Содержание

Предисловие

Дискретная математика является фундаментом для всего компьютинга, включая программную инженерию. Она столь же важна для компьютерных дисциплин, как и математический анализ для остальных инженерных специальностей.

Дискретная математика есть область науки, посвященная изучению дискретных объектов и структур. В широком смысле она включает в себя: теорию множеств, отношения и функции, теорию чисел, абстрактную алгебру, математическую логику, булеву алгебру, логику высказываний, цифровую логику, логику предикатов, методы доказательства, комбинаторный анализ, рекуррентные соотношения, теорию графов и сетей, основы алгоритмизации, теорию автоматов и формальных языков, теорию алгоритмов, вычислимость и вычислительную сложность, дискретную вероятность, целочисленную оптимизацию, криптографию, теорию информации и кодирования.

Дискретная математика стала важным звеном математического образования инженера.

Настоящая книга является первой в серии задуманных авторским коллективом книг по дискретной математике. Она предназначается студентам бакалавриата, изучающим академический курс «Дискретная математика» для формирования у студентов следующих компетенций:

1) способность к самоорганизации и самообразованию в области дискретных математических моделей;
2) готовность применить аппарат дискретной математики для решения поставленных практических задач;
3) способность применить соответствующую задаче математическую модель с проверкой ее адекватности;
4) способность провести анализ результатов моделирования для принятия решений на основе полученных результатов.

В предлагаемой книге авторы сосредоточились на изложении математических основ современной теории кодирования и криптографии, доступных для понимания студентов первых лет обучения.

Основные теоретические и практические положения, изложение и анализ практических алгоритмов, иллюстрируемые большим числом примеров, позволят сформировать прочную теоретическую базу, необходимую для дальнейшей работы практикующих программистов и ИТ-специалистов.

В приложении предлагаются задачи, которые могут быть использованы как для проведения практических занятий, так и для самостоятельной работы.

Авторы выражают глубокую благодарность рецензентам Калягину В. А., Ульянову М. В. и научному редактору книги Захарову В. А. за замечания, позволившие существенно улучшить качество книги. Мы также благодарны преподавателям

департамента программной инженерии НИУ ВШЭ Ахметсафиной Р. З., Гринкругу Е. М., Дворянскому Л. В., Дегтяреву К. Ю., Каленковой А. А., Ломазовой И. А., Подбельскому В. В., Шилову В. В., а также Амосову А. А., Дубинскому Ю. А., Фролову А. Б. из НИУ МЭИ за стимулирующие беседы. Авторы благодарят студентов Горденко М. К., Сапожкова Е. Д., Чиркову Е. Н. за активное участие в составлении и апробации задач и упражнений приложения.

Введение

1. Множество

Понятие множества неопределимо. Это простейшее исходное понятие человечество сформировало из опыта всего своего исторического развития. То же можно сказать о смысле простейшего отношения принадлежности: элемент a принадлежит множеству A (обозначение $a \in A$) – и о смысле отношения тождества (совпадения, равенства) двух элементов a и b из некоторого множества (обозначение $a = b$). Другими словами, предполагается, что читатель умеет распознавать совпадение или несовпадение двух элементов и устанавливать факт принадлежности или непринадлежности элемента множеству.

Пусть U есть некоторое множество. A есть подмножество множества U, если всякий элемент из множества A принадлежит множеству U. Множество U универсально (универсум), если все рассматриваемые множества есть подмножества множества U.

Пусть A, B, C есть произвольные подмножества множества U; a, b, c есть элементы множества U. Обозначим символом $\varnothing$ пустое множество, то есть множество без элементов.

Основными неопределяемыми отношениями в теории множеств являются следующие отношения:

- $a = b$, элементы a и b равны (совпадают);
- $a \in A$, элемент a принадлежит множеству A.

Пусть знак $\leftrightarrow$ означает «если и только если»; а знаки $\&$, $\vee$, $\neg$, $\rightarrow$, $\forall$, $\exists$ есть логические знаки конъюнкции, дизъюнкции, отрицания, импликации, квантора общности и квантора существования. Используем их в общепринятом содержательном смысле. Знак $\exists!$ означает квантор существования единственного элемента.

Обозначим через $a \notin A$ отношение элемент a не принадлежит множеству A и через $a \neq b$ отношение элементы a и b не равны (не совпадают).

Введем далее следующие отношения:

- $A \subseteq B \leftrightarrow \forall a\ (a \in A \rightarrow a \in B)$, отношение включения множеств, при этом множество A называется подмножеством множества B, а множество B называется надмножеством множества A;
- $A \supseteq B \leftrightarrow B \subseteq A$;
- $A = B \leftrightarrow A \subseteq B \ \& \ A \supseteq B$, отношение равенства множеств;
- $A \subset B \leftrightarrow A \subseteq B \ \& \ A \neq B$, отношение строгого включения множеств;
- $A \supset B \leftrightarrow B \subset A$.

Обозначим через $P(A)$ (или 2^A) множество всех подмножеств множества A. Введем следующие операции над множествами:

- $A \cup B = \{x \in U: x \in A \vee x \in B\}$, объединение множеств A и B;
- $A \cap B = \{x \in U: x \in A \,\&\, x \in B\}$, пересечение множеств A и B;
- $A - B = \{x \in U: x \in A \,\&\, x \notin B\}$, разность множеств A и B;
- $\overline{A} = U - A$, дополнение к множеству A;
- $A \div B = (A \cup B) - (A \cap B)$, симметрическая разность множеств A и B;
- $A \times B = \{(a, b): a \in A \,\&\, b \in B\}$, декартово произведение множеств A и B.

Под натуральным числом понимаем количество элементов конечного множества. Количество элементов пустого множества есть 0.

Распространим декартово произведение на несколько сомножителей:

$$A_1 \times A_2 \times ... \times A_n = \{(a_1, a_2, ..., a_n): a_1 \in A_1, a_2 \in A_2, ..., a_n \in A_n\}.$$

Определим декартову степень множества

$$A^n = A \times A \times ... \times A \ (n \text{ раз}), A^0 = \varnothing.$$

Множества $\varnothing$ и A называются несобственными (тривиальными) подмножествами множества A. Если $A \subset B \,\&\, A \neq \varnothing$, то A есть собственное подмножество множества B.

Иногда пишут $A \cdot B$ или AB вместо $A \cap B$.

Примем следующие обозначения.

Множество натуральных чисел $\mathbb{N} = \{0, 1, 2, ...\}$.

Множество положительных натуральных чисел $\mathbb{N}_+ = \{1, 2, ...\}$.

Множество целых чисел $\mathbb{Z} = \{..., -2, -1, 0, 1, 2, ...\}$.

Множество $\mathbb{Z}_n = E_n = \{0, 1, 2, ..., n - 1\}$.

Множество рациональных чисел $\mathbb{Q} = \{\frac{m}{n}: m \in \mathbb{Z}, n \in \mathbb{N}_+\}$.

Множество вещественных чисел $\mathbb{R} = (-\infty, +\infty)$.

Множество неотрицательных вещественных чисел $\mathbb{R}_+ = [0, +\infty)$.

Множество комплексных чисел $\mathbb{C} = \{x + i\,y: x \in \mathbb{R}, y \in \mathbb{R}\}$, здесь $i^2 = -1$.

2. Функция

Определение. Пусть A и B есть два множества. *Функция* $f: A \to B$ есть отображение, которое каждому элементу x из A ставит в соответствие некоторый элемент y из B. Это обстоятельство записывается как $y = f(x)$.

Замечание. В этом определении функция f всюду определена. Частично определенная функция $f: A \to B$ есть отображение, которое каждому элементу из множества A сопоставляет не более одного элемента из множества B. Всюду определенная функция является частным случаем частично определенной функции.

Если $f(a) = b$, то элемент b есть образ элемента a, элемент a есть прообраз элемента b. Область определения функции f есть множество $D(f) = \{a \in A: \exists b \in B(f(a) = b)\}$. Область значений функции f есть множество $R(f) = \{b \in B: \exists a \in A(f(a) = b)\}$.

Иногда множество $R(f)$ обозначают как $Im(f)$ или $f(A)$. Полный прообраз элемента $b \in B$ есть множество $f^{-1}(b) = \{a \in A: f(a) = b\}$. Полный прообраз множества $C \subseteq B$ есть множество $f^{-1}(C) = \{a \in A: f(a) \in C\}$.

Сужение функции f, заданной на множестве A, на подмножество S множества A есть функция g – такая, что $\forall a \in S(g(a) = f(a))$.

Расширение функции f, заданной на множестве A, на надмножество T множества A есть функция h – такая, что $\forall a \in A(h(a) = f(a))$.

Функцию с конечной областью определения удобно задавать таблицей. Например, пусть множества $A = \{1, 2, 3, 4\}$, $B = \{1, 2, 3, 4, 5\}$, функция $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & & 1 & 2 \end{pmatrix}$. Здесь $f(1) = 3$, $f(2)$ не определено, $f(3) = 1$, $f(4) = 2$. Порядок столбцов несущественен.

Область определения $D(f) = \{1, 3, 4\}$, область значений $R(f) = Im(f) = f(A) = \{1, 2, 3\}$.

Определение. Функция φ: $A \to B$ есть *взаимно-однозначное отображение* (1–1-отображение) между множествами A и B, если

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

2) $\forall a \in A\ \forall b \in A\ (a \neq b \neq f(a) \neq f(b))$.

Замечание. Последнее условие можно заменить на условие

2') $\forall a \in A\ \forall b \in A\ (f(a) = f(b) \to a = b)$.

Функции f: $A \to B$ и g: $C \to D$ равны, если $A = C$, $B = D$, $\forall x \in A\ (f(x) = g(x))$.

Функция I_A: $A \to A$, для которой $\forall x \in A\ (I(x) = x)$, называется *тождественной* функцией.

Функция f: $A \to B$ есть отображение *в* (*инъективная функция*, или *инъекция*), если $\forall a \in A\ \forall b \in A$ условие $a \neq b$ влечет $f(a) \neq f(b)$.

Инъективная функция различные элементы из области определения переводит в различные элементы из области значений.

Функция f: $A \to B$ есть отображение *на* (*сюръективная функция*, или *сюръекция*), если область значений B совпадает с образом $f(A)$, то есть если $f(A) = B$.

Функция f: $A \to B$ есть *взаимно-однозначная функция* (или *биекция*), если f является отображением *в* и отображением *на*, то есть является одновременно инъективной и сюръективной функцией: 1) $a \neq b \to f(a) \neq f(b)$, 2) $Im(f) = B$.

Определение. Композиция $g \circ f$ функций f: $A \to B$ и g: $B \to C$ есть функция $g \circ f$: $A \to C$, для которой $\forall x \in A\ ((g \circ f)(x) = g(f(x)))$.

Замечание. Символ композиции $\circ$ иногда опускается.

Утверждение. $(h \circ g) \circ f = h \circ (g \circ f)$.

Доказательство. Пусть f: $A \to B$, g: $B \to C$, h: $C \to D$. Тогда $((h \circ g) \circ f)(x) = ((hg)f)(x) = (h \circ g)f(x)) = h(g(f(x))) = h((g \circ f)(x)) = (h \circ (g \circ f))(x)$.

Замечание. Для тождественной функции $f \circ I_A = I_B \circ f = f$.

Определение. Функция f^{-1}: $B \to A$ называется *обратной* к функции f: $A \to B$, если $f \circ f^{-1} = I_B$ и $f^{-1} \circ f = I_A$.

Замечание. 1. g обратна к $f \leftrightarrow f$ обратна к g.

2. Функция f: $A \to B$ имеет обратную функцию, $\leftrightarrow$ функция f есть взаимно-однозначное отображение.

Утверждение. Если обратная функция для функции f существует, то она единственна.

Доказательство. Пусть функции f^{-1} и g обратны к функции f: $A \to B$. Тогда $f^{-1} \circ I_B = f^{-1} \circ (f \circ g) = (f^{-1} \circ f) \circ g = I_A \circ g = g$.

Следствие. Пусть для функций f и g существуют обратные функции f^{-1} и g^{-1}. Тогда справедливы утверждения:

1. $(f^{-1})^{-1} = f$.
2. $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$.

Доказательство. 1. Так как f^{-1} обратна к f, то f обратна к f^{-1}, то есть $f = (f^{-1})^{-1}$.

2. $(f \circ g) \circ (g^{-1} \circ f^{-1}) = f \circ (g \circ g^{-1}) \circ f^{-1} = f \circ I_B \circ f^{-1} = f \circ f^{-1} = I_B$.

Аналогично $(g^{-1} \circ f^{-1}) \circ (f \circ g) = I_B$. Тогда функция $g^{-1} \circ f^{-1}$ обратна к $f \circ g$, то есть $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$.

Теорема. Функция f: $A \to B$ имеет обратную функцию тогда и только тогда, когда отображение f взаимно-однозначно.

Доказательство. Пусть функция f имеет обратную функцию f^{-1}. Покажем, что отображение f взаимно-однозначно, то есть что $a \neq b \to f(a) \neq f(b)$ и $B = Im(f)$. В самом деле, пусть $f(a) = f(b)$. Тогда $a = I_A(a) = f^{-1}(f(a)) = f^{-1}(f(b)) = I_A(b) = b$, то есть $f(a) = f(b) \to a = b$, откуда $a \neq b \to f(a) \neq f(b)$.

Пусть $b \in B$. Тогда $b = I_B(b) = (f \circ f^{-1})(b) = f(f^{-1}(b))$, то есть всякий b есть образ некоторого $a = f^{-1}(b) \in A$. Поэтому $B = Im(f)$.

Пусть теперь f есть взаимно-однозначное отображение. Покажем, что функция f имеет обратную функцию. В самом деле, так как $B = Im(f)$, то каждый элемент b из B есть образ в точности одного элемента a из A: $f(a) = b$. Пусть $g(b) = a$. Для соответствия g: $B \to A$ имеем:

$$(g \circ f)(a) = g(f(a)) = g(b) = a = I_A,$$
$$(f \circ g)(b) = f(g(b)) = f(a) = b = I_B.$$

Следовательно, g есть обратная функция для f. Теорема доказана.

3. Отношение

Пусть $A_1, A_2, ..., A_n$ есть произвольные множества, вообще говоря, разнородные.

Определение. *n-арное отношение* p^n на множествах $A_1, A_2, ..., A_n$ есть подмножество p^n декартова произведения $A_1 \times A_2 \times ... \times A_n$.

Замечание. n-арное отношение p^n на множестве A есть подмножество p^n натуральной степени множества A^n, $n > 0$. Индекс n-арности (местности) отношения p иногда опускается.

Возможна множественная (суффиксная) $(x_1, ..., x_n) \in \rho$ и предикатная (префиксная) $\rho(x_1, ..., x_n)$ формы записи отношений. В последнем случае отношение ρ называют также предикатом. Для бинарного отношения используется инфиксная запись $x \rho y$. Унарное отношение $\rho \subseteq E$ есть подмножество множества E. Предикат $\rho(x)$, соответствующий унарному отношению, называется свойством.

Набор $a = (a_1, a_2, ..., a_n) \in \rho$ (допустима запись $\rho(a_1, a_2, ..., a_n)$) называется элементом отношения.

Определение. Отношение *конечно*, если оно состоит из конечного числа элементов.

4. Отношение эквивалентности

Пусть A есть произвольное множество.

Определение. Бинарное отношение $\sigma \subseteq A \times A$ есть *отношение эквивалентности* (обозначение $a \sim b$), если оно удовлетворяет следующим аксиомам:

1) $a \sim a$, рефлексивность;

2) $a \sim b \to b \sim a$, симметричность;

3) $a \sim b \,\&\, b \sim c \to a \sim c$, транзитивность.

Обозначение. $a \sim b$, $\sigma(a, b)$, $(a, b) \in \sigma$, $a \,\sigma\, b$.

Определение. *Разбиение I множества A* есть семейство попарно непересекающихся непустых подмножеств множества A, таких, что: $A = \bigcup_{i \in I} A_i$, $\forall i \neq j$ $(A_i \bigcap A_j = \varnothing)$.

Подмножества A_i называются *смежными классами* разбиения I.

Пример. $A = \{0, 1, 2, 3, 4, 5\} = \{0, 1, 5\} \cup \{2\} \cup \{3, 4\}$.

Теорема. 1. Каждому отношению эквивалентности, определенному на множестве A, соответствует некоторое разбиение множества A.

2. Каждому разбиению множества A соответствует некоторое отношение эквивалентности, определенное на множестве A.

Коротко: между классом всех определенных на множестве A эквивалентностей и классом всех разбиений множества A существует взаимно-однозначное соответствие.

Доказательство. 1. Пусть σ есть отношение эквивалентности, определенное на множестве A и $a \in A$. Построим множество $K_a = \{x \in A: x \sim a\}$ всех элементов x, эквивалентных a. Оно обозначается также через $[a]_\sigma$. Множества K_a называются *смежными классами A по* σ, или классами эквивалентности.

Заметим, что если $b \in K_a$, то $b \sim a$. Покажем, что $a \sim b \leftrightarrow K_a = K_b$. В самом деле, пусть $a \sim b$. Пусть произвольный элемент $c \in K_a$. Тогда $c \sim a$, $a \sim b$, $c \sim b$, $c \in K_b$, и потому $K_a \subseteq K_b$. Аналогично показываем, что $K_b \subseteq K_a$. Тогда $K_a = K_b$. Пусть теперь $K_a = K_b$. Тогда $a \in K_b$ и $a \sim b$. Утверждение доказано.

Если два класса K_a и K_b имеют общий элемент c, то они совпадают. В самом деле, если $c \in K_a$, $c \in K_b$, то $b \sim c$, $c \sim a$ и $b \sim a$, откуда $K_a = K_b$. Поэтому всякие два класса эквивалентности либо не пересекаются, либо (в случае непустого пересечения) совпадают. Всякий элемент c попадает в класс эквивалентности K_c. Поэтому система смежных классов есть разбиение множества A.

2. Пусть задано некоторое разбиение множества A. Определим на A отношение $\sim$, положив $a \sim b \leftrightarrow$ элементы a и b принадлежат одному и тому же классу разбиения. Отношение $\sim$ удовлетворяет аксиомам 1) $a \sim a$, 2) $a \sim b \to b \sim a$, 3) $a \sim b \,\&\, b \sim c$, и потому оно есть отношение эквивалентности.

Замечание. 1. Разбиение множества A на одноэлементные подмножества $A = \bigcup_{a \in A} \{a\}$ и разбиение A, состоящее из одного только множества A, называются тривиальными (несобственными) разбиениями.

2. Разбиение A на одноэлементные подмножества соответствует отношению эквивалентности, которое есть равенство.

3. Разбиение множества A, состоящее из одного только множества A, соответствует отношению эквивалентности, содержащему все множество $A \times A$.

4. $a \sigma b \leftrightarrow [a]_\sigma = [b]_\sigma$.

Определение. Совокупность классов эквивалентности множества A называется *фактор-множеством* A/σ множества A по эквивалентности σ.

Определение. Отображение p: $A \to A/\sigma$, при котором $p(a) = [a]_\sigma$, называется *каноническим* (естественным).

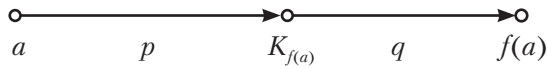
5. Каноническое разложение функции

Пусть f: $A \to B$ есть некоторая функция. Определим на A отношение $\sigma \in A \times A$, положив $\leftrightarrow a \in A \leftrightarrow b \in A$ ($a \sim b \leftrightarrow f(a) = f(b)$). Отношение σ есть отношение эквивалентности, так как выполняются следующие свойства:

1) $a \sim a$, ибо $f(a) = f(a)$;
2) $a \sim b \to b \sim a$, ибо $f(a) = f(b) \to f(b) = f(a)$;
3) $a \sim b \ \& \ b \sim c \to a \sim c$, ибо $f(a) = f(b) \ \& \ f(b) = f(c) \to f(a) = f(c)$.

Введенное отношение σ называется ядерной эквивалентностью для отображения f. Классы эквивалентности A/σ есть полные прообразы элементов множества B при отображении f, то есть $A_b = f^{-1}(b)$.

Отображение f можно разложить в композицию двух отображений, согласно следующему рисунку:



Имеет место равенство $f = q \circ p$, то есть $f(a) = q(p(a))$.

Представление $f = q \circ p$ называется каноническим разложением (представлением) функции f.

Пример. Получить каноническое разложение функции

$$f\colon E_{10} \to E_{10}, f = 0112105533 = \begin{pmatrix} 0\,1\,2\,3\,4\,5\,6\,7\,8\,9 \\ 0\,1\,1\,2\,1\,0\,5\,5\,3\,3 \end{pmatrix}.$$

Область определения $D(f) = E_{10}$. Область значений $Im(f) = \{0, 1, 2, 3, 5\}$. Классы эквивалентности:

$K_0 = [0]_\sigma = f^{-1}(0) = \{0, 5\}$, $q(K_0) = 0$;
$K_1 = [1]_\sigma = f^{-1}(1) = \{1, 2, 4\}$, $q(K_1) = 1$;
$K_2 = [2]_\sigma = f^{-1}(2) = \{3\}$, $q(K_2) = 2$;
$K_3 = [3]_\sigma = f^{-1}(3) = \{8, 9\}$, $q(K_3) = 3$;
$K_5 = [5]_\sigma = f^{-1}(5) = \{6, 7\}$, $q(K_5) = 5$.

Функции p и q задаются следующим образом:

$$p(a) = K_{f(a)} = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ K_0 & K_1 & K_1 & K_2 & K_1 & K_0 & K_5 & K_5 & K_3 & K_3 \end{pmatrix},$$

$D(p) = E_{10}$, $Im(p) = \{K_0, K_1, K_2, K_3, K_5\}$; $q(K_a) = a = \begin{pmatrix} K_0 K_1 K_2 K_3 K_5 \\ 0\ 1\ 2\ 3\ 5 \end{pmatrix}$,

$D(q) = \{K_0, K_1, K_2, K_3, K_5\}$, $Im(q) = \{0, 1, 2, 3, 5\}$; $f(a) = q(p(a))$.

6. Мощность множества. Счетные и несчетные множества

Определение. *Множества A* и *B эквивалентны* ($A \sim B$), если между их элементами можно установить взаимно-однозначное соответствие.

Отношение эквивалентности множеств обладает следующими свойствами:

1. $A \sim A$, рефлексивность;
2. $A \sim B \to B \sim A$, симметричность;
3. $A \sim B \,\&\, B \sim C \to A \sim C$, транзитивность.

Определение. *Мощность множества A* (обозначение $|A|$) есть класс эквивалентных ему множеств. *Мощность конечного множества* есть число его элементов.

Замечание. Эквивалентные множества A и B равномощны, то есть $A \sim B \leftrightarrow |A| = |B|$.

Определение. Множество A *счетно*, если A эквивалентно множеству $\mathbb{N}$ натуральных чисел. В противном случае множество A *несчетно*.

Утверждение. Из всякого бесконечного множества можно выделить счетное подмножество.

Доказательство. Пусть A есть бесконечное множество. Выделим в A произвольный элемент a_0. Множество $A - \{a_0\}$ бесконечно. Выделим в нем элемент a_1. Множество $A - \{a_0, a_1\}$ бесконечно. Выделим в нем элемент a_2. И так далее. В бесконечном множестве A выделено счетное подмножество $B = \{a_0, a_1, a_2, ...\}$.

Утверждение. Множество $\mathbb{Q}_+$ положительных рациональных чисел счетно.

Доказательство. Расположим элементы из $\mathbb{Q}_+$ в следующей таблице:

1	1/2	1/3	1/4	1/5	...
2	2/2	2/3	2/4	2/5	...
3	3/2	3/3	3/4	3/5	...
4	4/2	4/3	4/4	4/5	...
		...			

Выписываем элементы из $\mathbb{Q}_+$ по диагонали сверху вниз, выпуская ранее встречавшиеся числа: 1, 1/2, 2, 1/3, 3, 2/3, ... Следовательно, множество $\mathbb{Q}_+$ счетно.

Утверждение. Объединение конечного или счетного множества счетных множеств счетно.

Доказательство. Расположим элементы множеств $A_1, A_2, A_3, ...$ (их число может быть и конечным) в следующей таблице:

$$\begin{array}{lllll} A_1: & a_{11}, & a_{12}, & a_{13}, & a_{14}, \quad \ldots \\ A_2: & a_{21}, & a_{22}, & a_{23}, & a_{24}, \quad \ldots \\ A_3: & a_{31}, & a_{32}, & a_{33}, & a_{34}, \quad \ldots \\ A_4: & a_{41}, & a_{42}, & a_{43}, & a_{44}, \quad \ldots \\ & & \ldots & & \end{array}$$

Выписываем элементы из $A_1 \cup A_2 \cup A_3 \cup \ldots$ по диагонали сверху вниз, выпуская ранее встречавшиеся элементы: $a_{11}, a_{12}, a_{21}, a_{13}, a_{22}, a_{31}, \ldots$ Следовательно, множество $A_1 \cup A_2 \cup \ldots$ счетно.

Замечание. Объединение конечного множества и счетного множества счетно. Множество рациональных чисел счетно, ибо $\mathbb{Q} = \mathbb{Q}_- \cup \mathbb{Q}_+ \cup \{0\}$, где $\mathbb{Q}_-$ есть множество отрицательных рациональных чисел.

7. Мощность континуума

Утверждение. Множество C всех бесконечных последовательностей из 0 и 1 несчетно.

Доказательство. Допустим противное: существует пересчет всех бесконечных последовательностей $A_1, A_2, A_3, \ldots$ из 0 и 1:

$$\begin{array}{lllll} A_1: & a_{11}, & a_{12}, & a_{13}, & a_{14}, \quad \ldots \\ A_2: & a_{21}, & a_{22}, & a_{23}, & a_{24}, \quad \ldots \\ A_3: & a_{31}, & a_{32}, & a_{33}, & a_{34}, \quad \ldots \\ A_4: & a_{41}, & a_{42}, & a_{43}, & a_{44}, \quad \ldots \\ & & \ldots & & \end{array}$$

Построим последовательность B: $b_1, b_2, b_3, \ldots$, где

$$b_i = \begin{cases} 1, \text{если } a_{ii} = 0, \\ 0, \text{если } a_{ii} = 1, \end{cases} \quad i = 1, 2, 3, \ldots$$

Последовательность B лежит вне указанного пересчета. B отличается от A_1 элементом $b_1 \neq a_{11}$, от A_2 – элементом $b_2 \neq a_{22}$, от A_3 – элементом $b_3 \neq a_{33}$ и т. д. Следовательно, исходное множество C несчетно.

Определение. Множество A имеет *мощность континуума c*, если A эквивалентно множеству всех бесконечных последовательностей из 0 и 1.

Следствие. Множество C всех бесконечных последовательностей из 0 и 1 имеет мощность континуума: $|C| = c$ (в силу рефлексивности).

Утверждение. Множество $P(\mathbb{N})$ всех подмножеств множества натуральных чисел имеет мощность континуума.

Доказательство. Всякую бесконечную последовательность из 0 и 1 можно рассматривать как характеристическую функцию некоторого подмножества множества натуральных чисел. Следовательно, множество $P(\mathbb{N})$ имеет мощность континуума: $|P(\mathbb{N})| = c$.

Следствие. Множество всех подмножеств множества натуральных чисел несчетно.

Утверждение. Если к бесконечному множеству добавить конечное или счетное множество элементов, то его мощность не изменится.

Доказательство. Пусть A есть бесконечное множество, а B есть конечное или счетное множество, причем $A \cap B = \varnothing$. Покажем, что $A \sim A \cup B$. Выделим из множества A счетное подмножество A_1. Тогда $A = C \cup A_1$, где $C = A - A_1$, и $A \cup B = (C \cup A_1) \cup B = C \cup (A_1 \cup B)$. Так как $A_1 \cup B \sim A_1$, то $A \cup B = C \cup (A_1 \cup B)$, $C \cup (A_1 \cup B) \sim C \cup A_1$ в силу транзитивности и с учетом того, что $A = C \cup A_1$, получаем $A \cup B \sim A$.

Утверждение. Если A есть несчетное множество, а B есть конечное или счетное его подмножество, то $A - B \sim A$.

Доказательство. Пусть $C = A - B$. Тогда $A = C \cup B$. Множество C несчетно, ибо в противном случае C конечно или счетно, и тогда $A = C \cup B$ конечно или счетно. Множество $C \cup B \sim C$, или $A \sim C$, то есть $A \sim A - B$.

Теорема. Множество $U = [0, 1]$ имеет мощность континуума c.

Доказательство. Множество U эквивалентно множеству всех последовательностей из 0 и 1.

Замечание. 1. $|[0, 1]| = |(0, 1)| = |(0, 1]| = |[0, 1)| = c$.

2. Если $a < b$, то $|[a, b]| = c$, ибо функция $y = a + x(b - a)$ отображает $[0, 1]$ на $[a, b]$ взаимно-однозначно.

3. $|[a, b]| = |(a, b)| = |(a, b]| = |[a, b)| = c$.

4. $|(-\infty, \infty)| = |\mathbb{R}| = c$, ибо функция $y = \mathrm{tg}(x)$ отображает интервал $(a, b) = (-\pi/2, \pi/2)$ на всю числовую ось $\mathbb{R}$ взаимно-однозначно.

8. Кардинальные числа. Сравнение мощностей

Определение. *Мощность множества* есть класс эквивалентных между собой множеств. *Кардинальное число*, или кардинал, есть знак (символ), приписываемый мощности как классу эквивалентных между собой множеств. Мощности конечных множеств называются *финитными кардиналами*. Мощности бесконечных множеств называются *трансфинитными кардиналами*.

Пример. Счетной мощности (мощность множества натуральных чисел) присваивается кардинальное число $\aleph_0$ (алеф-нуль). Мощности множества вещественных чисел присваивается кардинальное число c.

Замечание. Мощность множества A обозначается через $|A|$, а также через $card(A)$ или $c(A)$. Мощность конечного множества есть число его элементов.

Пусть A, B есть произвольные множества и $|A|$, $|B|$ есть их мощности.

Априори возможны четыре случая.

1. Множество A эквивалентно некоторому подмножеству множества B, а множество B эквивалентно некоторому подмножеству множества A.

2. Множество A эквивалентно некоторому подмножеству множества B, а множество B не эквивалентно никакому подмножеству множества A.

3. Множество B эквивалентно некоторому подмножеству множества A, а множество A не эквивалентно никакому подмножеству множества B.

4. Множество A не эквивалентно никакому подмножеству множества B, а множество B не эквивалентно никакому подмножеству множества A.

Определение.

$|A| = |B|$, если $A \sim B$.

$|A| \le |B|$, если A эквивалентно некоторому подмножеству в B.

$|A| < |B|$, если A эквивалентно некоторому подмножеству в B, а множество B не эквивалентно никакому подмножеству множества A.

$|A| \ge |B|$, если $|B| \le |A|$.

$|A| > |B|$, если $|B| < |A|$.

Замечание. Случай, когда множество A не эквивалентно никакому подмножеству множества B, а множество B не эквивалентно никакому подмножеству множества A, невозможен.

Теорема (Кантор–Бернштейн). Если множество A эквивалентно некоторому подмножеству B_1 множества B, а множество B эквивалентно некоторому подмножеству A_1 множества A, то множества A и B эквивалентны (то есть имеют равную мощность). Коротко: $|A| \le |B| \ \& \ |B| \le |A| \to |A| = |B|$.

Доказательство. Случаи $B_1 = B$ и $A_1 = A$ можно исключить, ибо если $B_1 = B$, то условие теоремы утверждает, что $A \sim B$, из чего, естественно, следует $A \sim B$. Случай $A_1 = A$ аналогичен.

Итак, пусть $A_1 \subset A$, $B_1 \subset B$. Пусть функции $f\colon A \to B_1$, $g\colon B \to A_1$ устанавливают взаимно-однозначное соответствие между A и B_1 и между B и A_1, то есть $A \leftrightarrow_f B_1$, $B \leftrightarrow_g A_1$. С помощью функций f и g расслоим множества A и B на «кольца» следующим образом. Имеем:

$$A \leftrightarrow_f B_1 \subset B, B \leftrightarrow_g A_1 \subset A,$$
$$A_1 \leftrightarrow_f B_2 \subset B_1, B_1 \leftrightarrow_g A_2 \subset A_1,$$
$$A_2 \leftrightarrow_f B_3 \subset B_2, B_2 \leftrightarrow_g A_3 \subset A_2,$$
$$\ldots$$

Сформируем множества («кольца»):

$$K_0^A = A - A_1,\ K_0^B = B - B_1,$$
$$K_1^A = A_1 - A_2,\ K_1^B = B_1 - B_2,$$
$$K_2^A = A_2 - A_3,\ K_2^B = B_2 - B_3,$$
$$\ldots$$

Функции f и g устанавливают следующие взаимно-однозначные соответствия:

$$K_0^A \leftrightarrow_f K_1^B,\ K_0^B \leftrightarrow_g K_1^A,$$
$$K_2^A \leftrightarrow_f K_3^B,\ K_2^B \leftrightarrow_g K_3^A,$$
$$\ldots$$

Пусть множества $C = \bigcap_{i=1}^{\infty} A_i$, $D = \bigcap_{i=1}^{\infty} B_i$. Функции f и g устанавливают взаимно-однозначные соответствия между C и D. Если бы это было не так, то возникли бы аналогичные кольца в C и D, что по построению C и D невозможно.

Пусть множества

$$A_{\text{чет}} = \bigcup_{i=1}^{\infty} K_{2i}^{A} = K_0^A \cup K_2^A \cup K_4^A \cup \ldots$$

$$A_{\text{неч}} = \bigcup_{i=1}^{\infty} K_{2i+1}^{A} = K_1^A \cup K_3^A \cup K_5^A \cup \ldots$$

Аналогично построим множества $B_{\text{чет}}$, $B_{\text{неч}}$. Тогда

$A = A_{\text{чет}} \cup A_{\text{неч}} \cup C$, $B = B_{\text{чет}} \cup B_{\text{неч}} \cup D$.

Функция f устанавливает взаимно-однозначные соответствия:

$A_{\text{чет}} \leftrightarrow_f B_{\text{неч}}$, $A_{\text{неч}} \leftrightarrow_g B_{\text{чет}}$, $C \leftrightarrow_{f \text{ или } g} D$.

Тогда функция h: $A \to B$, определенная как

$$h(x) = \begin{cases} f(x), \text{если } x \in A_{\text{чет}} \cup C, \\ g(x), \text{если } x \in A_{\text{неч}} \end{cases}$$

устанавливает взаимно-однозначное соответствие между A и B. Следовательно, $|A| = |B|$. Теорема доказана.

Следствие. Если $A \subseteq B$, то $|A| \le |B|$.

Кардинальные числа можно сравнивать по величине.

Пусть A есть некоторое множество и $P(A)$ есть множество всех подмножеств множества A. Очевидно, что $|A| \le |P(A)|$, ибо взаимно-однозначное соответствие между A и частью $P(A)$ устанавливается, если каждому элементу a из A сопоставить одноэлементное множество $\{a\}$ из $P(A)$.

Теорема (Кантор). $|A| < |P(A)|$.

Доказательство. Покажем, что $|A| \ne |P(A)|$. Допустим противное: $|A| = |P(A)|$ для некоторого множества A. Тогда существует взаимно-однозначное соответствие f: $A \to P(A)$ между множествами A и $P(A)$. Пусть

$A_1 = \{a \in A: a \in f(a)\}$, $A_2 = \{a \in A: a \notin f(a)\}$.

Тогда $A_2 = A - A_1$. Множество $A_2 \in P(A)$. Пусть в нашем соответствии $f(b) = A_2$ для некоторого b из A. Каждый элемент из A попадает либо в A_1, либо в A_2. Если $b \in A_1$, то по построению A_1 будет $b \in f(b)$ и $f(b) = A_2$. Противоречие, ибо $b \in A_1$ и $b \in A_2$, что одновременно невозможно. Если $b \in A_2$, то по построению A_2 будет $b \notin f(b)$ и $f(b) = A_2$. Противоречие, ибо $b \in A_2$ и $b \notin A_2$, что одновременно невозможно. Следовательно, наше предположение о равенстве $|A|$ и $|P(A)|$ не верно. Остается взять $|A| \ne |P(A)|$, а так как $|A| \le |P(A)|$, то $|A| < |P(A)|$. Теорема доказана.

Иногда множество $P(A)$ всех подмножеств множества A обозначается через 2^A, а мощность $P(A)$ – через $2^{|A|}$. Тогда по теореме $|A| < 2^{|A|}$.

Отправляясь от произвольного множества A, по теореме Кантора можно построить возрастающую последовательность кардинальных чисел:

$$|A| < 2^{|A|} < 2^{2^{|A|}} < \ldots$$

Отправляясь от счетного множества $\mathbb{N}$ натуральных чисел, можно построить возрастающую последовательность кардиналов:

$$\aleph_0 < 2^{\aleph_0} = c = \aleph_1 < 2^{\aleph_1} = \aleph_2 < 2^{\aleph_2} = \aleph_3 < \ldots$$

Мощности $\aleph_0, \aleph_1 = c, \aleph_2 = 2^c, \aleph_3 = 2^{2^c}$, ... – это счетная мощность, континуум, гиперконтинуум, гипергиперконтинуум и т. д.

Кантор поставил проблему о существовании промежуточной мощности между $\aleph_0$ и $\aleph_1$ (континуум-гипотеза) и промежуточных мощностей между всякими $\aleph_i$ и $\aleph_{i+1}$ (обобщенная континуум-гипотеза). В работах К. Геделя и П. Коэна было установлено, что обе гипотезы не противоречат аксиоматической теории множеств (существует модель, в которой истинны аксиомы теории множеств, континуум-гипотеза, причем правила вывода сохраняют истинность выводимых формул) и не могут быть в ней доказаны (существует модель, в которой истинны аксиомы теории множеств и ложна континуум-гипотеза, причем правила вывода сохраняют истинность выводимых формул, а потому континуум-гипотеза не может быть доказана в теории множеств). Отсюда следует, что обе гипотезы независимы в аксиоматической теории множеств.

Часть I

МОДУЛЯРНАЯ АЛГЕБРА

В результате освоения учебного материала данной части студент должен:

- знать математический аппарат теории сравнений целых чисел и полиномов, универсальной и абстрактной алгебр, а также конечных полей, методику работы с математической литературой и методику самостоятельного изучения новых алгоритмов модулярной алгебры;
- уметь самостоятельно изучать методы и алгоритмы решения задач модулярной алгебры, проводить анализ результатов работы алгоритмов, самостоятельно изучать новые разделы модулярной алгебры;
- иметь навыки расширения своих знаний в применении математического моделирования при разработке алгоритмов решения прикладных задач модулярной алгебры.

Глава 1

Делимость

1.1. Позиционная система счисления

Пусть $\mathbb{Z} = \{..., -2, -1, 0, 1, 2, ...\}$ есть множество целых чисел, $\mathbb{N} = \{0, 1, 2, 3, ...\}$ есть множество натуральных чисел, $\mathbb{N}_+$ есть множество положительных натуральных чисел.

Сложение, вычитание, умножение, деление целых чисел определяются обычным образом.

Пусть a, b, c есть целые числа. Примем следующие обозначения.

$b \mid a$, b делит a (без остатка).

$b \nmid a$, b не делит a (без остатка).

$a \vdots b$, a делится на b (без остатка).

$\lfloor a/b \rfloor$ есть частное от деления a на b.

$\mathrm{mod}(a,b)$ есть остаток от деления a на b.

Определение. $b \mid a$, если $a = b \cdot q$ при некотором q. *a кратно b*, если $a = b \cdot q$ при некотором q. Число b есть *собственный делитель* a, если $b \mid a$, $b \neq \pm 1$, $b \neq \pm a$.

Замечание. 1. Если a кратно b и b кратно c, то a кратно c.

2. $1 \mid a$, $a \mid a$. Если $a \mid b$ и $b \mid a$, то $a = +b$ или $a = -b$.

3. Если $a \mid b$, $b \mid c$, то $a \mid c$.

4. Если $a \mid b$, то $\forall c \in \mathbb{Z}$ $(a \mid bc)$.

5. Если $k \in \mathbb{Z}$, $k \neq 0$, то $a \mid b \leftrightarrow ka \mid kb$.

6. Если $a \mid b$, $a \mid c$, то $\forall k \in \mathbb{Z}\ \forall l \in \mathbb{Z}(a \mid (bk + cl))$.

7. Если $a_1 \mid b_1$, ..., $a_n \mid b_n$, то $(a_1 \cdot ... \cdot a_n) \mid (b_1 \cdot ... \cdot b_n)$.

8. Если $a \mid b$, то $a^n \mid b^n$ $\forall n \in \mathbb{Z}$.

9. Если целые $l, ..., n, p, q, ..., s$ делятся на b и удовлетворяют равенству $k + l + ... + n = p + q + ... + s$, то k делится на b. В самом деле, $l = l_1 b$, ..., $n = n_1 b$, $p = p_1 b$, $q = q_1 b$, ..., $s = s_1 b$ и $k = p + q + ... + s - l - ... - n = (p_1 + q_1 + ... + s_1 - l_1 - ... - n_1)b$.

Утверждение (деление с остатком). Пусть $b \in \mathbb{N}_+$. Всякое $a \in \mathbb{Z}$ можно единственным образом представить в виде $a = bq + r$, где $q \in \mathbb{Z}$, $0 \leq r < b$.

Доказательство. Одно такое представление $a = bq + r$, $0 \leq r < b$ можно получить, если bq есть наибольшее кратное для b, не большее a. Если $a = bq_1 + r_1$, $0 \leq r_1 < b$, есть другое такое представление, то вычитание дает $0 = b(q - q_1) + r - r_1$, $r_1 - r = b(q - q_1)$, $r_1 - r$ кратно b. Так как $|r_1 - r| < b$, то $r_1 - r = 0$, $r_1 = r$, $q_1 = q$.

Замечание. 1. Если $a \in \mathbb{Z}$, $b \in \mathbb{Z}$, $b \neq 0$, то $\mathrm{mod}(a,b) = a - \lfloor a/b \rfloor \cdot b$.

2. Положим $\mathrm{rest}(a, b) = \begin{cases} \mathrm{mod}(a,b), & \text{если } \mathrm{mod}(a,b) \geq 0, \\ \mathrm{mod}(a,b) + b, & \text{если } \mathrm{mod}(a,b) < 0. \end{cases}$

Пример. Пусть $b = 12$.

$129 = 12 \cdot 10 + 9, 0 \leq 9 < 12;$
$-65 = 12 \cdot (-5) - 5 + 12 - 12 = 12 \cdot (-6) + 7, 0 \leq 7 < 12;$
$5 = 12 \cdot 0 + 5, 0 \leq 5 < 12;$
$-5 = 12 \cdot (-1) + 7, 0 \leq 7 < 12;$
$204 = 12 \cdot 17 + 0, 0 \leq 0 < 12.$

Теорема. Для всяких целых $a \geq 0$, $h \geq 2$ при некотором $s \geq 0$ существует единственное представление a в виде

$$a = a_s h^s + a_{s-1} h^{s-1} + ... + a_1 h + a_0, \tag{1.1}$$

где $0 \leq a_i \leq h - 1$ $(i = 0, 1, .., s)$, $a_s \neq 0$.

Доказательство. 1. *Существование*. Индукция по a.

Базис. $a = 0$. Тогда $0 = 0 \cdot h^0$, $a_0 = 0$, $s = 0$.

Предположение индукции. Допустим, что теорема верна для всякого натурального $a < n$.

Шаг индукции. Покажем, что теорема верна для $a = n$. По предыдущей теореме $n = hb + r$, $0 \leq r \leq h - 1$, $b < n$. Возможны два случая.

1. $b = 0$. Тогда $n = r$. Представление (1.1) выполняется при $s = 0$, $c_0 = r$.

2. $b \geq 1$. Так как $1 \leq b < n$, то по предположению индукции $b = b_u h^u + b_{u-1} h^{u-1} + ... + b_0$ при некотором $u \geq 0$ и $0 \leq b_i \leq h - 1$ $(i = 0, 1, ..., u)$, $b_u \geq 1$. Тогда $n = hb + r = h(b_u h^u + + b_{u-1} h^{u-1} + ... + b_0) + r = b_u h^{u+1} + b_{u-1} h^u + ... + b_0 h + r$, и мы опять имеем представление в виде (1.1). Существование доказано.

2. *Единственность*. Если

$$a = a_s h^s + a_{s-1} h^{s-1} + ... + a_1 h + a_0 = a'_u h^u + ... + a'_1 h + a'_0, \tag{1.2}$$

то $a = h(a_s h^{s-1} + ... + a_1) + a_0 = h(a'_u h^{u-1} + ... + a'_1) + a'_0$. Так как представление $a = hq + r$, $0 \leq r \leq h - 1$, единственно, то $a_0 = a'_0$ и $d = a_s h^{s-1} + ... + a_1 = a'_u h^{u-1} + ... + a'_1$. Аналогично $a_1 = a'_1$, $a_2 = a'_2$ и т. д. Пусть $s < u$. Тогда $a_0 = a'_0$, $a_1 = a'_1$, ..., $a_s = a'_s$. Удалим одинаковые слагаемые a_0, $a_1 h$, ..., $a_s h^s$ в (1.2) и получим $a'_u h^u + ... + a'_{s+1} h^{s+1} = 0$. Противоречие, ибо $a'_u \geq 1$. Поэтому $s < u$ невозможно. Неравенство $s > u$ тоже невозможно. Остается $s = u$.

Теорема доказана.

Определение. Представление (1.1) называется *представлением числа a* (*в системе счисления*) *по основанию h*. Числа a_s, a_{s-1}, ..., a_0 называются *цифрами* числа a по основанию h, и тогда пишут, что по основанию h число

$$a = (a_s a_{s-1} ... a_0)_h.$$

Замечание. Представление (1.1) числа a можно рассматривать как многочлен степени s относительно h, который можно использовать для представления

в компьютере сверхбольших чисел (порядка нескольких сот цифр в десятеричном представлении) и для производства целочисленных арифметических операций над ними – сложения, умножения, вычитания, нахождения частного и остатка при их делении, перехода от одной системы счисления к другой и т. д.

Алгоритм вычисления h-ричной записи 10-ричного числа a

ВХОД. Натуральные числа $a > 0$ и $h \geq 2$.
ВЫХОД. h-ричная запись числа $a = (a_t a_{t-1} \ldots a_1 a_0)_h$.
1. $i := 0$.
2. Пока $q \neq 0$, выполняется следующее.
   2.1. $r := \mathrm{mod}(a, h)$, $q := (a - r)/h$.
   2.2. $a := q$, $a_i := r$.
   2.3. $i := i + 1$.
3. Вернуть a.

Пример. Записать 10-ричное число 160 в 7-ричной системе.
Решение. По основанию h число $a_{10} = (a_t a_{t-1} \ldots a_1 a_0)_h$.

$i := 0$, $a := 160$,
$r := \mathrm{mod}(a,h) = \mathrm{mod}(160,7) = 6$, $q := (a - r)/h = (160 - 6)/7 = 22$,
$a_0 := r = 6$, $i := i + 1 = 0 + 1 = 1$; $a := q = 22$,
$r := \mathrm{mod}(a,h) = \mathrm{mod}(22,7) = 1$, $q := (a - r)/h = (22 - 1)/7 = 3$,
$a := q = 3$, $a_1 := r = 1$, $i := i + 1 = 1 + 1 = 2$.
$r := \mathrm{mod}(a,h) = \mathrm{mod}(3,7)=3$; $q := q := (a - r)/h = (3 - 3)/7 = 0$.
$a := q = 0$, $a_2 := r = 3$, $i := i + 1 = 2 + 1 = 3$.

Ответ. $a = 160_{10} = (a_2 a_1 a_0)_7 = 316_7$.

1.2. Простые числа

Определение. Натуральное число $p \geq 2$ есть *простое число*, если p делится только на 1 и на p, то есть p не имеет собственных делителей. Целое $a > 2$ есть *составное число*, если a имеет собственные делители.

Замечание. 1. Наименьший положительный делитель q целого $a > 1$ есть простое число. В самом деле, пусть $q|a$. Если q есть составное число, то q имеет делитель q_1, для которого $1 < q_1 < q$. Так как $q_1|q$, $q|a$, то $q_1|a$. Противоречие с минимальностью q.

2. Если $q > 1$ есть наименьший делитель составного целого $a > 1$, то $q \leq \sqrt{a}$. В самом деле, так как q есть наименьший делитель a, то $a = qa_1$, $a_1 \geq q$. Перемножим оба выражения и получим $aa_1 \geq qa_1 q$, $a \geq q^2$, $q \leq \sqrt{a}$.

Теорема. Существует бесконечно много простых чисел.

Доказательство. Пусть $p_1, p_2, \ldots, p_k$ есть простые числа. Если число $s = p_1 p_2 \ldots p_k + 1$ простое, то s есть новое простое число. Если s составное, то наименьший больший единицы делитель p для s есть новое простое число. Делитель p не есть один из p_1, $p_2, \ldots, p_k$, иначе $p|s$, $p|(p_1 p_2 \ldots p_k + 1)$, и тогда $p|1$. Противоречие.

Утверждение (число простых чисел). Пусть $\pi(x)$ есть число простых чисел, не превосходящих x. Тогда

1. $\lim_{x\to\infty} \frac{\pi(x)}{x/\ln x} = 1$.
2. Для $x \geq 17 \pi(x) > \frac{x}{\ln x}$; для $x > 1 \pi(x) < 1{,}25506 \frac{x}{\ln x}$.
3. Для $x \geq 17 \frac{x}{\ln x} < \pi(x) < 1{,}25506 \frac{x}{\ln x}$.

Тест Миллера–Рабина для простоты числа

ВХОД. Нечетное целое $n \geq 3$ и параметр безопасности $t \geq 1$.

ВЫХОД. Ответ «простое» или «составное» на вопрос: «Является ли n простым числом?»

1. Найти s и нечетное r, для которых $n - 1 = 2^s r$.
2. Для i от 1 до t выполнить следующее.
   2.1. Выбрать случайное целое a, $2 \leq a \leq n - 1$.
   2.2. Вычислить $y := a^r \pmod n$.
   2.3. Если $y \neq 1$ и $y \neq n-1$, то выполнить следующее.
   $j := 1$.
   Пока $j \leq s - 1$ и $y \neq n - 1$, выполнить следующее.
   Вычислить $y := y^2 \pmod n$.
   Если $y = 1$, то вернуть «составное».
   $j := j + 1$.
   Если $y \neq n - 1$, то вернуть «составное».
3. Вернуть «простое».

Замечание. Вероятность получить неверный ответ для целого положительного n меньше $(1/4)^t$.

1.3. Факторизация целых чисел

Всякое целое a и p могут иметь общими делителями только 1 или p. В последнем случае a делится на p.

Если произведение нескольких множителей делится на простое p, то хотя бы один множитель делится на p. Допустим противное: все множители не делятся на p. Тогда произведение этих множителей не делится на p. Противоречие. Тогда хотя бы один множитель делится на p.

Теорема (основная теорема арифметики). Всякое целое большее единицы число можно факторизовать (разложить в произведение (положительных) простых сомножителей) единственным образом с точностью до порядка сомножителей.

Доказательство. Пусть целое $a > 1$. Пусть p_1 есть наименьший (положительный) простой делитель a. Тогда $a = p_1 a_1$. Если $a_1 = 1$, нужная факторизация получена. Если $a_1 > 1$, то аналогично получаем $a_1 = p_2 a_2$. Если $a_2 = 1$, нужная факторизация получена. Если $a_2 > 1$, то получаем $a_2 = p_3 a_3$. И так далее. Последовательность a, a_1,

a_2, ... убывает. Поэтому процесс закончится при некотором $a_{n-1} = p_n a_n$, $a_n = 1$. В результате получаем факторизацию $a = p_1 p_2 ... p_n$.

Покажем единственность этой факторизации. Допустим существование другой: $a = q_1 q_2 ... q_s$, и пусть для определенности $s \geq n$. Тогда $p_1 p_2 ... p_n = q_1 q_2 ... q_s$. Правая часть равенства делится на простое p_1. Тогда левая часть равенства делится на q_1 и хотя бы один ее множитель делится на q_1. Пусть $q_1 | p_1$. Тогда $p_1 = q_1$. Сократим равенство на q_1, и пусть $p_2 ... p_n = q_2 ... q_s$. Аналогично получим:

$q_2 = p_2,\ p_3 ... p_n = q_3 ... q_s,$
$q_3 = p_3,\ p_4 ... p_n = q_4 ... q_s,$
...
$q_n = p_n,\ 1 = q_{n+1} ... q_s.$

Поэтому $q_{n+1} = ... = q_s = 1$ и факторизация единственна.

Замечание. 1. Простые сомножители в факторизации могут повторяться. Пусть $p_1 < p_2 < ... < p_k$ есть все различные сомножители в факторизации числа a и a_i есть число вхождений простого p_i в факторизацию. Тогда представление $a = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$ есть каноническая факторизация числа a, которая единственна.

2. Если $a = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$ есть каноническая факторизация целого a, то

$$d \mid a \leftrightarrow d = p_1^{b_1} p_2^{b_2} \dots p_k^{b_k},$$

где $0 \leq b_1 \leq a_1$, ..., $0 \leq b_k \leq a_k$. Поэтому число a имеет $f(a) = (a_1 + 1)(a_2 + 1) ... (a_k + 1)$ различных делителей.

3. Иногда каноническая факторизация $a = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$ включает все отсутствующие простые числа p между 2 и p_k в виде p^0.

4. Распознавание простоты целого числа с 125 цифрами в его десятеричном представлении существующими методами может быть выполнено в несколько минут. Факторизация такого числа на существующих компьютерах потребует миллионы лет компьютерных вычислений, то есть практически неосуществима. С появлением квантовых компьютеров задача факторизации такого числа может быть практически решена за реальное время. Так, например, квантовый компьютер D-Wave канадской фирмы D-Wave Systems способен за секунду решать задачи, на выполнение которых у классического компьютера с одноядерным процессором ушло бы 10 тыс. лет.

Замечание. Если положительное целое n удовлетворяет неравенству $b^{k-1} \leq n < b^k$, то n имеет k цифр по основанию b. Логарифмируем неравенства по основанию b и получаем $k - 1 \leq \log_b n < k$, откуда $k = \lfloor \log_b n \rfloor + 1 = \left\lfloor \dfrac{\ln n}{\ln b} \right\rfloor + 1$.

1.4. Наибольший общий делитель

Определение. *Общий делитель* од(a, b, ..., l) целых a, b, ..., l есть всякое целое, которое делит каждое из a, b, ..., l.

Пример. Целое 3 есть общий делитель для 18, 24, 36. Целое 6 есть тоже общий делитель для 18, 24, 36.

Определение. *Наибольший общий делитель* нод(a, b, ..., l) или (a, b, ..., l) чисел a, b, ..., l есть наибольший положительный делитель среди всех общих делителей для a, b, ..., l. Полагают, что нод(0, ..., 0) = 0.

Замечание. 1. (a, b, ..., l) есть наибольшее положительное целое, которое делит каждое целое из a, b, ..., l.

2. $d = (a, b)$, если 1) d = од(a, b), 2) если $c|a$, $c|b$, то $c|d$.

Определение. Целые a, b, ..., l *взаимно-просты*, если (a, b, ..., l) = 1.

Замечание. Если целые числа попарно взаимно-просты, то они взаимно-просты. Обратное неверно.

Пример. $(18, 24, 36) = 6, (12, 24, 36) = 12, (14, 28) = 7, (8, 13, 21) = 1, \forall a \neq 0\ ((0,a) = a)$, $\forall a \neq 0$ ((1, a) = 1).

Замечание. 1. Если $a = bq + c$, то множество общих делителей для a и b совпадает с множеством общих делителей для b и c. В частности, $(a, b) = (b, c)$.

2. Если $c = 0$ и не все целые a, ..., b равны нулю, то (a, ..., b, c) = (a, ..., b).

Теорема. Если целые $a > 1$, $b > 1$ и их канонические факторизации

$$a = p_1^{a_1} p_2^{a_2} \dots p_s^{a_s},\ b = p_1^{b_1} p_2^{b_2} \dots p_s^{b_s}$$

где p_1, ..., p_s есть все различные простые делители для a или b, то

$$d = (a,b) = p_1^{\min(a_1, b_1)} \cdot p_2^{\min(a_2, b_2)} \cdot \ldots \cdot p_s^{\min(a_s, b_s)}.$$

Доказательство. Пусть $a > 1$, $b > 1$ и p_1, ..., p_s есть множество всех простых чисел, которые делят хотя бы один из a, b. Если простое p из p_1, ..., p_s отсутствует в канонической факторизации a, то добавим к ней множитель p^0. Далее имеем следующее.

1. $d > 0$.
2. Так как $a_1 \geq \min(a_1, b_1)$, ..., $a_s \geq \min(a_s, b_s)$, то $d|a$, $d|b$.
3. Если $h|a$, $h|b$, то $h = p_1^{d_1} p_2^{d_2} \dots p_s^{d_s}$, где

   $d_1 \leq a_1$, $d_1 \leq b_1$, откуда $d_1 \leq \min(a_1, b_1)$,

   ...

   $d_s \leq a_s$, $d_s \leq b_s$, откуда $d_s \leq \min(a_s, b_s)$.

   Тогда $h|d$. Следовательно, $d = (a,b)$.

Замечание. 1. Если $a_1 > 1$, ..., $a_n > 1$,

$$a_1 = p_1^{a_{11}} p_2^{a_{12}} \dots p_s^{a_{1s}},\ a_n = p_1^{a_{n1}} p_2^{a_{n2}} \dots p_s^{a_{ns}},$$

где p_1, ..., p_s есть множество всех различных простых делителей чисел a_1, ..., a_n, то $(a_1, ..., a_n) = p_1^{\min(a_{11}, a_{1s})} \cdot p_2^{\min(a_{n2}, a_{ns})}$.

2. $(a_1, ..., a_{n-1}, a_n) = ((a_1, ..., a_{n-1}), a_n)$.

1.4.1. Алгоритм Евклида вычисления наибольшего общего делителя

Пусть a и b есть натуральные числа и $a \geq b$. Деление с остатком дает следующую последовательность равенств:

$a = bq_1 + r_2,\ 0 < r_2 < b,$
$b = r_2q_2 + r_3,\ 0 < r_3 < r_2,$
$r_2 = r_3q_3 + r_4,\ 0 < r_4 < r_3,$
$r_3 = r_4q_4 + r_5,\ 0 < r_5 < r_4,$
...
$r_{n-2} = r_{n-1}\, q_{n-1} + r_n,$
$r_{n-1} = r_n\, q_n$ (здесь $r_{n+1} = 0$).

Так как последовательность остатков $r_2, r_3, \ldots$ строго убывает, то $r_{n+1} = 0$ при некотором n. Пусть $d = (a, b)$. Тогда из первого равенства получаем, что $d|a$, $d|b$, $d|r_2$, откуда $d = (b, r_2)$, ибо если $d'|b$, $d'|r_2$ для некоторого $d' > d$, то $d'|a$ и $d \neq (a, b)$. Аналогичные рассуждения, примененные к вышенаписанным равенствам, последовательно дают:

$$d = (a, b) = (b, r_2) = (r_2, r_3) = \ldots = (r_{n-1}, r_n) = r_n.$$

Следовательно, $(a, b) = r_n$.

Замечание. Множество общих делителей для a и b совпадает с множеством делителей для $d = (a, b)$.

Алгоритм Евклида вычисления наибольшего общего делителя

ВХОД. Натуральные числа a и b, $a \geq b$.
ВЫХОД. (a, b).
1. Пока $b \neq 0$, выполнять следующее.
   $q := \lfloor a/b \rfloor$, $r := a - qb$, $a := b$, $b := r$.
2. Вернуть a.

Пример. Найти (1050, 231).
$1050 = 231 \cdot 4 + 126$, остаток $r = 126$.
$231 = 126 \cdot 1 + 105$, остаток $r = 105$.
$126 = 105 \cdot 1 + 21$, остаток $r = 21$.
$105 = 21 \cdot 5$, остаток $r = 0$.
$d = (1050, 231) = 21$.

Утверждение. $\forall m \in \mathbb{N}\ ((am, bm) = (a, b)m)$.

Доказательство. Умножим равенства алгоритма Евклида на m и получим $(am, bm) = r_nm$. Так как $(a, b) = r_n$, то $(am, bm) = (a, b)m$.

Замечание. Теорема верна для нескольких чисел.

Утверждение. Если $d = \text{од}(a,b)$, то $\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{(a,b)}{d}$.

Доказательство.

$$(a,b) = \left(\frac{a}{d} \cdot d, \frac{b}{d} \cdot d\right) = \left(\frac{a}{d}, \frac{b}{d}\right)d, \text{ откуда } \left(\frac{a}{d}, \frac{b}{d}\right) = \frac{(a,b)}{d}.$$

Следствие. $\left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right) = 1.$

Замечание. Теорема верна для нескольких чисел.

Утверждение. Если $(a, b) = 1$, то $(ac, b) = (c, b)$.

Доказательство. (ac, b) делит ac, b и ac, bc. Тогда (ac, b) делит $(ac, bc) = (a, b)c = c$, то есть (ac, b) делит c. Но (ac, b) делит b. Поэтому(ac, b) делит (c, b).

(c, b) делит c, b и ac, b. Тогда (c, b) делит (ac, b).

(ac, b) и (c, b) делят друг друга. Тогда $(ac, b) = (c, b)$.

Утверждение. Если $(a, b) = 1$ и $b|ac$, то $b|c$.

Доказательство. Из $(a, b) = 1$ следует $(ac, b) = (c, b)$. Так как $b|ac$, то $(c, b) = (ac, b) = b$ делит c.

Теорема. Если каждое из $a_1, ..., a_m$ взаимно-просто с каждым из $b_1, ..., b_n$, то произведение $a_1 \cdot ... \cdot a_m$ взаимно-просто с произведением $b_1 \cdot ... \cdot b_n$.

Доказательство. Пусть $k = 1, 2, ... n$. Тогда

$(a_1, b_k) = 1 \to (a_1a_2, b_k) = (a_2, b_k) = 1.$
$(a_1a_2, b_k) = 1 \to (a_1a_2a_3, b_k) = (a_3, b_k) = 1.$
...
$(a_1a_2 ... a_{n-1}, b_k) = 1 \to (a_1a_2 ... a_{n-1}a_n, b_k) = (a_n, b_k) = 1.$

Пусть $A = a_1 a_2 ... a_n$. Тогда $(A, b_k) = (b_k, A) = 1$, $k = 1, 2, ..., n$.

Далее

$(b_1, A) = 1 \to (b_1b_2, A) = (b_2, A) = 1.$
$(b_1b_2, A) = 1 \to (b_1b_2b_3, A) = (b_1b_2, A) = 1.$
...
$(b_1...b_{n-1}, A) = 1 \to (b_1...b_{n-1}b_n, A) = (b_1...b_{n-1}, A) = 1.$
$(a_1 \cdot ... \cdot a_m, b_1 \cdot ... \cdot b_n) = 1.$

Замечание. 1. Если $(a, b) = 1$, то $\forall n \in \mathbb{N}\ \forall m \in \mathbb{N}\ ((a^n, b^m) = 1)$.

2. Если для некоторых положительных натуральных n и m $(a^n, b^m) = 1$, то $(a, b) = 1$. В самом деле, если $(a, b) = d$, то $d|a$, $d|b$, $d|a^n$, $d|b^m$, $d|((a^n, b^m))$, $d|1$, $d = 1$.

3. Если p есть простое число, $(a, p^m) \neq 1$, то $(a, p) \neq 1$, $p|a$.

4. Если $(a_1, a_2) = d_2$, $(d_2, a_3) = d_3$, ..., $(d_{n-1}, a_n) = d_n$, то $(a_1, a_2, ..., a_n) = d_n$. В самом деле, множество общих делителей для a_1, a_2 совпадает с множеством делителей для $d_2 = (a_1, a_2)$. Множество общих делителей для d_2, a_3 (множество общих делителей для a_1, a_2, a_3) совпадает с множеством делителей для $d_3 = (d_2, a_3)$. И так далее. Множество общих делителей для a_1, a_2, a_3 совпадает с множеством делителей для $d_n = (d_{n-1}, a_n)$. Так как d_n есть наибольший делитель для d_n, то $(a_1, ..., a_n) = d_n$.

Теорема. $\forall a_1 \in \mathbb{Z} ... \forall a_n \in \mathbb{Z}\ \exists \lambda_1 \in \mathbb{Z} ... \exists \lambda_n \in \mathbb{Z}$ (нод$(a_1, ..., a_n) = \sum_{i=1}^{n} \lambda_i a_i$).

Доказательство. Пусть $S = \{\sum_{i=1}^{n} \mu_i a_i$: все $\mu_i \in \mathbb{Z}\}$. Пусть $d = \sum_{i=1}^{n} \lambda_i a_i$ есть наименьшее положительное целое из S. Покажем, что $d = (a_1, ..., a_n)$. Так как $d \neq 0$, то каждое $a_i = q_i d + r_i$ с $0 \leq r_i < d$. Покажем, что все $r_i = 0$. Пусть для простоты $i = 1$. Допустим противное: $r_1 \neq 0$. Целое $r_1 = a_1 - q_1 d = a_1 - q_1(\lambda_1 a_1 + ... + \lambda_n a_n) = (1 - \lambda_1 q_1)a_1 - q_1\lambda_2 a_2 - - ... - q_1\lambda_n a_n \in S$ и $0 < r_1 < d$. Противоречие с минимальностью d. Следовательно, все $r_i = 0$, $a_i = q_i d$, $d|a_i$, $d =$ од$(a_1, ..., a_n)$.

Если s есть любой другой од$(a_1, ..., a_n)$, то

$a_i = h_i s$, $d = \sum_{i=1}^{n} \lambda_i a_i = \sum_{i=1}^{n} \lambda_i h_i s = s\sum_{i=1}^{n} \lambda_i h_i$, и $s|d$.

Тогда $d =$ нод$(a_1, ..., a_n)$.

Следствие. 1. $\forall a_1 \in \mathbb{Z}\ \forall a_2 \in \mathbb{Z}\ \exists \lambda_1 \in \mathbb{Z}\ \exists \lambda_2 \in \mathbb{Z}\ ((a_1, a_2) = \lambda_1 a_1 + \lambda_2 a_2)$.

2. Если $a_1 \in \mathbb{Z}$, $a_2 \in \mathbb{Z}$ и $1 = (a_1, a_2)$, то $\lambda_1 \in \mathbb{Z}$, $\lambda_2 \in \mathbb{Z}$ $(1 = \lambda_1 a_1 + \lambda_2 a_2)$.

1.4.2. Расширенный алгоритм Евклида вычисления наибольшего общего делителя

Алгоритм Евклида может быть описан следующим образом:

$a = bq_1 + r_2$, $0 < r_2 < b$, $q_1 = \lfloor a/b \rfloor$, $r_2 = a - bq_1$,
$b = r_2 q_2 + r_3$, $0 < r_3 < r_2$, $q_2 = \lfloor b/r_2 \rfloor$, $r_3 = b - r_2 q_2$,
$r_2 = r_3 q_3 + r_4$, $0 < r_4 < r_3$, $q_3 = \lfloor r_2/r_3 \rfloor$, $r_4 = r_2 - r_3 q_3$,
$r_3 = r_4 q_4 + r_5$, $0 < r_5 < r_4$, $q_4 = \lfloor r_3/r_4 \rfloor$, $r_5 = r_3 - r_4 q_4$,
...
$r_{n-2} = r_{n-1} q_{n-1} + r_n$, $q_{n-1} = \lfloor r_{n-2}/r_{n-1} \rfloor$, $r_n = r_{n-2} - r_{n-1} q_{n-1}$,
$r_{n-1} = r_n q_n + r_n$, $q_{n-1} = \lfloor r_{n-2}/r_{n-1} \rfloor$, $r_n = r_{n-2} - r_{n-1} q_{n-1}$,
$r_{n-1} = r_n q_n$ (здесь $r_{n+1} = 0$), $d = r_n$.

Тогда

$r_2 = a - bq_1 = a \cdot 1 + b(-q_1) = aq_1 + bv_1$, $u_1 = 1$, $v_1 = -q_1$,
$r_3 = b - r_2 q_2 = b - (ar_1 + bv_1) = b(1 - v_1) + a(-u_1) = au_2 + bv_2$, $u_2 = 1 - v_1$, $v_2 = -u_1$,
$r_4 = r_2 - r_3 q_3 = (au_1 + bv_1) - (au_2 + bv_2)q_3 = a(u_1 - u_2 q_3) + b(v_1 - v_2 q_3) = au_3 + bv_3$,
$u_3 = u_1 - u_2 q_3$, $v_3 = v_1 - v_2 q_3$,
$r_5 = r_3 - r_4 q_4 = (au_2 + bv_2) - (au_3 + bv_3)q_3 = a(u_2 - u_3 q_4) + b(v_2 - v_3 q_4) = au_4 + bv_4$,
$u_4 = u_2 - u_3 q_4$, $v_4 = v_2 - v_3 q_4$,
...
$d = r_n = r_{n-2} - r_{n-1} q_{n-1} = (au_{n-3} + bv_{n-3}) - (au_{n-2} + bv_{n-2})q_{n-1} =$
$= a(u_{n-3} - u_{n-2} q_{n-1}) + b(v_{n-3} - v_{n-2} q_{n-1}) = au_{n-1} + bv_{n-1}$,
$u_{n-1} = u_{n-3} - u_{n-2} q_{n-1}$, $v_{n-1} = v_{n-3} - v_{n-2} q_{n-1}$.

Получили: $d = r_n$, $u = u_{n-1}$, $v = v_{n-1}$.

Расширенный алгоритм Евклида вычисления $d =$ нод(a,b), $a \geq b$, и чисел u, v, для которых $d = ua + vb$

ВХОД. Натуральные числа a и b, $a \geq b$.
ВЫХОД. $d =$ нод(a,b) и целые u, v, для которых $d = ua + vb$.
1. Если $b = 0$, то $d := a$, $u := 1$, $v := 0$ и вернуть (d, u, v).
2. $u_2 := 1$, $u_1 := 0$, $v_2 := 0$, $v_1 := 1$.
3. Пока $b > 0$, выполнять следующее.
   3.1. $q := \lfloor a/b \rfloor$, $r := a - qb$, $u := u_2 - q\,u_1$, $v := v_2 - q\,v_1$.
   3.2. $a := b$, $b := r$, $u_2 := u_1$, $u_1 := u$, $v_2 := v_1$, $v_1 := v$.
4. $d := a$, $u := u_2$, $v := v_2$, вернуть (d, u, v).

Пример. Найти $d = (a, b)$ и целые u, v, для которых $d = au + bv$.
Целые $a = 5187$, $b = 1520$.
Решение. Вычисления приведены в следующей таблице.

n	q	r	u	v	a	b	u_2	u_1	v_2	v_1
0	–	–	–	–	5187	1520	1	0	0	1
1	3	627	1	–3	1520	627	0	1	1	–3
2	2	266	–2	7	627	266	1	–2	–3	7
3	2	95	5	–17	266	95	2	5	7	–17
4	2	76	–12	41	95	76	5	–12	–17	41
5	1	19	17	–58	76	19	–12	17	41	–58
6	4	0	–80	273	19	0	17	–80	–58	273

Ответ. $d = (a, b) = (3549, 1040) = 19$, $u = 17$, $v = -58$.
Теорема. $\forall s \in \mathbb{N}_+ \; \forall t \in \mathbb{N}_+ \; \forall r \in \mathbb{N}_+, \; s \le t$ (нод(s, t) = нод$(s, t - rs)$).
Доказательство. Если $d|s$, $d|t$, то $d|(t - rs)$. Поэтому всякий од(s, t) есть также од$(s, t - rs)$. Аналогично всякий од$(s, t - rs)$ есть также од(s,t), ибо $t = (t - rs) + rs$. Получено, что множество всех од(s, t) совпадает со множеством всех од$(s, t - rs)$. Следовательно, нод(s, t) = нод$(s, t - rs)$.
Замечание. Эта теорема дает алгоритм вычисления (s, t) последовательным вычитанием меньшего из большего, пока получающиеся два целых числа не совпадут. Эти равные целые есть (s, t).
Теорема. Если t, m, n есть положительные целые, то

$$\text{нод}(t^n - 1, t^m - 1) = t^{\text{нод}(n,m)} - 1.$$

Доказательство. Индукция по max(n, m). Если max$(n, m) = 1$ или $n = m$, то результат тривиален. Иначе допустим $m < n$ и заметим, что

$$(t^n - 1) - t^{n-m}(t^m - 1) = t^{n-m} - 1.$$

Тогда по предыдущей теореме

$$(t^n - 1, t^m - 1) = \left(\underbrace{t^m - 1}_{s}, \underbrace{t^n - 1}_{t}\right) = \left(\underbrace{t^m - 1}_{s}, \underbrace{t^n - 1}_{t} - \underbrace{t^{n-m}}_{r}\left(\underbrace{t^m - 1}_{s}\right)\right) =$$

$$= (t^m - 1, t^{n-m} - 1) = t^{(m, n-m)} - 1 = t^{(n, m)} - 1.$$

Следствие. При тех же допущениях $(x^{q^n} - x, x^{q^d} - x) = x^{q^{(n,d)}}$.

1.5. Наименьшее общее кратное

Определение. *Общее кратное* ок$(a, b, ..., l)$ целых $a, b, ..., l$ есть всякое целое, которое кратно каждому из $a, b, ..., l$.
Определение. *Наименьшее общее кратное* нок$(a, b, ..., l)$ или $[a, b, ..., l]$ целых $a, b, ..., l$ есть наименьшее неотрицательное целое среди всех общих кратных для $a, b, ..., l$.

Замечание. 1. $[a, b, ..., l]$ есть наименьшее неотрицательное целое, которое делится на каждое целое из $a, b, ..., l$.

2. $d = [a, b]$, если 1) $a|d, b|d$, 2) если $a|c, b|c$, то $d|c$.

Пример. ок$(18, 21) = 18 \cdot 21 = 378$, ок$(6, 12, 18) = 72$; $[18, 21] = 126$, $[6, 12, 18] = 36$.

Замечание. 1. $[a_1, ..., a_n] = m \leftrightarrow$ 1) $0 < m, m \in \mathbb{Z}$ 2) $a_1|m, ..., a_n|m$, 3) если $0 < M, M \in \mathbb{Z}$ и $a_1|M, ..., a_n|M$, то $m \le M$.

2. Если $a_n = 1$, то $[a_1, ..., a_{n-1}, a_1] = [a_1, ..., a_{n-1}]$.

Утверждение. Если целые $a > 1$, $b > 1$ и их факторизации

$$a = p_1^{a_1} p_2^{a_2} \dots p_s^{a_s}, \ b = p_1^{b_1} p_2^{b_2} \dots p_s^{b_s},$$

где $p_1, ..., p_s$ есть все различные простые делители для a или b, то

$$m = [a,b] = p_1^{\max(a_1, b_1)} \cdot p_2^{\max(a_2, b_2)} \cdot \dots \cdot p_s^{\max(a_s, b_s)}.$$

Доказательство. Пусть $a > 1$, $b > 1$ и $p_1, ..., p_s$ есть все простые числа, которые делят хотя бы одно из a, b. Если простое p из $p_1, ..., p_s$ отсутствует в канонической факторизации a, то добавим к ней множитель p^0. Аналогично для b. Далее имеем следующее.

1. $m > 0$ есть целое число.

2. $a_1 \le \max(a_1, b_1), ..., a_s \le \max(a_s, b_s)$. Поэтому $a_1|m, ..., a_n|m$.

3. Пусть $M > 0$ есть целое число и $a_1|M, ..., a_n|M$. Целое $M = p_1^{l_1} p_2^{l_2} \dots p_s^{l_s} N$ (все $l_i \ge 0$). Так как $a_1|M, ..., a_n|M$, то $a_1 \le l_1, b_1 \le l_1, ..., a_s \le l_s, b_s \le l_s$, откуда $l_1 \ge \max(a_1, b_1), ..., l_s \ge \max(a_s, b_s)$. Поэтому $m|M$, откуда $m \le M$. Следовательно, m есть наименьшее общее кратное для a и b.

Замечание. 1. Если $a_1 > 1, ..., a_n > 1$,

$$a_1 = p_1^{a_{11}} p_2^{a_{12}} \dots p_s^{a_{1s}}, \dots, a_n = p_1^{a_{n1}} p_2^{a_{n2}} \dots p_s^{a_{ns}},$$

где $p_1, ..., p_s$ есть множество всех различных простых делителей чисел $a_1, ..., a_n$, то

$$[a_1, ..., a_n] = p_1^{\max(a_{11}, \dots, a_{n1})} \cdot \dots \cdot p_s^{\max(a_{1s}, \dots, a_{ns})}.$$

2. $[a_1, ..., a_{n-1}, a_n] = [[a_1, ..., a_{n-1}], a_n]$.

Теорема. Пусть $a \ge 1$, $b \ge 1$ есть натуральные числа, $d = (a, b)$, $m = [a, b]$. Тогда $dm = ab$.

Доказательство. Пусть $a > 1$, $b > 1$ и $a = p_1^{a_1} p_2^{a_2} \dots p_s^{a_s}$, $b = p_1^{b_1} p_2^{b_2} \dots p_s^{b_s}$, где $p_1, ..., p_s$ есть все различные простые делители чисел a или b. Если простое p из $p_1, ..., p_s$ отсутствует в канонической факторизации a, то добавим к ней множитель p^0. Аналогично для b. Далее имеем следующее.

$$d = (a,b) = p_1^{\min(a_1, b_1)} \cdot p_2^{\min(a_2, b_2)} \cdot \dots \cdot p_s^{\min(a_s, b_s)},$$
$$m = [a,b] = p_1^{\max(a_1, b_1)} \cdot p_2^{\max(a_2, b_2)} \cdot \dots \cdot p_s^{\max(a_s, b_s)},$$
$$\min(a_1, b_1) + \max(a_1, b_1) = a_1 + b_1,$$
$$\dots$$
$$\min(a_s, b_s) + \max(a_s, b_s) = a_s + a_s, \text{ откуда } dm = ab.$$

Следствие. $[a, b] = \dfrac{a \cdot b}{(a,b)}$.

Замечание. 1. Всякое ок$(a, b) = [a, b] \cdot t$ для некоторого натурального t.

2. $[a_1,\ldots,a_n] = \dfrac{a_1 \cdot \ldots \cdot a_n}{(a_1,\ldots,a_n)}$.

3. Наименьшее общее кратное взаимно-простых чисел равно их произведению.

4. Если $m_1|a, \ldots, m_k|a$, то $[m_1, \ldots, m_k]|a$.

Теорема. Пусть натуральные числа $a \geq 2$, $b \geq 2$. Тогда a, b взаимно-просты, если и только если канонические факторизации для a, b не имеют общих простых множителей.

Доказательство. Если $(a, b) = 1$, то канонические факторизации a, b не имеют общих простых множителей, иначе $(a, b) > 1$.

Пусть канонические факторизации для a, b не имеют общих простых множителей. Тогда $a = p_1^{a_1} p_2^{a_2} \ldots p_s^{a_s}$, $b = p_1^{b_1} p_2^{b_2} \ldots p_s^{b_s}$, где $c_i = \min(a_i, b_i) = 0$, $i = 1, 2, \ldots, s$. Поэтому $d = (a,b) = p_1^{\min(a_1, b_1)} \cdot p_2^{\min(a_2, b_2)} \cdot \ldots \cdot p_s^{\min(a_s, b_s)} = 1$.

Следствие. Если p – простое число, то верно следующее.

1. $p \nmid a \leftrightarrow$ в канонической факторизации a нет множителя с p.
2. $p \nmid a \leftrightarrow (a, p) = 1$.

1.6. Непрерывные (цепные) и подходящие дроби

Пусть c есть вещественное число. Пусть q_1 есть наибольшее целое не больше, чем c. При нецелом c имеем

$$c = q_1 + \frac{1}{c_2}, c_2 > 1.$$

Аналогично

$$c_2 = q_2 + \frac{1}{c_3}, c_3 > 1; c_3 = q_3 + \frac{1}{c_4}, c_3 > 1; \ldots; c_{s-1} = q_{s-1} + \frac{1}{c_s}, c_s > 1.$$

Получили представление c в виде непрерывной (цепной) дроби:

$$c = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{q_4 + \cdots + \cfrac{1}{q_{s-1} + \cfrac{1}{c_s}}}}}.$$

Если число c иррационально, то всякое c_s иррационально и дробь продолжается до бесконечности. Если число c рационально, то $c = a/b$ для некоторых целых a, b с $(a, b) = 1$, $b > 0$. Тогда непрерывная дробь будет конечной, и с помощью алгоритма Евклида ее можно получить следующим образом:

$$a = bq_1 + r_2, \frac{a}{b} = q_1 + \frac{r_2}{b} = q_1 + \frac{1}{b/r_2},$$
$$b = r_2q_2 + r_3, \frac{b}{r_2} = q_2 + \frac{1}{r_2/r_3},$$
$$r_2 = r_3q_3 + r_4, \frac{r_2}{r_3} = q_3 + \frac{1}{r_3/r_4},$$
$$\ldots$$
$$r_{n-2} = r_{n-1}q_{n-1} + r_n, \frac{r_{n-2}}{r_{n-1}} = q_{n-1} + \frac{1}{r_{n-1}/r_n},$$
$$r_{n-1} = r_nq_n, r_{n+1} = 0, \frac{r_{n-1}}{r_n} = q_n.$$

Тогда непрерывная дробь

$$\frac{a}{b} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{q_4 + \cdots + \cfrac{1}{q_{n-1} + \cfrac{1}{q_n}}}}}.$$

Дроби $\delta_1 = q_1, \delta_2 = q_1 + \frac{1}{q_2}, \delta_3 = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3}}$, ... называются *подходящими дробями*.

1.6.1. Вычисление подходящих дробей

δ_s можно получить из δ_{s-1} заменой q_{s-1} в δ_{s-1} на $q_{s-1} + 1/q_s$.

Получим $P_0 = 1$, $Q_0 = 0$. Тогда

$$\delta_1 = \frac{q_1}{1} = \frac{P_1}{Q_1}, \begin{cases} P_1 = q_1, \\ Q_1 = 1, \end{cases} \delta_2 = \delta_1(q_1)\big|_{q_1 := q_1 + 1/q_2},$$
$$\delta_2 = \frac{q_1 + \cfrac{1}{q_2}}{1} = \frac{q_1q_2 + 1}{q_2 \cdot 1 + 0} = \frac{q_2P_1 + P_0}{q_2Q_1 + Q_0} = \frac{P_2}{Q_2},$$
$$\delta_3 = \frac{P_1\left(q_2 + \cfrac{1}{q_3}\right) + P_0}{Q_1\left(q_2 + \cfrac{1}{q_3}\right) + Q_0} = \frac{(P_1q_2 + P_0)q_3 + P_1}{(Q_1q_2 + Q_0)q_3 + Q_1} = \frac{q_3P_2 + P_1}{q_3Q_2 + Q_1} = \frac{P_3}{Q_3},$$
$$\ldots$$
$$\delta_s = \frac{q_sP_{s-1} + P_{s-2}}{q_sQ_{s-1} + Q_{s-2}} = \frac{P_s}{Q_s},$$
$$\ldots$$

1.6.2. Алгоритм вычисления подходящих дробей

$$P_0 = 1,\ Q_0 = 0,\ P_1 = q_1,\ Q_1 = 1,\ \delta_1 = \frac{P_1}{Q_1},$$

$$\delta_s = \frac{P_s}{Q_s},\ \text{где}\ \begin{cases} P_s = q_s P_{s-1} + P_{s-2} \\ Q_s = q_s Q_{s-1} + Q_{s-2} \end{cases},\ s = 2, 3, 4, \ldots$$

Пример. Найдем непрерывную дробь для числа 105/38.

$105 = 38 \cdot 2 + 29,\ q_1 = 2,$
$38 = 29 \cdot 1 + 9,\ q_2 = 1,$
$29 = 9 \cdot 3 + 2,\ q_3 = 3,$
$9 = 2 \cdot 4 + 1,\ q_4 = 4,$
$2 = 1 \cdot 2,\ q_5 = 2.$

$$\frac{105}{38} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{q_4 + \cfrac{1}{q_5}}}} = 2 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{4 + \cfrac{1}{2}}}}.$$

Подходящие дроби. $P_0 = 1$, $Q_0 = 0$, $P_1 = q_1 = 2$, $Q_1 = 1$,

$$\begin{cases} P_0 = 1, P_1 = q_1 = 2, \\ Q_0 = 0, Q_1 = 1, \end{cases} \quad \delta_1 = \frac{P_1}{Q_1} = \frac{2}{1} = 2;$$

$$\begin{cases} P_2 = q_2 P_1 + P_0 = 1 \cdot 2 + 1 = 3, \\ Q_2 = q_2 Q_1 + Q_0 = 1 \cdot 1 + 0 = 1, \end{cases} \quad \delta_2 = \frac{P_2}{Q_2} = \frac{3}{1} = 3;$$

$$\begin{cases} P_3 = q_3 P_2 + P_1 = 3 \cdot 3 + 2 = 11, \\ Q_3 = q_3 Q_2 + Q_1 = 3 \cdot 1 + 1 = 4, \end{cases} \quad \delta_3 = \frac{P_3}{Q_3} = \frac{11}{4};$$

$$\begin{cases} P_4 = q_4 P_3 + P_2 = 4 \cdot 11 + 3 = 47, \\ Q_4 = q_4 Q_3 + Q_2 = 4 \cdot 4 + 1 = 17, \end{cases} \quad \delta_4 = \frac{P_4}{Q_4} = \frac{47}{17};$$

$$\begin{cases} P_5 = q_5 P_4 + P_3 = 2 \cdot 47 + 11 = 105, \\ Q_5 = q_5 Q_4 + Q_3 = 2 \cdot 17 + 4 = 38, \end{cases} \quad \delta_5 = \frac{P_5}{Q_5} = \frac{105}{38}.$$

Теорема. Подходящие дроби δ_s, $s > 1$, несократимы.
Доказательство.

$$\delta_s - \delta_{s-1} = \frac{P_s}{Q_s} - \frac{P_{s-1}}{Q_{s-1}} = \frac{P_s Q_{s-1} - Q_s P_{s-1}}{Q_s Q_{s-1}} = \frac{h_s}{Q_s Q_{s-1}};$$

$$\begin{aligned} h_s &= P_s Q_{s-1} - Q_s P_{s-1} = \\ &= (q_s P_{s-1} + P_{s-2})\, Q_{s-1} - (q_s Q_{s-1} + Q_{s-2}) P_{s-1} = \\ &= q_s P_{s-1} Q_{s-1} + P_{s-2} Q_{s-1} - q_s Q_{s-1} P_{s-1} - Q_{s-2} P_{s-1} = \\ &= P_{s-2} Q_{s-1} - Q_{s-2} P_{s-1} = -(P_{s-1} Q_{s-2} - Q_{s-1} P_{s-2}) = -h_{s-1}. \end{aligned}$$

Аналогично получаем

$h_s = (-1)h_{s-1} = (-1)^2 h_{s-2} = (-1)^3 h_{s-3} = ... = (-1)^{s-1} h_{s-(s-1)} = (-1)^{s-1} h_1 =$
$= (-1)^{s-1} (P_1Q_0 - Q_1P_0) = (-1)^{s-1} (q_1 \cdot 0 - 1 \cdot 1) = (-1)^{s-1} \cdot (-1) = (-1)^s.$

Тогда

$$P_s Q_{s-1} - Q_s P_{s-1} = (-1)^s, s > 1, \quad (1.3)$$
$$\delta_s - \delta_{s-1} = (-1)^s/(Q_s Q_{s-1}), s > 1. \quad (1.4)$$

Так как (P_s, Q_s) делит P_s, Q_s и левую часть в (1.3), то (P_s, Q_s) делит правую часть в (1.3). Поэтому $(P_s, Q_s) = 1$. Следовательно, подходящие дроби $\delta_s = P_s/Q_s$, $s > 1$, несократимы.

Замечание. Если c есть вещественное число, $s \geq 2$, $c \neq \delta_s$ то по (1.4) c лежит между δ_{s-1}, δ_s и $|c - \delta_{s-1}| \leq |\delta_s - \delta_{s-1}| \leq 1/(Q_s Q_{s-1})$.