a = p_1 b \implies \delta(b) < \delta(a)$$

Следовательно, представление для b единственно, то есть $k = m$, и, после перестановки сомножителей, p_i ассоциирован с q_i при $i \geq 2$
Для $i = 1$ это уже доказано

$\square$

Следствие. Кольцо многочленов над любым полем факториально

38. Разложение многочлена на неприводимые множители над $\mathbb{R}$ и $\mathbb{C}$

Определение 59. Пусть K – поле, $P \in K[x], c \in K$, и c – корень $P(x)$
Показателем кратности корня c называется такое число $n \in \mathbb{N}$, что $\begin{cases} P(x) \vdots (x-c)^n \\ P(x) \not\vdots (x-c)^{n+1} \end{cases}$
Если показатель кратности равен 1, корень называется простым, если больше 1 – кратным

Теорема 35 (основная теорема алгебры). Любой многочлен с комплексными коэффициентами, отличный от константы, имеет комплексный корень

Без доказательства

Следствие. Многочлен с комплексными коэффициентами степени n имеет ровно n корней с учётом кратности (т. е. корень кратности k учитывается как k корней)
Многочлен можно представить в виде

$$P(x)a(x - x_1)(x - x_2)\ldots(x - x_n)$$

Доказательство. **Индукция** по n
База. $n = 1$ – очевидно
Переход. $n \to n+1$
Нужно доказать для $P(x)$, $\deg P = n+1$
По основной теореме алгебры, P имеет корень. Обозначим его c
По теореме Безу, $P(x) \vdots (x-c)$, то есть $P(x) = (x-c)G(x)$, где $\deg G = \deg P - \deg(x-c) = n$
По индукционному предположению, $G(x)$ имеет n корней $\square$

Лемма 8 (сопряжённые корни вещественного многочлена). Пусть $P(x) \in \mathbb{R}[x]$, и c – корень $P(x)$
Тогда $\overline{c}$ – тоже корень $P(x)$

Доказательство. Пусть $P(x) = \sum a_n x^n$
Тогда $\sum a_n c^n = 0$
$a_n \in \mathbb{R} \implies \overline{a_n} = a_n$
Подставим $\overline{c}$ в $P(x)$:

$$P(\overline{c}) = \sum a_n (\overline{c})^n = \sum \overline{a_n} (\overline{c})^n = \overline{\sum a_n c^n} = \overline{0} = 0$$

$\square$

Теорема 36 (разложение многочлена с вещественными коэффициентами). Пусть $P(x) \in \mathbb{R}[x]$
Тогда $P(x)$ можно представить в виде

$$P(x) = a(x-x_1)(x-x_2)...(x^2+p_1x+q_1)(x^2+p_2x+q_2)...$$

где $x^2 + p_i x + q_i$ – квадратные трёхчлены, не имеющие вещественных корней

Доказательство. Пусть $n = \deg P$
Докажем утверждение **индукцией** по n
База. $n = 0$. Многочлен $P(x)$ – константа
Переход. Пусть утверждение доказано для всех многочленов степени меньше n. Докажем его для многочленов степени n

- У многочлена $P(x)$ есть вещественный корень x_1
  Тогда $P(x) = (x-x_1)Q(x)$, причём $Q(x) \in \mathbb{R}[x]$
  Применим к многочлену $Q(x)$ индукционное предположение, и умножим полученное для $Q(x)$ разложение на $x - x_1$

- У многочлена $P(x)$ нет вещественных корней
  По основной теореме алгебры, у $P(x)$ есть корень $z_1 \in \mathbb{C} \setminus \mathbb{R}$
  Тогда $\overline{z_1}$ – тоже корень $P(x)$ и $\overline{z_1} \neq z_1$
  По теореме Безу, $P(x) = (x-z_1)Q_1(x)$ для некоторого многочлена $Q_1(x)$
  $P(\overline{z_1}) = 0 \implies Q_1(\overline{z_1}) = 0$
  По теореме Безу, $Q_1(x) = (x - \overline{z_1})Q_2(x)$
  Положим $H(x) \coloneqq (x-z_1)(x-\overline{z_1})$
  Тогда $P(x) = H(x)R(x)$

  $$H(x) = x^2 + p_1 x + q_1, \qquad \text{где } p_1 = -(z_1 - \overline{z_1}), \quad q_1 = z_1\overline{z_1}$$

  По лемме, коэффициенты $H(x)$ вещественные
  Следовательно, коэффициенты $R(x)$ вещественные
  Применим к многочлену $R(x)$ индукционное предположение, и умножим полученное для $R(x)$ разложение на $(x^2 + p_1 x + q_1)$

$\square$

Следствие. Пусть $P(x) \in \mathbb{R}[x]$, и c – корень $P(x)$
Тогда показатели кратности корней c и $\overline{c}$ равны

Доказательство. **Индукция** по $\deg P$
Пусть $c \in \mathbb{R} \setminus \mathbb{C}$, пусть $H(x) \coloneqq (x-c)(x-\overline{c})$, и $P(x) \coloneqq H(x)R(x)$

- Если c не является корнем $R(x)$, то c и $\overline{c}$ – корни $P(x)$ кратности 1

- Пусть c – корень $R(x)$ кратности m
  Тогда $\overline{c}$ – тоже корень $R(x)$ кратности m

Следовательно, c и $\overline{c}$ – корни $P(x)$ кратности $m+1$ $\square$

39. Производная многочлена, её свойства

Определение 60. Производной многочлена $P(x) = a_nx^n + a_{n-1}x^{n-1} + ... + a_1x + a_0$ называется многочлен $na_nx^n + (n-1)a_{n-1}x^{n-2} + ... + a_1$

Обозначение. $P'(x)$

Короткая запись. Если $P(x) = \sum_{n\geq 0} a_nx^n$, то $P'(x) = \sum_{n\geq 1} na_nx^{n-1}$

Свойства.

1. Если $P(x)$ – константа, то $P'(x) = 0$
2. Пусть K – поле, $P(x) \in K[x]$, и $P(x)$ не константа. Тогда $\deg P' = \deg P - 1$
3. $\Big(P(x) + Q(x)\Big)' = P'(x) + Q'(x)$

   Доказательство. Пусть $P(x) = \sum_{n\geq 0} a_nx^n, \quad Q(x) = \sum_{n\geq 0} b_nx^n$. Тогда

   $$\Big(P(x) + Q(x)\Big)' = \Big(\sum_{n\geq 0}(a_n + b_n)(x^n)\Big)' = \sum_{n\geq 1} n(a_n + b_n)x^{n-1}$$

   $$P'(x) + Q'(x) = \sum_{n\geq 1} na_nx^{n-1} + \sum_{n\geq 1} nb_nx^{n-1}$$

   $\square$

   Следствие. $\Big(P_1(x) + P_2(x) + ... + P_n(x)\Big)' = P_1'(x) + P_2'(x) + ... + P_n'(x)$

   Доказательство. Выводится **индукцией** из третьего свойства $\square$

4. Если c – константа,то $\Big(cP(x)\Big)' = cP'(x)$

   Доказательство. Пусть $P(x) = \sum_{n\geq 0} a_nx^n$. Тогда

   $$\Big(cP(x)\Big)' = \Big(c\sum_{n\geq 0} a_nx^n\Big)' = \Big(\sum_{n\geq 0} ca_nx^n\Big)' = \sum_{n\geq 1} nca_nx^{n-1}$$

   $$cP'(x) = c\Big(\sum_{n\geq 0} a_nx^n\Big)' = c\sum_{n\geq 1} na_nx^{n-1} = \sum_{n\geq 1} nca_nx^{n-1}$$

   $\square$

5. $\Big(P(x)Q(x)\Big)' = P'(x)Q(x) + P(x)Q'(x)$

Доказательство.

- Сначала докажем равенство для случая, когда $Q(x)$ – одночлен, то есть $Q(x) = bx^k$
Случай $k = 0$ следует из свойств 1 и 4. Считаем, что $k > 0$
Найдём $\Big(P(x)Q(x)\Big)'$:
$$P(x)Q(x) = \sum_{n\geq 0} a_n bx^{n+k}$$
и $n + k > 0$ для любого $n \geq 0$, следовательно,
$$\Big(P(x)Q(x)\Big)' = \sum_{n\geq 0}(n+k)a_n bx^{n+k-1}$$
Найдём $P'(x)Q(x) + P(x)Q'(x)$:
$$P'(x)Q(x) + P(x)Q'(x) = \sum_{n\geq 1} na_n x^{n-1} \cdot bx^k + \sum n \geq 0 a_n x^n \cdot kbx^{k-1} =$$
$$= \sum_{n\geq 1} na_n bx^{n+k-1} + \sum_{n\geq 0} ka_n bx^{n+k-1}$$
Заметим, что, если добавить в первую сумму в правной части слагаемое, соответствующее $n = 0$, то есть $0a_0bx^{-1}$, то сумма не изменится:
$$P'(x)Q(x) + P(x)Q'(x) = \sum_{n\geq 0} na_n bx^{n+k-1} + \sum_{n\geq 0} ka_n bx^{n+k-1} = \sum_{n\geq 0}(n+k)a_n bx^{n+k-1}$$
Равенство для случая $Q(x) = bx^k$ доказано
- Докажем утверждение для произвольного $Q(x)$, пользуясь тем, что оно верно для случая, когда $Q(x)$ является одночленом, и свойством производной суммы:
Представим $Q(x)$ в виде суммы одночленов:
$$Q(x) \coloneqq Q_0(x) + Q_1(x) + \ldots + Q_m(x)$$
где $Q_k(x) = b_k x^k$, Тогда
$$\Big(P(x)Q(x)\Big)' = \Big(\sum P(x)Q_k(x)\Big)' = \sum \Big(P'(x)Q_k(x) + P(x)Q'_k(x)\Big) =$$
$$= \sum P'(x)Q_k(x) + \sum P(x)Q'_k(x) = P'(x)\sum Q_k(x) + P(x)\sum Q'_k(x) =$$
$$= P'(x)Q(x) + P(x)\Big(\sum Q_k(x)\Big)' = P'(x)Q(x) + P(x)Q'(x)$$

□

Следствие.
$$\Big(P_1(x)P_2(x)\ldots P_k(x)\Big)' = P_1(x)P_2(x)\ldots P_k(x) + P_1(x)P'_2(x)\ldots P_k(x) + \ldots + P_1(x)P_2(x)\ldots P'_k(x)$$

Доказательство. **Индукция** по k
База. $k = 2$ – предыдущее свойство
Переход. $k \to k+1$
Положим $Q(x) = P_1(x)P_2(x)...P_k(x)$. Тогда

$$\Big(P_1(x)P_2(x)...P_k(x)P_{k+1}(x)\Big)' = \Big(Q(x)P_{k+1}(x)\Big)' = Q'(x)P_{k+1}(x) + Q(x)P'_{k+1}(x) =$$
$$= \Big(P'_1(x)P_2(x)...P_k(x) + P_1(x)P'_2(x)...P_k(x) + ... + P_1(x)P_2(x)...P'_k(x)\Big)P_{k+1}(x) +$$
$$+ P_1(x)P_2(x)...P_k(x)P'_{k+1}(x) =$$
$$= P'_1(x)P_2(x)...P_k(x)P_{k+1}(x) + P_1(x)P'_2(x)...P_k(x)P_{k+1}(x) + ... +$$
$$+ P_1(x)P_2(x)...P'(x)P_{k+1}(x) + P_1(x)P_2(x)...P_k(x)P'_{k+1}(x)$$

□

6. $\Big(P^k(x)\Big)' = kP'(x)P^{k-1}(x)$

Доказательство. Следует из предыдущего свойства, применённого к

$$P_1(x) = P_2(x) = ... = P_k(x) = P(x)$$

□

Примечание. Производные высших порядков определяются как обычно:

$$P''(x) = \Big(P'(x)\Big)', \quad ..., \quad P^{(k)}(x) = \Big(P^{(k-1)}(x)\Big)'$$

40. Кратные корни и производная

Теорема 37 (кратный корень и производная). K – поле, $P(x) \in K[x]$, и c – корень $P(x)$
Тогда равносильны утверждения:

- c – кратный корень $P(x)$
- $P'(c) = 0$

Доказательство. По теореме Безу, $P(x) = (x-c)Q(x)$ для некоторого $Q(x)$
Применяя теорему Безу к $Q(x)$, получаем, что

$$c \text{ – кратный корень} \iff P(x) \vdots (x-c)^2 \iff Q(x) \vdots (x-c) \iff Q(c) = 0$$

Найдём производную $P(x)$ как производную произведения:

$$P'(x) = (x-c)'Q(x) + (x-c)Q'(x) = 1 \cdot Q(x) + (x-c)Q'(x) = Q(x) + (x-c)Q'(x)$$

Подставим $x = c$:

$$P'(c) = Q(c) + (c-c)Q'(x) = Q(c)$$

Следовательно, $P'(c) = 0 \iff Q(c) = 0$ □

Следствие. Пусть c – корень многочлена $P(x)$, и число n таково, что $P^{(i)}(c) = 0$ при $i \leq n-1$, и $P^{(n)}(c) \neq 0$
Тогда n – показатель кратности корня c

Доказательство. Докажем по **индукции**
База. $n = 1$ – по теореме
Переход.

Положим $P_1(x) = P'(x)$
Тогда $P_1^{(i)}(x) = P^{(i+1)}(x)$ для любого i
Достаточно доказать, что показатель кратности c для $P_1(x)$ на один меньше, чем для $P(x)$
Пусть $P(x) = (x-c)^m Q(x)$, где $Q(x) \not\vdots\, (x-c)$. Тогда

$$P_1(x) = \Big((x-c)^m Q(x)\Big)' = \Big((x-c)^m\Big)' Q(x) + (x-c)^m Q'(x) = k(x-c)'(x-c)^{m-1}Q(x) + (x-c)^m Q'(x) =$$
$$= k(x-c)^{m-1}Q(x) + (x-c)^m Q'(x) = (x-c)^{m-1}\Big(kQ(x) + (x-c)Q'(x)\Big)$$

второй сомножитель не делится на $(x-c)$ □

41. Формула Тейлора

Теорема 38 (формула Тейлора)**.** Пусть $P \in \mathbb{R}[x], \quad \deg P = n$
Тогда для любого $c \in K$ выполнено

$$P(x) = P(c) + \frac{P'(c)}{1!}(x-c) + \frac{P''(c)}{2!}(x-c)^2 + ... + \frac{P^{(n)}(c)}{n!}(x-c)^n$$

Доказательство.

- Докажем, что существуют некоторые $d_0, d_1, ..., d_n$, для которых выполнено

$$P(x) = d_0 + d_1(x-c) + ... + d_n(x-c)^n$$

  Индукция по n
  База. $n \le 0$. Тогда $P(x)$ – константа, $P(x) = d_0$ для некоторого d_0
  Переход. Пусть для всех многочленов степени $(n-1)$ утверждение верно, докажем для многочлена $P(x)$ степени n:
  Поделим $P(x)$ на $(x-c)$ с остатком. Пусть $P(x) = Q(x)(x-c) + r$
  Применим к $Q(x)$ предположение индукции. Пусть $Q(x) = c_0 + c_1(x-c) + ... + c_{n-1}(x-c)^{n-1}$
  Тогда подойдут $d_0 = r, \quad d_i = c_{i-1}$ при $i \ge 1$

- Докажем, что $d_k = \dfrac{P^{(k)}(c)}{k!}$:
  Найдём значение k-й производной в точке c для суммы

$$d_0 + d_1(x-c) + ... + d_n(x-c)^n$$

  Положим $H_i(x) = (x-c)^i$

  – При $i < k$ выполнено $\deg H_i < k$, следовательно, $H_i^{(k)}(x) = 0$
  – При $i \ge k$ выполнено $H_i^{(k)}(x) = k(k-1)...(k-i+1)(x-c)^{k-i}$
    Следовательно,
    * При $i = k$ выполнено

$$H_k^{(k)}(x) = k(k-1)...1(x-c)^0 = k!, \qquad H_k^{(k)}(c) = k!$$

    * При $i > k$ выполнено

$$H_k^{(k)}(c) = k(k-1)...(k-i+1) \cdot 0^{k-i} = 0$$

  Получаем, что $P^{(k)}(c) = d_k k! \implies d_k = \dfrac{p^{(k)}(c)}{k!}$

□

42. Построение поля частных: леммы о классах эквивалентности

Обозначение. Будем использовать сдлующие обозначения:

- A – область целостности
- M – множество пар (a, b), где $b \neq 0$
- ρ – отношение на M, заданное правилом:

$$(a, b)\ \rho\ (c, d), \quad \text{если } ad = bc$$

Лемма 9. Отношение ρ является отношениием эквивалентности

Доказательство.

- Рефлексивность:
$$ab = ab \implies (a, b)\ \rho\ (b, a)$$
- Симметричность:
$$(a, b)\ \rho\ (c, d) \implies ad = bc \implies cb = da \implies (c, d)\ \rho\ (a, b)$$
- Транзитивность:
Докажем, что из условий $(a, b)\ \rho\ (c, d)$ и $(c, d)\ \rho\ (e, f)$ следует $(a, b)\ \rho\ (e, f)$:
Нужно доказать, что из равенств $ad = bc$ и $cf = ed$ следует равенство $af = be$
Домножим на "знаменатели" и сложим:
$$0 = (ad - bc)f + (cf - ed)b = adf - edb = d(af - eb) \underset{d \neq 0}{\implies} af = be$$

□

Определение 61. Пусть $(a, b), (c, d) \in M$
Их суммой и произведением называются пары $(ad + bc, bd)$ и (ac, bd)

Замечание о корректности. Пары $(ad + bc, bd)$ и (ac, bd) принадлежат M, так как

$$\left.\begin{matrix} b \neq 0 \\ d \neq 0 \end{matrix}\right\} \implies bd \neq 0$$

Лемма 10. Пусть $u, v, u', v' \in M$, $u\ \rho\ u'$, $v\ \rho\ v'$
Тогда $(u + v)\ \rho\ (u' + v')$, $\quad (uv) = (u'v')$

Доказательство. Отношение ρ транзитивно, поэтому достаточно проверить, что сумма (произведение) переходдят в эквивалентную при замене одного слагаемого (сомножителя) на эквивалентный, то есть

$$v\ \rho\ v' \implies (u + v)\ \rho\ (u + v'), \quad (uv) = (uv'), \qquad u\ \rho\ u' \implies (u + v)\ \rho\ (u' + v), \quad (uv) = (u'v)$$

Проверим первое утверждение (второе проверяется аналогично):
Пусть $u = (a, b)$, $\quad v = (c, d)$, $\quad v' = (c', d')$. Тогда $cd = dc'$
Нужно доказать, что:

- $(ad + bd, bd)\ \rho\ (ad' + bc', bd')$
$$(ad + bc)bd' - bd(ad' + bc') = b^2(cd' - dc') = b^2 \cdot 0 = 0$$
- $(ac, bd)\ \rho\ (ac', bd')$
$$ac \cdot bd' - bd \cdot ac' = ab(cd' - dc') = ab \cdot 0 = 0$$

□

Следствие. Операции сложения и умножения можно определить на классах эквивалентности множества M по отношению ρ

43. Построение поля частных: доказательство теоремы

Теорема 39 (поле частных)**.** Пусть A – область целостности с единицей
Пусть K – множество классов эквивалентности M по отношению ρ с введёнными выше операциями сложения и умножения
Тогда K – поле

Доказательство. Будем обозначать через $\overline{x}$ класс элемента x
Пусть $x = (a, b), \quad y = (c, d), \quad z = (e, f)$

- Ассоциативность сложения:

$$x + y = (ad + bc, bd), \qquad (x + y) + z = \Big((ad + bc)f + (bd)e, (bd)f\Big) = (adf + bcf + bde, bdf)$$

$$y + z = (cf + de, df), \qquad x + (y + z) = \Big(a(df) + b(cf + de), b(df)\Big) = (adf + bcf + bde, bdf)$$

- Нейтральный элемент по сложению: $0 = (0, 1)$

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

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

Докажем, что для любого $b \neq 0$ выполнено $\overline{(0, b)} = 0$:

$$0 \cdot 1 = b \cdot 0 \implies (0, b)\ \rho\ (0, 1) \implies \overline{(0, b)} = \overline{(0, 1)} = 0$$

Докажем, что если $\overline{(a, b)} = 0$, то $a = 0$:

$$\overline{(a, b)} = \overline{(0, 1)} \implies a \cdot 1 = b \cdot 0 \implies a = 0$$

- Обратный по сложению: $-(a, b) = (-a, b)$

$$(a, b) + (-a, b) = (ab + b(-a), b^2) = (0, b^2) \implies \overline{(a, b)} + \overline{(-a, b)} = 0$$

- Коммутативность сложения, дистрибутивность, асоциативность и коммутативность сложения доказываются аналогично

- Обратный по умножению:
Пусть $\overline{(a, b)} \neq 0$. Тогда $a \neq 0$
Докажем, что $\overline{(b, a)}$ является обратным к $\overline{(a, b)}$:

$$\overline{(a, b)} \cdot \overline{(b, a)} = \overline{(ab, ba)} = 1$$

□

Определение 62. Построенное поле называется полем частных области целостности A

Примечание. Существование единицы не обязательно. Достаточно, чтобы область целостности содержала хотя бы один ненулевой элемент

Переход к стандартным обозначениям. Вложим A в K, по правилу $a \mapsto \overline{(a, 1)}$
Операции сложения и умножения согласованы:

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

$$(a,1)\cdot(b,1)=(a\cdot b,1\cdot 1)=(ab,1)$$

Пусть $a,b\in A,\quad b\neq 0$. Проверим, что частное a и b равно $\overline{(a,b)}$:

$$\overline{(a,b)}\cdot\overline{(b,1)}=\overline{(ab,b)},\qquad (ab,b)\ \rho\ (a,1)$$

Далее вместо $\overline{(a,b)}$ будем писать $\frac{a}{b}$

44. Поле рациональных функций. Правильные дроби

Определение 63. Пусть K – поле
Поле частных кольца $K[x]$ называется полем рациональных функций над K

Обозначение. $K(x)$

Элементы $K(x)$ называются рациональными функциями или рациональными дробями (над K)

Далее рассмтариваются многочлены и рациональные функции над некоторым полем K

Определение 64. Рациональная дробь $\frac{F}{G}$ называется несократимой, если НОД$(F,G)=1$

Определение 65. Многочлен называется нормализованным, если его старший коэффициент равен 1

Определение 66. Рациональная дробь называется нормализованной, если она несократима, и её знаменатель – нормализованный многочлен

Свойство. Для любой рациональной дроби существует равная ей нормализованная дробь

Определение 67. Рациональная дробь $\frac{F}{G}$ называется правильной, если $\deg F<\deg G$

Свойства.

1. Если $\frac{F_1}{G_1}=\frac{F_2}{G_2}$, и $\frac{F_1}{G_1}$ – правильная дробь, то $\frac{F_2}{G_2}$ – тоже правильная дробь

   Доказательство. $F_1G_2=G_1F_2 \implies \deg F_1+\deg G_2=\deg G_1+\deg F_2 \implies \deg G_2-\deg F_2=\deg G_1-\deg F_1>0$ □

2. Сумма и произведение правильных рациональных дробей является правильной рациональной дробью

   Доказательство. Пусть $\frac{F_1}{G_1},\frac{F_2}{G_2}$ – правильные дроби

   $$a:=\deg F_1,\qquad b:=\deg G_1,\qquad c:=\deg F_2,\qquad d:=\deg G_2$$

   Тогда $a<b,\quad c<d$

   $$\deg(F_1G_2+F_2G_1)\leq\max\{\,a+d,b+c\,\}<b+d=\deg(G_1G_2)$$

   $$\deg(F_1F_2)=a+c<b+d=\deg(G_1G_2)$$

   □

3. Любую рациональную дробь можно единственным образом представить в виде суммы многочлена и правильной дроби

Доказательство. Пусть $\frac{F}{G}$ – рациональная дробь

- Существование
  Разделим F на G с остатком, пусть $F = QG + R, \quad \deg R < \deg G$. Тогда подходит представление
$$\frac{F}{G} = Q + \frac{R}{G}$$
- Единственность
  Пусть
$$P_1 + \frac{R_1}{S_1} = P_2 + \frac{R_2}{S_2}, \qquad P_1 \neq P_2$$
  Положим $P \coloneqq P_1 - P_2$. Тогда P является разностью правильных дробей, следовательно, P можно представить в виде
$$P = \frac{R}{S}, \qquad \deg R < \deg S$$
  Умножим на S:
$$SP = R$$
  Степень многочлена в левой части больше, чем в правой. Противоречие

□

45. Лемма о дроби, знаменатель которой разложен на взаимно простые множители

Лемма 11 (сумма дробей с взаимно простыми знаменателями)**.** Пусть $\dfrac{F}{G_1 ... G_k}$ – правильная рациональная дробь, многочлены G_i – попарно взаимно просты
Тогда дробь $\dfrac{F}{G_1 ... G_k}$ можно представить в виде
$$\frac{F_1}{G_1} + ... + \frac{F_k}{G_k}$$
где $\dfrac{F_i}{G_i}$ – правильные дроби, причём такое разложение единственно

Доказательство.

- Существование
  Индукция по k
  База. $k = 2$
  По теореме о линейном представлении НОД, можно представить F в виде $F = H_1G_1 + H_2G_2$
  Разделим на G_1G_2:
$$\frac{F}{G_1G_2} = \frac{H_1}{G_2} + \frac{H_2}{G_1}$$
  Представим каждое слагаемое в виде суммы многочлена и правильной дроби:
$$\frac{F}{G_1G_2} = \left(P_1 + \frac{F_1}{G_1}\right) + \left(P_2 + \frac{F_2}{G_2}\right)$$
  Преобразуем:
$$P_1 + P_2 = \frac{F}{G_1G_2} - \left(\frac{F_1}{G_1} + \frac{F_2}{G_2}\right)$$
  Левая часть равенства – многочлен, правая – правильная дробь. Следовательно, обе части равентсва равны 0, и
$$\frac{F}{G_1G_2} = \frac{F_1}{G_1} + \frac{F_2}{G_2}$$

Переход. $k \to k+1$

Многочлены $G_1 ... G_k$ и G_{k+1} взаимно просты. Представим дробь $\dfrac{F}{G_1 ... G_k G_{k+1}}$ в виде суммы правильных дробей:

$$\frac{H}{G_1 ... G_k} + \frac{F_{k+1}}{G_{k+1}}$$

Теперь применим индукционное предположение к первому слагаемому

- Единственность
  Пусть
  $$\frac{F_1}{G_1} + \frac{F_2}{G_2} + ... + \frac{F_k}{G_k} = \frac{H_1}{G_1} + \frac{H_2}{G_2} + ... + \frac{H_k}{G_k}$$
  где $\dfrac{F_i}{G_i}, \dfrac{H_i}{G_i}$ – правильные дроби
  Положим $T_i := F_i - H_i$. Тогда $\deg T_i < \deg G_i$, и
  $$\frac{T_1}{G_1} + \frac{T_2}{G_2} + ... + \frac{T_k}{G_k} = 0$$
  Требуется доказать, что $T_i = 0$ для любого i
  Для удобства обозначений докажем это для случая $i = 1$, то есть докажем, что $F_1 = H_1$
  Преобразуем равенство:
  $$\frac{T_1}{G_1} = \frac{-T_2}{G_2} + ... + \frac{-T_k}{G_k}$$
  $$T_1 G_2 ... G_k = -T_2 \prod_{i \neq 2} G_i - ... - T_k \prod_{i \neq k} G_i$$
  Правая часть равенства делится на G_1, следовательно, левая тоже делится на G_1
  При этом, $G_2 ... G_k$ и G_1 взаимно просты. Следовательно, $T_1 \vdots G_1$
  $$\left.\begin{matrix} T_1 \vdots G_1 \\ \deg T_1 < \deg G_1 \end{matrix}\right\} \implies T_1 = 0$$

□

46. Разложение правильной дроби в сумму правильных примарных дробей

Определение 68. Нормализованная рациональная дробь называется примарной, если она имеет вид $\dfrac{F}{P^n}$, где P – неприводимый нормализованный многочлен

Лемма 12 (сумма примарных дробей)**.** Любую правильную дробь можно представить в виде суммы правильных примарных дробей

$$\frac{F_1}{P_1^{S_1}} + ... + \frac{F_k}{P_k^{S_k}}, \qquad P_i \text{ различны}$$

Причём, такое разложение единственно

Доказательство. Пусть $\frac{F}{G}$ – нормализованная правильная дробь. Разложим G в произведение нормализованных неприводимых многочленов: $G = P_1^{S_1} ... P_k^{S_k}$

- Существование
  Применим лемму о сумме дробей с взаимно простыми знаменателями к $G_i = P_i^{S_i}$
- Еслинственность

Пусть есть два представления. Добавив, если нужно, слагаемые вида $\frac{0}{P^k}$, будем считать, что

$$\frac{F_1}{P_1^{S_1}} + \ldots + \frac{F_k}{P_k^{S_k}} = \frac{H_1}{P_1^{t_1}} + \ldots + \frac{H_k}{P_k^{t_k}}, \qquad P_i \text{ различны}$$

Вычтем:

$$\frac{F_1 P_1^{t_1} - H_1 P_1^{S_1}}{P_1^{S_1+t_1}} + \ldots + \frac{F_k P_1^{t_k} - H_k P_1^{S_k}}{P_k^{S_k+t_k}} = 0$$

Получили представление 0 в виде суммы дробей с взаимно простыми знаменателями
Такое представление единственно, следовательно, числители всех дробей равны 0
Следовательно, соответствующие слагаемые равны

□

47. Разложение правильной примарной дроби и произвольной дроби в сумму простейших

Определение 69. Нормализованная рациональная дробь называется простейшей, если она имеет вид $\frac{F}{P^n}$, где P – нормализованный неприводимый многочлен, и $\deg F < \deg P$

Лемма 13 (разложение примарной дроби в сумму простейших)**.** Любую правильную примарную дробь $\frac{F}{P^n}$ можно представить в виде суммы простейших дробей со знаменателями P^i, причём такое представление единственно

Доказательство.

- Существование
  Докажем, что примарную дробь $\frac{F}{P^n}$ можно представить в виде суммы простейших
  Индукция по n
  База. $n = 1$. В этом случае, $\deg F < \deg P$, и дробь является простейшей
  Переход. $n \to n+1$
  Разделим F на P с остатком:

$$F = PQ + R, \qquad \deg R < \deg P$$

  Подставим в формулу:

$$\frac{F}{P^{n+1}} = \frac{PQ+R}{P^{n+1}} = \frac{Q}{P^n} + \frac{R}{P^{n+1}}$$

  К первому слагаемому можно применить индукционное предположение, а второе является простейшей дробью

- Единственность
  Пусть есть два представления. Добавив, если нужно, слагаемые вида $\frac{0}{P^i}$, будем считать, что

$$\frac{F_1}{P} + \frac{F_2}{P^2} + \ldots + \frac{F_k}{P^k} = \frac{H_1}{P} + \frac{H_2}{P^2} + \ldots + \frac{H_k}{P^k}$$

  где $\deg F_i < \deg P, \quad \deg H_i < \deg P$
  Положим $T_i := F_i - H_i$. Тогда

$$\frac{T_1}{P} + \frac{T_2}{P^2} + \ldots + \frac{T_k}{P^k} = 0, \qquad \deg T_i < \deg P$$

  Предположим, что не все T_i равны нулю
  Пусть m таково, что $T_m \neq 0$ и $T_i = 0$ при $i > m$. Тогда

$$\frac{T_1 P^{k-1} + T_2 P^2 + \ldots + T_{m-1} P + F_m}{P^m} = 0, \qquad T_m \neq 0$$

Числитель раен 0, следовательно, $F_m \vdots P$. Это противоречит тому, что $F_m \neq 0$, и $\deg F_m < \deg P$

□

Теорема 40 (разложение дроби в сумму простейших)**.** Правильная рациональная дробь может быть представлена в виде суммы простейших дробей, причём такое представление единственно

Доказательство.

- Существование
  Правильную дробь можно представить в виде суммы примарных, а примарную – в виде суммы простейших
- Единственность
  Пусть есть два представления:

$$\left(\frac{T_{11}}{P_1} + \frac{T_{12}}{P_1^2} + ...\right) + \left(\frac{T_{21}}{P_2} + \frac{T_{22}}{P_2^2} + ...\right) + ... = \left(\frac{H_{11}}{P_1} + ... + \frac{H_{12}}{P_1^2} + ...\right) + \left(\frac{H_{21}}{P_2} + \frac{H_{22}}{P_2^2} + ...\right) + ...$$

Обозначим $F_{ij} \coloneqq T_{ij} - H_{ij}$

$$\left.\begin{matrix} \deg T_{ij} < \deg P_i \\ \deg H_{ij} < \deg P_i \end{matrix}\right\} \implies \deg F_{ij} < \deg P_i \implies \frac{F_{ij}}{P_i^j} \text{ – простейшая}$$

Вычтем одно разложение из другого (в новых обозначениях):

$$\left(\frac{F_{11}}{P_1} + \frac{F_{12}}{P_1^2} + ...\right) + \left(\frac{F_{21}}{P_2} + \frac{F_{22}}{P_2^2} + ...\right) + ... = 0$$

Сумма в каждой скобке является примарной дробью вида $\frac{F_i}{P_i^{n_i}}$

Представление в виде суммы примарных дробей единственно, следовательно, сумма в каждой скобке равна 0

Разложение примарной дроби $\frac{F_i}{P_i^{n_i}}$ в сумму простейших $\sum_j \frac{F_{ij}}{P_i^j}$ единственно, следовательно, каждое слагаемое в каждой скобке равно 0

□

48. Рациональный корень целочисленного многочлена. Следствие о целом корне

Теорема 41 (рациональный корень)**.** Пусть $F \in \mathbb{Z}[x]$, и

$$F(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$$

Пусть $\frac{p}{q}$ – корень $F(x)$, и НОД $(p, q) = 1$

Тогда $\begin{cases} a_n \vdots q \\ a_0 \vdots p \end{cases}$

Доказательство. Подставим:

$$a_n \left(\frac{p}{q}\right)^n + a_{n-1}x^{n-1}\left(\frac{p}{q}\right)^{n-1} + ... + a_1 \frac{p}{q} + a_0 = 0$$

Умножим на q^n:

$$a_n p^n + a_{n-1}p^{n-1}q + ... + a_1 p q^{n-1} + a_0 q^n = 0$$

Все слагаемые, кроме последнего, делятся на p, следовательно, последнее слагаемое тоже делится на p

Учитывая, что НОД $(p, q) = 1$, получаем что $a_0 \vdots p$
Все слагаемые, кроме первого, делятся на q. Аналогично получаем $a_n \vdots q$ $\square$

Следствие. Пусть $F \in \mathbb{Z}[x]$, и старший коэффициент $F(x)$ равен 1
Тогда любой рациональный корень $F(x)$ является целым числом, и свободный член a_0 делится на любой ненулевой целый корень

Доказательство. Пусть $\frac{p}{q}$ – корень $F(x)$, и НОД $(p, q) = 1$. Тогда

$$q \vdots q \implies q = \pm 1 \implies \frac{p}{q} \in \mathbb{Z}$$

$\square$

49. Многочлены над $\mathbb{Z}$: содержание многочлена, примитивные многочлены

Определение 70. Пусть $F(x) \in \mathbb{Z}[x], \quad F(x) = a_0 + a_1x + ... + a_nx^n$
Содержанием многочлена $F(x)$ называется НОД $(a_0, a_1, ..., a_n)$

Обозначение. $c(F)$

Определение 71. Многочлен F называется примитивным, если $F \in \mathbb{Z}[x]$, и $c(F) = 1$

Свойства.

1. Пусть $F \in \mathbb{Z}[x]$, и $F_1(x) = \dfrac{1}{c(F)} \cdot F(x)$. Тогда $F_1(x)$ – примитивный многочлен

   Доказательство. Коэффициенты многочлена разделим на их НОД. В результате получим целые взаимно простые числа $\square$

2. Пусть $F_1(x), F_2(x)$ – примитивные, $q \in \mathbb{Q}, \quad F_2(x) = qF_1(x)$. Тогда $q = \pm 1$

   Доказательство. Пусть $q = \frac{r}{s}$ – несократимая дробь. Тогда $rF_1(x) = sF_2(x)$
   Пусть $F_1(x) = \sum a_ix^i, \quad F_2(x) = \sum b_ix^i$. Тогда

   $$ra_i = sb_i \quad \forall i \implies sb_i \vdots r \quad \forall i \implies r = \pm 1$$

   Аналогично, $s = \pm 1$ $\square$

3. Пусть $F(x) \in \mathbb{Q}[x]$. Тогда существует единственное положительное число $q \in \mathbb{Q}$, для которого многочлен $qF(x)$ является примитивным

   Доказательство.

   - Существование
     Пусть N – общее кратное знаменателей всех коэффициентов, и $F_1 = NF(x)$
     Тогда $F_1(x) \in \mathbb{Z}[x]$
     По (1), многочлен $\dfrac{1}{c(F_1)}F_1(x)$ – целочисленный и примитивный
     Число $q = \dfrac{N}{c(F_1)}$ подходит
   - Единственность
     Пусть $F_1(x) = q_1F(x)$, и $F_2(x) = q_2F(x)$ – целочисленные примитивные
     Применим (2) к $q = \dfrac{q_1}{q_2}$, получим, что $\dfrac{q_1}{q_2} = 1$

   $\square$

50. Лемма Гаусса

Лемма 14 (Гаусса)**.** Пусть $F(x), G(x) \in \mathbb{Z}[x]$, и $H(x) = F(x)G(x)$. Тогда

- Если $F(x), G(x)$ – примитивные, то $H(x)$ – примитивный

  Доказательство. Пусть $P(x) = \sum a_i x^i, \quad G(x) = \sum b_i x^i, \quad H(x) = \sum d_i x^i$
  Предположим, что $H(x)$ не примитивный
  Тогда для некоторого $p \in \mathbb{P}$ выполнено $d_i \in p \quad \forall i$
  Из того, что $F(x), G(x)$ – примитивные, следует, что **не** все a_i делятся на p, и **не** все b_i делятся на p
  Пусть
  $$k \min \{ i \mid a_i \not{\vdots}\, p \}, \qquad l = \min \{ i \mid b_i \not{\vdots}\, p \}$$
  Тогда
  $$d_{k+l} = a_0 b_{k+l} + \ldots + a_k b_l + \ldots + a_{k+l} b_0 \not{\vdots}\, p$$
  так как $a_k b_l \not{\vdots}\, p$, а остальные слагаемые делятся на p. Противоречие ☐

- $c(H) = c(F)c(G)$

  Доказательство. Пусть $F_1(x) = \dfrac{1}{c(F)} F(x), \quad G_1(x) = \dfrac{1}{c(G)} G(x)$. Тогда
  $$\frac{1}{c(F)c(G)} H(x) = F_1(x) G_1(x)$$
  Применяя (1), получаем, что $\dfrac{1}{c(F)c(G)} H(x)$ – примитивный многочлен
  При этом, $\dfrac{1}{c(H)} H(x)$ – тоже примитивный многочлен
  Следовательно, $c(H) = c(F)c(G)$ ☐

51. Редукционный критерий неприводимости. Следствие про рациональный корень

Определение 72. Многочлен $P \in \mathbb{Z}[x]$ называется неприводимым над $\mathbb{Z}$, если его нельзя разложить в произведение двух многочленов из $\mathbb{Z}[x]$, отличных от константы

Теорема 42 (редукционный критерий неприводимости)**.**

1. Пусть $F(x) \in \mathbb{Z}[x]$, и $F(x)$ неприводим над $\mathbb{Z}$. Тогда $F(x)$ неприводим над $\mathbb{Q}$
2. Пусть $F(x) \in \mathbb{Z}[x], \quad G(x), H(x) \in \mathbb{Q}[x]$, и $F(x) = G(x)H(x)$
   Тогда существуют $G_1(x), H_1(x) \in \mathbb{Z}[x]$, ассоциированные с $G(x), H(x)$ над $\mathbb{Q}$, такие, что $F(x) = G_1(x)H_1(x)$

Доказательство. Достаточно доказать (2)

- Докажем утверждение для случая, когда $F(x)$ – примитивный
  По свойству (14), сущетсвуют такие $q_G, q_H \in \mathbb{Q}$, что $q_G, q_H > 0$, и многочлены $q_G G(x), q_H H(x)$ принадлежат $\mathbb{Z}[x]$ и являются примитивными
  Тогда многочлен
  $$(q_G q_H) F(x) = q_g G(x) \cdot q_H H(x)$$
  является примитивным по лемме Гаусса
  Многочлены $F(x)$ и $(q_g q_H)F(x)$ – примитивные, следовательно, по свойству 2, выполнено $q_g q_H = 1$
  Получаем, что
  $$F(x) = q_g G(x) \cdot q_H H(x)$$
  Многочлены $q_G G(x)$ и $q_H H(x)$ подойдут в качестве $H_1(x)$ и $G_1(x)$

- Докажем утверждение в общем случае
Многочлен $\frac{1}{c(F)}F(x)$ – примитивный, и он раскладывается в произведение

$$\frac{1}{c(F)}F(x) = \frac{1}{c(F)}G(x) \cdot H(x)$$

Существуют целочисленные многочлены $G_0(x)$ и $H_0(x)$, асоцированные с $G(x)$ и $H(x)$, для которых выполнено

$$\frac{1}{c(F)}F(x) = G_0(x)H_0(x)$$

В качетсве $G_1(x)$ и $H_1(x)$ подойдут $c(F)G_0(x)$ и $H_0(x)$

□

52. Факториальность $\mathbb{Z}[X]$

Теорема 43. Любой многочлен с целыми коэффициентами можно представить в виде произведения простых чисел и примитивных многочленов, неприводимых над $\mathbb{Q}$
Такое представление единственно с точностью до перестановки сомножителей и умножения сомножиелей на -1

Доказательство.

- Существование
Пусть $F(x) \in \mathbb{Z}[x]$
Расссмотрим $F(x)$ как элемент $\mathbb{Q}[x]$
Кольцо $\mathbb{Q}[x]$ факториально, поэтому $F(x)$ можно представить в виде произведения обратимого элемента и неразложимых элементов
В $\mathbb{Q}[x]$ обратимыми элементами являются ненулевые константы, а неразложимыми – неприводимые над $\mathbb{Q}$ многочлены
Пусть

$$F(x) = aP_1(x)...P_k(x)$$

Заменив $P_1(x)$ на $aP_1(x)$, будем считать, что

$$F(x) = aP_1(x)...P_k(x), \qquad P_i \text{ неприводим над } \mathbb{Q}$$

По редукционному критерию неприводимости, существуют многочлены $H_i \in \mathbb{Z}[x]$, такие, что $H_i(x) = q_iP_i(x)$, и

$$F(x) = H_1(x)...H_k(x)$$

Пусть $T_i(x) := \frac{1}{c(H_i)}H_i(x)$
Тогда многочлены $T_i(x)$ примитивны и неприводимы над $\mathbb{Q}$, так как ассоциированы с неприводимыми многочленами $P_i(x)$. Получили разложение

$$F(x) = aT_1(x)...T_k(x), \qquad \text{где } b = c(H_1)...c(H_k)$$

Разложим b в произведение простых чисел, и если нужно, -1
Получится требуемое разложение $P(x)$

- Единственность
Пусть

$$F(x) = \pm p_1p_2...T_1(x)T_2(x)..., \qquad F(x) = \pm q_1q_2...H_1(x)H_2(x)...$$

где $p_i, q_i \in \mathbb{P}$, и $T_i(x), H_i(x)$ – примитивные многочлены, неприводимые над $\mathbb{Q}$
По лемме Гаусса, произведения $T_1(x)T_2(x)...$ и $H_1(x)H_2(x)...$ являются примитивными многочленами, следовательно,

$$c(F) = \pm p_1p_2..., \qquad c(F) = \pm q_1q_2...$$

Из факториальности кольца $\mathbb{Q}[x]$ следует, что произведения $T_1(x)T_2(x)...$ и $H_1(x)H_2(x)...$ совпадают с точностью до перестановки сомножителей и замены на ассоциированные

То есть, можно так перенумеровать $H_i(x)$, что $H_i(x) = q_i T_i(x)$ для некоторого $q_i \in \mathbb{Q}$
Многочлены $T_i(x)$ и $H_i(x)$ примитивные, следовательно, $q_i = \pm 1$

$\square$

53. Критерий неприводимости Эйзенштейна

Теорема 44 (критерий неприводимости Эйзенштейна)**.** Пусть $a_0, a_1, \ldots, a_{n-1} \in \mathbb{Z}$, $\quad p \in \mathbb{P}$, $\quad a_i \,\vdots\, p$ для любого i, и $a_0 \not\vdots\, p^2$
Тогда многочлен $F(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ неприводим над $\mathbb{Q}$

Доказательство. Предположим, что $F(x)$ приводим над $\mathbb{Q}$
Тогда $F(x)$ приводим над $\mathbb{Z}$
Пусть

$$F(x) \coloneqq G(x)H(x), \qquad G(x), H(x) \in \mathbb{Z}[x], \qquad G(x) \coloneqq \sum b_i x^i, \quad H(x) \coloneqq \sum c_i x^i$$

причём, $G(x)$ и $H(x)$ – не константы
Число $b_0 c_0 = a_0$ делится на p и **не** делится на p^2
Следовательно, одно из чисел b_0, c_0 делится на p, а второе – не делится
НУО будем считать, что $b_0 \,\vdots\, p$, $\quad c_0 \not\vdots\, p$
Старший коэффициент $F(x)$ не делится на p, следовательно, не все b_i делятся на p
Пусть $k \coloneqq \min\{\, i \mid b_i \not\vdots\, p \,\}$
Тогда $k \le \deg G < \deg F = n$
Имеем $a_k = b_0 c_k + \ldots + b_{k-1} c_1 + b_k c_0 \not\vdots\, p$, так как все слагаемые, кроме последнего, делятся на p, а последнее – не делится на p – $\lightning$ $\square$