Министерство науки и высшего образования Российской Федерации
Министерство внутренних дел Российской Федерации

Московский университет Министерства внутренних дел
Российской Федерации имени В.Я. Кикотя

И. В. Атласов,
В. Н. Думачев,
Е. И. Таранина

ОСНОВЫ ОБЩЕЙ АЛГЕБРЫ И ТЕОРИИ ЧИСЕЛ

Учебное пособие

Москва
Московский университет
МВД России имени В.Я. Кикотя

2022

УДК 512
ББК 22.14
А92

Рецензенты:
начальник кафедры специальных информационных технологий Санкт-Петербургского университета МВД России доктор технических наук, профессор **А. И. Примакин**; доцент кафедры математики и моделирования систем Воронежского института МВД России кандидат педагогических наук, доцент **С. А. Телкова**

Атласов, И. В.

А92 **Основы общей алгебры и теории чисел** : учебное пособие / И. В. Атласов., В. Н. Думачев, Е. И. Таранина. – М. : Московский университет МВД России имени В.Я. Кикотя, 2022. – 111 с.

ISBN 978-5-9694-1134-0

Учебное пособие содержит систематическое изложение материала по курсу «Алгебра и геометрия» и предназначено для проведения практических занятий, выполнения типового расчета, лабораторных работ и самоподготовки для курсантов факультета подготовки специалистов в области информационной безопасности, обучающихся по специальности 10.05.03 – Информационная безопасность автоматизированных систем.

УДК 512
ББК 22.14

ISBN 978-5-9694-1134-0

ОГЛАВЛЕНИЕ

ГЛАВА I. ОСНОВНЫЕ АЛГЕБРАИЧЕСКИЕ СТРУКТУРЫ

§ 1.1. Элементы теории множеств

Понятия множества и элемент множества являются первичными и неопределяемы в математике.

Множество – это совокупность объектов, которая расматривается как одно целое, т. е. нам придется использовать термин **совокупность**, который тоже необходимо определить (через множество).

Объекты, входящие в множество, называются его **элементами**. В теории множеств используются следующие обозначения:

$\equiv$	тождественно	$\vee$	или (дизъюнкция)
$\bar{x}$	не x	$\wedge$	и (конъюнкция)
$\leftrightarrow$	тогда и только тогда	$\rightarrow$	влечет
$\forall$	для всех	$\exists$	существует
$a \in A$	элемент a принадлежит множеству A		
$A = B$	множества A и B содержат одни и те же элементы		
$A \subset B$	включение (A является подмножеством B)		

Согласно определению: $A \subset B \leftrightarrow (\forall x, x \in A \rightarrow x \in B)$.

Отношение включения имеет следующие свойства:

- рефлексивности: $\forall A : A \subset A$;
- транзитивности: $\forall A,B,C : (A \subset B \,\&\, B \subset C) \rightarrow A \subset C$;
- антисимметричности: $\forall A,B : (A \subset B \,\&\, B \subset A) \rightarrow A = B$.

Множество, не содержащее ни одного элемента, называется пустым множеством $\varnothing$. Сами множества A, B, C, ... содержатся в некотором фиксированном универсальном множестве U. Из двух множеств можно получить новое множество с помощью следующих операций:

1) объединение $A \cup B = \{x \mid x \in A \vee x \in B\}$;

2) пересечение $A \cap B = \{x \mid x \in A \,\&\, x \in B\}$;

3) разность $A \setminus B = \{x \mid x \in A \,\&\, x \notin B\}$.

Теорема. Свойства теоретико-множественных операций.

1. Коммутативность:

$$A \cup B = B \cup A, \quad A \cap B = B \cap A.$$

$$x \in A \cup B \leftrightarrow x \in A \vee x \in B \leftrightarrow x \in B \vee x \in A \leftrightarrow x \in B \cup A.$$

2. Ассоциативность:

$$A \cup (B \cup C) = (A \cup B) \cup C, \quad A \cap (B \cap C) = (A \cap B) \cap C.$$

$$x \in A \cup (B \cup C) \leftrightarrow x \in A \vee x \in (B \cup C) \leftrightarrow x \in A \vee x \in B \vee x \in C$$

$$\leftrightarrow x \in (A \cup B) \vee x \in C \leftrightarrow x \in (A \cup B) \cup C.$$

3. Дистрибутивность:

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C), \quad A \cup (B \cap C) = (A \cup B) \cap (A \cup C).$$

$$x \in A \cap (B \cup C) \leftrightarrow x \in A \,\&\, x \in (B \cup C) \leftrightarrow x \in A \,\&\, (x \in B \vee x \in C)$$

$$\leftrightarrow (x \in A \,\&\, x \in B) \vee (x \in A \,\&\, x \in C)$$

$$\leftrightarrow x \in (A \cap B) \cup (A \cap C).$$

4. Идемпотентность:

$$A \cup A = A, \qquad A \cap A = A.$$

$$x \in A \cup A \leftrightarrow x \in A \vee x \in A \leftrightarrow x \in A.$$

5. Свойства действий с $\varnothing$ и U:

$$M \cup U = U, M \cap U = M, M \cup \overline{M} = U,$$

$$M \cap \overline{M} = \varnothing, M \cup \varnothing = M, M \cap \varnothing = \varnothing.$$

$$x \in M \cup U \leftrightarrow x \in M \vee x \in U \leftrightarrow x \in U.$$

6. Законы де Моргана:

$$\overline{A \cup B} = \overline{A} \cap \overline{B}, \quad \overline{A \cap B} = \overline{A} \cup \overline{B}.$$

$$x \in \overline{A \cup B} \leftrightarrow x \notin (A \cup B) \leftrightarrow x \notin A \,\&\, x \notin B$$

$$\leftrightarrow x \in \overline{A} \,\&\, x \in \overline{B} \leftrightarrow x \in \overline{A} \cap \overline{B}.$$

7. Отрицание отрицания $\overline{\overline{M}} = M$.

$$x \in \overline{\overline{M}} \leftrightarrow x \in U \setminus \overline{M} \leftrightarrow x \in U \,\&\, x \notin \overline{M} \leftrightarrow x \in M.$$

8. Законы склеивания:

$$(A \cap B) \cup (A \cap \overline{B}) = A, \quad (A \cup B) \cap (A \cup \overline{B}) = A.$$

$$x \in (A \cap B) \cup (A \cap \overline{B}) \leftrightarrow x \in (A \cap B) \vee x \in (A \cap \overline{B})$$
$$\leftrightarrow (x \in A \,\&\, x \in B) \vee (x \in A \,\&\, x \notin B)$$
$$\leftrightarrow (x \in A \,\&\, x \in A) \vee (x \in B \,\&\, x \notin B)$$
$$\leftrightarrow (x \in A) \vee \varnothing \leftrightarrow x \in A.$$

9. Законы поглощения:

$$A \cup (A \cap B) = A, \quad A \cap (A \cup B) = A.$$

$$x \in A \leftrightarrow x \in A \vee x \in (A \cap B) \leftrightarrow x \in A \cup (A \cap B).$$

10. Законы Порецкого:

$$A \cup (\overline{A} \cap B) = A \cup B, \quad A \cap (\overline{A} \cup B) = A \cap B.$$

$$x \in A \cup (\overline{A} \cap B) \leftrightarrow x \in (A \cup \overline{A}) \cap (A \cup B)$$
$$\leftrightarrow x \in (U \cap (A \cup B)) \leftrightarrow x \in (A \cup B).$$

Число – основное понятие математики, используемое для количественной характеристики, сравнения, нумерации объектов и их частей.

В дальнейшем мы будем обозначать:

N – множество натуральных чисел;

Z – множество целых чисел;

Q – множество рациональных чисел;

R – множество действительных чисел;

C – множество комплексных чисел.

При этом $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.

Натуральные числа – числа, возникающие естественным образом при счете (перечислении) конкретных предметов (1, 2, 3...). Поскольку отрицательных предметов нет, то отрицательные числа не входят в множество натуральных. Мы не будем включать в множество натуральных чисел и ноль, поскольку

совокупность предметов количеством 0 штук нельзя увидеть, потрогать, измерить и т. д.

Целые числа – расширение множества натуральных чисел, получаемое добавлением нуля и отрицательных чисел (...–3, –2, –1, 0, 1, 2, 3, ...).

Рациональное число – отношение двух чисел в виде обыкновенной дроби $\frac{m}{n}$, числитель $m \in \mathsf{Z}$ – целое число, а знаменатель $n \in \mathsf{N}$ – натуральное.

Иррациональное число – это число, которое не является рациональным, т. е. не может быть представлено в виде дроби $\frac{m}{n}$, но может быть представлено в виде бесконечной непериодической десятичной дроби.

Множество **вещественных чисел** является объединением множества рациональных и иррациональных чисел.

Комплексное число – число, записываемое в виде $z = x + iy$, где i – мнимая единица, для которой выполняется равенство $i^2 = -1$.

Алгебраическое число – это вещественное или комплексное число, являющееся корнем многочлена с целыми коэффициентами.

Трансцендентное число – это вещественное или комплексное число, не являющееся алгебраическим – иными словами, число, которое не может быть корнем многочлена с целыми коэффициентами.

§ 1.2. Бинарные отношения

Пусть даны элементы a и b. Множество $\{a,b\}$ называется неупорядоченной парой, если всегда $\{a,b\} = \{b,a\}$. В противном случае пара называется упорядоченной. Для упорядоченной

пары введем обозначение $\langle a,b\rangle$. В данной паре элемент a будет первым, а элемент b – вторым.

Прямым произведением множеств A и B называется множество всех упорядоченных пар $\langle a,b\rangle$:

$$A\times B=\{\langle a,b\rangle \mid x\in A \,\&\, y\in B\}$$

Пример 1. Пусть $A=\{0,1\}$ и $B=\{0,3,4\}$. Тогда:

$$A\times B=\{\langle 0,0\rangle,\langle 0,3\rangle,\langle 0,4\rangle,\langle 1,0\rangle,\langle 1,3\rangle,\langle 1,4\rangle\}$$

$$B\times A=\{\langle 0,0\rangle,\langle 0,1\rangle,\langle 3,0\rangle,\langle 3,1\rangle,\langle 4,0\rangle,\langle 4,1\rangle\}$$

$$A\times A=\{\langle 0,0\rangle,\langle 0,1\rangle,\langle 1,0\rangle,\langle 1,1\rangle\}$$

$$B\times B=\{\langle 0,0\rangle,\langle 0,3\rangle,\langle 0,4\rangle,\langle 3,0\rangle,\langle 3,3\rangle,\langle 3,4\rangle,\langle 4,0\rangle,\langle 4,3\rangle,\langle 4,4\rangle\}.$$

n-я степень множества определяется как n – кратное прямое произведение множеств A:

$$A^1=A,\ A^2=A\times A,\ A^3=A\times A\times A\,.$$

Бинарным отношением R между множествами называется любое подмножество прямого произведения этих двух множеств. Запись xRy или $\langle a,b\rangle\in R$ означает, что элемент x находится в отношении R к элементу y.

Рассмотрим наиболее часто встречающиеся бинарные отношения.

1. Рефлексивные $\forall\, x\in A\to xRx$.

– отношение параллельности на множестве прямых плоскости;

– отношение равенства на каком-либо множестве чисел;

– отношение делимости на какой-либо совокупности целых чисел.

2. Антирефлексивные: $\forall\, x\in R, \langle a,b\rangle\notin R$.

– отношение неравенства $\neq$ на каком-либо множестве чисел;

– отношение перпендикулярности на множестве прямых плоскости.

3. Транзитивные: $\forall\, x, y, z, \left(xRy \;\&\; yRz\right) \to xRz.$

– отношение делимости на множестве целых чисел;

– отношение равенства (но не отношение неравенства $\neq$).

4. Симметричные: $\forall\, x, y, \left(xRy \to yRx\right).$

– отношение параллельности прямых;

– отношение перпендикулярности прямых;

– отношение равенства.

5. Антисимметричные: $\forall\, x, y, \left(xRy \;\&\; yRx\right) \to x = y.$

– отношение включения $\subset$.

Бинарное отношение R на множестве A называется **отношением эквивалентности** ($:$ или $\approx$ или $\equiv$), если оно рефлексивно, симметрично и транзитивно.

Пусть A – непустое множество, $I = \left\{\langle x, x\rangle \mid x \in A\right\}$ – отношение тождества на множестве A. Тогда I – отношение эквивалентности.

Пусть A – множество прямых на плоскости и $R = \left\{\langle x, y\rangle \mid x, y \in A; x \parallel y\right\}$ – отношение параллельности. Тогда R – отношение эквивалентности.

Пусть Z – множество всех целых чисел; $m \in \mathsf{Z}, m \neq 0$.

Отношение $\mathrm{R} = \{\langle x,\ y\rangle \mid x,\ y \in \mathsf{Z};\ x - y$ *делится на* $m\}$ называется отношением сравнения по модулю m. Это отношение эквивалентности на Z.

Отношение подобия на множестве треугольников данной плоскости – отношение эквивалентности.

Бинарной операцией на множестве A называется отображение множества $A \times A$ в себя, или $A \times A \to A$.

Сложение и умножение целых чисел на множество целых чисел есть бинарные операции.

Если $P(M)$ – множество всех подмножеств множества M, то $\cup$ и $\cap$ – это бинарные операции на $P(M)$.

Обобщая данное определение, можно выделить:

$A^0 \to A$ – нульарные операции;

$A^1 \to A$ – унарные операции;

$A^2 \to A$ – бинарные операции;

$A^n \to A$ – n-арные операции.

Степень n называется **рангом** операции.

Бинарная операция $*$ называется **коммутативной**, если

$$\forall a,b \in A \qquad a*b = b*a.$$

Бинарная операция $*$ называется **ассоциативной**, если

$$\forall a,b,c \in A \qquad a*(b*c) = (a*b)*c.$$

Бинарная операция $*$ называется **дистрибутивной** относительно бинарной операции $\oplus$, если $\forall a,b,c \in A$ $(a \oplus b)*c = (a*b) \oplus (b*c)$ *и* $c*(a \oplus b) = (c*a) \oplus (c*b)$.

Сложение и умножение рациональных чисел являются коммутативными, ассоциативными бинарными операциями.

Операция вычитания на множестве рациональных чисел не коммутативна и не ассоциативна.

Операции $\cup$ и $\cap$ коммутативны и ассоциативны на $P(M)$.

Операции $\cup$ и $\cap$ взаимно дистрибутивны относительно друг друга.

Умножение целых чисел дистрибутивно относительно сложения.

Сложение не дистрибутивно относительно умножения.

Элемент $e \in A$ называется **нейтральным** относительно бинарной операции $*$, если $\forall a \in A$, $e*a = a = a*e$.

Теорема. Если нейтральный элемент существует, то он единственен.

Пусть e и e' – нейтральные элементы относительно $*$. Тогда $e' = e * e' = e$.

Число 0 – нейтральный элемент относительно сложения в множестве целых чисел $\mathbb{Z}$.

Число 1 – нейтральный элемент относительно умножения в множестве целых чисел $\mathbb{Z}$.

Пустое множество $\varnothing$ – нейтральный элемент относительно операции объединения.

Универсальное множество U – нейтральный элемент относительно операции пересечения.

Элемент $a \in A$ называется **регулярным** относительно операции $*$, если $\forall b, c \in A$

$$(a * b) = (a * c) \to b = c \quad и \quad (b * a) = (c * a) \to b = c.$$

В случае регулярности выражения можно сокращать на a.

Всякое целое число регулярно относительно сложения.

Всякое целое число, отличное от нуля, регулярно относительно умножения.

Число 0 не регулярно относительно умножения.

Пусть $*$ – бинарная операция на множестве А, обладающая нейтральным элементом e. Элемент $a' \in A$ называется **симметричным** элементу к $a \in A$ относительно операции $*$, если $a * a' = a' * a = e$.

Относительно сложения число $(-k)$ симметрично числу (k).

Относительно умножения число $(1/k)$ симметрично числу (k).

Число (0) не имеет симметричного относительно умножения.

Пусть $*$ – бинарная операция на множестве А и $B \subset A$. Подмножество В множества А называется **замкнутым** относительно операции $*$, если $\forall a, b \in B, a * b \subset B$.

Множество всех целых чисел замкнуто относительно сложения и умножения целых чисел.

Множество всех нечетных чисел замкнуто относительно умножения, но не замкнуто относительно сложения.

В дальнейшем бинарную операцию сложения будем называть аддитивной операцией, а бинарную операцию умножения – мультипликативной.

§ 1.3. Алгебры

В предыдущих параграфах множества и операции над элементами множества рассматривались отдельно. В реальных вычислениях работа с каким-либо множеством подразумевает не только существование самих его элементов, но и определенные допустимые операции над ними.

Универсальной **алгеброй** называется структура в виде упорядоченной пары $A = \langle A, V \rangle$, где A – непустое множество, V – множество операций на A.

По существу алгебра **A** определяется двумя множествами:

– носителем алгебры с элементами $a \in A$;

– сигнатурой с главными операциями $v \in V$.

Если структура $\langle A, V \rangle$ – алгебра, то мы будем проще называть множество A – алгеброй относительно операций V.

Типом алгебры называется последовательность рангов ее главных операций:

$\langle \mathsf{Z}, +, \times \rangle$ – алгебра типа (2,2);

$\langle \mathsf{N}, +, \times \rangle$ – алгебра типа (2,2);

$\langle P(U), \cup, \cap, \neg \rangle$ – алгебра типа (2,2,1).

Если ранги операций $v_{1,2} \in V_{1,2}$ двух алгебр A_1 и A_2 совпадают, то такие алгебры называют **однотипными**.

Алгебра $A = \langle A, *, e \rangle$ типа (2,0), где $*$ – ассоциативная бинарная операция; e – нейтральный элемент относительно $*$, называется **моноидом**:

Алгебра $\langle \mathsf{N}, +, 0 \rangle$ – моноид;

Алгебра $\langle \mathsf{N}, \times, 1 \rangle$ – моноид.

Гомоморфизмом алгебры A_1 в однотипную алгебру A_2 называется такое отображение h множества A_1 в A_2, которое сохраняет все главные операции $v_1 \in V_1$ алгебры A_1.

Гомоморфизм алгебры A_1 на A_2 называется **эпиморфизмом**.

Гомоморфизм h алгебры A_1 на A_2 называется **изоморфизмом**, если h есть инъективное отображение множества A на B (биекция). Алгебры A_1 и A_2 называются изоморфными, если существует изоморфизм A_1 на A_2.

Гомоморфизм h алгебры A_1 в A_2 называется **мономорфизмом** или вложением, если h является инъективным отображением множества A_1 в A_2 (инъекцией).

Гомоморфизм алгебры A в себя называется **эндоморфизмом**.

Гомоморфизм алгебры A на себя называется **автоморфизмом**. Тождественное отображение A на себя – автоморфизм.

Пример 2. Пусть имеем две алгебры:

$\langle \mathsf{R}^*, \times, 1 \rangle$ – мультипликативная алгебра над множеством положительных действительных чисел R^*;

$\langle \mathsf{R}, +, 0 \rangle$ – аддитивная алгебра над множеством действительных чисел R.

Показать, что они изоморфны.

Решение: каждая из алгебр $\langle \mathsf{R},+,0\rangle$ и $\langle \mathsf{R}^*,\times,1\rangle$ имеет тип (2,0). Рассмотрим отображение $h(x)=\log x,\ \forall x\in \mathsf{R}^*$.

Очевидно, что h есть отображение R^* на R (сюръекция). Отображение h инъективно, так как для любых $x,y\in \mathsf{R}^*$ выполняется условие, если $\log x=\log y$, то $x=y$.

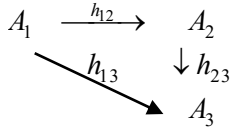
Кроме того, $h(1)=0$ и для любых $x,y\in \mathsf{R}^*$ имеем $\log(x\times y)=\log(x)+\log(y)$, т. е. $h(x,y)=h(x)+h(y)$.

Таким образом, отображение h сохраняет главные операции алгебры $\langle \mathsf{R}^*,\times,1\rangle$. Следовательно, h является изоморфизмом первой алгебры R^* на вторую R.

$$\begin{array}{ccc} \langle x,y\rangle & \xrightarrow{\times} & x\times y \\ \downarrow h & & \downarrow h \\ \langle h(x),h(y)\rangle & \xrightarrow{+} & h(x)+h(y)=h(x\times y) \end{array}.$$

Решение задачи можно изобразить с помощью данной коммутативной диаграммы.

Теорема. Пусть h_{12} – гомоморфизм алгебры A_1 в алгебру A_2 и h_{23} – гомоморфизм алгебры A_2 в алгебру A_3. Тогда их композиция $h_{12}\cdot h_{23}=h_{13}$ является гомоморфизмом h_{13} алгебры A_1 в алгебру A_3.



Аналогичные утверждения справедливы и для композиции других морфизмов.

Композиция эпиморфизмов есть эпиморфизм.

Композиция изоморфизмов есть изоморфизм.

Определение. Пусть f – n-арная операция на множестве A и B – непустое подмножество множества A ($B \in A$). Операция g на B является ограничением операции f множеством B, если

$$g(b_1,b_2,...,b_n) = f(b_1,b_2,...,b_n), \quad \forall\, b_1,b_2,...,b_n \in B.$$

0-арная операция g на B является ограничением 0-арной операции f на A множеством B, если $g = f$, т. е. если g и f выделяют в B и A соответственно один и тот же элемент.

Пусть $A = \langle A, V_1 \rangle$ и $B = \langle B, V_2 \rangle$ – однотипные алгебры. Алгебра B называется подалгеброй алгебры A, если $B \subset A$ и каждая главная операция v_B алгебры **B** является ограничением соответствующей операции v_A алгебры **A** множеством B.

Алгебра $\langle \mathsf{N}, + \rangle$ есть подалгебра алгебры $\langle \mathsf{Z}, + \rangle$.

Алгебра $\langle \mathsf{N}, + \rangle$ не является подалгеброй алгебры $\langle \mathsf{Z}, \times \rangle$.

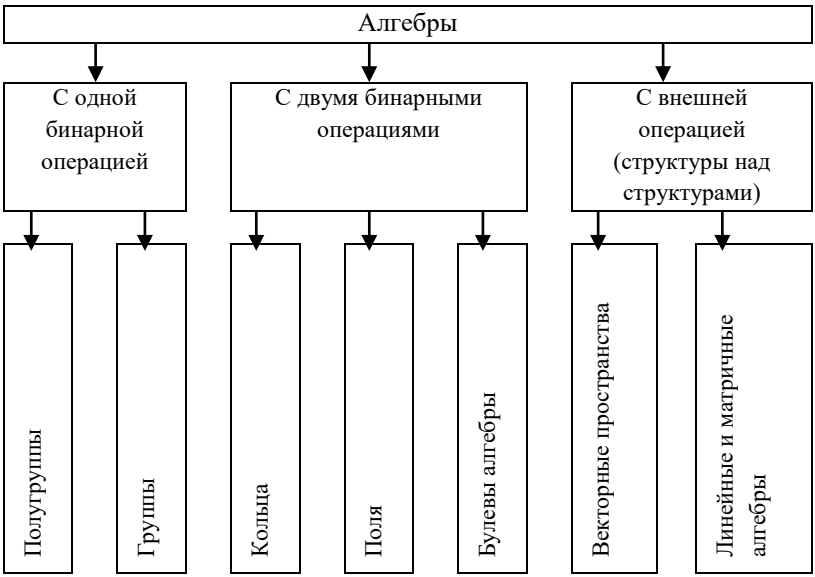
Алгебра $\langle \mathsf{N}, + \rangle$ не является подалгеброй алгебры $\langle \mathsf{Z}, +, \times \rangle$.

Алгебра $\langle \mathsf{N}, +, \times \rangle$ есть подалгебра алгебры $\langle \mathsf{Z}, +, \times \rangle$.

Алгебра $\langle \{\varnothing, U\}, \cup, \cap, \neg \rangle$ есть подалгебра алгебры $\langle P(U), \cup, \cap, \neg \rangle$.

Если **A** – подалгебра **B**, а **B** – подалгебра **C**, то **A** – подалгебра **C**.

В дальнейшем мы будем выделять следующие основные (фундаментальные) алгебры:



1.3.1. Полугруппы

Полугруппой называется алгебра $\langle A,* \rangle$ типа (2) с бинарной ассоциативной операцией $*$:

$$a*(b*c)=(a*b)*c, \quad \forall\, a,b,c \in A.$$

Алгебра $\langle \mathbb{N},+ \rangle$ есть аддитивная полугруппа натуральных чисел.

Пусть A – совокупность отображений множества M в себя ($M \bullet ... \bullet M \to M$) с законом композиции $\bullet$. Алгебра $\langle A,\bullet \rangle$ есть полугруппа.

Алгебра $\langle \mathbb{N},+,0 \rangle$ – моноид.

Алгебра $\langle \mathbb{N},\times,1 \rangle$ – моноид.

Пусть A – совокупность отображений множества в себя и e – тождественное отображение этого множества. Алгебра $\langle A,\bullet,e \rangle$ – моноид.

Рассмотрим **моноид** – это полугруппа с нейтральным элементом. Напомним определение моноида. Алгебра $A = \langle A, *, e \rangle$ типа (2,0), где $*$ – ассоциативная бинарная операция; e – нейтральный элемент относительно $*$, называется **моноидом**.

Множество строк символов некоторого алфавита. На этом множестве А определим операцию конкатенации e таким образом: если $a_1, a_2 \in A$, то $a_1 \mathsf{e} a_2 = a_1 a_2$. Обозначим пустую строку символом Λ. Тогда алгебра $\langle A, \mathsf{e}, \Lambda \rangle$ – моноид.

1.3.2. Группы

Группой называется алгебра $G = \langle G, *, \overline{\ } \rangle$ типа (2,1), удовлетворяющая следующим свойствам $\forall a, b, c \in G$:

– ассоциативность бинарной операции * *a*(b*c)=(a*b)*c;*

– наличие нейтрального (единичного) элемента относительно *: *a*e=e*a=a;*

– наличие обратного (симметричного) элемента $a * \bar{a} = \bar{a} * a = e.$

Заметим, что ассоциативность операции практически означает то, что можно вообще не ставить скобок. Если же операция неассоциативна, то порядок композиции играет большую роль и скобки ставить обязательно. В качестве примера возьмем: $2 + 2 * 2 \neq (2 + 2) * 2$.

Таким образом, группа – это алгебра с двумя операциями: * – бинарной, и | – унарной. Бинарная операция ассоциативна и обладает нейтральным элементом, а унарная является переходом к обратному элементу относительно бинарной операции.

Группа $G = \langle G, *, \rceil \rangle$ называется **абелевой**, если $a * b = b * a, \quad \forall a, b \in G.$

Коммутатором двух элементов алгебры называется операция $[a,b] = a * b - b * a.$

Элементы алгебры, для которых коммутатор равен нулю ($[a,b] = 0$) называют коммутирующими. Элементы алгебры, для которых коммутатор не равен нулю ($[a,b] \neq 0$), называют некоммутирующими. Абелевы группы называют еще коммутативными в отличие от некоммутативных (неабелевых) групп.

Порядком группы называется количество ее элементов ($a_1, a_2, ..., a_n \in G$). Если G – бесконечное множество, то это группа бесконечного порядка.

Алгебра $\langle \mathsf{Q}, +, \rceil \rangle$ типа (2,1) – аддитивная группа рациональных чисел.

Если Q^* – множество всех отличных от нуля рациональных чисел: ($\mathsf{Q}^* = \mathsf{Q}^* \setminus \{0\}$), то алгебра $\langle \mathsf{Q}^*, *, \rceil \rangle$ мультипликативная группа рациональных чисел.

Алгебра $\langle \mathsf{R}, +, \rceil \rangle$ – аддитивная группа действительных чисел.

Если R^* – множество всех отличных от нуля действительных чисел: ($\mathsf{R}^* = \mathsf{R}^* \setminus \{0\}$), то алгебра $\langle \mathsf{R}^*, *, \rceil \rangle$ мультипликативная группа действительных чисел.

Пусть S_n – совокупность всех подстановок множества $M = \{1,2,...,n\}, n \in \mathsf{N}$, т. е. совокупность инъективных отображений этого множества на себя. Тогда алгебра $\langle S_n, \bullet, \rceil \rangle$ – симметрическая группа подстановок степени n. При $n > 2$ – это неабелева группа.

Пусть G – множество векторов данной плоскости с обычной бинарной операцией $+$ сложения векторов и унарной операцией $|$, ставящей в соответствие каждому вектору $a \in G$ противоположный вектор $(-a) \in G$. Алгебра $\langle G, +, \overline{\ } \rangle$ – аддитивная группа векторов плоскости.

Теорема. Свойства группы.

1. Для любого элемента группы $a \in G$ правый обратный равен левому обратному:

$$a * \bar{a} = \bar{a} * a = e.$$

$$\bar{a} = \bar{a}\, e = \bar{a}(a\bar{a}) = (\bar{a}a)\bar{a} = e\,\bar{a} = \bar{a}.$$

2. Для любого элемента группы $a \in G$ правая единица равна левой:

$$a * e = e * a.$$

$$a\, e = a(\bar{a}a) = (a\bar{a})a = e\, a.$$

3. Для любых элементов группы $a, b \in G$ уравнение $a * x = b$ имеет единственное решение.

Пусть $\bar{a}b$ есть решение уравнения $a * x = b$: $a(\bar{a}b) = (a\bar{a})b = eb = b.$

Тогда, если c является произвольным решением уравнения, то $a * x = b$, то $c = ec = (\bar{a}a)c = \bar{a}(ac) = \bar{a}b.$

Следовательно, элемент $\bar{a}b$ является единственным решением уравнения $a * x = b$.

4. Для любых элементов группы $a, b, c \in G$ из $a * c = b * c$ следует $a = b$.

$$a * c = b * c$$

$$a * c * \bar{c} = b * c * \bar{c}$$

$$a * e = b * e$$

$$a = b.$$

5. Для любых элементов группы $a,b \in G$ из $a*b=a$ следует $a=e$.

$$a*b=a$$
$$\bar{a}*a*b=\bar{a}*a$$
$$e*b=e$$
$$b=e.$$

Цифровые сигналы (коды) образуют относительно операции покоординатного сложения абелеву группу. Группы являются математической моделью цифровых сигналов, а цифровая обработка информации сводится к преобразованию на конечных группах. Отсчеты цифрового сигнала (кода) можно рассматривать как координаты некоторого вектора.

Подгруппой H группы **G** называется любая подалгебра этой группы. Любая подгруппа группы тоже является группой. Нейтральный элемент группы является нейтральным элементом любой ее подгруппы.

Аддитивная группа рациональных чисел $\langle \mathsf{Q},+,- \rangle$ есть подгруппа группы действительных чисел $\langle \mathsf{R},+,- \rangle$.

$\langle \mathsf{Q}^*,+,\urcorner \rangle$ есть подгруппа $\langle \mathsf{R}^*,+,\urcorner \rangle$.

Подгруппа **H** группы **G** называется **нормальным делителем** группы **G**, если $\forall g \in G, \forall h \in H: \; g^{-1}hg \in H.$

Любая подгруппа абелевой группы является ее нормальным делителем.

Подгруппа всех четных подстановок A_n является нормальным делителем S_n – симметрической группы подстановок n-й степени.

1.3.3. Кольца

Кольцом называется алгебра $K=\langle K,+,\urcorner,*,1 \rangle$ типа (2,1,2,0), главные операции которой удовлетворяют следующие условия:

– алгебра $\langle K,+,\urcorner\rangle$ – абелева группа;

– алгебра $\langle K,*,1\rangle$ – моноид $a*(b+c)=a*b+a*c.$

Если кольцо имеет мультипликативную единицу, то его называют **кольцом с единицей**. В общем случае определение кольца не требует наличия у него мультипликативной единицы.

Абелева группа $\langle K,+,\urcorner\rangle$ называется аддитивной группой кольца **K**. Ноль этой группы, т. е. нейтральный элемент относительно сложения, называется нулем кольца и обозначается через 0_K.

Алгебра $\langle K,*,1\rangle$ называется мультипликативным моноидом кольца **K**. Нейтральный относительно умножения элемент 1_K называется единицей кольца **K**.

Кольцо называется **коммутативным**, если $a*b=b*a.$

Кольцо K называется **областью целостности**, если оно коммутативно; $0_K\neq 1_K$; из условия $ab=0$ следует, что либо $a=0$, либо $b=0$.

Элементы a и b кольца **K** называются **делителями нуля**, если $a\neq 0, b\neq 0$ и $ab=0$.

Отметим, что любая область целостности делителей нуля не имеет.

$\langle \mathsf{Z},+,\urcorner,*,1\rangle$ – кольцо целых чисел.

$\mathsf{Q}[\sqrt{2}]=\{a+b\sqrt{2}\mid a,b\in\mathsf{Q}\};\ \langle \mathsf{Q}[\sqrt{2}],+,\urcorner,*,1\rangle$ – кольцо.

$\langle K^{2\times 2},+,\urcorner,*,I\rangle$ – неабелево кольцо (2×2) матриц.

Последнее кольцо матриц не является областью целостности, поскольку оно имеет делители нуля. Например:

$\begin{pmatrix}1 & -1\\ 2 & -3\end{pmatrix}\begin{pmatrix}1 & 5\\ -4 & 5\end{pmatrix}=\begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix}$, т. е. $a\neq 0, b\neq 0$, но $ab=0$.

Теорема. Свойства кольца.

Пусть $\left\langle K^{2\times 2},+,\urcorner,*,I\right\rangle$ – кольцо.

$$\text{если } a+b=a, \text{ то } b=0;$$
$$\text{если } a+b=0, \text{ то } b=-a;$$
$$-(-a)=a;$$
$$0\cdot a=a\cdot 0=0;$$
$$(-a)\cdot b=a\cdot(-b)=-(a\cdot b);$$
$$(-a)\cdot(-b)=a\cdot b;$$
$$a\cdot(b-c)=a\cdot b-a\cdot c.$$

1.3.4. Поля

Элемент a кольца **K** называется обратимым элементом кольца, если в кольце существует элемент b такой, что $a\cdot b=b\cdot a=1_K$.

При этом элементы a и b называются взаимно обратными.

Полем называется кольцо, которое является абелевым; в котором нуль отличен от единицы: $0_K\neq 1_K$; в котором всякий ненулевой элемент является обратимым элементом кольца:

$$\forall\, a\neq 0\in K\ \exists\, b\neq 0\in K: a\cdot b=b\cdot a=1.$$

Подполем поля $F=\left\langle F,+,\urcorner,*,1\right\rangle$ называется подкольцо поля, в котором каждый ненулевой элемент обратим. Каждое подполе является полем.

Пусть $a,b\in F$ и $b\neq 0$. Уравнение $bx=a$ имеет в поле **F** решение ab^{-1}, притом единственное.

Теорема. Свойства поля.

Пусть $F=\left\langle F,+,\urcorner,*,1\right\rangle$ – поле. Тогда $\forall\, a,b,c\in F$:

если $ab=1$, то $a\neq 0$ и $b=a^{-1}$;

если $ac=bc$ и $c\neq 0$, то $a=b$;

если $ab = 0$, то $a = 0$ или $b = 0$;

если $a \neq 0$ и $b \neq 0$, то $ab \neq 0$;

$\frac{a}{b} = \frac{c}{d}$ тогда и только тогда, когда $ad = bc, b \neq 0, d \neq 0$;

$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$;

$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$;

$\frac{a}{b} + \frac{-a}{b} = 0$;

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

$\frac{ac}{bc} = \frac{a}{b}$.

Поле F^*, содержащее данное поле F в качестве подполя, называется **расширением** поля F.

1.3.5. Основные числовые системы

Система натуральных чисел N

Системой натуральных чисел называется алгебра $N = \langle \mathsf{N}, +, *, 0, 1 \rangle$ типа (2,2,0,0), удовлетворяющая следующим аксиомам ($\forall\, m, n \in \mathsf{N}$):

Система аксиом Пеано

I	$n+1\neq 0$	IV	$m+(n+1)=(m+n)+1$
II	$((m+1)=(n+1))\to m=n$	V	$m\cdot 0=0$
III	$m+0=m$	VI	$m(n+1)=m\cdot n+1$

VII Если $A\subset N$, а) $0\in A$,

б) $\forall n$, если $n\in A$, то $(n+1)\in A$, тогда $A=N$

Из аксиомы математической индукции (VII) вытекает, что любое подмножество множества N, содержащее 0, 1 и замкнутое относительно сложения, совпадает с множеством N. Другими словами, единственной подалгеброй алгебры $N=\langle N,+,*,0,1\rangle$ является сама алгебра N.

Элементы множества N называются натуральными числами. Элементы **0** и **1** называются соответственно нулем и единицей системы N. Для записи чисел 1+1, 1+1+1, 1+1+1+1, ... используется обычная десятичная символика 2, 3, 4, ...

Свойства сложения

Алгебра $\langle N,+,0\rangle$ называется **аддитивным моноидом натуральных чисел**.

1. Сложение натуральных чисел ассоциативно, т. е.:

$$\forall a,b,c\in N \quad a+(b+c)=(a+b)+c.$$

2. Сложение натуральных чисел коммутативно, т. е.:

$$\forall a,b\in N \quad a+b=b+a.$$

3. Закон сокращения для сложения:

$$\forall a,b,c\in N \quad (a+c=b+c)\to a=b.$$

4. Закон транзитивности:

$$\forall a,b\in N \text{ либо } a=0, \text{ либо } a=b+1.$$

5. $\forall a,b\in N$ выполняется одно и только одно из трех условий:

1) $a=b$;

2) $a+k=b \quad \forall k\in N/\{0\}$;

3) $a=b+m \quad \forall m\in N/\{0\}$.

Разностью двух натуральных чисел a и b называется такое натуральное число k, что $b+k=a$.

Свойства умножения

Алгебра $\langle \mathsf{N},+,0\rangle$ называется **аддитивным моноидом натуральных чисел**.

1. Умножение натуральных чисел ассоциативно:

$$\forall\, a,b,c\in \mathsf{N}\quad a\cdot(b\cdot c)=(a\cdot b)\cdot c.$$

2. Умножение натуральных чисел коммутативно:

$$\forall\, a,b\in \mathsf{N}\quad a\cdot b=b\cdot a.$$

3. Умножение дистрибутивно относительно сложения:

$$\forall\, a,b,c\in \mathsf{N}\quad (a+b)\cdot c=a\cdot b+b\cdot c.$$

4. Закон сокращения умножения:

$$\forall\, a,b,c\in \mathsf{N}\quad (a\cdot c=b\cdot c)\ \text{и}\ c\neq 0\to a=b\,.$$

5. Отсутствие делителя нуля:

$$\forall\, a,b,c\in \mathsf{N}\ (a\neq 0\ \text{и}\ b\neq 0)\to a\cdot b\neq 0\,.$$

Кольцо целых чисел Z

Как известно, для данных $\forall\, a,b\in \mathsf{N}$ не всегда можно найти положительное решение уравнения $a+x=b$. Другими словами, не всегда разность $x=b-a$ – неотрицательна.

Аддитивной группой целых чисел называется абелева группа $\mathsf{Z}=\langle Z,+,-\rangle$ со следующими свойствами:

– $\mathsf{N}\subset \mathsf{Z}$ и сумма любых двух натуральных чисел m и n в группе Z совпадает с суммой этих элементов в N;

– для любых целых a существуют такие натуральные m и n, что $n+a=m$.

Таким образом, всякий элемент из Z можно представить как разность натуральных чисел: $\mathsf{Z}=\{m-n\mid m,n\in \mathsf{N}\}$.

В группе Z определяем **естественное умножение** следующим образом:

$$\forall\,(m-n),(p-q)\in \mathsf{Z}\qquad (m-n)(p-q)=(mp+nq)-(mq+np),$$

где mp, nq, mq, np – произведения натуральных чисел в системе N.

Так как любой элемент из Z представим в виде разности натуральных чисел неоднозначно, то введенное умножение не зависит от способа представления множителей в виде разности натуральных чисел.

Кольцо K называется **кольцом целых чисел**, если аддитивная группа кольца K является аддитивной группой целых чисел и умножение в кольце K коммутативно и продолжает умножение натуральных чисел.

Определение. Пусть $\langle Z, +, - \rangle$ аддитивная группа целых чисел, $(\cdot)$ есть естественное умножение в ней и **1** – единица системы N натуральных чисел. Тогда алгебра $\mathsf{Z} = \langle Z, +, -, \cdot, 1 \rangle$ является **кольцом целых чисел**.

Поле рациональных чисел Q

Как известно, для данных $\forall\, a, b \in \mathsf{Z}$ не всегда можно найти решение уравнения $a = b \cdot x$ в целых числах. Другими словами, не всегда число b делится на число a без остатка $x = \dfrac{b}{a} \notin \mathsf{Z}$.

Множество чисел, которое можно представить в виде частного целых чисел, называется **полем рациональных чисел** $\mathsf{Q} = \langle Q, +, -, \cdot, 1 \rangle$.

С точки зрения теории групп поле рациональных чисел состоит из двух групп $\langle Z, +, 0 \rangle$ аддитивной и $\langle Z, *, 1 \rangle$ мультипликативной, связанных соотношением дистрибутивности: $a \cdot (b + c) = a \cdot b + a \cdot c$.

Поле действительных чисел R

Как известно, для данных $\forall\, n \in \mathsf{Z}, a \in \mathsf{Q}, a > 0$ не всегда можно найти решение уравнения $x^n = a$ в рациональных числах Q. Однако для любого положительного числа a существует

единственное положительное действительное число c такое, что $c^n = a$.

Пусть a – положительное действительное число и n – натуральное число, отличное от нуля. Единственное положительное число c такое, что $c^n = a$, называется арифметическим корнем n-й степени из a и обозначается $c^{1/n}$ или $\sqrt[n]{c}$.

На множестве Q рациональных чисел можно ввести отношение порядка $<$ следующим образом: для любых двух рациональных чисел $\frac{p}{q}$ и $\frac{r}{s}$, где $p,r \in Z; q,s \in /\{0\}$ имеем

$$\frac{p}{q} < \frac{r}{s} \leftrightarrow ps < qr.$$

Свойства отношения порядка на Q:

– если $a < b$ и $b < c$, то $a < c$;

– имеет место только одно из трех соотношений $a < b$, или $a = b$, или $a > b$;

– если $a < b$, то $(a + c) < (b + c)$;

– если $a < b$ и $0 < c$, то $ac < bc$.

Упорядоченное поле $\mathsf{F} = \langle F, +, -, \cdot, 1, < \rangle$ называется **архимедовски упорядоченным**, если для любых положительных элементов a и b поля существует натуральное число n такое, что $b < na$.

Пусть $\{a_k\} = \{a_1, a_2, a_3, ...\}$ – бесконечная упорядоченная последовательность. Элемент a упорядоченного поля F называется **пределом последовательности** $\{a_k\}$ элементов поля, если для любого положительного элемента ε поля существует натуральное число n_0 такое, что $|a_k - a| < \varepsilon$ для любого натурального $k \geq n_0$. Последовательность $\{a_k\}$,

имеющая предел в поле F, называется **сходящейся** в этом поле. Последовательность $\{a_k\}$ элементов упорядоченного поля F называется **фундаментальной** над F, если для каждого положительного элемента ε поля существует натуральное число n_0 такое, что $|a_k - a_n| < \varepsilon$ для любых натуральных k, n, больших, чем n_0. Упорядоченное поле называется **полным**, если всякая фундаментальная последовательность элементов поля сходится в этом поле. Системой действительных чисел называется полное архимедовски упорядоченное поле.

Определение. Пусть $\langle R,+,-,\cdot,1,< \rangle$ – система действительных чисел. Тогда алгебра $\mathsf{R} = \langle R,+,-,\cdot,1 \rangle$ есть поле, называемое **полем действительных чисел**. Множество R называется множеством действительных чисел.

Поле комплексных чисел C

Как известно квадрат любого ненулевого числа больше нуля, т. е. уравнение $x^2 = -1$ – не имеет решения в R.

Теперь мы построим такую алгебру, в которой данное уравнение имело бы решение. Пусть $\mathsf{R} = \langle R,+,-,\cdot,1 \rangle$ – поле действительных чисел, в котором квадрат каждого элемента отличен от (–1).

Полем комплексных чисел $\mathsf{C} = \langle C,+,-,\cdot,1 \rangle$ называется комплексное расширение поля действительных чисел R, для которого выполняются следующие условия:

– R есть подполе поля C;

– в C имеется элемент i такой, что $i^2 = -1$;

– каждый элемент z поля C можно представить единственным образом в виде $z = a + ib, \quad a, b \in \mathsf{R}$.

Это представление называется **алгебраической формой** числа z. Число (i) называется мнимой единицей поля комплексных чисел.

Свойства комплексных чисел $z \in \mathbb{C}$.

Пусть $a,b,c,d \in \mathbb{R}$, тогда:

– $a+ib=c+id$ тогда и только тогда, когда $a=c$ и $b=d$;

– $(a+ib)+(c+id)=(a+c)+i(b+d)$;

– $-(a+ib)=(-a)+i(-b)$;

– $(a+ib)(c+id)=(ac-bd)+i(ad+bc)$;

– если $a+ib\neq 0$, то $(a+ib)^{-1}=\dfrac{a}{a^2+b^2}+i\dfrac{-b}{a^2+b^2}$;

Комплексные числа $z=a+ib$ и $\bar{z}=a-ib$ называются **сопряженными**.

Модулем комплексного числа $z=a+ib$ называется арифметический квадратный корень из числа a^2+b^2: $|z|=\sqrt{a^2+b^2}$.

§ 1.4. Системы счисления

Пусть q – натуральное число, большее 1, и $M=\{0,1,2,3,..,q-1\}$. Говорят, что натуральное число a записано в **позиционной системе** с основанием q, если

$$a=a_0+a_1q^1+a_2q^2+...+a_kq^k,$$

где $s\in\mathbb{N}, a_i\in M$.

Если каждое число множества $M=\{0,1,2,3,..,q-1\}$ обозначено специальным символом, то эти символы называются **цифрами** q-ичной позиционной системы. Число a в q-ичной позиционной системе сокращенно записывают в виде $a=(a_0a_1a_2...a_k)_q$.

Количество различных цифр, используемых в позиционной системе счисления для изображения произвольных натуральных чисел, называют **основанием** системы счисления, а эти цифры называют **базисными**.

Основания систем счисления:

– двоичная система: (0, 1);

– троичная система: (0, 1, 2);

– шестеричная система: (0, 1, 2, 3, 4, 5);

– десятеричная система: (0, 1, 2, 3, 4, 5, 6, 7, 8, 9);

– шестнадцатиричная система: (0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F).

Рассмотренные системы потому и называются позиционными, что значение каждой цифры меняется с изменением ее положения (позиции) в последовательности.

$$(2315)_{10} = 2\cdot10^3 + 3\cdot10^2 + 1\cdot10^1 + 5\cdot10^0;$$

$$(101001)_2 = 1\cdot2^5 + 0\cdot2^4 + 1\cdot2^3 + 0\cdot2^2 + 0\cdot2^1 + 1\cdot2^0;$$

$$(A19D0B)_{16} = A\cdot16^5 + 1\ 16^4 + 9\ 16^3 + D\cdot16^2 + 0\cdot16^1 + B\cdot2^0.$$

Системы счисления, в которых каждый коэффициент p-ичного разложения числа записывается в q-ичной системе, $q < p$ называется **смешанными**. В такой системе p называется **старшим основанием**, q – **младшим основанием**, а сама смешанная система называется $q-p$-ичной.

Для того чтобы запись числа в смешанной системе счисления была однозначной, для изображения любой p-ичной цифры отводится одно и то же количество q-ичных разрядов, достаточное для изображения любой p-ичной цифры.

Пример 3. Запишем $(925)_{10}$ в (2–10)-й (двоично-десятичной) системе.

Поскольку 9 = 1001, 2 = 0010, 5 = 0101, то $(925)_{10} = (1001\ 0010\ 0101)$.

Заметим, что это не то же самое, что $(925)_{10} = (111\ 001110\ 1)_2$.

Смешанные системы широко используются на практике для сокращения записи чисел, заданных в системе счисления

с небольшим основанием. Для этого в исходной записи числа разряды объединяются вправо и влево от запятой в группы некоторой длины, и каждая такая группа записывается одной цифрой другой системы.

$$(101110{,}1)_2 = (46{,}5)_{10};$$

$$10\ 11\ 10,\ 10 = (232{,}2)_4;$$

$$101\ 110,\ 100 = (56{,}4)_8;$$

$$0010\ 1110,\ 1000 = (2\ E,\ 8)_{16}.$$

Рассмотрим теперь общую задачу перевода чисел из одной системы счисления в другую. Пусть известна запись числа x в p-ичной системе счисления: $x = (p_n p_{n-1} \ldots p_2 p_1 p_0 p_{-1} p_{-2} \ldots)_p$.

Требуется найти запись этого же числа в q-ичной системе счисления $x = (q_s q_{s-1} \ldots q_2 q_1 q_0 q_{-1} q_{-2} \ldots)_q$.

При рассмотрении правил перевода необходимо учитывать, средствами какой арифметики дожен быть осуществлен перевод, т. е. в какой системе счисления должны быть выполнены все арифметические действия. Допустим, перевод осуществляется средствами p-ичной арифметики.

Перевод $q \to p$

Перевод q-ичного числа в p-ичное сводится к вычислению значения полинома:

$$x = q_n Q^n + q_{n-1} Q^{n-1} + \ldots + q_1 Q + q_0 + q_{-1} Q^{-1} + \ldots + q_{-m} Q^{-m},$$

где все числа q_i и основание Q заменяются их p-ичными изображениями.

$(371)_8 = (3 \cdot 8^2 + 7 \cdot 8 + 1)_{10} = (3 \cdot 64 + 7 \cdot 8 + 1)_{10} = (249)_{10}$

$(B3D9{,}4)_{16} = (B \cdot 16^3 + 3 \cdot 16^2 + D \cdot 16 + 9 + 4 \cdot 16^{-1})_{10}$

$= (11 \cdot 4096 + 3 \cdot 256 + 13 \cdot 16 + 9 + \frac{4}{16})_{10} = (46038.25)_{10};$

$(110101.10\ 1)_2 =$

$= (2\cdot 2^5 + 1\cdot 2^4 + 0\cdot 2^3 + 1\cdot 2^2 + 0\cdot 2 + 1\cdot + 1\cdot 2^{-1} + 0\cdot 2^{-2} + 1\cdot 2^{-3})_{10}$

$= (2\cdot 32 + 1\cdot 16 + 1\cdot 4 + 1\cdot + \frac{1}{2} + \frac{1}{8})_{10} = (\frac{685}{8})_{10} = (85.625)_{10}.$

Перевод $p \to q$

Поскольку для перевода любого числа достаточно уметь переводить отдельно его целую и дробную части, рассмотрим оба эти случаи отдельно.

Перевод целых чисел

Утверждение. Пусть N – целое число в p-ичной системе исчисления. Тогда $N = (q_s q_{s-1} \ldots q_1 q_0)_Q$, где искомые цифры определяются по следующим реккурентным формулам:

$$q_i = Q\left\{\frac{N_i}{Q}\right\}, \qquad N_{i+1}\left[\frac{N_i}{Q}\right], \qquad (N_0 = N_i)$$

и процесс продолжается до тех пор, пока не станет $N_{i+1} = 0$.

Пусть известна запись целого числа N в системе счисления с основанием P и требуется перевести это число в систему счисления с основанием Q. Запись числа N в q-ичной системе счисления будет иметь вид $N = (q_s q_{s-1} \ldots q_1 q_0)_Q$, где q_i – подлежащие определению цифры q-ичной системы.

Для определения q_0 разделим обе части равенства $N = q_s Q^s + q_{s-1} Q^{s-1} + \ldots + q_1 Q + q_0$ на число Q, причем в левой части равенства произведем фактическое деление, так как запись числа N в системе счисления с основанием P нам известна, а в правой части деление выполним аналитически:

$$\frac{N}{Q} = q_s Q^{s-1} + q_{s-1} Q^{s-2} + \ldots + q_1 + \frac{q_0}{Q}.$$

Приравнивая между собой полученные целые и дробные части (с учетом того, что $q_i < Q$), имеем:

$$\left[\frac{N}{Q}\right] = q_s Q^{s-1} + q_{s-1} Q^{s-2} + \ldots + q_1, \qquad \left\{\frac{N}{Q}\right\} = \frac{q_0}{Q}.$$

Отсюда получаем, что младший коэффициент q_0 в разложении определяется соотношением:

$$q_0 = Q\left\{\frac{N}{Q}\right\},$$

т. е. является остатком от деления N на Q.

Положим далее, что

$$N_1 = \left[\frac{N}{Q}\right], \text{ т. е. } N_1 = q_s Q^{s-1} + q_{s-1} Q^{s-2} + \ldots + q_1.$$

Тогда N_1 есть целое число и к нему можно применить ту же процедуру для определения искомой цифры q_1 и т. д.

Поскольку все операции выполняются в системе счисления с основанием P, в этой системе будут получены и искомые коэффициенты q. Для окончательной записи числа в q-ичной системе необходимо каждый из полученных коэффициентов записать q-ичной цифрой.

Пример 4. Запишем $(47)_{10}$ в двоичной, пятеричной и шестнадцатиричной системе.

$(47)_{10} = 2\cdot 23 + 1 = 2\cdot 2\ 111) + 1$

$= 2^{2}\cdot 11 + 2 + 1 = 2^2 (2\cdot 5 + 1) + 2 + 1$

$= 2^{3}\cdot 5 + 2^2 + 2 + 1 = 2^3\cdot(2^2 + 1) + 2^2 + 2 + 1$

$= 2^{5}\cdot + 2^3 + 2^2 + 2 + 1 = 1\cdot 2^5 + 0\cdot 2^4 + 1\cdot 2^3 + 1\cdot 2^2 + 1\cdot 2 + 1\cdot 2^0 = (101111)_2$

$(47)_{10} = 2\cdot 16 + 15 = 2\cdot 16^1 + 15\cdot 16^0 = (2F)_{16}$

$(47)_{10} = 9\cdot 5 + 2 = (5 + 4)\cdot 5^1 + 2\cdot 5^0 = 1\cdot 5^{2}\cdot + 4\cdot 5^1 + 2\cdot 5^0 = (142)_5$

Процесс вычисления можно представить и по-другому:

47	|2							47	|5			
46	23	|2						45	9	|5		
1	22	11	|2					2	5	1	|5	
	1	10	5	|2					4	0	0	
		1	4	2	|2					1		
			1	2	1	|2						
				0	0	0		47	|16			
					1			32	2	|16		
								15	0	0		
									2			

Пример 5. Запишем $(3060)_{10}$ в двоичной и шестнадцатиричной системе.

$(3060)_{10} = 191 \cdot 16 + 4 = (11 \cdot 16 + 15) \cdot 16 + 4$

$= 11 \cdot 16^2 + 15 \cdot 16 + 4 = 11 \cdot 16^2 + 15 \cdot 16^2 + 15 \cdot 16^1 + 4 \cdot 16^0 = (BF4)_{16}$

$(3060)_{10} = 1530 \cdot 2 = 765 \cdot 2^2 = (382 \cdot 2 + 1) \cdot 2^2 = 382 \cdot 2^3 + 2^2$

$= 191 \cdot 2^4 + 2^2 = 191 \cdot 2^4 + 2^2 = (95.2 + 1) \cdot 2^4 + 2^2$

$= 95 \cdot 2^5 + 2^4 + 2^2 = 47 \cdot 2^6 + 2^5 + 2^4 + 2^2$

$= 23 \cdot 2^7 + 2^6 + 2^5 + 2^4 + 2^2 = 11 \cdot 2^8 + 2^7 + 2^6 + 2^5 + 2^4 + 2^2$

$= 5 \cdot 2^9 + 2^8 + 2^7 + 2^6 + 2^5 + 2^4 + 2^2$

$= 2^{11} + 2^9 + 2^8 + 2^7 + 2^6 + 2^5 + 2^4 + 2^2$

$= (101111110\ 100)_2$

Или

3060	|2											
3060	1530	|2										
0	1530	765	|2									
	0	764	382	|2								
		1	382	191	|2							
			0	190	95	|2						
				1	94	47	|2					
					1	46	23	|2				
						1	22	11	|2			
3060	|16						1	10	5	|2		
3056	191	|16						1	4	2	|2	
4	176	11	|16						1	2	1	|2
	15	0	0							0	0	0
		11									1	

Перевод дробных чисел

Пусть x – правильная дробь, заданная в p-ичной системе счисления. Тогда $x = (0, q_{-1}, q_{-2}, ..., q_{-m})$, где искомые цифры определяются по следующим рекуррентным формулам:

$$q_{-(i+1)} = [x \cdot Q], \qquad x_{i+1} = \{x_i \cdot Q\}, \qquad i = 0,1,2,...; \quad x_0 = x,$$

и процесс продолжается до тех пор, пока не будет получено $x_{i+1} = 0$ либо не будет достигнута требуемая точность изображения числа.

Пример 6. Запишем $(3,14)_{10}$ в двоичной, троичной, семиричной и шестнадцатиричной системе.

Для целой части имеем

$$(3)_{10} = (11)_2 = (10)_3 = (3)_7 = (3)_{16}.$$

Для дробной части произведем умножение столбиком, записывая целые части в двоичной, троичной, семиричной и шестнадцатиричной системе.

0,14	0,14	0,14	0,14
2	3	7	16
0,28	0,42	0,98	2,24
2	3	7	16
0,56	1,26	6,86	3,84
2	3	7	16
1,12	0,78	6,02	13,44
2	3	7	16
0,24	2,34	0,14	7,04
2	3	7	16
0.48	1.02	0.98	0.64
2	3	7	16
0,96	0,06	6,86	10,24
2	3	7	16
1,92	0,18	6,02	3,84
2	3	7	16
1,84	0,54	0,14	13,44
2	3	7	16
1,68	1,62	0,98	7,04
2	3	7	16
1,36	1,86	6,86	0,64
2	3	7	16
0,72	2,58	6,02	10,24
...	...	...	...

Собирая целые части, получим:

$$(3,14)_{10} = (11,001000\ 1010)_2$$
$$= (10,010210\ 00112)_3$$
$$= (3,0660066\ 0066\ldots)_7$$
$$= (3,23\ D\ 70\ A\ 3\ D\ 70\ A\ldots)_h.$$

§ 1.5. Группы перестановок

Рассмотрим множество некоторых элементов $M = \{1,2,\ldots,n\}$. Тогда множество всех перестановок этих элементов образует группу и обозначается S_n.

Группа S_2 состоит из двух элементов: (1, 2) и (1, 2).

Группа S_3 состоит из шести элементов: (1, 2, 3), (1, 3, 2), (2, 1, 3), (2, 3, 1), (3, 2, 1), (3, 1, 2).

Группа S_4 состоит из $4! = 24$ элементов.

Группа S_5 состоит из $5! = 120$ элементов.

Группа S_n состоит из $n!$ элементов.

Для удобства начальное состояние множества фиксируется и записывается в верхней строке матрицы перестановок. Тогда преобразованное некоторой перестановкой состояние записывается в нижней строке.

Для S_3:

$$\alpha_1 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \qquad \alpha_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

Для α_1 мы говорим, что 1 переходит в 3, 2 переходит в 2, а 3 переходит в 1.

Для α_2 1 переходит в 1, 2 переходит в 3, а 3 переходит в 2.

Для S_4:

$$\beta_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}, \qquad \beta_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}.$$

Тождественным называется преобразование e, оставляющее все элементы на своих местах:

Для S_4 Для S_5 Для S_6:

$$e = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} \quad e = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} \quad e = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}$$

Элементы группы перестановок α_1 и α_2 можно перемножать. Для этого переставляют столбцы таблицы α_2 так, чтобы ее верхний ряд совпадал с нижним рядом таблицы α_1.

$$\alpha_1 = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}, \qquad \alpha_2 = \begin{pmatrix} 1 & 2 & \dots & n \\ j_1 & j_2 & \dots & j_n \end{pmatrix}$$

$$\alpha_1 = \begin{pmatrix} 1 & 2 & \dots & n \\ \underline{i_1} & \underline{i_2} & \dots & \underline{i_n} \end{pmatrix}, \qquad \alpha_2 = \begin{pmatrix} \underline{i_1} & \underline{i_2} & \dots & \underline{i_n} \\ k_1 & k_2 & \dots & k_n \end{pmatrix}.$$

После чего вычеркивают совпадающие ряды, а оставшиеся два ряда соответствуют произведению $\alpha_1 \cdot \alpha_2$.

$$\alpha_1 \cdot \alpha_2 = \begin{pmatrix} 1 & 2 & \dots & n \\ k_1 & k_2 & \dots & k_n \end{pmatrix}.$$

Пример 7. Вычислить произведение элементов $(\alpha_1, \alpha_2) \in S_3$:

$$\alpha_1 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \qquad \alpha_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

Решение:

$$\alpha_1 \cdot \alpha_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ \underline{3} & \underline{2} & \underline{1} \end{pmatrix} \cdot \begin{pmatrix} \underline{3} & \underline{2} & \underline{1} \\ 2 & 3 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \cdot \begin{pmatrix} 3 & 2 & 1 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

Пример 8. Вычислить произведение элементов $(\alpha_1, \alpha_2) \in S_4$:

$$\alpha_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \qquad \alpha_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}.$$

Решение:

$$\alpha_1 \cdot \alpha_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 \\ \underline{2} & \underline{1} & \underline{4} & \underline{3} \end{pmatrix} \cdot \begin{pmatrix} \underline{2} & \underline{1} & \underline{4} & \underline{3} \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \cdot \begin{pmatrix} 2 & 1 & 4 & 3 \\ 4 & 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}.$$

Перестановки удобно записывать в циклической форме. Тогда индексы, остающиеся на месте, не пишутся, а записываются только переходы индексов.

Для S_4:

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix} = (143), \qquad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = (14)(23).$$

Для S_5:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 2 & 1 \end{pmatrix} = (13425), \qquad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 2 & 4 & 5 \end{pmatrix} = (23).$$

Пусть e – единичный элемент группы G. Если $a^n = e$, то наименьшее такое n называют **порядком** элемента.

Для S_3: $(12)^2 = (12)(12) = e$ т. е. элемент (12) – 2-го порядка.

Для S_3: $(123)^2 = (132), (123)^3 = e$ т. е. элемент (123) – 3-го порядка.

Для S_4 : 1234) ^{2}= (13)(24),(1234) ^{3}= (1432),$(1234)^4 = e$ –4-го порядка.

Подгруппой H называется множество элементов a, принадлежащих группе G и являющихся самостоятельной групой, т. е. $a \in G, a \in H, H \subseteq G$. Очевидно, что любая группа – сама себе подгруппа и единичный элемент $e \in G$ любой группы образует единичную подгруппу. Далее эти две подгруппы мы будем называть **тривиальными**.

Самым простым способом отыскания подгрупп в группе является последовательное перемножение всех элементов группы в различных комбинациях. К сожалению, даже для групп небольшого порядка это не всегда является посильной задачей.

Пример 9. Найти все подгруппы группы S_3.

Решение. Запишем все возможные элементы группы S_3 в циклической форме:

$$\alpha_0 = e = (1), \alpha_1 = (12), \alpha_2 = (23), \alpha_3 = (31), \alpha_4 = (123), \alpha_5 = (321).$$

Умножаем $\alpha_1 \cdot \alpha_1 = \alpha_1, \quad e \cdot e = e, \quad e \cdot \alpha_1 = \alpha_1,$ т. е. элементы (e, α_1) образуют подгруппу группы S_3. Аналогично:

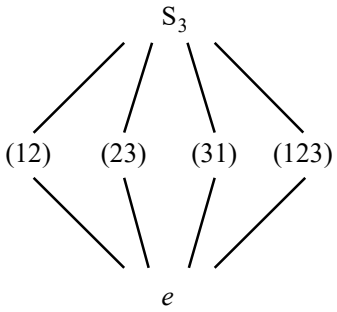
$$\alpha_2 \cdot \alpha_2 = \alpha_2, \quad e \cdot e = e, \quad e \cdot \alpha_2 = \alpha_2,$$
$$\alpha_3 \cdot \alpha_3 = \alpha_3, \quad e \cdot e = e, \quad e \cdot \alpha_3 = \alpha_3,$$

т. е. подгруппами являются множества (e, α_2) и (e, α_3). Далее:

$$\alpha_4 \cdot \alpha_4 = \alpha_5, \quad \alpha_5 \cdot \alpha_5 = \alpha_4, \quad \alpha_4 \cdot \alpha_5 = e,$$

т. е. элементы (e, α_4, α_5) образуют подгруппу группы S_3.

Дальнейшие всевозможные комбинации элементов никаких новых (замкнутых относительно умножения) подгрупп не создают, поэтому мы заключаем, что группа S_3 содержит (кроме тривальных) три подгруппы второго порядка типа (12) и одну подгруппу третьего порядка типа (123). Графически это можно представить в виде решетки подгрупп:



В циклических обозначениях группа S_1 имеет только 1 элемент (1), группа S_2 имеет два элемента (1), (1, 2), т. е. $S_2 ; Z_2$.

Для группы S_3 получим:

Циклическая структура	Количество элементов	Порядок
(1)	1	0
(12)	3	2
(123)	2	3
Всего	6	

Для группы S_4 получим:

Циклическая структура	Количество элементов	Порядок
(1)	1	0
(12)	6	2
(123)	8	3
(1234)	6	4
(12)(34)	3	0
Всего	24	

Для группы S_5 получим:

Циклическая структура	Количество элементов	Порядок
(1)	1	0
(12)	10	2
(123)	20	3
(1234)	30	4
(12345)	24	5
(12)(34)	15	0
(12)(345)	20	6
Всего	120	

Для нахождения **взаимно обратной** перестановки α^{-1} необходимо верхнюю строку перестановки поменять с нижней и упорядочить индексы верхней строки.

Пример 10. Вычислить элемент α^{-1}, обратный к $\alpha = (123) \in S_3$.

Решение. Записываем перестановку в виде матрицы:

$$\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

Поменяем верхнюю строку с нижней:

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \Rightarrow \begin{pmatrix} 2 & 3 & 1 \\ 1 & 2 & 3 \end{pmatrix}.$$

Упорядочим индексы верхней строки:

$$\alpha^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

Таким образом, $\alpha^{-1} = (132)$.

Теперь мы можем проверить наши вычисления ($\alpha \cdot \alpha^{-1} = e$):

$$\alpha \cdot \alpha^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ \underline{2} & \underline{3} & \underline{1} \end{pmatrix} \cdot \begin{pmatrix} \underline{2} & \underline{3} & \underline{1} \\ 1 & 2 & 3 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \cdot \begin{pmatrix} 2 & 3 & 1 \\ 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = e.$$

Пример 11. Вычислить элемент α^{-1}, для $\alpha = (125)(34) \in S_5$.

Решение. Записываем перестановку в виде матрицы:

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 \end{pmatrix}.$$

Поменяем верхнюю строку с нижней:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 \end{pmatrix} \Rightarrow \begin{pmatrix} 2 & 5 & 4 & 3 & 1 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}.$$

Упорядочим индексы верхней строки:

$$\alpha^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 4 & 3 & 2 \end{pmatrix}.$$

Таким образом $\alpha^{-1} = (152)(34)$.

Теперь мы можем проверить наши вычисления ($\alpha \cdot \alpha^{-1} = e$):

$$\alpha \cdot \alpha^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 4 & 3 & 2 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ \underline{2} & \underline{5} & \underline{4} & \underline{3} & \underline{1} \end{pmatrix} \cdot \begin{pmatrix} \underline{2} & \underline{5} & \underline{4} & \underline{3} & \underline{1} \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 \end{pmatrix} \cdot \begin{pmatrix} 2 & 5 & 4 & 3 & 1 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = e.$$

Введение понятия обратной перестановки позволяет быстро найти **решение линейного уравнения** типа $\alpha \cdot x = \beta$ по формуле $x = \alpha^{-1} \cdot \beta$.

Пример 12. Решить уравнение $(132)x = (13)$ в группе S_3.

Решение. Записывая перестановки в виде матриц, получим:

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \cdot x = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

Здесь $\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$, $\beta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$.

Вычисляя для элемента α обратный, получим: $\alpha^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, тогда

$$x = \alpha^{-1} \cdot \beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (12).$$

Пример 13. Решить уравнение $(13254)x = (14)(25)$ в группе S_5.

Решение. Записывая перестановки в виде матриц, получим

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 2 & 1 & 4 \end{pmatrix} \cdot x = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 3 & 1 & 2 \end{pmatrix}.$$

Здесь $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 2 & 1 & 4 \end{pmatrix}$, $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 3 & 1 & 2 \end{pmatrix}$.

Вычисляя для элемента α обратный, получим $\alpha^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 1 & 5 & 2 \end{pmatrix}$, тогда

$$x = \alpha^{-1} \cdot \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 1 & 5 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 3 & 1 & 2 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 4 & 2 & 5 \end{pmatrix} = (234).$$

1.5.1. Группы малых размерностей

Важность изучения групп перестановок основана на теореме Кэли.

Теорема Кэли. Не существует такой группы, которую нельзя было бы представить перестановками.

Группа первого порядка $C_1; S_1$. Группа первого порядка имеет всего один элемент e.

Группа второго порядка $C_2; S_2$. Группа второго порядка имеет два элемента e и $\alpha = (21)$.

Группа третьего порядка C_3. Группа третьего порядка имеет три элемента $e, \alpha_1 = (123), \alpha_2 = (132)$.

Группы четвертого порядка C_4**.** Имеются две группы четвертого порядка. Собственно C_4 и C_2C_2 с различными законами умножения.

Все группы порядка не более 5 – абелевы.

Пусть e – единичный элемент группы G. Если $a^n = e$, то наименьшее такое n называют порядком элемента.

Пример 14. Определить порядок элемента $a = 5$ в Z_{14}.

Решение. Возводя элемент $a = 5$ последовательно в степень $k = 0,1,2,3,..$, находим:

$$5^0 = 1,\ 5^1 = 5,\ 5^2 = 25 - 14 = 11,$$

$$5^3 = 125 - 14 \cdot 8 = 13,\ 5^4 = 9, 5^5 = 3,\ 5^6 = 1.$$

Поскольку $5^6 = 1 = e$, то элемент $a = 5$ имеет порядок 6.

Если порядок элемента совпадает с порядком группы (количеством элементов группы), то такой элемент называют генератором группы. В таком случае любой элемент $b \in G$ группы является степенью генератора $a^k = b$. Для описания групп простого порядка достаточно одного генератора. Описание групп составного порядка требует нескольких генераторов. Часто нам известны только некоторые соотношения между элементами групп по которым необходимо определить ее структуру.

$$G = \langle \{a\} \mid \{a^n = e\} \rangle \Rightarrow G; \mathsf{Z}_n,$$

$$G = \langle \{a, b\} \mid \{a^n = b^k = e\} \rangle \Rightarrow G; \mathsf{Z}_n \oplus \mathsf{Z}_k; \mathsf{Z}_{nk}.$$

$$D_{2n} = \langle \{a, b\} \mid \{a^n = b^2 = e, bab = a^{-1}\} \rangle.$$

или $D_n = \langle \{a,b\} \mid \{a^2 = b^2 = (ab)^n = e\} \rangle$ – диэдральная группа.

$D_{2n}; \mathsf{Z}_n \times \mathsf{Z}_2$.

$S_n; \mathsf{A}_n \times \mathsf{Z}_2$.

$D_6; S_3; \mathsf{Z}_3 \times \mathsf{Z}_2$.

$D_{12}; S_3 \times \mathsf{Z}_2$.

$\mathsf{Z}_6 = \langle \{a\} \mid \{a^6 = e\} \rangle; \langle a \rangle / \langle a^6 \rangle$.

$\mathsf{Z}_6 = \langle \{a,b\} \mid \{a^3 = b^2 = aba^{-1}b^{-1} = e\} \rangle$.

$A_4 = \langle \{a,b\} \mid \{a^2 = b^3 = (ab)^3 = e\} \rangle$ – тетраэдральная группа.

$A_5 = \langle \{a,b\} \mid \{a^2 = b^3 = (ab)^5 = e\} \rangle$ – икосаэдральная группа.

$A_5 = \langle \{a,b,c\} \mid \{a^2 = b^3 = c^5 = abc = e\} \rangle$.

$S_4 = \langle \{a,b\} \mid \{a^2 = b^3 = (ab)^4 = e\} \rangle$ – октаэдральная группа.

$Q = \langle \{a,b\} \mid \{a^4 = e, b^2 = a^2, bab^{-1} = a^{-1} = a^3\} \rangle$ – группа кватернионов (восьмого порядка).

$Q = \langle \{a,b\} \mid \{a^2 = b^2, aba = b\} \rangle$.

$D_8 = \langle \{a,b\} \mid \{a^4 = e, b^2 = e, bab^{-1} = a^{-1}\} \rangle$.

$T = \langle \{a,b\} \mid \{a^6 = e, b^2 = a^3 = (ab)^2\} \rangle$ – группа двенадцатого порядка.

В самом общем случае можно определить полиэдральную группу соотношениями $P(l,m,n) = \langle \{a,b\} \mid \{a^l = b^m = (ab)^n = e\} \rangle$.

$P(n,2,2) = D_{2n}$ $\qquad$ $P(2,3,3) = A_4$

$P(2,3,4) = S_4$ $\qquad$ $P(2,3,5) = A_5$

Любая неабелева группа G порядка 12 изоморфна (A_4, D_{12}, T).

Приведем таблицу групп малых порядков.

Порядок	Количество	Группы
4	2	Z_4, V
6	2	Z_2Z_3, S_3
8	5	Z_8, Z_4Z_2, $Z_2Z_2Z_2$, D_8, Q
9	2	Z_9, Z_3Z_3
10	2	Z_{10}, D_{10}
12	5	Z_{12}, Z_6Z_2, A_4, D_{12}, T
14	2	Z_{14}, D_{14}
15	1	Z_{15}

Пример 15. Для группы:

$$G = \langle \{a,b,c\} \mid \{a^7, b^3, c^2, ba = a^3b, ca = ac, cb = b^2c\} \rangle$$

переписать каждое выражение в форме $a^p b^q c^r$.

Решение:

$$(bc)^2 = bcbc = b(cb)c = b(b^2c)c = b^3c^2 = ee = e$$

$$b^2a^3 = b(ba)aa = b(a^3b)aa = ba^3baa$$

$$= ba^3a^3a^3b = ba^9b = ba^2b = a^3a^3bb = a^6b^2$$

$$c^3a^{-2} = ca^{-2} = ca^5 = aca^4 = a^2ca^3 = a^4ca = a^5c$$

$(abc)^{-1}$. Пусть $(abc)^{-1} = x$ тогда $(abc) = x^{-1}$ и

$(ab) = x^{-1}c^{-1}, (a) = x^{-1}c^{-1}b^{-1}, e = x^{-1}c^{-1}b^{-1}a^{-1}, x = c^{-1}b^{-1}a^{-1}$

После преобразований получим:

$$(abc)^{-1} = c^{-1}b^{-1}a^{-1} = cb^2a^6 = b^4ca^6$$

$$= b^4a^6c = ba^6c = (a^3)^6bc = a^{18}bc = a^4bc$$

$$(ab)^3 = ababab = abaa^3bb = aba^4b^2$$

$$= a(a^3)^4b^3 = a^6 = a^{13} = a^6 = a^{-1}.$$

Пример 16. Определить структуру группы:

$$G = \langle \{a,b\} \mid \{a^3b = a^4 = b^3 = e\} \rangle$$

Решение: имеем $a^3b = e$.

Домножим слева на a, $a^4b = a$, поскольку $a^4 = e$, имеем $a^4b = eb = b = a$.

Тогда $a^4 = b^3, \Rightarrow a^4 = a^3, \Rightarrow a = e, b = a = e$ и значит $G;\{e\}$ – тривиальная группа.

Пример 17. Определить количество элементов группы:

$G = \langle \{a,b\} \mid \{a^2 = b^2 = e\} \rangle$.

Решение. Перебирая всевозможные комбинации a и b, имеем $1, a, ab, aba, abab, ababa, ..., b, ba, bab, baba, babab, ...$.

т. е. G – группа бесконечного порядка.

Пример 18. Определить количество элементов группы

$$G = \langle \{a,b\} \mid \{a^4 = b^2 = (ab)^2 = e\} \rangle.$$

Решение. Перебирая всевозможные комбинации a и b, имеем:

$$1, a, ab, aba, abab, ababa, \ldots$$

$$a^2, a^2b, a^2ba, a^2bab, a^2baba, ..., a^2ba^2, a^2ba^2b, a^2ba^2ba, ...$$

$$a^3, a^3b, a^3ba, a^3bab, a^3baba, ..., a^3ba^3, a^3ba^3b, a^3ba^3ba, ...$$

$$b, ba, bab, baba, babab, ...$$

$$b^2, b^2a, b^2ab, b^2aba, b^2abab, ..., b^2ab^2, b^2ab^2a, b^2ab^2ab, ...$$

$$b^3, b^3a, b^3ab, b^3aba, b^3abab, ..., b^3ab^3, b^3ab^3a, b^3ab^3ab, ...$$

Поскольку $a^{-1} = a^3$, $b^{-1} = b$, то произведение $(ab)^2 = e$ можно переписать в виде $ba = a^{-1}b^{-1}$, или $ba = a^3b$.

Другими словами, любую комбинацию генераторов $a^ib^ka^lb^m...$, переставляя a и b, можно привести к виду a^rb^s, где r = (0, 1, 2, 3), s = (0, 1). Но тогда мы получим только восемь элементов $a^0b^0 = e, a^0b^1, a^1b^0, a^1b^1, a^2b^0, a^2b^1, a^3b^0, a^3b^1$.

т. е. мы имеем диэдральную группу восьмого порядка.

Пример 19. Определить структуру группы:

$$G = \langle \{a,b\} \mid \{a^5 = b^3 = e, ba = a^2b\} \rangle.$$

Решение: имеем $bab^{-1} = a^2$,

$$b(bab^{-1})b^{-1} = ba^2b^{-1} = bab^{-1}bab^{-1} = (ba^2b^{-1})^2 = (a^2)^2 .$$

т. е. $b^2ab^{-2} = a^4$, тогда $b^3ab^{-3} = a^8 = a^3$, но $b^3 = e$, значит $a = a^3$ или $a^2 = e$. По условию $a^5 = e$, т. е. мы получили противоречие, поэтому $a = e$. Но тогда группа имеет вид $G = \langle \{b\} \mid \{b^3 = e\} \rangle$; Z_3.

Согласно **китайской теореме об остатках**, если p и q – два взаимно простых числа, то абелевы группы $Z_p \oplus Z_q$ и Z_{pq} изоморфны: $Z_p \oplus Z_q \cong Z_{pq}$.

Для произвольных порядков имеем более общее выражение

$$Z_n \oplus Z_m \cong Z_{n \wedge m} \oplus Z_{n \vee m}.$$

где $n \wedge m$ – НОД(n,m), $n \vee m$ - НОК(n,m).

$$Z_2 \oplus Z_3 \cong Z_{2\wedge 3} \oplus Z_{2\vee 3} \cong Z_1 \oplus Z_6; Z_6 ;$$

$$Z_4 \oplus Z_3 \cong Z_{4\wedge 3} \oplus Z_{4\vee 3} \cong Z_1 \oplus Z_{12} \cong Z_{12};$$

$$Z_2 \oplus Z_2 \cong Z_{2\wedge 2} \oplus Z_{2\vee 2} \cong Z_2 \oplus Z_2 \neq Z_4 .$$

Пример 20. Найти изоморфные группы порядка 180.

Решение: имеем $180 = 2^2 \cdot 3^2 \cdot 5$. Найдем всевозможные парные комбинации полученного разложения числа 180:

$$Z_1 \oplus Z_{180} \cong Z_{1\wedge 180} \oplus Z_{1\vee 180} \cong Z_1 \oplus Z_{180} \cong Z_{180},$$

$$Z_2 \oplus Z_{90} \cong Z_{2\wedge 90} \oplus Z_{2\vee 90} \cong Z_2 \oplus Z_{90},$$

$$Z_3 \oplus Z_{60} \cong Z_{3\wedge 60} \oplus Z_{3\vee 60} \cong Z_3 \oplus Z_{60},$$

$$Z_4 \oplus Z_{45} \cong Z_{4\wedge 45} \oplus Z_{4\vee 45} \cong Z_1 \oplus Z_{180} \cong Z_{180},$$

$$Z_5 \oplus Z_{36} \cong Z_{5\wedge 36} \oplus Z_{5\vee 36} \cong Z_1 \oplus Z_{180} \cong Z_{180},$$

$$Z_6 \oplus Z_{30} \cong Z_{6\wedge 30} \oplus Z_{6\vee 30} \cong Z_6 \oplus Z_{30},$$

$$Z_{10} \oplus Z_{18} \cong Z_{10\wedge 18} \oplus Z_{10\vee 18} \cong Z_2 \oplus Z_{90},$$

$$Z_{12} \oplus Z_{15} \cong Z_{12\wedge 15} \oplus Z_{12\vee 15} \cong Z_3 \oplus Z_{60},$$

$$Z_{20} \oplus Z_9 \cong Z_{20\wedge 9} \oplus Z_{20\vee 9} \cong Z_1 \oplus Z_{180} \cong Z_{180}.$$

Отсюда следует:

$$\mathsf{Z}_{20} \oplus \mathsf{Z}_9 \cong \mathsf{Z}_2 \oplus \mathsf{Z}_{36} \cong \mathsf{Z}_4 \oplus \mathsf{Z}_{45} \cong \mathsf{Z}_{180},$$

$$\mathsf{Z}_{10} \oplus \mathsf{Z}_{18} \cong \mathsf{Z}_2 \oplus \mathsf{Z}_{90},$$

$$\mathsf{Z}_{12} \oplus \mathsf{Z}_{15} \cong \mathsf{Z}_3 \oplus \mathsf{Z}_{60}.$$

Аналогичное решение можно получить и для произведения трех групп:

$$\mathsf{Z}_{12} \oplus \mathsf{Z}_3 \oplus \mathsf{Z}_5 \cong \mathsf{Z}_1 \oplus \mathsf{Z}_{60} \oplus \mathsf{Z}_2 \cong \mathsf{Z}_2 \oplus \mathsf{Z}_{60}.$$

Пусть $T(\mathsf{Z}_p) = \varphi(p)$ – порядок первообразного корня группы Z_p. Тогда порядок первообразного корня группы Z_{pq} вычисляется как $T(\mathsf{Z}_{pq}) = T(\mathsf{Z}_p) \vee T(\mathsf{Z}_q)$.

$$T(\mathsf{Z}_{15}) = T(\mathsf{Z}_3) \vee T(\mathsf{Z}_5) = \varphi(3) \vee \varphi(5) = 2 \vee 4 = 4;$$

$$T(\mathsf{Z}_{85}) = T(\mathsf{Z}_5) \vee T(\mathsf{Z}_19) = \varphi(5) \vee \varphi(19) = 4 \vee 18 = 36.$$

Существует несложный алгоритм, позволяющий определить общее количество различных групп заданного порядка. Для этого необходимо знать разложение порядка группы на простые множители. Тогда количество неизоморфных групп будет равно количеству возможных комбинаций, формируемых из простых множителей.

Пример 21. Определить количество различных групп порядка $n = 36$.

Решение: $36 = 2^2 \cdot 3^2$, то получим следующие комбинации:

36=	2^2	3^2
$\mathsf{Z}_{36} \oplus \mathsf{Z}_1$		

18=	2	3^2
2=	2	
$\mathsf{Z}_{18} \oplus \mathsf{Z}_2$		

12=	2^2	3
3=		3
$\mathsf{Z}_{12} \oplus \mathsf{Z}_3$		

6=	2	3
6=	2	3
$\mathsf{Z}_6 \oplus \mathsf{Z}_6$		

Пример 22. Определить количество различных групп порядка $n = 360$.

Решение: $360 = 2^3 \cdot 3^2 \cdot 5$, то:

2^3	3^2	5
$Z_{360} \oplus Z_1$		

2^3	3	5
	3	
$Z_{120} \oplus Z_3$		

2^2	3	5
2	3	
$Z_{60} \oplus Z_6$		

2^2	3^2	5
2		
$Z_{180} \oplus Z_2$		

2	3^2	5
2		
2		
$Z_{90} \oplus Z_2 \oplus Z_2$		

2	3	5
2	3	
2		
$Z_{30} \oplus Z_6 \oplus Z_2$		

Всего шесть различных групп.

1.5.2. Представление абелевых групп

Если генераторы $a, b \in G$ коммутируют (т. е. $ab = ba$), то такая группа называется **абелевой**. Для таких групп существует несложный матричный способ определения их структуры по порождающим соотношениям между генераторами.

Так, матричное представление группы:

$$G = \langle \{a, b\} \mid \{a^4 = b^2 = c^3 = e\} \rangle .$$

имеет вид:

$$\begin{bmatrix} 4 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{bmatrix} \cong Z_4 \oplus Z_2 \oplus Z_3 .$$

Матричное представление группы

$$G = \langle \{a, b\} \mid \{a^7 = b^{11} = c^{13} = d^{19} = e\} \rangle$$

имеет вид:

$$\begin{bmatrix} 7 & 0 & 0 & 0 \\ 0 & 11 & 0 & 0 \\ 0 & 0 & 13 & 0 \\ 0 & 0 & 0 & 19 \end{bmatrix} \cong \mathsf{Z}_7 \oplus \mathsf{Z}_{11} \oplus \mathsf{Z}_{13} \oplus \mathsf{Z}_{19}.$$

Матричная запись позволяет упрощать более сложные соотношения между генераторами. Напомним, что к элементарным преобразованиям матрицы относятся:

– перестановка строк или столбцов матрицы;

– умножение строки или столбца на число;

– сложение строк или столбцов матрицы.

Далее i-ю строку матрицы будем обозначать C_i, а i-ю колонку матрицы K_i.

Пример 23. Определить структуру абелевой группы:

$$G = \langle \{a,b\} \mid ab^2, a^3b^4 \rangle .$$

Решение. Имеем:

$$G \cong \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}.$$

Умножая первую строку на третью и вычитая ее из второй строки, получим:

$$\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 0 & -2 \end{bmatrix}.$$

Умножая первую колонку на вторую и вычитая ее из второй колонки, получим:

$$\begin{bmatrix} 1 & 2 \\ 0 & -2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -2 \end{bmatrix}.$$

Умножая вторую колонку на -2 получим:

$$\begin{bmatrix} 1 & 0 \\ 0 & -2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}, \text{ т. е. } G \cong \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \cong \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} \cong \mathsf{Z} \oplus \mathsf{Z}_2 .$$

Пример 24. Определить структуру абелевой группы:

$$G = \langle \{a,b,c\} \mid a^1b^2c^3, a^6b^5c^4, a^7b^8c^9 \rangle.$$

Решение. Имеем:

$$\begin{bmatrix} 1 & 2 & 3 \\ 6 & 5 & 4 \\ 7 & 8 & 9 \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 & 0 \\ 6 & -7 & -14 \\ 7 & -6 & -12 \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 & 0 \\ 0 & -7 & -14 \\ 0 & -6 & -12 \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 & 0 \\ 0 & 7 & 0 \\ 0 & 6 & 0 \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

$$G \cong \mathsf{Z} \oplus \mathsf{Z}.$$

Пример 25. Определить структуру абелевой группы:

$$G = \langle \{a,b,c\} \mid a^{10}b^{14}c^4, a^{12}b^{16}c^8, a^{14}b^{18}c^8 \rangle.$$

Решение. Имеем:

$$\begin{bmatrix} 10 & 14 & 4 \\ 12 & 16 & 8 \\ 14 & 18 & 8 \end{bmatrix} \equiv \begin{bmatrix} 10 & 14 & 4 \\ -8 & -12 & 0 \\ -6 & -10 & 0 \end{bmatrix} \equiv \begin{bmatrix} 2 & 2 & 4 \\ 8 & 12 & 0 \\ 2 & 2 & 0 \end{bmatrix} \equiv \begin{bmatrix} 0 & 0 & 4 \\ 0 & 4 & 0 \\ 2 & 2 & 0 \end{bmatrix} \equiv \begin{bmatrix} 0 & 0 & 4 \\ 0 & 4 & 0 \\ 2 & 0 & 0 \end{bmatrix}$$

т. е. $G \cong \mathsf{Z}_2 \oplus \mathsf{Z}_4 \oplus \mathsf{Z}_4$.

ГЛАВА II. ТЕОРИЯ ЧИСЕЛ И МОДУЛЯРНАЯ АРИФМЕТИКА

§ 2.1. Деление с остатком

Пусть $a, b \in \mathbb{Z}, a \neq 0$. Если число a делит b без остатка, то такое действие обозначим так $a \mid b$. В этом случае существует такое $c \in \mathbb{Z}$, что $b = ac$. Другие определения бинарной операции $a \mid b$: b делится на a; a делитель b.

Эта операция рефлексивна, транзитивна, но не симметрична.

Свойства отношения $a \mid b$

1.	$a\|a$	6.	если $c\|a$, то $c\|ab$
2.	$a\|0$	7.	если $c\|a$ и $c\|b$, то $c\|(a\pm b)$
3.	если $0\|a$, то $a=0$	8.	если $b\|a$, то $ba\|ac$
4.	$\pm 1\|a$	9.	если $a\|c$ и $b\|d$, то $ab\|cd$
5.	если $a\|b$ и $b\|c$, то $a\|c$	10.	если $a\|b$ и $a\|c$, то $a\|(mb+nc)$

Теорема. Если произведение ab натуральных чисел равно единице, то $a = b = 1$.

Доказательство. Из условия $ab = 1$ следует, что a и b отличны от нуля. Тогда их можно представить в виде $a = c + 1, b = d + 1$.

Следовательно, $ab = cd + c + d + 1 = 1$ и $cd + c + d = 0$.

Если сумма натуральных чисел равна нулю, то каждое из слагаемых равно нулю. В частности, $c = d = 0$, следовательно, $a = b = 1$.

Теорема. Если целое a делит единицу, то $a = \pm 1$.

Доказательство. Предположим, что a делит единицу, т. е. $ab = 1$ для некоторого целого b. Тогда $a^2 b^2 = 1$. Так как a^2 либо b^2 – натуральные числа, то по предыдущей теореме, $a^2 = 1$. Следовательно, либо $a \cdot a = 1$, либо $(-a) \cdot (-a) = 1$. Поскольку

a или $-a$ является натуральным числом, то или $a=1$, или $-a=1$.

Теорема. Если целые числа a и b ассоциативны (т. е. $a \mid b$ и $b \mid a$), то $a=\pm b$.

Доказательство. По условию a делит b и b делит a, т. е. $b=ac$ и $a=bd$ для некоторых целых c и d, поэтому $a=acd$.

Если $a=0$, то $b=0\cdot c=0$ и теорема верна.

Если $a\neq 0$, то $1=cd$. По предыдущей теореме из этого равенства следует, что $d=\pm 1$, кроме того, $a=bd$; следовательно, $a=\pm b$.

Теорема. Для любых целых a и b существует единственная пара целых q и $r\,(0\le r<b)$, удовлетворяющих условиям:

$$a=bq+r.$$

Доказательство. Доказательство возможности. Пусть bq – наибольшее кратное числа b, не превышающее a, тогда

$$bq\le a<b(q+1) \quad \text{è} \quad 0\le a-bq<b.$$

Полагая $a-bq=r$, получим исходное представление.

Доказательство единственности. Допустим, что для целого a существует два представления:

$$a=bq_1+r_1;$$
$$a=bq_2+r_2.$$

Если $r_1>r_2$, то вычитая из одного выражения другое, получим

$$b(q_1-q_2)=r_1-r_2,$$

т. е. (r_1-r_2) – кратно b. С другой стороны, из

$$0\le r_1<b,$$
$$0\le r_2<b,$$

следует, что $(r_1-r_2)\le b$. Это возможно лишь при $(r_1-r_2)=0$ или $r_1=r_2$. Отсюда следует, что и $q_1=q_2$.

§ 2.2. Наибольший общий делитель

Любое целое число $c \in \mathbb{Z}$, делящее числа a и b, называется их **общим делителем**. Максимальный общий делитель для чисел a и b называется **наибольшим общим делителем** (НОД) и обозначается (a,b). В пакете Mathematica для нахождения наибольшего общего делителя используется функция GCD$[a,b]$ (Greatest Common Divisor).

GCD [36, 45] = 9;
GCD [21 + 28i, –33 – 44i] = 3 + 4i;
GCD [36, 45, 18] = 9.

Лемма 1.

$$b \mid a \Rightarrow (a,b) = b .$$

Очевидно, что совокупность общих делителей a и b совпадает с совокупностью делителей b.

Лемма 2.

$$a = bq + c \Rightarrow (a,b) = (b,c) .$$

По свойствам делимости у пары a,b те же общие делители, что и у пары b,c.

Натуральное число $p > 1$ называется **простым**, если оно делится только на себя и на 1.

Теорема. Евклид. Существует бесконечно много простых чисел.

Пусть $p_1, p_2, p_3, ... p_n$ – различные простые числа. Простой делитель числа:

$$p_1 \cdot p_2 \cdot p_3 \cdot ... \cdot p_n + 1$$

не может совпадать ни с одним из чисел $p_1, p_2, p_3, ... p_n$.

Свойства простых чисел (p – простое).

$$(p,a) \neq 1 \quad \Rightarrow p \mid a$$

Действительно, (p,a) будучи делителем p, может быть равен или 1, или p. Следовательно:

$$(p, a) = p \quad \Rightarrow p / a +$$
$$p \mid ab \quad \Rightarrow \quad p \mid a \text{ либо } p \mid b.$$

Допустим $(p,a) = (p,b) = 1$.

Тогда по свойству $(a,b) = 1 \ (a,c) = 1 \ \Rightarrow (a,bc) = 1$

получим $(p,ab) = 1$. Поэтому хотя бы один из множителей делится на p. Свойство легко обобщается на случай нескольких чисел $a,b,c,....$

Теорема. Всякое целое $n > 1$ разложимо в произведение простых множителей.

Доказательство. Допустим целое a – не простое. Тогда $a = p_1 a_1$, где p_1 – наименьший простой делитель. В случае, если a_1 – не простое, то $a_1 = p_2 a_2$. В итоге придем к случаю $a_n = 1$. Следовательно, $a = p_1 p_2 p_3 ... p_n$.

Допустим, существует еще одно разложение $a = q_1 q_2 q_3 ... q_n$.

Тогда $p_1 p_2 p_3 \ldots p_n = q_1 q_2 q_3 \ldots q_n$.

По свойству $p \mid ab \ \Rightarrow \ p \mid a$ либо $p \mid b$, p_1 делит хотя бы одно из чисел в правой части. Пусть, например, $p_1 \mid q_1$. Это значит $p_1 = q_1$. Сокращая обе части на p_1, имеем $p_2 p_3 \ldots p_n = q_2 q_3 \ldots q_n \ldots$.

Аналогичным образом доказывают совпадение p_2 с каким-либо множителем в правой части. В итоге получим тождественность разложений.

В разложении $a = p_1 p_2 p_3 ... p_n$ некоторые множители могут повторяться. Если объединить повторения, то получится **каноническое разложение** числа a на простые множители:

$$a = p_1^{k_1} p_2^{k_2} p_3^{k_3} ... p_s^{k_s}.$$

$$30 = 2 \cdot 3 \cdot 5, 64 = 2^6, 300 = 2^2 \cdot 3 \cdot 5^2, 105 = 3 \cdot 5 \cdot 7.$$

С учетом $(p_1, p_2) = 1$ важное свойство $(ap_1, ap_2) = a(p_1, p_2) = a$, позволяет быстро находить НОД небольших чисел легко раскладывающихся на простые множители:

$$(30,20)=(2\cdot 3\cdot 5,2^2\cdot 5)=2\cdot 5\cdot(3,2)=2\cdot 5=10.$$
$$(4,6)=(2\cdot 2,2\cdot 3)=2\cdot(2,3)=2.$$
$$(6,15)=(3\cdot 2,3\cdot 5)=3\cdot(2,5)=3.$$
$$(35,77)=(5\cdot 7,7\cdot 11)=7\cdot(5,11)=7.$$

Однако, если факторизовать число сложно, то используют **алгоритм Евклида** для нахождения наибольшего общего делителя:

$$\begin{aligned}
&a = b\,q_1 + r_1, && 0 \le r_1 < b,\\
&b = r_1 q_2 + r_2, && 0 \le r_2 < r_1,\\
&r_1 = r_2 q_3 + r_3, && 0 \le r_3 < r_2,\\
&\ldots && \ldots\\
&r_{n-2} = r_{n-1} q_n + (r_n), && 0 \le r_n < r_{n-1},\\
&r_{n-1} = r_n q_{n+1} + 0. &&
\end{aligned}$$

Тогда, согласно лемме 2:

$$(a,b)=(b,r_1)=(r_1,r_2)=\ldots=(r_n-1,r_n)=r_n.$$

Последнее равенство выполняется в силу леммы 1.

Таким образом, НОД равен последнему отличному от нуля остатку в алгоритме Евклида.

Пример 26. Найти НОД (175, 77) с помощью алгоритма Евклида.

Решение:

$$175=77\cdot 2+21,$$
$$77=21\cdot 3+14,$$
$$21=14\cdot 1+(7),$$
$$14=7\cdot 2+0.$$

Последний положительный остаток $r_3=7$. Значит $(175,77)=7$.

Пример 27. Найти НОД (39, 15) с помощью алгоритма Евклида.

Решение:

$$39=15\cdot 2+9,$$

$$15 = 9 \cdot 1 + 6,$$
$$9 = 6 \cdot 1 + (3),$$
$$6 = (3) \cdot 2 + 0.$$

Последний положительный остаток $r_3 = 3$, значит $(39,15) = 3$.

Пример 28. Найти НОД (460, 321) с помощью алгоритма Евклида.

Решение:

$$460 = 321 \cdot 1 + 139,$$
$$321 = 139 \cdot 2 + 43,$$
$$139 = 43 \cdot 3 + 10,$$
$$43 = 10 \cdot 4 + 3,$$
$$10 = 3 \cdot 3 + (1),$$
$$3 = (1) \cdot 3 + 0.$$

Последний положительный остаток $r_5 = 1$. Значит $(460,321) = 1$.

Умножая равенство $(a,b) = b$ на натуральное $m \in \mathbb{N}$, убеждаемся в справедливости свойства $(am,bm) = (a,b)m.$

Пусть δ – делитель a и b. Тогда:

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

Отсюда получаем:

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

Пример 29. Найти НОД $\left(\frac{2}{3}, \frac{4}{5}\right)$ с помощью алгоритма Евклида.

Решение: приведем исходные дроби к общему знаменателю:

$$\left(\frac{2}{3},\frac{4}{5}\right)=\left(\frac{10}{15},\frac{12}{15}\right)=\frac{(10,12)}{15}.$$

С помощью алгоритма Евклида найдем НОД числителя:

$$10=12\cdot 0+10,$$
$$12=10\cdot 1+(2),$$
$$10=(2)\cdot 5+0.$$

Последний положительный остаток $r_2=2$. Значит $(10,12)=2$ и $\left(\frac{2}{3},\frac{4}{5}\right)=\frac{2}{15}$.

Понятие наибольшего общего делителя можно ввести и для нескольких чисел $(a_1,a_2,a_3,...,a_n)$, который вычисляется последовательно. Например:

$$(a_1,a_2,a_3)=((a_1,a_2),a_3),$$
$$(a_1,a_2,a_3,a_4)=((a_1,a_2,a_3),a_4)=(((a_1,a_2),a_3),a_4).$$

Задача. Найти НОД $\left(\frac{1}{2},\frac{1}{3}\right),\left(\frac{2}{3},\frac{3}{4}\right),\left(\frac{12}{132},\frac{13}{3}\right)$.

§ 2.3. Наименьшее общее кратное

Если $a\,|\,m$ и $b\,|\,m$, то число $m\in\mathbb{N}$ называют **общим кратным** целых чисел $a,b\in\mathbb{Z}$. **Наименьшее общее кратное** (НОК) чисел a и b принято обозначать $[a,b]$.

Теорема. Если m – общее кратное целых чисел a и b, то $[a,b]\,|\,m$.

Доказательство. Разделим с остатком m на $[a,b]$:

$$m=[a,b]q+r.$$

Ввиду того, что:

$$r=m-[a,b]q,$$
$$\text{из } a\,|\,m, a\,|\,[a,b] \text{, следует } a\,|\,r,$$
$$\text{из } b\,|\,m, b\,|\,[a,b] \text{, следует } b\,|\,r.$$

Поскольку $0\le r<[a,b]$, то это возможно лишь при $r=0$.

Теорема. Справедливо соотношение:

$$[a,b]=\frac{ab}{(a,b)}.$$

Доказательство. Пусть сначала $(a,b)=1$. Тогда:

$$\text{из} \begin{vmatrix} a\,|\,c \\ b\,|\,c \\ (a,b)=1 \end{vmatrix} \text{ следует } ab\,|\,c\,.$$

Получим:

$$\begin{vmatrix} a\,|\,[a,b], \\ b\,|\,[a,b] \end{vmatrix} \Rightarrow ab\,|\,[a,b] \Rightarrow [a,b]=ab.$$

Пусть теперь $(a,b)=d\neq 1$. Тогда:

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

Следовательно,

$$\left[\frac{a}{d},\frac{b}{d}\right]=\frac{ab}{d^2}.$$

Выносим множитель $\frac{1}{d}$:

$$\left[\frac{a}{d},\frac{b}{d}\right]=\frac{[a,b]}{d}=\frac{ab}{d^2},$$

и получаем:

$$[a,b]=\frac{ab}{d}=\frac{ab}{(a,b)}.$$

Понятие наименьшего общего кратного можно ввести и для нескольких чисел $[a_1, a_2, a_3 \ldots a_n]$, который вычисляется последовательно. Например,

$$[a_1,a_2,a_3]=[[a_1,a_2],a_3],$$

$$[a_1,a_2,a_3,a_4]=[[a_1,a_2,a_3],a_4]=[[[a_1,a_2],a_3],a_4].$$

С учетом $[p_1,p_2]=p_1\cdot p_2$ важное свойство

$$[ap_1, ap_2] = a[p_1, p_2] = a \cdot p_1 \cdot p_2$$

позволяет быстро находить НОК небольших чисел, легко раскладывающихся на простые множители.

$$[30,20] = [2 \cdot 3 \cdot 5, 2^2 \cdot 5] = 2 \cdot 5 \cdot [3,2] = 10 \cdot [3,2] = 10 \cdot 6 = 60.$$

$$[4,6] = [2 \cdot 2, 2 \cdot 3] = 2 \cdot [2,3] = 2 \cdot 6 = 12.$$

$$[6,15] = [3 \cdot 2, 3 \cdot 5] = 3 \cdot [2,5] = 3 \cdot 10 = 30.$$

$$[35,77] = [5 \cdot 7, 7 \cdot 11] = 7 \cdot [5,11] = 7 \cdot 55 = 385.$$

Однако, если факторизовать число сложно, то для нахождения НОК используют формулу:

$$[a,b] = \frac{ab}{(a,b)},$$

где НОД находят с помощью алгоритма Евклида.

Пример 30. Найти НОК [24, 60] с помощью алгоритма Евклида.

Решение. Найдем НОД:

$$24 = 60 \cdot 0 + 24,$$
$$60 = 24 \cdot 2 + (12),$$
$$24 = (12) \cdot 2 + 0.$$

Последний положительный остаток $r_2 = 12$. Значит НОД $[24,60) = 12$. Поэтому НОК:

$$[a,b] = \frac{ab}{(a,b)} \text{ или } [24,60] = \frac{24 \cdot 60}{(24,60)} = \frac{24 \cdot 60}{12} = 120.$$

§ 2.4. Разложение Безу

Если $(a,b) = 1$, то числа a и b называются **взаимно простыми**.

Теорема. Критерий взаимной простоты Безу. Два целых a и b будут **взаимно простыми** тогда и только тогда, когда найдутся целые x и y такие, что $ax + by = 1$.

Доказательство. Докажем условие достаточности:

$$\begin{vmatrix}(a,b)\mid a\\(a,b)\mid b\end{vmatrix} \Rightarrow (a,b)\mid ax+by=1 \Rightarrow (a,b)=1.$$

Свойства НОД, вытекающие из критерия Безу:

$$\begin{vmatrix}(a,b)=1\\(a,c)=1\end{vmatrix} \Rightarrow (a,bc)=1;$$

$$\begin{vmatrix}a\mid bc\\(a,c)=1\end{vmatrix} \Rightarrow a\mid b; \qquad \begin{vmatrix}a\mid c\\b\mid c\\(a,b)=1\end{vmatrix} \Rightarrow ab\mid c.$$

Опишем итерационную процедуру алгоритма, позволяющую параллельно алгоритму Евклида вычислять числа x, y:

$a = b\,q_1 + r_1$	$1 - 0\ \cdot q_1 = x_1$	$0 - 1 \cdot q_1 = y_1$
$b = r_1 q_2 + r_2$	$0 - x_1 q_2 = x_2$	$1 - y_1 q_2 = y_2$
$r_1 = r_2 q_3 + r_3$	$x_1 - x_2 q_3 = x_3$	$y_1 - y_2 q_3 = y_3$
$r_2 = r_3 q_4 + r_4$	$x_2 - x_3 q_4 = x_4$	$y_2 - y_3 q_4 = y_4$
...	...	...
$r_{n-2} = r_{n-1} q_n + r_n$	$x_{n-2} - x_{n-1} q_n = x_n$	$y_{n-2} - y_{n-1} q_n = y_n$
$r_{n-1} = r_n q_{n+1} + 0$		

тогда $r_n = a \cdot x_n + b \cdot y_n$.

Пример 31. Найти НОД (443,328) и коэффициенты Безу с помощью алгоритма Евклида.

Решение:

443 = 328·1 + 115	1 – 0·1 = 1	0 – 1·1 = –1
328 = 115·2 + 98	0 – 1·2 = –2	1 – (–1)·2 = 3
115 = 98·1 + 17	1 – (–1) ·1 = 3	–1 – 3·1 = –4
98 = 17·5 + 13	–2 – 3·5 = –17	3 – (–4)·5 = 23
17 = 13·1 + 4	2 – (–17) ·1 = 20	–3 – 23·1 = –27
13 = 4·3 + 1	–17 – 20·3 = –77	23 – (–27)·3 = 104
4 = 1·4 + 0		

Последний положительный остаток $r_6 = 1$, коэффициенты Безу $x = -77, y = 104$. Значит (443, 328) = 1 и (443, 328) = 443 (–77) + 328 · 104 или $328 \cdot 104 - 443 \cdot 77 = 1$.

§ 2.5. Классы вычетов

Пусть Z – кольцо целых чисел. Будем рассматривать остатки от деления произвольного $a \in \mathsf{Z}$ на натуральное число n, называемое **модулем**. В математических пакетах остаток от деления a на n вычисляется с помощью функции Mod (a,n):

Mod(14,9) = 5; Mod(26,13) = 0; Mod(215,11) = 6.

Если два целых a и b имеют одинаковые остатки при делении на n, то они называются **сравнимыми по модулю** n. В таком случае сравнимость по модулю чисел a и b записывают в виде $a \equiv b \,(\mathrm{mod}\, n)$ или $a \equiv b \,(\mathsf{Z}_n)$.

$$14 \equiv 5 \,(\mathrm{mod}\, 9); \quad 26 \equiv 0 \,(\mathrm{mod}\, 13); \quad 215 \equiv 6 \,(\mathsf{Z}_{11}).$$

Отношение сравнимости по модулю m обладает свойствами рефлексивности, симметричности и транзитивности, т. е. является отношением эквивалентности.

Свойства сравнений.

1. $a \equiv b \,(\mathrm{mod}\, m) \Leftrightarrow m \mid (a - b)$;

2. $a \equiv b \,(\mathrm{mod}\, m),\ b \equiv c \,(\mathrm{mod}\, m) \Rightarrow a \equiv c \,(\mathrm{mod}\, m)$;

Действительно,

$m \mid (b - c) \Rightarrow m \mid ((a - b) + (b - c)) \Rightarrow m \mid (a - c) + m \mid (a - b)$.

3. Сравнения можно почленно складывать.

Пусть:

$$a_1 = b_1 \,(\mathrm{mod}\, m),$$
$$a_2 = b_2 \,(\mathrm{mod}\, m).$$

Тогда:

$$m \mid (a_1 - b_1),$$
$$m \mid (a_2 - b_2).$$

В силу свойства:

$$\begin{vmatrix} a \mid b \\ a \mid c \end{vmatrix} \Rightarrow a \mid b \pm c,$$

получим $m \mid (a_1 - b_1 + a_2 - b_2)$, т. е. $m \mid ((a_1 + a_2) - (b_1 + b_2))$.

4. Сравнения можно почленно перемножать.

Пусть:

$$a_1 = mq_1 + r_1, \quad a_2 = mq_3 + r_2,$$
$$b_1 = mq_2 + r_1, \quad b_2 = mq_4 + r_2.$$

Тогда:

$$a_1 a_2 = m(mq_1 q_3 + q_1 r_2 + q_3 r_1) + r_1 r_2,$$
$$b_1 b_2 = m(mq_2 q_4 + q_2 r_2 + q_4 r_1) + r_1 r_2.$$

Следовательно:

$$a_1 a_2 = r_1 r_2 \pmod{m},$$
$$b_1 b_2 = r_1 r_2 \pmod{m}.$$

5. К обеим частям сравнения можно прибавить одно и то же число, кратное модулю $a \equiv b \pmod{m} \Rightarrow a \equiv b + mk \pmod{m}$.

6. Обе части сравнения можно умножать на одно и то же число: $a \equiv b \pmod{m} \Rightarrow ak \equiv bk \pmod{m}$.

7. Обе части сравнения можно возводить в любую положительную степень: $a \equiv b \pmod{m} \Rightarrow a^k \equiv b^k \pmod{m}$.

8. Если $f(x)$ – произвольная аддитивная или мультипликативная функция, то:

$$a \equiv b \pmod{m} \Rightarrow f(a) \equiv f(b) \pmod{m}.$$

9. Обе части сравнения можно разделить на их общий делитель, если он взаимно прост с модулем.

Пусть: $a_1 d \equiv b_1 d \pmod{m}$.

Тогда: $m \mid d(a_1 - b_1)$.

В силу свойства:

$$\begin{vmatrix} a \mid bc \\ (a,b)=1 \end{vmatrix} \Rightarrow a \mid c,$$

получим $m \mid (a_1 - b_1)$, поскольку $(m,d)=1$.

10. Обе части сравнения и модуль можно сокращать на их общий делитель.

$$ad \equiv bd \pmod{md} \quad \Rightarrow \quad a \equiv b \pmod{m}.$$

11.

$$\begin{vmatrix} a \equiv b \pmod{m_1} \\ a \equiv b \pmod{m_2} \end{vmatrix} \Rightarrow a \equiv b \pmod{[m_1, m_2]}.$$

12.

$$\begin{vmatrix} a \equiv b \pmod{m} \\ d \mid b \\ d \mid m \end{vmatrix} \Rightarrow d \mid a.$$

Действительно,

$$m \mid (a-b) \quad \Rightarrow \quad d \mid (a-b) \quad \Rightarrow \quad d \mid (a-b+b) \quad \Rightarrow \quad d \mid a \ .$$

13. $a \equiv b \pmod{m} \quad \Rightarrow \quad (a,m) = (b,m).$

Ввиду $a = mq + b$, непосредственно следует из свойства:

$$a = bq + c \quad \Rightarrow \quad (a,b) = (b,c).$$

Бинарное отношение сравнимости $a \equiv b \pmod{m}$ индуцирует разбиение множества $\mathbb{Z}$ целых чисел на классы эквивалентности $\bar{a}$, которые называют классами вычетов по модулю m, так числа, сравнимые по модулю m, образуют класс вычетов по модулю m. Все числа из одного класса имеют один и тот же остаток r от деления на m. Всего имеется m классов вычетов по модулю m: $\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{m-1}$.

По модулю 10 все числа класса, дающие остаток 3, имеют вид $10 \cdot q + 1$ и представляются рядом чисел:

$$\ldots -27, -17, -7, 3, 13, 23, \ldots$$

Сложение и умножение классов

Если из двух классов C_k и C_l выбрать по вычету и сложить их или перемножить, то всегда получим вычеты вполне определенных классов.

Действительно, пусть выбранные представители имеют вид

$$C_k : mq_1 + k, \qquad C_l : mq_2 + l.$$

Тогда при сложении имеем $C_k + C_l : mq + k + l$, где $q = q_1 + q_2$.

Если $k + l < m$, то полученное число принадлежит классу C_{k+l}.

Если $k + l > m$, то полученное число принадлежит классу C_{k+l-m}.

Свойства классов вычетов

1. $a \equiv b \pmod m \quad \Leftrightarrow \quad \bar{a} = \bar{b}$;

2. $a \neq b \pmod m \quad \Leftrightarrow \quad \bar{a} \cap \bar{b} = \varnothing$.

Взяв из каждого класса по одному вычету, получим полную систему вычетов. Например, наряду с 0, 1, 2, …, *m – 1*. полной системой вычетов будет 1, 2, …, *m*.

3. Любые m чисел, попарно несравнимые по модулю m, образуют полную систему вычетов.

4. Если $(a, m) = 1$ и x пробегает полную систему вычетов по модулю m, то $ax + b$, где b – любое целое, также пробегает полную систему вычетов по модулю m.

Допустим $ax_1 + b \equiv ax_2 + b \pmod m$, получим:

$$ax_1 \equiv ax_2 \pmod m, \qquad \Rightarrow \qquad x_1 \equiv x_2 \pmod m.$$

По модулю 10 два любых вычета соответственно из классов C_3 и C_4 в сумме всегда дают вычет из класса C_7, а в качестве произведения – вычет из класса C_2.

Числа одного класса вычетов имеют с модулем m один и тот же общий делитель. Рассмотрим те классы, для которых этот делитель равен единице. Взяв от каждого такого класса по одному вычету, получим приведенную систему вычетов.

5. Если $(a,m)=1$ и x пробегает приведенную систему вычетов по модулю m, то ax также будет пробегать приведенную систему вычетов по модулю m.

Достаточно показать, что числа ax попарно несравнимы и взаимно просты с модулем m. Второе следует из $(m,a)=1, (m,x)=1$.

§ 2.6. Функция Эйлера

Функция Эйлера $\varphi(n)$ – определяет количество классов вычетов в приведенной системе вычетов. Она определена для всех натуральных чисел $n \in \mathbb{N}$ и представляет собой количество чисел ряда 1, 2, 3, …, n, взаимно простых с n.

$$\varphi(1)=1, \varphi(2)=1, \varphi(3)=2,$$
$$\varphi(4)=2, \varphi(5)=4, \varphi(6)=2,$$
$$\varphi(7)=6, \varphi(8)=4, \varphi(9)=6.$$

Свойства функции Эйлера $\varphi(p)$ для простых p.

1. $\varphi(p) = p-1$.
2. $\varphi(p^k) = p^{k-1}(p-1)$.
3. $\varphi(p_1 p_2) = \varphi(p_1)\varphi(p_2)$.

При $k=1$ имеем свойство 1. При $k \neq 1$ в ряду $i = 1, 2, 3, \ldots, p^k$, условие $(i, p^k)=1$ нарушается лишь для каждого p-го члена. Всего таких членов $\dfrac{p^k}{p} = p^{k-1}$.

Лемма. Мультипликативность функции Эйлера.

$$(a,b)=1 \quad \Rightarrow \quad \varphi(ab)=\varphi(a)\varphi(b).$$

Поместим числа 1,2, 3, … , *ab* в таблицу:

1	2	3	...	b
b+1	*b+2*	*b+3*	...	*2b*
2b+1	*2b+2*	*2b+3*	...	*3b*
...	...	...	...	...
(a-1)b+1	*(a-1)b+2*	*(a-1)b+3*	...	*ab*

Числа, взаимно простые с b, могут быть лишь в столбцах, номера которых взаимно простые с b. Все числа такого столбца взаимно простые с b. Таких столбцов всего $\varphi(b)$. По свойству четырех классов вычетов любой такой столбец представляет полную систему вычетов по модулю a. Поэтому он содержит $\varphi(a)$ чисел, взаимно простых с a. Воспользуемся тем, что

$$(i,ab)=1 \qquad \Rightarrow \qquad (i,a)=(i,b)=1.$$

Поэтому:

$$\varphi(ab)=\varphi(a)\varphi(b).$$

Используя лемму и каноническое разложение числа на простые множители $a=p_1^{k_1}p_2^{k_2}p_3^{k_3}\ldots p_s^{k_s}$, имеем

$$\varphi(a)=\left(p_1^{k_1}-p_1^{k_1-1}\right)\left(p_2^{k_2}-p_2^{k_2-1}\right)\ldots\left(p_s^{k_s}-p_s^{k_s-1}\right)$$

$$\text{или } \varphi(a)=p_1^{k_1}p_2^{k_2}p_3^{k_3}\ldots p_s^{k_s}\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\left(1-\frac{1}{p_s}\right),$$

$$\varphi(a)=a\prod_{p|a}\left(1-\frac{1}{p}\right).$$

В математическом пакете Mathcad разложение чисел осуществляется с помощью оператора «+ factor→».

$$123\,\text{factor}\rightarrow 3\cdot 41,$$

$$11001\,\text{factor}\rightarrow 11\cdot 73\cdot 137,$$

$$16200\,\text{factor}\rightarrow 2^3\cdot 3^4\cdot 5^2.$$

Мультипликативность функции Эйлера постоянно используется при вычислениях:

$\varphi(105)=\varphi(3\cdot5\cdot7)=\varphi(3)\varphi(5)\varphi(7)=2\cdot4\cdot6=48;$

$\varphi(512)=\varphi(2^9)=2^8(2-1)=256;$

$\varphi(840)=\varphi(2^3\cdot3\cdot5\cdot7)=\varphi(2^3)\varphi(3)\varphi(5)\varphi(7)=192;$

$\varphi(360)=\varphi(2^3\cdot3^2\cdot5)=\varphi(2^3)\varphi(3^2)\varphi(5)=2^2(2-1)3(3-1)(5-1)=96.$

Малая теорема Ферма. (1636 г.) Если p – простое, то для любого x:

$$x^{p-1}\equiv1\,(\mathsf{Z}_p).$$

Доказательство. Это выражение непосредственно проверяется для x = 0, 1, 2, 3. Перепишем равенство в виде:

$$x^p-x\equiv0\,(\mathrm{mod}\,p).$$

По индукции получим:

$$x^p-x=(x-1+1)^p-x=(x-1)^p+\sum_{i=1}^{p-1}C_p^i(x-1)^i+1-x$$

$$=(x-1)^p-(x-1)=(x-2)^p-(x-2)=\ldots=(x-k)^p-(x-k).$$

$$\text{Т. е. } (x-k)^p\equiv(x-k)\,(\mathrm{mod}\,p).$$

Здесь мы учли, что $C_p^i\equiv0\,(\mathsf{Z}_p)$.

Можно дать еще одно (прямое доказательство):

При $(x,p)=1$ имеем $x^{p-1}\equiv1\,(\mathrm{mod}\,p)$.

При $(x,p)\neq1$ имеем $x\equiv0\,(\mathrm{mod}\,p)$.

Перемножая два сравнения, получим $x^p\equiv x\,(\mathrm{mod}\,p)$.

Теорема. Эйлера. Если n – составное, то для любого x, взаимно простого с n:

$$x^{\varphi(n)}\equiv1\,(\mathrm{mod}\,n).$$

Пример 32. Пусть $p=11,\ x=8$, тогда:

$$8\equiv(-3)\,(\mathrm{mod}11),$$

$$8^{10}\equiv(-3)^{10}\,(\mathrm{mod}11).$$

Но $(-3)^{10}=3^{10}=(3^2)^5=9^5\equiv(-2)^5=-32\equiv1$ и $8^{10}\equiv1\,(\mathrm{mod}11)$.

Пример 33. Пусть $p=9$, $x=14$, тогда:

$$\varphi(9)=\varphi(3^2)=3\cdot(3-1)=6,$$
$$14\equiv 5\,(\mathrm{mod}9),$$
$$14^{\varphi(9)}\equiv 5^{\varphi(9)}\,(\mathrm{mod}9),$$
$$14^6\equiv 5^6\,(\mathrm{mod}9).$$

Из $(5)^6=(5^3)^2=125^2\equiv(-1)^2=1$ следует $14^6\equiv 1(\mathrm{mod}9)$.

Теоремы Эйлера и Ферма имеют многочисленные применения. Рассмотрим примеры вычисления остатков при делении степеней на данное число.

Пример 34. Найти остаток при делении 2^{26} на 13.

Решение. По теореме Ферма $2^{12}\equiv 1(\mathrm{mod}13)$, тогда:

$$2^{26}=2^{12+12+2}=2^{12}\cdot 2^{12}\cdot 2^2=1\cdot 1\cdot 2^2=2^2\equiv 4\,(\mathrm{mod}13).$$

Искомый остаток равен 4.

Пример 35. Найти остаток при делении 3^{443} на 56.

Решение. Учитывая, что $56=8\cdot 7=2^3\cdot 7$ найдем функцию Эйлера $\varphi(56)=\varphi(2^3)\cdot\varphi(7)=2^2\cdot\varphi(2)\cdot\varphi(7)=2^2\cdot 1\cdot 6=24$.

По теореме Эйлера $3^{\varphi(56)}\equiv 1(\mathrm{mod}56)$ или $3^{24}\equiv 1(\mathrm{mod}56)$, тогда $3^{443}=3^{24\cdot 18+11}=(3^{24})^{18}\cdot 3^{11}=1^{18}\cdot 3^{11}=3^{11}\equiv 19(\mathrm{mod}56)$.

Искомый остаток равен 19.

Пример 36. Найти остаток при делении 317^{259} на 15.

Решение. Учитывая, что:

$317\equiv 2\,(\mathrm{mod}15)$, имеем $317^{259}\equiv 2^{259}\,(\mathrm{mod}15)$,

и по теореме Эйлера $2^{\varphi(15)}\equiv 1(\mathrm{mod}15)$, где:

$$\varphi(15)=\varphi(3\cdot 5)=\varphi(3)\cdot\varphi(5)=(3-1)\cdot(5-1)=8,$$

получим $2^8\equiv 1(\mathrm{mod}15)$.

Но тогда $2^{259}=2^{8\cdot 32+3}=2^{8\cdot 32}2^3=2^3=8\,(\mathrm{mod}15)$.

Искомый остаток равен 8.

Контрольная задача. Найти: $\frac{1}{3}\pmod 7, \frac{1}{21}\pmod{26}$.

Практическое занятие

Модулярная арифметика

Задача 1. Найти НОД(a,b)

№	a	b	№	a	b	№	a	b
1.	165	14	**11.**	396	385	**21.**	2688	1155
2.	140	66	**12.**	660	84	**22.**	396	770
3.	105	22	**13.**	1820	1287	**23.**	3220	2277
4.	756	220	**14.**	2310	896	**24**	1320	168
5.	210	55	**15.**	210	165	**25.**	525	550
6.	660	42	**16.**	3024	880	**26.**	1820	2574
7.	1155	896	**17.**	1683	2380	**27.**	945	594
8.	1512	440	**18.**	630	198	**28.**	2772	140
9.	3465	1152	**19.**	2660	1881	**29.**	4060	1827
10.	210	110	**20.**	1100	420	**30.**	210	330

Задача 2. Найти НОД(a,b) и коэффициенты Безу (X,Y) разложения $aX+bY=1$.

	a	b	№	a	b	№	a	b
1.	1257	374	**11.**	435	302	**21.**	697	486
2.	1825	543	**12.**	592	411	**22.**	991	691
3.	2393	712	**13.**	749	520	**23.**	1285	896
4.	2961	881	**14.**	906	629	**24.**	1579	1101
5.	3529	1050	**15.**	1063	738	**25.**	1873	1306
6.	4097	1219	**16.**	1220	847	**26.**	2167	1511
7.	4665	1388	**17.**	1377	956	**27.**	2461	1716
8.	5233	1557	**18.**	1534	1065	**28.**	2755	1921
9.	5801	1726	**19.**	1691	1174	**29.**	3049	2126
10.	4255	1266	**20.**	1161	806	**30.**	1133	790

Задача 3. Найти остаток от деления $\frac{11^A}{B}$, используя малую теорему Ферма:

№	A	B	№	A	B	№	A	B
1.	96	7	**11.**	97	13	**21.**	70	13
2.	91	13	**12.**	54	13	**22.**	61	19
3.	88	13	**13.**	76	17	**23.**	66	13
4.	94	7	**14.**	79	17	**24.**	67	13
5.	87	13	**15.**	74	17	**25.**	71	17
6.	73	17	**16.**	95	13	**26.**	74	17
7.	89	13	**17.**	57	23	**27.**	72	17
8.	93	13	**18.**	65	13	**28.**	73	17
9.	78	17	**19.**	53	23	**29.**	59	19
10.	94	13	**20.**	68	13	**30.**	69	13

Задача 4. Найти остаток от деления $\frac{A^B}{C}$ методом Эйлера:

№	A	B	C	№	A	B	C	№	A	B	C
1.	13	52	15	**11.**	11	73	32	**21.**	5	85	32
2.	5	65	27	**12.**	17	89	35	**22.**	23	75	35
3.	11	71	32	**13.**	13	53	15	**23.**	7	75	32
4.	13	50	15	**14.**	7	74	35	**24.**	17	83	33
5.	13	71	32	**15.**	19	76	33	**25.**	13	70	32
6.	17	77	33	**16.**	19	88	21	**26.**	5	63	27
7.	13	55	15	**17.**	13	71	20	**27.**	11	69	32
8.	5	87	27	**18.**	17	81	33	**28.**	7	75	35
9.	7	70	20	**19.**	7	66	20	**29.**	13	61	32
10.	19	89	21	**20.**	17	81	21	**30.**	11	73	35

§ 2.7. Китайская теорема об остатках

2.7.1. Сравнения первой степени

Решения сравнений методом подбора

Рассмотрим сравнение $ax \equiv b \pmod{m}$, при условии $(a, m) = 1$. Решением любого сравнения называется класс вычетов по модулю m, один элемент которого (а значит, и все) удовлетворяет сравнению. В нашем случае найдутся целые u, v такие, что $au + mv = 1$.

Следовательно, сравнение имеет единственное решение по модулю m.

Пусть $(a, m) = d > 1$. По 10-му свойству сравнений условие $d \mid b$ является необходимым условием разрешимости сравнения $ax \equiv b \pmod{m}$. Будем считать его выполненным. Пусть

$$a = a_1 d, \quad b = b_1 d, \quad m = m_1 d.$$

Тогда наше сравнение равносильно $a_1 x \equiv b_1 \pmod{m_1}$.

Имеем одно решение $x \equiv x_1 \pmod{m_1}$. По модулю m имеем d решений: $x_1, x_1 + m_1, x_1 + 2m_1, \ldots, x_1 + (d-1)m_1$.

Теорема. Пусть $(a, m) = d$. Сравнение $ax \equiv b \pmod{m}$ разрешимо тогда и только тогда, когда $d \mid b$. В этом случае оно имеет d решений.

При небольшом m сравнение $ax \equiv b \pmod{m}$ решается методом подбора. Для этого достаточно найти число u, такое, что $au \equiv 1 \pmod{m}$; это можно сделать с помощью алгоритма Евклида. В качестве u можно взять $u = a^{\varphi(m)-1}$.

Еще раз напомним основные правила при решении сравнений типа $ax \equiv b \pmod{p}$:

1) если $(a, p) = 1$ – взаимно простые, то решение существует и единственно;

2) если $(a, p) = d > 1$, то при $d \mid b$ – существует d решений; при $d \nmid b$ – решений нет.

Решение сравнения надо начинать с определения $d=(a,b)$ и проверки $d \mid b$.

Решения сравнений методом Эйлера

Если $(a, p)=1$, то $a^{\varphi(p)} \equiv 1 \pmod{p}$ откуда $a^{\varphi(p)} b \equiv b \pmod{p}$.

При сопоставлении этого сравнения с $ax \equiv b \pmod{p}$ видим, что $x \equiv a^{\varphi(p)-1} b \pmod{p}$ является его решением. Несмотря на то что данное выражение является явным решением, задачу можно считать эффективно решенной лишь тогда, когда для $a^{\varphi(p)-1} b$ будет найден наименьший неотрицательный или абсолютно наименьший вычет по модулю p.

Решения сравнений с использованием коэффициентов Безу

Если $(a,m)=1$, то по теореме Безу существуют такие целые X и Y, что $aX+mY=1$.

По модулю m это выражение дает $aX \equiv 1 \pmod{m}$.

Для решения сравнения $ax \equiv b \pmod{m}$ умножим его на X:

$$ax \equiv b \pmod{m} \quad \times X,$$
$$aXx \equiv bX \pmod{m},$$
$$x \equiv bX \pmod{m}.$$

Напомним, что кольцо Z_n имеет $\varphi(n)$ обратимых элементов, а из них только $\varphi(\varphi(n))$ генераторов.

Пример 37. Решить сравнение $3x \equiv 7 \pmod{11}$.

Решение 1. Поскольку $(3,11)=1$ – взаимно простые, то, пользуясь формулой Эйлера $x \equiv a^{\varphi(p)-1} b \pmod{p}$, найдем $\varphi(p)=\varphi(11)=11-1=10$ и $x \equiv a^{10-1} b \pmod{11}$,

$$\equiv 3^9 \cdot 7 \equiv (3^3)^3 \cdot 7 \equiv 27^3 \cdot 7 \equiv 5^3 \cdot 7 \equiv 125 \cdot 7 \equiv 4 \cdot 7 \equiv 28 \equiv 6 \pmod{11}.$$

Решение 2. Поскольку (3, 11) = 1 – взаимно простые, то, пользуясь расширенным алгоритмом Евклида, получим коэффициенты Безу: $a \cdot X + m \cdot Y = 1$,

$$3 \cdot X + 11 \cdot Y = 1.$$

	X	Y
$3 = 11 \cdot 0 + 3;$	$1 - 0 \cdot 0 = 1;$	$0 - 1 \cdot 0 = 0;$
$11 = 3 \cdot 3 + 2;$	$0 - 1 \cdot 3 = -3;$	$1 - 0 \cdot 3 = 1;$
$3 = 2 \cdot 1 + 1;$	$1 - (-3) \cdot 1 = 4.$	$0 - 1 \cdot 1 = 1.$
$2 = 1 \cdot 2 + 0;$		

т. е. $X = 4$, $Y = -1$ и $3 \cdot 4 - 11 \cdot 2 = 1$.

Тогда решение сравнения дается формулой:

$$x \equiv Xb \pmod{11} \equiv 4 \cdot 7 \equiv 28 \equiv 6 \pmod{11}.$$

Пример 38. Решить сравнение $17x \equiv 25 \pmod{28}$.

Решение 1. Поскольку $(17,28)=1$ – взаимно простые, то, пользуясь формулой Эйлера $x \equiv a^{\varphi(p)-1} b \pmod{p}$, найдем

$$\varphi(p) = \varphi(28) = \varphi(2^2 \cdot 7) = \varphi(2^2) \cdot \varphi(7) = 2 \cdot (2-1) \cdot (7-1) = 2 \cdot 6 = 12$$

и:

$$x \equiv a^{12-1} b \pmod{28},$$

$$x \equiv 17^{11} \cdot 25 \pmod{28}.$$

Но по модулю 28:

$$17^{11} = (17^2)^5 \cdot 17 = 9^5 \cdot 17 = (9^2)^2 \cdot 9 \cdot 17$$

$$= (-3)^2 \cdot 9 \cdot 17 = 81 \cdot 17 = (-3) \cdot 17 = -51 = 5 \pmod{28}.$$

Таким образом $x \equiv 5 \cdot 25 = 125 \equiv 13 \pmod{28}$.

Решение 2. Поскольку (17, 28) = 1 – взаимно простые, то, пользуясь расширенным алгоритмом Евклида, получим коэффициенты Безу:

$$a \cdot X + m \cdot Y = 1,$$

$$17 \cdot X + 28 \cdot Y = 1.$$

	X	Y
$17 = 28 \cdot 0 + 17;$	$1 - 0 \cdot 0 = 1;$	$0 - 1 \cdot 0 = 0;$
$28 = 17 \cdot 1 + 11;$	$0 - 1 \cdot 1 = -1;$	$1 - 0 \cdot 1 = 1;$
$17 = 11 \cdot 1 + 6;$	$1 - (-1) \cdot 1 = 2;$	$0 - 1 \cdot 1 = -1;$
$11 = 6 \cdot 1 + 5;$	$-1 - 2 \cdot 1 = -3;$	$1 - (-1) \cdot 1 = 2;$
$6 = 5 \cdot 1 + 1;$	$2 - (-3) \cdot 1 = 5;$	$-1 - 1 \cdot 1 = -3.$
$5 = 1 \cdot 5 + 0;$		

т. е. $X = 5$, $Y = -3$ и $17 \cdot 5 - 28 \cdot 3 = 1$.

Тогда решение сравнения дается формулой:

$$x \equiv Xb \,(\mathrm{mod}\, 28) = 5 \cdot 25 \equiv 5 \cdot (-3) \equiv -15 \equiv 13 \,(\mathrm{mod}\, 28).$$

2.7.2. Уравнения первой степени с двумя неизвестными

Пусть требуется решить неопределенное уравнение:

$$ax + by = c, \qquad (a,b) = 1.$$

Это уравнение можно переписать в следующем виде:

$$ax = c - by;$$

но так как y должно быть целым числом, то:

$$ax \equiv c \,(\mathrm{mod}\, b).$$

Решая это сравнение, получаем:

$$x \equiv x_1 \,(\mathrm{mod}\, b) \text{ или } x = x_1 + bt.$$

Для определения соответствующих значений y имеем уравнение:

$$a(x_1 + bt) + by = c,$$

откуда $by = c - ax_1 - abt, \quad y = \dfrac{c - ax_1}{b} - at.$

Следовательно, $y_1 = \dfrac{c - ax_1}{b}$ должно быть целым числом, при этом оно является частным значением неизвестного y, соответствующим x_1. Поэтому общее решение исходного уравнения примет вид:

$$\begin{cases} x = x_1 + bt, \\ y = y_1 - at. \end{cases}$$

Пример 39. Решить уравнение $53x + 17y = 25$.

Решение. Перепишем уравнение в виде:

$$53x = 25 - 17y.$$

Поскольку y должно быть целым, получим сравнение:

$$53x \equiv 25 \,(\mathrm{mod}\, 17).$$

Решая его методом Эйлера:

$$x \equiv 25 \cdot 53^{\varphi(17)-1} \pmod{17},$$

$$\equiv 25 \cdot 53^{15} \equiv 8 \cdot 2^{15} \equiv 8 \cdot 32^3 \equiv 8 \cdot (-2)^3 \equiv -64 \equiv 4 \pmod{17},$$

получим $x = 4 + 17t$.

Подставляя x в исходное уравнение:

$$53x + 17y = 25,$$

$$53 \cdot (4 + 17t) + 17y = 25$$

и выражая y, получим решение:

$$\begin{cases} x = 4 + 17t, \\ y = -11 - 53t. \end{cases}$$

2.7.3. Системы сравнений первой степени

Система сравнений:

$$\begin{cases} a_1 x \equiv b_1 \pmod{m_1}; \\ a_2 x \equiv b_2 \pmod{m_2}; \\ \quad\vdots \\ a_n x \equiv b_n \pmod{m_n} \end{cases}$$

сводится к системе вида:

$$\begin{cases} x \equiv b_1 \pmod{m_1}; \\ x \equiv b_2 \pmod{m_2}; \\ \quad\vdots \\ x \equiv b_n \pmod{m_n}. \end{cases}$$

Рассмотрим способ решения простой системы:

$$\begin{cases} x \equiv b_1 \pmod{m_1}; \\ x \equiv b_2 \pmod{m_2}. \end{cases}$$

Из первого сравнения имеем $x = b_1 + m_1 t$.

Подставляя это выражение во второе сравнение, получим:

$$m_1 t \equiv (b_2 - b_1) \pmod{m_1}.$$

Мы получили критерий разрешимости системы в виде:

$$(m_1, m_2) \mid (b_2 - b_1).$$

Тогда одно решение по модулю есть:

$$\frac{m_2}{(m_1,m_2)}:t\equiv t_0\left(\mathrm{mod}\,\frac{m_2}{(m_1,m_2)}\right).$$

Поэтому:

$$x=b_1+m_1\left(t_0+\frac{m_2}{(m_1,m_2)}\,l\right)=b_0+[m_1,m_2]t.$$

Таким образом, система из двух сравнений в случае ее разрешимости имеет единственное решение по модулю $[m_1,m_2]$. Система из n сравнений в случае ее разрешимости имеет единственное решение по модулю $[m_1,m_2,m_3,\ldots,m_n]$.

В случае, когда все модули $m_1,m_2,m_3,\ldots,m_n$ попарно взаимно простые, к системе сравнений применим китайский способ. В этом случае из условий:

$$\begin{cases} m_2m_3\ldots m_nx_1\equiv 1\,(\mathrm{mod}\,m_1);\\ m_1m_3\ldots m_nx_1\equiv 1\,(\mathrm{mod}\,m_2);\\ m_1m_2\ldots m_nx_1\equiv 1\,(\mathrm{mod}\,m_3);\\ \qquad\qquad\vdots\\ m_1m_2\ldots m_{n-1}x_1\equiv 1\,(\mathrm{mod}\,m_n) \end{cases}$$

определяются числа $x_1,x_2,x_3,\ldots,x_n$. Тогда решением исходной системы сравнений будет число:

$$x=m_2m_3\ldots m_nx_1b_1+m_1m_3\ldots m_nx_2b_2+\ldots+m_1m_2\ldots m_{n-1}x_nb_n.$$

Китайская теорема об остатках

Система сравнений:

$$x_i\equiv a_i\ (\mathrm{mod}\,m_i)$$

при попарно взаимно простых модулях $(m_i,m_j)=\delta_{ij}$ имеет единственное решение по модулю произведения:

$$x\equiv\sum_i a_iM_i\overline{M_i}\ (\mathrm{mod}\,M),$$

где $M=\prod_i M_i$, $M_i=M/a_i$, $\overline{M_i}=M_i^{-1}\ (\mathrm{mod}\,m_i)$.

Пример 40. Решить систему:

$$x \equiv 5 \,(\mathrm{mod}\, 18),$$
$$x \equiv 8 \,(\mathrm{mod}\, 21).$$

Решение. Поскольку $(m_1, m_2) = (18,21) = 3$ – не являются взаимно простыми, то китайским методом решить систему не удастся. В общем случае выразим переменную из одного сравнения и подставим во второе. Из первого сравнения вытекает: $x = 5 + 18 \cdot t_1$.

Подставим это выражение во второе сравнение:

$$5 + 18 \cdot t_1 \equiv 8 \,(\mathrm{mod}\, 21),$$
$$18 \cdot t_1 \equiv 8 - 5 \,(\mathrm{mod}\, 21),$$
$$18 \cdot t_1 \equiv 3 \,(\mathrm{mod}\, 21), \text{ разделим все на 3:}$$
$$6 \cdot t_1 \equiv 1 \,(\mathrm{mod}\, 7).$$

Поскольку 6, 7 = 1 – взаимно простые, то, пользуясь формулой Эйлера $t_1 \equiv a^{\varphi(p)-1} b \,(\mathrm{mod}\, p)$, найдем $\varphi(p) = \varphi(7) = (7-1) = 6$ и $t_1 \equiv 6^{6-1} \cdot 1 \equiv 6^5 \equiv (-1)^5 \equiv -1 \,(\mathrm{mod}\, 7)$.

Таким образом, для t_1 запишем: $t_1 = -1 \pm 7 \cdot t_2$, а для x:

$$x = 5 + 18 \cdot t_1 = 5 + 18 \cdot (-1 \pm 7 \cdot t_2) = -13 \pm 18 \cdot 7 \cdot t_2 = -13 \pm 126 \cdot t_2.$$

Для минимального положительного x ответ будет $x = 113$.

Пример 41. Решить систему:

$$x \equiv 2 \,(\mathrm{mod}\, 5),$$
$$x \equiv 3 \,(\mathrm{mod}\, 7).$$

Решение. Поскольку модули $(m_1, m_2) = (5,7) = 1$ – являются взаимно простыми, то решим систему китайским методом. Здесь:

$$M = 5 \cdot 7 = (5) \cdot 7 = 5 \cdot (7) = (5) \cdot M_1 = M_2 \cdot (7)$$

тогда:

$$M = 35, \quad M_1 = 7, \quad M_2 = 5.$$

Найдем t_1, t_2 из сравнений:

$$M_1 t_1 \equiv 1 \,(\mathrm{mod}\, 5),$$
$$M_2 t_2 \equiv 1 \,(\mathrm{mod}\, 7)$$

или:

$$7t_1 \equiv 1 \pmod 5,$$
$$5t_2 \equiv 1 \pmod 7.$$

По формуле Эйлера получим:

$$t_1 \equiv 7^{\varphi(5)-1} \pmod 5,$$
$$t_2 \equiv 5^{\varphi(7)-1} \pmod 7,$$
$$t_1 \equiv 7^3 \equiv 2^3 = 8 \equiv 3 \pmod 5,$$
$$t_2 \equiv 5^5 \equiv (-2)^5 = -32 \equiv 3 \pmod 7.$$

Составляем x_0:

$$x_0 = M_1 \cdot t_1 \cdot b_1 + M_2 \cdot t_2 \cdot b_2 = 7 \cdot 3 \cdot 2 + 5 \cdot 3 \cdot 3 = 29 \cdot 3.$$

Тогда:

$$x \equiv x_0 \pmod M$$
$$x \equiv 29 \cdot 3 = 87 \equiv 17 \pmod{35}.$$

Ответ: $x = 17$.

Пример 42. Решить систему

$$x \equiv 20 \pmod{21},$$
$$x \equiv 3 \pmod 5,$$
$$x \equiv 5 \pmod 8.$$

Решение. Поскольку модули $(m_1, m_2, m_3) = (21,5,8) = 1$ – являются взаимно простыми, то решим систему китайским методом. Здесь:

$$M = 21 \cdot 5 \cdot 8 = (21) \cdot 5 \cdot 8 = 21 \cdot (5) \cdot 8 = 21 \cdot 5 \cdot (8)$$
$$= (21) \cdot M_1 = (5) \cdot M_2 = (8) \cdot M_3,$$

тогда $M = 840$, $M_1 = 40$, $M_2 = 168$, $M_3 = 105$.

Найдем t_1, t_2, t_3 из сравнений:

$$40t_1 \equiv 1 \pmod{21},$$
$$168t_2 \equiv 1 \pmod 5,$$
$$105t_3 \equiv 1 \pmod 8$$

или:

$$t_1 \equiv 10 \,(\mathrm{mod}\, 21),$$
$$t_2 \equiv 2 \,(\mathrm{mod}\, 5),$$
$$t_3 \equiv 1 \,(\mathrm{mod}\, 8).$$

Составляем x_0: $x_0 = M_1 \cdot t_1 \cdot b_1 + M_2 \cdot t_2 \cdot b_2 + M_3 \cdot t_3 \cdot b_3$
$= 40 \cdot 10 \cdot 20 + 168 \cdot 2 \cdot 3 + 105 \cdot 1 \cdot 5 = 9533.$

Тогда:

$$x \equiv x_0 \,(\mathrm{mod}\, M)$$
$$x \equiv 9533 \equiv 293 \,(\mathrm{mod}\, 840).$$

Ответ: $x = 293$.

§ 2.8. Сравнения по простому и составному модулям

2.8.1. Упрощение сравнений

Сравнения по простому модулю представляют собой наиболее простой случай сравнений. Вместе с тем это и наиболее важный случай, так как решение сравнения по составному модулю можно свести к решению сравнению по простому модулю. Рассмотрим некоторые приемы упрощений сравнений вида:

$$f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_n \equiv 0 \,(\mathrm{mod}\, p),\ a_0, (a_0, p) = 1.$$

Прежде всего необходимо попытаться заменить коэффициенты $(a_0, a_1, a_2, \ldots, a_n)$ их абсолютно наименьшими вычетами. Затем необходимо добиться того, чтобы старший коэффициент был равен 1. Действительно, поскольку $(a_0, p) = 1$, то можно всегда найти такое a, что $a \cdot a_0 \equiv 1 \,(\mathrm{mod}\, p)$.

Умножая теперь обе части сравнения на a, получим сравнение с коэффициентом $a \cdot a_0 \equiv 1$ при x^n.

Пример 43. Упростить сравнение:

$$25x^3 + 17x^2 - 13 \equiv 0 \,(\mathrm{mod}\, 11).$$

Решение. Упростим коэффициенты. Так как:

$$25 \equiv 3 \,(\mathrm{mod}\, 11)$$

$$17 \equiv -5 \,(\mathrm{mod}11),$$
$$-13 \equiv -2 \,(\mathrm{mod}11),$$

то исходное сравнение принимает вид:

$$3x^3 - 5x^2 - 2 \equiv 0 \,(\mathrm{mod}11).$$

Для упрощения старшего коэффициента решим сравнение:

$$3 \cdot a \equiv 1 \,(\mathrm{mod}11).$$

Методом Эйлера получим:

$$a \equiv 3^{\varphi(11)-1} \equiv 3^9 \equiv (9)^4 3 \equiv (-2)^4 3 \equiv 16 \cdot 3 \equiv 4 \,(\mathrm{mod}11).$$

Умножая теперь правую часть сравнения на $a = 4$

$$3x^3 - 5x^2 - 2 \equiv 0 \,(\mathrm{mod}11), \times (4)(4)$$
$$12x^3 - 20x^2 - 8 \equiv 0 \,(\mathrm{mod}11)$$

и учитывая, что:

$$12 \equiv 1 \,(\mathrm{mod}11)$$
$$-20 \equiv 2 \,(\mathrm{mod}11),$$
$$-8 \equiv 3 \,(\mathrm{mod}11),$$

окончательно получим:

$$x^3 + 2x^2 + 3 \equiv 0 \,(\mathrm{mod}11).$$

Более существенное упрощение сравнений достигается использованием следующей теоремы.

Теорема. Сравнение n-й степени по простому модулю p равносильно сравнению степени не выше $p-1$.

Доказательство 1. Разделим $f(x)$ на $(x^p - x)$. На основании теоремы деления с остатком для многочленов мы можем утверждать, что в остатке получится многочлен $R(x)$ степени не выше $p-1$. Если частное равно $Q(x)$, то имеем тождественное равенство:

$$f(x) = (x^p - x) \cdot Q(x) + R(x),$$

где все коэффициенты в $Q(x)$ и $R(x)$ – целые. Теперь сравнение:

$$f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_n \equiv 0 \,(\mathrm{mod}\, p)$$

можно представить в виде:

$$(x^p - x)\cdot Q(x) + R(x) \equiv 0 \,(\mathrm{mod}\, p).$$

Но так как:

$$(x^p - x)\cdot Q(x) \equiv 0 \,(\mathrm{mod}\, p),$$

то исходное сравнение равносильно:

$$R(x) \equiv 0 \,(\mathrm{mod}\, p).$$

Пример 44. Решить сравнение:

$$7x^5 - 11x^3 + 2x + 1 \equiv 0 \,(\mathrm{mod}\, 3).$$

Решение. Поскольку модуль сравнения $n = 3$, найдем остаток от деления:

$$f(x) = 7x^5 - 11x^3 + 2x + 1 \text{ на } (x^3 - x):$$

$$f(x) = (x^3 - x)\cdot Q(x) + R(x)$$

$$= (x^3 - x)\cdot(7x^2 - 4) + 1 - 2x$$

т. е. $R(x) = 1 - 2x$, поэтому исходное сравнение приобретает вид:

$$R(x) \equiv 0 \,(\mathrm{mod}\, p),$$

$$1 - 2x \equiv 0 \,(\mathrm{mod}\, 3),$$

$$2x \equiv 1 \,(\mathrm{mod}\, 3).$$

Решая его методом Эйлера, получим:

$$2x \equiv 1 \,(\mathrm{mod}\, 3),$$

$$x \equiv 2^{\varphi(3)-1} \equiv 2 \,(\mathrm{mod}\, 3).$$

Для практического применения этой теоремы нет необходимости делить $P_m(x) = f(x)$ на $x^p - x$, проще пользоваться приемом сведения x^m к степени x не выше $p - 1$.

Доказательство 2. Разделим m на $p - 1$ и определим остаток r в пределах от 1 до $p - 1$ [1], так что:

$$m = (p - 1)\cdot k + r.$$

[1] В отличие от обычных остатков, которые при делении на *p*–1 берутся в пределах от 0 до *p*–2, здесь вместо остатка 0 возьмем число *p*–1.

Умножая далее обе части тождественного сравнения:

$$x \equiv x^p \pmod p$$

на x^{r-1}, $x^{(p-1)\cdot k+r-1}$, …, $x^{(p-1)\cdot(k-1)+r}$,

по цепочке получим:

$$x^r \equiv x^{(p-1)\cdot 1+r} \equiv x^{(p-1)\cdot 2+r} \equiv \ldots \equiv x^{(p-1)\cdot(k-1)+r} \equiv x^{(p-1)\cdot k+r} \pmod p.$$

Заметим, что здесь нельзя брать $r = 0$, так как умножение на x^{r-1} означало бы умножение на x^{-1}. Таким образом:

$$x^m = x^{(p-1)\cdot k+r} \equiv x^r \pmod p.$$

Пример 45. Упростить сравнение:

$$f(x) = x^8 + 2x^7 + x^5 - x^4 - x + 3 \equiv 0 \pmod 5.$$

Решение 1. Поскольку модуль сравнения $n = 5$, найдем остаток от деления:

$$f(x) = x^8 + 2x^7 + x^5 - x^4 - x + 3 \quad \text{íà} \quad (x^5 - x):$$

$$f(x) = (x^5 - x)\cdot Q(x) + R(x)$$

$$= (x^5 - x)\cdot(x^3 + 2x^2 + 1) + 2x^3 + 3,$$

т. е. $R(x) = 2x^3 + 3$, поэтому исходное сравнение приобретает вид:

$$R(x) \equiv 0 \pmod p;$$

$$2x^3 + 3 \equiv 0 \pmod 5.$$

Решение 2. Заменим степени x по формулам:

$$x^m \equiv x^{(p-1)\cdot k+r} \pmod p,$$

$$x^8 \equiv x^{(5-1)\cdot 2+0} \equiv x^0 \pmod 5,$$

$$x^7 \equiv x^{(5-1)\cdot 1+3} \equiv x^3 \pmod 5,$$

$$x^5 \equiv x^{(5-1)\cdot 1+1} \equiv x^1 \pmod 5,$$

$$x^4 \equiv x^{(5-1)\cdot 1+0} \equiv x^0 \pmod 5,$$

$$x^1 \equiv x^{(5-1)\cdot 0+1} \equiv x^1 \pmod 5,$$

$$x^0 \equiv x^{(5-1)\cdot 0+0} \equiv x^0 \pmod 5.$$

Тогда для исходной функции получим:

$$f(x) = x^8 + 2x^7 + x^5 - x^4 - x + 3 \equiv 0 \,(\mathrm{mod}\, 5),$$
$$= x^0 + 2x^3 + x^1 - x^0 - x + 3 \equiv 0 \,(\mathrm{mod}\, 5),$$
$$= 1 + 2x^3 + x - 1 - x + 3 \equiv 0 \,(\mathrm{mod}\, 5),$$
$$= 2x^3 + 3 \equiv 0 \,(\mathrm{mod}\, 5).$$

2.8.2. О максимальном числе решений

Аналогично теореме Безу в алгебре доказывается следующая теорема.

Теорема. Сравнение степени n по простому модулю имеет не более n решений.

Доказательство. Пусть сравнение:

$$f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_n \equiv 0 \,(\mathrm{mod}\, p),$$

имеет решение x_1, т. е. : $f(x_1) \equiv 0 \,(\mathrm{mod}\, p)$.

Тогда по теореме Безу имеем тождество:

$$f(x) = (x - x_1) f_1(x) + f(x_1),$$

где $f_1(x)$ – многочлен с целыми коэффициентами степени $n-1$ с неизменным старшим коэффициентом a_0, а $f(x_1)$ делится на p.

По модулю p это тождество переходит в сравнение:

$$f(x) \equiv (x - x_1) f_1(x) \,(\mathrm{mod}\, p).$$

Тогда:

$$(x - x_1) f_1(x) \equiv 0 \,(\mathrm{mod}\, p).$$

Подобным же образом можно получить сравнение для второго корня x_2, третьего x_3 и т. д.:

$$f_1(x) \equiv (x - x_2) f_2(x) \,(\mathrm{mod}\, p),$$
$$f_2(x) \equiv (x - x_3) f_3(x) \,(\mathrm{mod}\, p),$$
$$a_0 (x - x_n) \equiv 0 \,(\mathrm{mod}\, p).$$

Подстановкой по обратной цепочке получаем:

$$f(x) \equiv (x - x_1)(x - x_2)\ldots(x - x_k) f_k(x) \,(\mathrm{mod}\, p),$$

где $f_k(x)) \equiv 0 \pmod{p}$ – последнее неразрешимое сравнение.

Если же $f(x) = a_0 (x - x_1) (x - x_2) \ldots (x - x_k) \pmod{p}$, то количество решений совпадает со степенью многочлена. В любом случае мы доказали, что сравнение степени n по простому модулю имеет не более n решений. Однако по составному модулю количество решений может быть больше n. Например, сравнение: $f(x) = x^2 - 5x + 6 \equiv 0 \pmod{6}$, имеет четыре решения $x \equiv 0,2,3,5 \pmod{6}$.

Теорема. Сравнение $f(x) \equiv 0 \pmod{p}$, степени $n < p$ имеет n решений тогда и только тогда, когда все коэффициенты остатка от деления $x^p - x$ на $f(x)$ кратны p.

Доказательство. Пусть при делении $x^p - x$ на $f(x)$ получилось частное $q(x)$ и остаток $r(x)$. Тогда имеем тождество

$$x^p - x = f(x) \cdot q(x) + r(x),$$

или

$$r(x) = x^p - x - f(x) \cdot q(x), \text{ причем:}$$

$q(x)$ и $r(x)$ имеют целые коэффициенты;

степень $q(x)$ равна $p - n$;

степень $r(x)$ не превосходит $n - 1$.

Пусть теперь $f(x) \equiv 0 \pmod{p}$ имеет n решений, тогда и $r(x) \equiv 0 \pmod{p}$ имеет этих же n решений, так как: $x^p - x \equiv 0 \pmod{p}$ выполняется тождественно. Но так как $r(x)$ имеет степень $\le n - 1$, то из этого следует, что все коэффициенты $r(x)$ делятся на p.

Если наоборот, все коэффициенты $r(x)$ делятся на p, то сравнение $f(x) \cdot q(x) \equiv 0 \pmod{p}$ выполняется тождественно, т. е. имеет p решений. Но любое решение этого сравнения удовлетворяет по крайней мере одному из сравнений:

$$f(x) \equiv 0 \pmod{p} \qquad q(x) \equiv 0 \pmod{p},$$

поэтому общее число решений этих двух сравнений не может быть меньше p, т. е. если число решений этих двух сравнений соответственно n_1 и n_2, то $n_1 + n_2 \geq p$. Учитывая, что $n_2 \leq p - n$, получаем $n_1 \geq n$, но так как $n_1 \leq n$, то $n_1 = n$ и теорема доказана.

Пример 46. Выяснить, имеет ли сравнение:

$$f(x) = x^3 + x - 3 \equiv 0 \,(\mathrm{mod}\, 5).$$

Три решения.

Решение. Так как $x^5 - x = (x^3 + x - 3)\cdot(x^2 - 1) + 3x^2 - 3$, то этого не может быть.

2.8.3. Приведение сравнения по составному модулю к системе

Покажем, что решение сравнения по составному модулю можно свести к решению системы сравнений по простому модулю.

Теорема. Пусть составной модуль сравнения:

$$f(x) \equiv 0 \,(\mathrm{mod}\, M),$$

представлен в виде произведения попарно простых множителей:

$$M = m_1 \cdot m_2 \cdot m_3 \cdot \ldots \cdot m_k, \quad (m_i, m_j) = 1,$$

а сравнение имеет N решений. Тогда исходное сравнение равносильно системе сравнений:

$$f(x) \equiv 0 \,(\mathrm{mod}\, m_1),$$
$$f(x) \equiv 0 \,(\mathrm{mod}\, m_2),$$
$$\ldots$$
$$f(x) \equiv 0 \,(\mathrm{mod}\, m_k)$$

с количеством решений $n_1, n_2, \ldots, n_k$ таким, что:

$$N = n_1 + n_2 + \ldots + n_k.$$

Если b_k – одно из решений k-го сравнения, тогда система сравнений:

$$x \equiv b_1 \,(\mathrm{mod}\, m_1),$$

$$x \equiv b_2 \pmod{m_2},$$
$$\ldots$$
$$x \equiv b_k \pmod{m_k}$$

имеет единственное решение:

$$x \equiv x_0 = M_1 \cdot M_{1'} b_{1'} + M_2 \cdot M_{2'} b_{2'} + \ldots + M_k \cdot M_{k'} b_{k'} \pmod{M},$$

которое является также и решением исходного сравнения по составному модулю. Здесь:

$$M_1 \cdot M_{1'} \equiv 1 \pmod{m_1},$$
$$M_2 \cdot M_{2'} \equiv 1 \pmod{m_2},$$
$$\ldots$$
$$M_k \cdot M_{k'} \equiv 1 \pmod{m_k}$$

и

$$b_1 \equiv b_{1'} \pmod{m_1},$$
$$b_2 \equiv b_{2'} \pmod{m_2},$$
$$\ldots$$
$$b_k \equiv b_{k'} \pmod{m_k}.$$

Пример 47. Решить сравнение:

$$f(x) = 3x^3 + 6x^2 + x + 10 \equiv 0 \pmod{15}.$$

Решение. Поскольку модуль $N = 15 = 3 \cdot 5$, запишем эквивалентную систему:

$$3x^3 + 6x^2 + x + 10 \equiv 0 \pmod{3},$$
$$3x^3 + 6x^2 + x + 10 \equiv 0 \pmod{5}.$$

с решениями:

$$x \equiv -1 \pmod{3}, \qquad x \equiv 0,1,20 \pmod{5}.$$

Теперь найдем решения системы:

$$x \equiv b_1 \pmod{3},$$
$$x \equiv b_2 \pmod{5}.$$

Здесь $M = 5 \cdot 3 = 3 \cdot 5$, поэтому:

$$5M_{1'} \equiv 1 \pmod{3} \quad \Rightarrow \quad 5M_{1'} \equiv -1 \pmod{3},$$
$$3M_{2'} \equiv 1 \pmod{5} \quad \Rightarrow \quad 5M_{2'} \equiv 2 \pmod{5},$$
$$x_0 = 5 \cdot (-1) b_1 + 3 \cdot 2 \cdot b_2 = -5b_1 + 6b_2.$$

Подставляя по порядку все значения корней b_k, получим:

$$x_1 = -5\cdot(-1)+6\cdot 0 \equiv 5\,(\mathrm{mod}15),$$
$$x_2 = 5+6\cdot 1 \equiv 11\,(\mathrm{mod}15),$$
$$x_3 = 5+6\cdot 2 \equiv 17 \equiv 2\,(\mathrm{mod}15).$$

Приведение сравнения по составному модулю к системе сравнений по модулям попарно простым можно также применять к решению сравнений 1-й степени.

Пример 48. Решить сравнение:

$$f(x) = 37x \equiv 17\,(\mathrm{mod}180).$$

Решение. Поскольку модуль $N = 180 = 36\cdot 5$, запишем эквивалентную систему:

$$37x \equiv 17\,(\mathrm{mod}36),$$
$$37x \equiv 17\,(\mathrm{mod}5),$$

с решениями $x \equiv 17\,(\mathrm{mod}36)$, $x \equiv 1\,(\mathrm{mod}5)$.

Решая последнюю систему с помощью китайской теоремы об остатках, получим: $x \equiv -19\,(\mathrm{mod}180)$.

§ 2.9. Сравнения второй степени

Китайская теорема об остатках основана на сравнениях первой степени:

$$ax + b \equiv 0\,(\mathrm{mod}\,m).$$

Теперь рассмотрим сравнения второй степени вида:

$$ax^2 + bx + c \equiv 0\,(\mathrm{mod}\,m).$$

Выделением полного квадрата получим:

$$(2ax+b)^2 \equiv b^2 - 4ac\,(\mathrm{mod}\,4am).$$

или

$$y^2 \equiv d\,(\mathrm{mod}\,4am),$$

где

$$y = 2ax + b,\ d = b^2 - 4ac.$$

Фактически данное сравнение приведено к виду:

$$x^2 \equiv a \,(\mathrm{mod}\, m).$$

Пример 49. Решить сравнение:

$$4x^2 - 11x - 3 \equiv 0 \,(\mathrm{mod}\, 13)$$

Решение. Перед тем, как решать сравнение, попытаемся его упростить. Приведем старший коэффициент к единице. Для этого найдем число y – обратное к 4 по модулю 13:

$$y \cdot 4 \equiv 1 \,(\mathrm{mod}\, 13).$$

По формуле Эйлера находим: $y \equiv 4^{\varphi(13)-1} \equiv 4^{11} \equiv 10 \,(\mathrm{mod}\, 13)$.

Умножая все сравнение на 10, получим:

$$4x^2 - 11x - 3 \equiv 0 \,(\mathrm{mod}\, 13), \quad (\times 10)$$

$$40x^2 - 110x - 30 \equiv 0 \,(\mathrm{mod}\, 13),$$

$$x^2 - 6x - 4 \equiv 0 \,(\mathrm{mod}\, 13).$$

Теперь приведем сравнение к полному квадрату:

$$x^2 - 6x - 4 \equiv 0 \,(\mathrm{mod}\, 13),$$

$$(x-3)^2 - 13 \equiv 0 \,(\mathrm{mod}\, 13),$$

$$(x-3)^2 \equiv 0 \,(\mathrm{mod}\, 13),$$

$$x \equiv 3 \,(\mathrm{mod}\, 13).$$

Пример 50. Решить сравнение: $3x^2 + 7x + 8 \equiv 0 \,(\mathrm{mod}\, 17)$.

Решение. Упростим сравнение. Приведем старший коэффициент к единице. Для этого найдем число y – обратное к 3 по модулю 17: $y \cdot 3 \equiv 1 \,(\mathrm{mod}\, 17)$.

По формуле Эйлера находим $y \equiv 3^{\varphi(17)-1} \equiv 3^{15} \equiv 6 \,(\mathrm{mod}\, 17)$.

Умножая все сравнение на 6, получим:

$$3x^2 + 7x + 8 \equiv 0 \,(\mathrm{mod}\, 17), \quad (\times 6)$$

$$18x^2 + 42x + 48 \equiv 0 \,(\mathrm{mod}\, 17),$$

$$x^2 + 8x - 3 \equiv 0 \,(\mathrm{mod}\, 17).$$

Теперь приведем сравнение к полному квадрату:

$$x^2+8x-3\equiv 0\,(\mathrm{mod}17),$$
$$(x+4)^2-19\equiv 0\,(\mathrm{mod}17),$$
$$(x+4)^2\equiv 19\,(\mathrm{mod}17),$$
$$(x+4)^2\equiv 2\,(\mathrm{mod}17),$$
$$x+4\equiv \pm 6\,(\mathrm{mod}17).$$

Отсюда:

$$x+4\equiv +6\,(\mathrm{mod}17) \quad \Rightarrow \quad x\equiv 2\,(\mathrm{mod}17),$$
$$x+4\equiv -6\,(\mathrm{mod}17) \quad \Rightarrow \quad x\equiv -10\equiv 7\,(\mathrm{mod}17).$$

Определение

Если сравнение $x^2\equiv a\,(\mathrm{mod}\ p)$ разрешимо, то a является квадратичным вычетом по модулю p; если неразрешимо, то a является квадратичным невычетом по модулю p.

Количество наименьших положительных квадратичных вычетов по модулю p есть $\dfrac{p-1}{2}$.

Пример 51. Найдем квадратичные вычеты по mod 7. Их число должно быть $\dfrac{p-1}{2}=\dfrac{7-1}{2}=3$. Возводим в квадрат все числа от 1 до 3: $1^2\equiv 1, 2^2\equiv 4, 3^2\equiv 9\equiv 2, (\mathrm{mod}7)$.

Таким образом: вычеты – это 1, 2, 4;

невычеты – это 3, 5, 6.

Пример 52. Найдем квадратичные вычеты по mod 17. Их число должно быть:

$$\frac{p-1}{2}=\frac{17-1}{2}=8.$$

Возводим в квадрат все числа от 1 до 8:

$1^2\equiv 1, 2^2\equiv 4, 3^2\equiv 9, 4^2\equiv 16, 5^2\equiv 8, 6^2\equiv 2, 7^2\equiv 15, 8^2\equiv 13, (\mathrm{mod}17)$.

Таким образом: вычеты – это 1, 2, 4, 8, 9, 13, 15, 16;

невычеты – это 3, 5, 6, 7, 10, 11, 12, 14.

Критерий Эйлера. Число a, которое не делится на нечетное простое p, является квадратичным вычетом по модулю p тогда и только тогда, когда:

$$a^{\frac{p-1}{2}} \equiv -1 \,(\mathrm{mod}\, p).$$

Доказательство. По теореме Ферма для:

$$(a, p) = 1, (2, p) = 1.$$

имеем:

$$a^{p-1} \equiv 1 \,(\mathrm{mod}\, p),$$

или:

$$\left(a^{\frac{p-1}{2}} + 1\right)\left(a^{\frac{p-1}{2}} - 1\right) \equiv 0 \,(\mathrm{mod}\, p).$$

Отсюда видно, что одна из скобок должна делиться на p.

Пример 53. Установить, сколько решений имеет сравнение:

$$x^2 \equiv 7 \,(\mathrm{mod}\, 19).$$

Пользуясь критерием Эйлера, необходимо исследовать с чем сравнимо:

$$7^{\frac{p-1}{2}} \equiv 7^9 \,(\mathrm{mod}\, 19).$$

По модулю 19 имеем

$$7^2 = 49 \equiv 11, \qquad 7^3 = 77 \equiv 1, \qquad 7^9 \equiv 1 \,(\mathrm{mod}\, 19).$$

Сравнение разрешимо и имеет два решения.

§ 2.10. Символ Лежандра

При больших значениях p критерием Эйлера неудобно выяснять, является ли a квадратичным вычетом или нет. Более эффективным способом является применение символа Лежандра $\left(\frac{a}{p}\right)$ – a по отношению к p.

Пусть p – простое число, $(a,p)=1$. **Символ Лежандра** $\left(\frac{a}{p}\right)$ определяется равенством

$$\left(\frac{a}{p}\right)=\begin{cases}1, \text{ если сравнение } x^2\equiv a \pmod p \ \textit{разрешимо},\\ -1, \text{ если сравнение } x^2\equiv a \pmod p \ \textit{неразрешимо}.\end{cases}$$

В первом случае a является квадратичным вычетом по модулю p. Во втором случае a является квадратичным невычетом по модулю p. Таким образом:

$$\left(\frac{a}{p}\right)=\pm 1.$$

Пример 54. Найдем квадратичные вычеты по mod 19. Их число должно быть

$$\frac{p-1}{2}=\frac{19-1}{2}=9.$$

Возводим в квадрат все числа от 1 до 9:

$$1^2\equiv 1, 2^2\equiv 4, 3^2\equiv 9, 4^2\equiv 16, 5^2\equiv 6, 6^2\equiv 17, 7^2\equiv 11, \pmod{19}.$$

Таким образом: вычеты – это 1, 4, 5, 6, 7, 9, 11, 16, 17;

невычеты – это 2, 3, 8, 10, 12, 13, 14, 15, 18.

Символы Лежандра:

$$\left(\frac{1}{19}\right)=\left(\frac{4}{19}\right)=\left(\frac{5}{19}\right)=\left(\frac{6}{19}\right)=\left(\frac{7}{19}\right)=\left(\frac{9}{19}\right)=\left(\frac{11}{19}\right)=\ldots=+1,$$

$$\left(\frac{2}{19}\right)=\left(\frac{3}{19}\right)=\left(\frac{8}{19}\right)=\left(\frac{10}{19}\right)=\left(\frac{12}{19}\right)=\left(\frac{13}{19}\right)=\left(\frac{14}{19}\right)=\ldots=-1.$$

Если g – первообразный корень по mod p, то каждое целое g^{2k} – квадратичный вычет, каждое g^{2k+1} – квадратичный невычет.

Действительно, сравнение $\left(g^t\right)^2\equiv g^{2k+1} \pmod p$ влечет $g^{|2k+1-2t|}\equiv 1 \pmod p$, а значит, $2k + 1 – 2t$ должно делиться на $p-1$. Поскольку первое число нечетно, а второе – четно, то мы

получили противоречие. Следовательно, существует $\frac{p-1}{2}$ квадратичных вычетов и столько же невычетов по mod p.

Свойства символа Лежандра

1. Критерий Эйлера. Если $(a, p) = 1$, то:

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

$$a^{p-1} - 1 = \left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right) \equiv 0 \pmod{p}.$$

Множители:

$$\left(a^{\frac{p-1}{2}} - 1\right) \qquad \text{и} \qquad \left(a^{\frac{p-1}{2}} + 1\right)$$

различаются на два. Поэтому только один из них делится на p. Для $a = g^{2k}$ это будет первый множитель.

2. Если $a \equiv a_1 \pmod{p}$, то:

$$\left(\frac{a}{p}\right) = \left(\frac{a_1}{p}\right).$$

Это свойство вытекает из того, что числа одного класса являются одновременно или квадратичными вычетами, или невычетами. Можно также записать:

$$\left(\frac{a}{p}\right) = \left(\frac{a + kp}{p}\right).$$

3. Символ $\left(\frac{1}{p}\right) = 1$.

Другими словами, 1 является квадратичным вычетом для любого нечетного простого p, или сравнение

$$x^2 \equiv 1 \pmod{p}, \qquad (2, p) = 1$$

всегда разрешимо, поскольку:

$$x \equiv \pm 1 \pmod{p}.$$

4. Символ

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}.$$

В силу сравнения Эйлера

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p},$$

имеем

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod{p}.$$

Символ $\left(\frac{-1}{p}\right)$ может иметь значение $+1$ или -1; то же можно сказать о выражении $(-1)^{\frac{p-1}{2}}$. Но так как по нечетному простому модулю p (+1) и (–1) не сравнимы, то мы должны иметь в обеих частях сравнения одновременно +1 или –1.

Поэтому здесь $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

Из этого свойства следует, что для простых чисел вида

$$p = 4m+1 \quad \Rightarrow \quad \left(\frac{-1}{p}\right) = 1,$$

а для простых чисел вида

$$p = 4m+3 \quad \Rightarrow \quad \left(\frac{-1}{p}\right) = -1,$$

Другими словами, для простых чисел вида $4m+1$ число (–1) является квадратичным вычетом, а для простых чисел вида $4m+3$ – квадратичным невычетом:

$$\left(\frac{-1}{p}\right)=\begin{cases}1, & p\equiv 1\,(\mathrm{mod}\,4),\\ -1, & p\equiv 3\,(\mathrm{mod}\,4).\end{cases}$$

5. Символ

$$\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \text{ где } (a,p)=(b,p)=1.$$

В силу сравнения Эйлера:

$$\left(\frac{a}{p}\right)\equiv a^{\frac{p-1}{2}}\ (\mathrm{mod}\,p)$$

имеем:

$$\left(\frac{ab}{p}\right)\equiv\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)(\mathrm{mod}\,p).$$

В частности, из этого свойства следует:

$$\left(\frac{a^2}{p}\right)=+1, \qquad \left(\frac{ab^2}{p}\right)=\left(\frac{a}{p}\right).$$

Произведение двух квадратичных вычетов или невычетов является квадратичным вычетом.

Произведение квадратичного вычета на квадратичный невычет является квадратичным невычетом.

6. Символ $\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}$.

Преобразуем данное свойство для практического применения.

Если $p=8m\pm 1$, то:

$\frac{p^2-1}{8}=\frac{(8m\pm 1)^2-1}{8}=\frac{64m^2\pm 16m}{8}=8m^2\pm 2m\equiv 0\ (\mathrm{mod}2)$ – четное число.

Если $p=8m\pm 3$, то: $\frac{p^2-1}{8}=\frac{(8m\pm 3)^2-1}{8}=\frac{64m^2\pm 48m+8}{8}=$ $8m^2\pm 6\mathrm{m}+1\equiv 1\ (\mathrm{mod}2)$ – нечетное число.

Другими словами, для простых чисел вида $8m \pm 1$ число 2 является квадратичным вычетом, а для простых чисел вида $4m \pm 3$ – квадратичным невычетом:

$$\left(\frac{2}{p}\right) = \begin{cases} 1, & p = 8m \pm 1 \equiv \pm 1 \pmod 4, \\ -1, & p = 8m \pm 3 \equiv \pm 3 \pmod 4. \end{cases}$$

Пример 55. Установить, разрешимо ли сравнение:

$$x^2 \equiv 2 \pmod{1097}.$$

Решение. Поскольку $1097 = 8 \cdot 137 + 1 \equiv 1 \pmod 8$, то число $p = 1097$ имеет вид $p = 8m + 1$, а 2 – является для него квадратичным вычетом, и наше сравнение $x^2 \equiv 2 \pmod{1097}$ разрешимо.

Пример 56. Установить, разрешимо ли сравнение:

$$x^2 \equiv 2 \pmod{1709}.$$

Решение. Поскольку $1709 = 8 \cdot 213 + 5 \equiv 5 \pmod 8$,
то число $p = 1097$ имеет вид $p = 8m + 5$, а 2 – является для него квадратичным невычетом, и наше сравнение $x^2 \equiv 2 \pmod{1709}$ неразрешимо.

2.10.1. Квадратичный закон взаимности

Очередное свойство символа Лежандра выражается в виде закона взаимности нечетных простых чисел.

Если p и q – нечетные простые числа, то

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.$$

Преобразуем данное выражение для удобства практического применения. Умножая обе части на $\left(\frac{p}{q}\right)$, получим

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \cdot \left(\frac{p}{q}\right).$$

Отсюда следует, что если хотя бы одно из чисел p или q имеет форму $4m+1$, то показатель в правой части равенства четный, поэтому

$$\left(\frac{q}{p}\right)=\left(\frac{p}{q}\right).$$

Если же p и q имеет форму $4m+3$, то показатель степени числа (–1) окажется числом нечетным, и мы будем иметь

$$\left(\frac{q}{p}\right)=-\left(\frac{p}{q}\right).$$

Пример 57. Установить, разрешимо ли сравнение

$$x^2\equiv 426 \pmod{491}.$$

Решение. Поскольку

$$426=2\cdot 3\cdot 71,$$

то символ Лежандра разлагается на множители

$$\left(\frac{426}{491}\right)=\left(\frac{2}{491}\right)\cdot\left(\frac{3}{491}\right)\cdot\left(\frac{71}{491}\right).$$

1. Поскольку $491\equiv 3 \pmod 8$,

то $\left(\frac{2}{491}\right)=-1.$

2. Поскольку $491\equiv 3 \pmod 4$ *и* $3\equiv 3 \pmod 4$, то

$$\left(\frac{3}{491}\right)=-\left(\frac{491}{3}\right)=-\left(\frac{2}{3}\right).$$

Но теперь $3\equiv 3 \pmod 8$ и $-\left(\frac{2}{3}\right)=-(-1)=1.$

3. $$\left(\frac{71}{491}\right)=-\left(\frac{491}{71}\right)=-\left(\frac{65}{71}\right)=-\left(\frac{5}{71}\right)\cdot\left(\frac{13}{71}\right)$$

$$=-\left(\frac{71}{5}\right)\cdot\left(\frac{71}{13}\right)=-\left(\frac{1}{5}\right)\cdot\left(\frac{6}{13}\right)$$

$$= -\left(\frac{2}{13}\right)\cdot\left(\frac{3}{13}\right) = -(-1)\cdot\left(\frac{13}{3}\right) = 1\cdot\left(\frac{1}{3}\right) = 1,$$

Следовательно, $\left(\frac{426}{491}\right) = (-1)\cdot 1\cdot 1 = -1$ – сравнение неразрешимо.

Гаусс доказал следующую лемму, упрощающую вычисление символа Лежандра.

Лемма Гаусса

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{i=1}^{p_1}\left(\frac{2ai}{p}\right)},$$

где $p_1 = \frac{p-1}{2}$.

Доказательство. Рассмотрим числа $a, 2a, 3a, \ldots, p_1 a$ и их абсолютно наименьшие вычеты

$$\varepsilon_1 r_1, \varepsilon_2 r_2, \varepsilon_3 r_3, \ldots, \varepsilon_{p_1} r_{p_1},$$

где $\varepsilon_j = \pm 1, |\varepsilon_j r_j| = r_j$. Числа $\pm a, \pm 2a, \pm 3a, \ldots, \pm p_1 a$ образуют приведенную систему вычетов по mod p, среди которых содержатся $r_1, r_2, r_3, \ldots, r_{p_1}$. последние лишь порядком отличаются от чисел 1, 2, 3, … , p_1. Перемножая почленно сравнения:

$$ia \equiv \varepsilon_i r_i \pmod{p}, \quad i = 1, 2, 3, \ldots, p_1$$

и сокращая произведение на $1, 2, 3, \ldots, p_1 = r_1, r_2, r_3, \ldots, r_{p_1}$,

получаем $a^{\frac{p-1}{2}} \equiv \varepsilon_1, \varepsilon_2, \varepsilon_3, \ldots, \varepsilon_{p_1} \pmod{p}$.

В силу $\left[\frac{2ia}{p}\right] = \left[2\left[\frac{ia}{p}\right] + 2\left\{\frac{ia}{p}\right\}\right] = 2\left[\frac{ia}{p}\right] + 2\left[\left\{\frac{ia}{p}\right\}\right]$

видно, что $\varepsilon_i = \begin{cases} 1, & при\ четном \left[\dfrac{2ia}{p}\right], \\ -1, при\ нечетном \left[\dfrac{2ia}{p}\right]. \end{cases}$

При нечетном a лемма формулируется следующим образом:

$$\left(\frac{2a}{p}\right) = \left(\frac{4\dfrac{a+p}{2p}}{p}\right) = \left(\frac{\dfrac{a+p}{2}}{p}\right) = (-1)^{\sum_{i=1}^{p_1}\left[\frac{(a+p)i}{p}\right]} = (-1)^{\sum_{i=1}^{p_1}\left[\frac{ai}{p}\right]} + (-1)^{\sum_{i=1}^{p_1} i}.$$

Поэтому $\left(\dfrac{2}{p}\right)\left(\dfrac{a}{p}\right) = (-1)^{\sum_{i=1}^{p_1}\left[\frac{ai}{p}\right] + \frac{p^2-1}{8}}$.

При $a = 1$ имеем $\left(\dfrac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$,

а при нечетном a:

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{i=1}^{p_1}\left[\frac{ai}{p}\right]}.$$

Теорема. Квадратичный закон взаимности. Для любых простых p, q выполнено равенство:

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right).$$

Доказательство. Для вычисления $\left(\dfrac{q}{p}\right)$ используем лемму Гаусса. Пусть $q_1 = \dfrac{q-1}{2}$.

Рассмотрим теперь p_1q_1 пар чисел p_i и q_i, где i= 1, 2 , 3, …, p_1; j = 1, 2, 3, … q_1. Все они попарно различны.

Образуем из них S_1 пар с условием $q_i < p_j$ или $i \le \frac{pj}{q}$ и S_2 пар с условием $q_i > p_j$.

Поэтому $S_1 = \sum_{j=1}^{q_1} \left[\frac{p}{q} j \right], \qquad S_2 = \sum_{i=1}^{p_1} \left[\frac{q}{p} i \right].$

В силу леммы Гаусса:

$$\left(\frac{p}{q}\right) = (-1)^{S_1}, \qquad \left(\frac{q}{p}\right) = (-1)^{S_2}.$$

Перемножая эти равенства, получим:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{p_1 q_1}.$$

2.10.2. Цепные дроби

Пусть $\alpha \in \mathbb{R}$ – положительное вещественное число. Обозначим целую часть этого числа $[\alpha] \in \mathbb{Z}$. Положим $q_1 = [\alpha]$. Тогда, если α – нецелое, то $\alpha = q_1 + \frac{1}{\alpha_2}$,

где $\alpha_2 > 1$. Продолжая этот процесс, получаем

$$\alpha_2 = q_2 + \frac{1}{\alpha_3}, \alpha_3 = q_3 + \frac{1}{\alpha_4}, ..., \alpha_s = q_s + \frac{1}{\alpha_{s+1}}.$$

Следовательно, $\alpha = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + ... + \cfrac{1}{q_s + \cfrac{1}{\alpha_{s+1}}}}}$.

Представление α в указанном виде называется разложением α в цепную (непрерывную) дробь. При иррациональном α дробь будет конечной. Пусть $\alpha = \frac{a}{b}$. Применим алгоритм Евклида:

$$a = b\,q_1 + r_1, \quad \frac{a}{b} = q_1 + \frac{1}{b/r_1}$$

$$b = r_1 q_2 + r_2, \quad \frac{b}{r_1} = q_2 + \frac{1}{r_1/r_2}$$

$$r_1 = r_2 q_3 + r_3, \quad \frac{r_1}{r_2} = q_3 + \frac{1}{r_2/r_3}$$

$$r_{n-2} = r_{n-1} q_n + r_n, \quad \frac{r_{n-2}}{r_{n-1}} = q_n + \frac{1}{r_{n-1}/r_n}$$

$$r_{n-1} = r_n q_{n+1}, \quad \frac{r_{n-1}}{r_n} = q_{n+1}.$$

Следовательно $\dfrac{a}{b} = q_1 + \dfrac{1}{q_2 + \dfrac{1}{q_3 + \ldots + \dfrac{1}{q_{n+1}}}}$.

Всякое иррациональное $\alpha \in \mathsf{R}$ разлагается в бесконечную цепную дробь.

Всякое рациональное $\alpha \in \mathsf{Q}$ разлагается в конечную цепную дробь.

Подходящие дроби

В цепной дроби

$$\alpha = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \ldots + \cfrac{1}{q_s + \cfrac{1}{\alpha_{s+1}}}}} = [q_1, q_2, q_3, \ldots, q_s, \alpha_{s+1}].$$

числа $q_1, q_2, q_3, \ldots, q_s$ назовем неполными частными, а рациональное число – s-й подходящей дробью числа α.

$$\delta_s = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \ldots + \cfrac{1}{q_s}}} = [q_1, q_2, q_3, \ldots, q_s]$$

Через P_s обозначим числитель, а через Q_s – знаменатель подходящей дроби δ_s. Например $P_1 = q_1, Q_1 = 1$ или $P_0 = 1, Q_0 = 0$.

Несократимую дробь $\frac{a}{b}\,(b > 0)$ **назовем наилучшим приближением первого рода** числа $\alpha \in \mathbb{R}$, если

$$\frac{a}{b} \neq \frac{c}{d}, \quad 0 < b \le d. \qquad \Rightarrow \qquad \left|\alpha - \frac{c}{d}\right| > \left|\alpha - \frac{a}{b}\right|.$$

В случае, когда выполняется условие:

$$\frac{a}{b} \neq \frac{c}{d}, \quad 0 < b < d. \qquad \Rightarrow |\alpha d - c| \le |\alpha b - a|,$$

говорят о наилучшем приближении второго рода, которое является и наилучшим приближением первого рода. В самом деле, перемножая неравенства

$$\left|\alpha - \frac{c}{d}\right| \le \left|\alpha - \frac{a}{b}\right|, \quad d \le b,$$

получаем $|\alpha d - c| \le |\alpha b - c|$. Обратное утверждение неверно.

Легко проверить, что 1/3 является наилучшим приближением первого рода числа 1/5.

Теорема. Всякая подходящая дробь $\delta_s, s > 1$ есть наилучшее приближение второго рода.

Пример 58. Разложить в цепную дробь выражение $\sqrt{6}$.

Решение. Поскольку $\sqrt{6};2.449$, то выделяем наибольшее целое $x=2$. Тогда $\sqrt{6}=x+\sqrt{6}-x$ и

$$\sqrt{6}=2+\sqrt{6}-2=2+\frac{(\sqrt{6}-2)(\sqrt{6}+2)}{\sqrt{6}+2}=2+\frac{(6-4)}{2+\sqrt{6}}=2+\frac{2}{2+\sqrt{6}}.$$

Мы получили выражение $\sqrt{6}$ как функцию $f(\sqrt{6})$:

$$\sqrt{6}=2+\frac{2}{2+\sqrt{6}}.$$

Подставляя ее в себя получим непрерывную цепную дробь.

$$\sqrt{6}=2+\cfrac{2}{4+\cfrac{2}{4+\cfrac{2}{4+\cfrac{2}{2+\ldots}}}}.$$

Видно, что рациональные функции разлагаются в конечные цепные дроби, а иррациональные выражения имеют бесконечные цепные дроби.

Для разложения квадратных корней натуральных чисел приведем общую формулу:

$$\sqrt{n}=\sqrt{k^2+m}=f(k,2k,m)=k+\cfrac{m}{2k+\cfrac{m}{2k+\cfrac{m}{2k+\ldots}}}.$$

где $0\le m<k^2$. Функция цепной дроби имеет интересное свойство: $f(k,2k,2k+1)=f(k+1,2k+1,0)$.

Заметим, что данное разложение было известно еще итальянскому математику Рафаэли Бомбелли (1572 г.).

2.10.3. Решение сравнений с помощью цепных дробей

Пусть дано сравнение: $ax\equiv b\pmod{p}$, $\quad(a,p)=1$.

Разложим $\frac{p}{a}$ в цепную дробь и обозначим ее подходящие дроби через $\delta_k = \frac{P_k}{Q_k}$. Тогда, согласно свойству несократимости подходящих дробей, имеем:

$$P_n = m, \qquad Q_m = a.$$

Поэтому вместо соотношения:

$$P_n \cdot Q_{n-1} - P_{n-1} \cdot Q_n = (-)^n$$

имеем:

$$p \cdot Q_{n-1} - P_{n-1} \cdot a = (-)^n.$$

Отсюда: $P_{n-1} \cdot a = p \cdot Q_{n-1} - (-)^n$.

Поскольку Q_{n-1} – целое число, получим:

$$P_{n-1} \cdot a \equiv (-)^{n+1} \pmod{p}.$$

Умножая обе части этого сравнения на $(-)^{n+1} b$, получим

$$P_{n-1} \cdot ab(-)^{n+1} \equiv b \pmod{p}.$$

Сравнивая это сравнение с исходным, приходим к выводу, что оно имеет решение:

$$x \equiv (-)^{n+1} \cdot P_{n-1} b \pmod{p},$$

где P_{n-1} – числитель предпоследней подходящей дроби в разложении $\frac{p}{a}$.

Пример 59. Решить сравнение:

$$285x \equiv 177 \pmod{924}.$$

Решение. Во-первых, разделим все на 3:

$$95x \equiv 59 \pmod{308}.$$

Поскольку $(95,308) = 1$ – взаимно простые, то сравнение имеет решение. Разлагая $\frac{308}{95}$ в цепную дробь, получим:

$$\delta_n = \frac{308}{95} = 3 + \cfrac{1}{4 + \cfrac{1}{7 + \cfrac{1}{1 + \cfrac{1}{2}}}}$$

или $\delta_n = \delta_5 = \frac{308}{95} = [3,4,7,1,2]$. Тогда:

$$\delta_{n-1} = \delta_4 = [3,4,7,1] = 3 + \cfrac{1}{4 + \cfrac{1}{7 + \cfrac{1}{1}}} = \frac{107}{33}$$

отсюда:

$$P_{n-1} = P_4 = 107.$$

Следовательно,

$$x \equiv (-)^4 \cdot 107 \cdot 59 \pmod{308},$$

$$x \equiv 153 \pmod{308}.$$

Возвращаясь к модулю $3 \cdot 308 = 924$, получим три решения:

$$x \equiv 153, 461, 769 \pmod{924}.$$

Задачи и упражнения для самостоятельного решения:

1. Найти остаток от деления:

$$\frac{3^{59}}{17},\quad \frac{7^{67}}{12},\quad \frac{317^{273}}{39},\quad \frac{4^{50}}{67},\quad \frac{267^{311}}{37},\quad \frac{197^{157}}{35}.$$

2. Найти остаток от деления:

$$\frac{4^{113}}{92},\quad \frac{6^{76}}{26},\quad \frac{21^{83}}{24},\quad \frac{35^{150}}{425}.$$

3. Найти остаток от деления:

$$\frac{3^{100}+4^{100}}{7},\quad \frac{5^{50}+7^{70}}{9},\quad \frac{3\cdot 5^{75}+4\cdot 7^{100}}{132}.$$

4. Найти последние цифры в десятичном представлении:

$$2^{153},\quad 3^{219},\quad 2^{2009}.$$

5. Найти остаток от деления:

$$\frac{a^{12}}{7},\quad \frac{a^{12}-b^{12}}{65},\quad \text{если}\quad (a,7)=(a,65)=(b,65)=1.$$

6. Разложить на простые множители числа:

$$5!\quad 10!\quad 15!\quad 20!\quad 30!\quad 50!$$

7. Сколько чисел в интервале от 1 до 120 не взаимно простых с 30?

8. Дано $\varphi(x)=120, x=p_1\cdot p_2$. Найти x, если $p_1-p_2=2$.

Библиографический список

1. Кострикин, А. И. Основные структуры алгебры / А. И. Кострикин. – М. : Наука, 2000. – 272 с.

2. Курош, А. Г. Курс высшей алгебры / А. Г. Курош. – СПб. : Лань, 2007. – 432 с.

3. Самсонов, Б. Б. Компьютерная информатика / Б. Б. Самсонов, Е. М. Плохов, А. И. Филоненков. – Ростов н/Д : Феникс, 2002. – 512 с.

4. Фаддеев, Д. К. Задачи по высшей алгебре / Д. К. Фаддеев, И. С. Соминский. – СПб. : Лань, 2007. – 288 с.

5. Фаддеев, Д. К. Лекции по алгебре / Д. К. Фаддеев. – СПб. : Лань, 2005. – 416 с.

6. Sherck J. Algebra. Toronto : University of Toronto, 2009. 419 p.

7. Vinogradov I. Elements of Number Theory. – NY. : Dover, 2016. 250 p.

8. Думачев, В. Н. Алгебра и геометрия / В. Н. Думачев, В. В. Меньших, С. А. Телкова. – Воронеж : Воронежский институт МВД России, 2014. – 431 с.

9. Данилова, О. Ю. Математические основы криптографии / О. Ю. Данилова, В. Н. Думачев. – Воронеж : Воронежский институт МВД России, 2017. – 301 с.

10. Думачев, В. Н. Модели и алгоритмы квантовой информации / В. Н. Думачев. – Воронеж : Воронежский институт МВД России, 2009. – 232 с.

Учебное издание

Атласов Игорь Викторович,
доктор физико-математических наук, профессор

Думачев Владислав Николаевич,
кандидат физико-математических наук, доцент

Таранина Екатерина Игоревна

Основы общей алгебры и теории чисел

Редактор *Абилова Ф. А.*
Корректор *Титова В. П.*
Компьютерная верстка *Абилова Ф. А.*

Московский университет МВД России имени В.Я. Кикотя
117997, г. Москва, ул. Академика Волгина, д. 12

Подписано в печать 31.05.2022	Формат 60×84 1/16	Тираж	138 экз.
		1-й завод	84 экз.
Заказ № 24	Цена договорная	Объем	1,7 уч.-изд. л.
			6,5 усл. печ. л.