Министерство образования Республики Беларусь

Учреждение образования
«Гомельский государственный технический
университет имени П. О. Сухого»

Кафедра «Высшая математика»

А. А. Бабич

ВЫСШАЯ АЛГЕБРА

ПОСОБИЕ
по курсу «Математика. Геометрия и алгебра»
для студентов специальности 1-40 04 01 «Информатика
и технологии программирования»
дневной формы обучения

Гомель 2020

УДК 517.9(075.8)
ББК 22.14я73
Б12

Рекомендовано научно-методическим советом
факультета автоматизированных и информационных систем
ГГТУ им. П. О. Сухого
(*протокол № 2 от 14.10.2019 г.*)

Рецензент: зав. каф. «Информтика» ГГТУ им. П. О. Сухого
канд. физ.-мат. наук, доц. *Т. А. Трохова*

Бабич, А. А.

Б12 Высшая алгебра : пособие по курсу «Математика. Геометрия и алгебра» для студентов специальности 1-40 04 01 «Информатика и технологии программирования» днев. формы обучения / А. А. Бабич. – Гомель : ГГТУ им. П. О. Сухого, 2020. – 64 с. – Систем. требования: PC не ниже Intel Celeron 300 МГц ; 32 Mb RAM ; свободное место на HDD 16 Mb ; Windows 98 и выше ; Adobe Acrobat Reader. – Режим доступа: https://elib.gstu.by. – Загл. с титул. экрана.

Пособие включает в себя три главы: «Основы арифметики», «Криптография и современные криптосистемы» и «Группы, кольца, поля». Каждая глава разбита на параграфы. Изложенный материал содержит большое количество примеров. Типовые примеры выделены в специальные разделы и приводится достаточно подробное их решение.

Для студентов специальности 1-40 04 01 «Информатика и технологии программирования» дневной формы обучения.

УДК 517.9(075.8)
ББК 22.14я73

ПРЕДИСЛОВИЕ

Настоящее пособие представляет собой вторую часть курса лекций по дисциплине «Математика. Геометрия и алгебра» и предназначено для студентов специальности 1-40 04 01 «Информатика и технологии программирования» дневной формы. Пособие включает в себя такие разделы математики, как теория чисел, теория конечных групп и колец, которые широко используются в современных методах кодирования информации, а также при разработке эффективных и надежных способах ее передачи и защиты. Цель пособия – представить в достаточно небольшом объеме весь основной теоретический материал, входящий в учебную программу дисциплины во втором семестре. Сжатость материала предполагает и стиль изложения. В частности, отсутствуют доказательства теорем. Тем не менее даны указания к доказательствам, а содержание теорем и их смысл раскрываются с помощью серии примеров.

Для удобства поиска используется тройная нумерация определений, теорем, формул, примеров: (глава, параграф, порядковый номер). Специальные математические термины выделены жирным шрифтом, а важные и существенные для понимания фрагменты текста – курсивом.

Решения примеров заканчиваются символом ■.

ГЛАВА 1
ОСНОВЫ АРИФМЕТИКИ

1.1. Целые числа

Натуральный ряд $1, 2, 3, \ldots$ обладает следующими основными свойствами:

1. *Аксиома индукции.*
   Если некоторое множество натуральных чисел содержит 1 и вместе с каждым натуральным числом, входящим в него, содержит следующее за ним число, то оно содержит весь натуральный ряд.

2. *Аксиома Архимеда.*
   Для любых натуральных чисел m и n всегда найдется число k такое, что
   $$m \cdot k > n.$$
3. Всякое непустое подмножество натуральных чисел содержит наименьшее число.

4. Всякое конечное подмножество натуральных чисел содержит наибольшее число.

5. *Принцип математической индукции.*
   Если известно, что некоторое утверждение
   1) верно для $n = 1$;
   2) из предположения, что утверждение верно при некотором k, вытекает, что оно верно для $k + 1$,

   то утверждение верно для любого натурального n.

6. *Принцип Дирихле (1834 г.)*
   Если $k \cdot n + 1$ предмет разложен по k ящикам, то по крайней мере в одном из ящиков лежит не менее, чем $n + 1$ предмет.

Пример 1.1.1. Даны $n + 1$ натуральных различных чисел меньших $2n$. Показать, что из них всегда можно выбрать 3 числа так, что одно из них будет равно сумме двух других: $m = k + l$.

Решение

Пусть m наибольшее число из выбранных $n+1$ чисел. По условию оно меньше $2n$. Предположим, что оно наибольшее из возможных, то есть $m = 2n-1$.

Далее все натуральные числа меньшие $2n-1$ (число их равно $2n-2$), разобьем на $n-1$ пару: $\{1, 2n-2\}$, $\{2, 2n-3\}$, ... , $\{n-1, n\}$, так, чтобы сумма чисел в каждой паре была равна $m = 2n-1$. Тогда среди n оставшихся выбранных чисел согласно принципу Дирихле обязательно найдутся два числа k и l из одной пары, а поэтому

$$k + l = 2n - 1 = m.$$

Случай, когда наибольшее из отобранных чисел меньше $2n-1$ рассматривается аналогично, если допустить наличие одноэлементных групп. ■

Множество натуральных чисел $\mathbb{N}$ замкнуто относительно арифметических операций сложения $(+)$ и умножения $(\times)$, и не замкнуто относительно операций вычитания $(-)$ и деления $(\div)$. Добавление к натуральному ряду отрицательных чисел и числа 0 расширяет множество натуральных чисел $\mathbb{N}$ до множества целых чисел $\mathbb{Z}$.

Теорема 1.1.1 (*о дискретности множества целых чисел* $\mathbb{Z}$)

Пусть a и b целые числа, причем $a > b$. Тогда справедливо неравенство

$$a \geq b + 1.$$

Множество целых чисел $\mathbb{Z}$ замкнуто относительно операций сложения $(+)$, вычитания $(-)$ и умножения $(\times)$, и не замкнуто относительно операции деления $(\div)$.

1.2. Деление целых чисел

Опр. 1.2.1 Пусть $a, b, c \in \mathbb{Z}$ и $a \neq 0$. Говорят, что *число* a *делит число* b, если найдется число c такое, что будет выполняться равенство

$$b = a \cdot c. \qquad (1.2.1)$$

Отношение делимости двух целых чисел обозначается как $a|b$.

Свойства операции деления.

1. Любое отличное от нуля число a делит 0:
$$\forall\, a \neq 0: \quad a|0.$$
2. Единица делит любое число:
$$\forall\, a: \quad 1|a.$$
3. Любое отличное от нуля число a делит себя:
$\forall\, a \neq 0: \quad a|a.$
4. Если число a делит число b, то оно будет делить и произведение числа b на любое целое число c:
$a|b \Rightarrow a|bc.$
5. Если a делит b, а b делит c, то a делит c:
$a|b, b|c \Rightarrow a|c.$
6. Если a делит b и c, то a будет делить и их сумму и разность:
$a|b, a|c \Rightarrow a|(b \pm c).$
7. Если число a делит отличное от нуля число b, то модуль числа a не превышает модуля числа b:
$a|b, b \neq 0 \Rightarrow |a| \leq |b|.$

Свойства 1 и 5 указывают на то, что отношение делимости является *рефлексивным* и *транзитивным*. Кроме этого на множестве целых положительных (то есть натуральных) чисел оно является и *антисимметричным*:
$a|b, b|a \Rightarrow a = b.$

Таким образом, на множестве натуральных чисел $\mathbb{N}$ отношение делимости является отношением *частичного порядка*.

Теорема 1.2.1 (*о делимости целых чисел*)

Для *любых* двух целых чисел a и $b \neq 0$ всегда найдутся и притом единственные целые числа q и r такие, что

$$a = b \cdot q + r, \text{ где } 0 \leq r < |b|. \qquad (1.2.2)$$

В равенстве (1.2.2) число a называют *делимым*, число b — *делителем*, число q — *неполным частным*, число r — *остатком от деления*.

Пример 1.2.1. Найти неполное частное и остаток для указанных чисел:

1) $a = 3, b = 5$; 2) $a = 3, b = -5$; 3) $a = 3, b = -5$; 4) $a = -3, b = -5$.

Решение

Записывая заданные числа a в виде (1.2.2), находим:

1) $3 = 0 \cdot 5 + 3 \Rightarrow q = 0,\ r = 3;$
2) $-3 = -1 \cdot 5 + 2 \Rightarrow q = -1,\ r = 2;$
3) $3 = 0 \cdot (-5) + 3 \Rightarrow q = 0,\ r = 3;$
4) $-3 = 1 \cdot (-5) + 2 \Rightarrow q = 1,\ r = 2.$

■

1.3. НОК и НОД

Опр. 1.3.1 Число $M \neq 0$ называется *общим кратным* целых чисел a и b, если $a|M$ и $b|M$. *Наименьшее положительное* из общих кратных M называется **наименьшим общим кратным** чисел, и обозначается как

$$\text{НОК}(a, b) \equiv [a, b].$$

Как следует из определения, по-существу, для любых целых чисел a и b $\text{НОК}(a, b)$ есть число *натуральное*, поэтому *далее без потери общности мы будем рассматривать только наборы натуральных чисел.*

Теорема 1.3.1

Если $m = \text{НОК}(a, b)$, то $m|M$, где M – любое общее кратное чисел a и b.

Опр. 1.3.2 Число N называется *общим делителем* чисел a и b, если $N|a$ и $N|b$. Наибольшее из чисел N называется **наибольшим общим делителем** и обозначается как

$$\text{НОД}(a, b) \equiv (a, b).$$

Введем важное отношение между числами.

Опр. 1.3.3 Числа a и b называются взаимнопростыми, если

$$\text{НОД}(a, b) = 1.$$

Свойства НОК и НОД:

1. Для любого числа n:
$$\text{НОД}(0, n) = n. \qquad (1.3.1)$$
2. Если $a|b$, то
$\text{НОД}(a, b) = a;\ \text{НОК}(a, b) = b.$

3. Если $a = b \cdot q + r$, то
$$\text{НОД}(a, b) = \text{НОД}(b, r). \qquad (1.3.2)$$

4. Для любых чисел a и b справедливо равенство
$$\text{НОК}(a, b) \cdot \text{НОД}(a, b) = a \cdot b. \qquad (1.3.3)$$

5. *Критерий взаимной простоты.*
Два числа a и b будут взаимнопростыми тогда и только тогда, когда найдутся два целых числа u и v такие, что
$a \cdot u + b \cdot v = 1.$

6. Если число a является взаимнопростым с числами b и c, то оно будет взаимнопростым и с их произведением:
$$\text{НОД}(a, b) = 1,\ \text{НОД}(a, c) = 1 \quad \Rightarrow \quad \text{НОД}(a, bc) = 1.$$

7. Если $a|bc$ и к тому же является взаимнопростым с b, то $a|c$.

8. Если $a|c$ и $b|c$, причем числа a и b взаимнопростые, то $ab|c$.

Свойство 3 вместе со свойством 1 позволяет сформулировать достаточно простой алгоритм вычисления $\text{НОД}(a, b) \equiv (a, b)$ (здесь $a > b$), основанный на алгоритме деления Евклида:

$$(a, b) = (b, r_1) = (r_1, r_2) = \cdots = (r_k, r_{k-1}) = \cdots = (r_n, 0) = r_n.$$

Пример 1.3.1 Найти НОК и НОД чисел 3009 и 894.

Решение

Выполняя деление числа 3009 на число 894, и переходя далее к делению делителей на остатки (в соответствии с указанной последовательностью действий), находим НОД:

$$\frac{3009}{894} = 3 + \frac{327}{894} \Rightarrow \frac{894}{327} = 2 + \frac{240}{327} \Rightarrow \frac{327}{240} = 1 + \frac{87}{240} \Rightarrow$$
$$\Rightarrow \frac{240}{87} = 2 + \frac{66}{87} \Rightarrow \frac{87}{66} = 1 + \frac{21}{66} \Rightarrow \frac{66}{21} = 3 + \frac{3}{21} \Rightarrow \frac{21}{3} = 7 + \frac{0}{3} \Rightarrow$$
$$\Rightarrow \text{НОД}(3009,894) = 3.$$

НОК заданных чисел найдем по формуле (1.3.3):

$$\text{НОК}(3009,894) = \frac{3009 \cdot 894}{3} = 896682.$$

Ответ: $\text{НОД}(3009,894) = 3$,
$\text{НОК}(3009,894) = 896682$. ■

Понятия НОК и НОД естественным образом переносятся и на наборы, состоящие из нескольких чисел:

$$\text{НОК}(a_1, a_2, \dots, a_k) \equiv [a_1, a_2, \dots, a_k],$$
$$\text{НОД}(a_1, a_2, \dots, a_k) \equiv (a_1, a_2, \dots, a_k).$$

Справедлива следующая теорема

Теорема 1.3.2

Для НОК и НОД совокупности n чисел $\{a_1, a_2, \dots, a_n\}$ имеют место соотношения

$$[a_1, \dots, a_{n-1}, a_n] = [[a_1, \dots, a_{n-1}], a_n], \qquad (1.3.4)$$

$$(a_1, \dots, a_{n-1}, a_n) = ((a_1, \dots, a_{n-1}), a_n), \qquad (1.3.5)$$

Теорема позволяет свести вычисление НОК и НОД совокупности чисел к вычислению НОК и НОД двух чисел.

Пример 1.3.2. Найти НОК и НОД чисел 12, 16 и 42.

Решение

Согласно общей формуле (1.3.5) имеем

$$(12, 16, 42) = ((12, 16), 42).$$

По алгоритму деления Евклида последовательно вычисляем:

$$\frac{16}{12} = 1 + \frac{4}{12} \Rightarrow \frac{12}{4} = 3 + \frac{0}{4} \Rightarrow (12, 16) = 4;$$

$$\frac{42}{4} = 10 + \frac{2}{4} \Rightarrow \frac{4}{2} = 2 + \frac{0}{2} \Rightarrow (4,42) = 2 \Rightarrow \text{НОД}(12,16,42) = 2.$$

Аналогично, для НОК:
$[12,16,42] = [[12,16],42]$.
Поэтому:

$$[12,16] = \frac{12 \cdot 16}{(12,\ 16)} = \frac{12 \cdot 16}{4} = 48;$$

$$\frac{48}{42} = 1 + \frac{6}{42} \Rightarrow \frac{42}{6} = 7 + \frac{0}{2} \Rightarrow (48,42) = 6 \Rightarrow (48,42) = 6;$$

$$[48,42] = \frac{48 \cdot 42}{(48,\ 42)} = \frac{48 \cdot 42}{6} = 336 \Rightarrow \text{НОК}(12,16,42) = 336.$$

Ответ: $\text{НОД}(12,16,42) = 2$,
$\text{НОК}(12,16,42) = 336$. ■

1.4. Линейные диофантовые уравнения

Опр. 1.4.1

Алгебраическое уравнение первой степени с целочисленными коэффициентами вида

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = b, \qquad (1.4.1)$$

решение которого ищется *на множестве целых чисел* $\mathbb{Z}$, называется **линейным диофантовым уравнением**.

Рассмотрим линейное диофантовое уравнение с двумя неизвестными:

$$ax + by = c. \qquad (1.4.2)$$

Полагая $c = 0$, получим **однородное линейное диофантовое уравнение:**

$$ax + by = 0. \qquad (1.4.3)$$

Теорема 1.4.1

Однородное диофантовое уравнение (1.4.3) всегда имеет бесчисленное множество решений, которые в параметрической форме можно записать как

$$(x, y) = (-bt, at), \text{ где } t \in \mathbb{Z}. \qquad (1.4.4)$$

Перейдем к решению неоднородного уравнения (1.4.2). Заметим, что если $\text{НОД}(a,b,c) = d \neq 1$, то уравнение можно поделить на d. Далее предположим, что $\text{НОД}(a,b,c) = 1$.

После подстановки

$$x = cu,\ y = cv, \qquad (1.4.4)$$

уравнение примет вид:

$$au + bv = 1. \qquad (1.4.5)$$

По форме это уравнение совпадает с соотношением **критерия взаимной простоты** двух целых чисел a и b (Свойство 5, § 3). Поэтому имеет место следующая теорема.

Теорема 1.4.2

Для того чтобы диофантовое уравнение (1.4.5) имело решение необходимо и достаточно, чтобы числа a и b были взаимнопростыми. При этом, если известно некоторое частное решение (u_0, v_0), то общее решение записывается в виде

$$u = u_0 - bt, \quad v = v_0 + at, \qquad (1.4.6)$$

где $t \in \mathbb{Z}$.

Таким образом, уравнение (1.4.5) не имеет решений, если $\text{НОД}(a, b) \neq 1$. Анализируя форму решения (1.4.6), можно прийти к выводу, что для линейных диофантовых уравнений структура пространства решений аналогична структуре решений обычных линейных систем. А именно, *общее решение неоднородного уравнения есть сумма некоторого частного решения и общего решения однородного уравнения*.

Остается вопрос: *как найти частное решение*. Ответ можно найти, анализируя алгоритм деления Евклида коэффициентов a и b. Без потери общности положим $a > b > 0$ (в случае отрицательных коэффициентов можно просто переопределить неизвестные u и v). Введем обозначения:

$$a = r_{-1}, \quad b = r_0.$$

Тогда выполняя деление числа a на число b по алгоритму Евклида, мы получаем следующую цепочку соотношений:

$$\begin{aligned}
a \equiv r_{-1} &= bq_1 + r_1, & 0 \le r_1 < b = r_0;\\
b \equiv r_0 &= r_1 q_2 + r_2, & 0 \le r_2 < r_1;\\
r_1 &= r_2 q_3 + r_3, & 0 \le r_3 < r_2;\\
&\dots\dots\dots\dots\dots\dots & \\
r_{n-2} &= r_{n-1} q_n + r_n, & 0 \le r_n < r_{n-1};\\
r_{n-1} &= r_n q_{n+1}, & r_{n+1} = 0;
\end{aligned}$$

$$\Downarrow$$

$$r_n = \text{НОД}(a,b) \equiv (a,b).$$

Дальнейший анализ удобно проводить с использованием матричной алгебры. Введем матрицу

$$A_k = \begin{pmatrix} q_k & 1 \\ 1 & 0 \end{pmatrix}. \qquad (1.4.7)$$

Тогда нетрудно заметить, что

$$\begin{pmatrix} r_{k-2} \\ r_{k-1} \end{pmatrix} = \begin{pmatrix} q_k & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} r_{k-1} \\ r_k \end{pmatrix} = A_k \begin{pmatrix} r_{k-1} \\ r_k \end{pmatrix},$$

следовательно,

$$\begin{pmatrix} a \\ b \end{pmatrix} = A_1 \begin{pmatrix} r_0 \\ r_1 \end{pmatrix} = A_1 A_2 \begin{pmatrix} r_1 \\ r_2 \end{pmatrix} = \cdots = A_1 A_2 \ldots A_n \begin{pmatrix} r_{n-1} \\ r_n \end{pmatrix}.$$

Заметим, что $\det A_k = -1 \neq 0$, поэтому все матрицы A_k невырождены и имеют обратные:

$$B_k \equiv A_k^{-1} = \begin{pmatrix} 0 & 1 \\ 1 & -q_k \end{pmatrix}. \qquad (1.4.8)$$

Умножая предыдущее равенство слева на обратные матрицы, получаем:

$$\begin{pmatrix} r_{n-1} \\ r_n \end{pmatrix} = A_n^{-1} A_{n-1}^{-1} \ldots A_1^{-1} \begin{pmatrix} r_{-1} \\ r_0 \end{pmatrix},$$

или

$$\begin{pmatrix} r_{n-1} \\ r_n \end{pmatrix} = B \begin{pmatrix} a \\ b \end{pmatrix}, \qquad (1.4.9)$$

где

$$B = B_n B_{n-1} \ldots B_1. \qquad (1.4.10)$$

Подставим в соотношение (1.4.9) явный вид матрицы B:

$$\begin{pmatrix} r_{n-1} \\ r_n \end{pmatrix} = \begin{pmatrix} s & t \\ u & v \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} as + bt \\ au + bv \end{pmatrix} \Rightarrow au + bv = r_n = (a,b).$$

Таким образом, *вторая строка матрицы B и будет искомым частным решением* (u_0, v_0).

Пример 1.4.1. Покупателю необходимо расплатиться за покупку ценой в 43 денежные единицы. У него в наличии имеются ассигнации только в 12 и 7 денежных единиц. Может ли покупатель сделать расчет (без сдачи)?

Решение

Обозначим количество ассигнаций разных достоинств через x и y. Тогда покупателю, по-существу, требуется решить уравнение:

$$12x + 7y = 43.$$

После подстановки $x = 43u,\ y = 43v$, получим уравнение

$$12u + 7v = 1.$$

Отметим, что $\text{НОД}(12,7) = 1$, следовательно, уравнение имеет решение. Выполним деление коэффициентов уравнения по алгоритму Евклида:

$$\begin{aligned} 12 \equiv r_{-1} &= 7 \cdot 1 + 5, \\ 7 \equiv r_0 &= 5 \cdot 1 + 2, \\ 5 \equiv r_1 &= 2 \cdot 3 + 1, \\ 2 \equiv r_2 &= 1 \cdot 2 + 0. \end{aligned}$$

Далее по формулам (1.4.8) и (1.4.10) находим матрицу B:

$$B = B_3B_2B_1 = \begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & -3 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} -1 & 2 \\ 3 & -5 \end{pmatrix} \Rightarrow$$

$$\Rightarrow\ (u_0, v_0) = (3, -5)\ \Rightarrow\ (x_0, y_0) = (3 \cdot 43, -5 \cdot 43) = (129, -215).$$

Общее решение:

$$x = x_0 - bt = 129 - 7t,$$
$$y = y_0 + at = -215 + 12t.$$

Решением задачи является *пара натуральных чисел*. Полагая $t = 18$, находим искомое решение:

$x = 3,\quad y = 1.$

Ответ: *расчет возможен* - для расчета покупателю потребуется 3 ассигнации номиналом 12 денежных единиц и 1 ассигнация номиналом 7 денежных единиц.

■

1.5. Простые числа

Опр. 1.5.1 Неравное 1 натуральное число p называется **простым**, если оно не имеет делителей отличных от 1 и p.

Опр. 1.5.2 Натуральные числа, не являющиеся простыми, называются **составными** числами.

Число 1 выделено по соглашению в специальный класс и не является ни простым, ни составным.

Отобрать простые числа среди чисел натурального ряда можно с помощью алгоритма, который носит название *решето Эратосфена*. При этом полезна следующая лемма.

Лемма

Пусть N составное число, а p – его наименьший делитель > 1. Тогда p – простое число, причем

$$p^2 < N. \qquad (1.5.1)$$

Из леммы следует, что любое составное число имеет простой делитель.

Пример 1.5.1. Установить является ли число $N = 1009$ простым.

Решение

Если число $N = 1009$ составное, то согласно лемме оно обязательно должно иметь простой делитель p, удовлетворяющий неравенству:

$$2 \le p \le 31,$$

так как $32^2 = 1024 > 1009$. Таким образом, простыми делителями числа 1009 могут быть только числа:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31.$$

Непосредственным делением убеждаемся, что ни одно из этих чисел делителем числа $N = 1009$ не является, следовательно, число 1009 простое.

Ответ: число 1009 простое.

■

Оказывается, что среди первых 100 натуральных чисел имеется 25 простых. Возникает вопрос: *а сколько простых чисел вообще?*

Теорема 1.5.1

Множество простых чисел счетно.

Одним из направлений развития теории чисел является поиск формул, по которым можно было бы генерировать простые числа. Так известны *формулы Мерсенна* $(2^p - 1)$, *Ферма* $(2^{2^n} + 1)$ и др. Но, к сожалению, следует отметить, что указанные формулы генерируют не только простые числа. Так, например, числа Ферма при $n = 1, 2, 3, 4$ действительно являются простыми: $\{5, 17, 257, 65537\}$, однако уже следующее число при $n = 5$ является составным:

$$2^{2^5} + 1 = 4\,294\,967\,297 = 641 \cdot 6\,700\,417.$$

Отметим некоторые известные общие результаты, имеющие непосредственное отношение к простым числам:

1. Если p – простое и $p|ab$, то $p|a$ или $p|b$ (*лемма Евклида*).

2. Если p – простое и a - натуральное, то $p|a^p - a$ (*малая теорема Ферма*).

3. Число p является простым тогда и только тогда, когда $p|(p-1)! + 1$ (*теорема Вильсона*).

4. Если n – натуральное, то всегда найдется простое число p такое, что $n < p < 2n$ (*постулат Бертрана*).

5. Любая арифметическая прогрессия, для которой первый член a_1 и разность d – взаимнопростые числа, содержит бесчисленное множество простых чисел (*теорема Дирихле*).

Издавна ведутся поиски наибольших простых чисел, за нахождение которых организацией Electronic Frontier Foundation было предложено несколько наград в зависимости от величины числа. Так, в 2009 году была вручена премия в размере 100 000 долларов США, назначенная за нахождение простого числа, десятичная запись которого содержит не менее 10 миллионов цифр.

Один из первых рекордов поставил в 1772 году Леонард Эйлер, найдя простое число $2^{31} - 1 = 2\,147\,483\,647$.

Наибольшее известное простое число (на период до середины 2019 года):

$$2^{82\,589\,933} - 1.$$

Оно было открыто Патриком Ларошем в рамках проекта GIMPS 7 декабря 2018 года и содержит 24 862 048 десятичных цифр.

Все известные максимальные натуральные числа являются числами Мерсенна. Это объясняется тем фактом, что для чисел Мерсенна существует достаточно простой для реализации алгоритм проверки простоты числа – тест Люка-Лемера.

Поиск максимальных простых чисел в настоящее время является чрезвычайно важной и актуальной задачей в связи с бурным развитием информационных технологий. Большие натуральные числа являются центральной частью современных методов кодирования, защиты и передачи цифровой информации.

Теорема 1.5.2 (*основная теорема арифметики*)

Любое натуральное число $a > 1$ единственным образом раскладывается на простые сомножители:

$$a = p_1^{k_1} p_2^{k_2} \dots p_m^{k_m} \quad (p_1 < p_2 < \dots < p_m). \quad (1.5.2)$$

Разложение (1.5.2) называется *каноническим разложением числа* a *на простые сомножители.* Оно предоставляет полную информацию о числе. В частности, с его помощью можно сформулировать достаточно простой алгоритм вычисления НОК и НОД наборов целых чисел.

Рассмотрим этот алгоритм на примере двух чисел a и b.

Алгоритм вычисления НОД и НОК

Шаг 1. Разложить числа a и b на простые сомножители:

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m}; \quad b = q_1^{\beta_1} q_2^{\beta_2} \dots q_l^{\beta_l}.$$

Шаг 2. Составить из простых делителей множества:

$$P = \{p_1, p_2, \dots, p_m\}; \quad Q = \{q_1, q_2, \dots, q_l\}.$$

Шаг 3. Найти пересечение и объединение множеств P и Q:

$$C = P \cap Q = \{c_1, c_2, \dots, c_k\}; \quad U = P \cap Q = \{u_1, u_2, \dots, u_n\}.$$

Шаг 4. Вычислить $\text{НОД}(a, b)$ и $\text{НОК}(a, b)$ по формулам:

$$\text{НОД}(a, b) = c_1^{\nu_1} c_2^{\nu_2} \dots c_m^{\nu_m}, \quad (1.5.3)$$

$$\text{НОК}(a, b) = u_1^{\mu_1} u_2^{\mu_2} \dots u_n^{\mu_n}, \quad (1.5.4)$$

где $\nu_i = \min\{\alpha_i, \beta_i\}$, а $\mu_i = \max\{\alpha_i, \beta_i\}$ для делителей c_i и u_i, соответственно.

Пример 1.5.2. Найти НОД и НОК чисел 12, 16 и 42 (Пример 1.3.2).

Решение

1. Запишем канонические разложения заданных чисел:

$$12 = 2^2 \cdot 3; \quad 16 = 2^4; \quad 42 = 2 \cdot 3 \cdot 7.$$

2. Составим множества делителей чисел, и определим их пересечение и объединение:

$$P_1 = \{2,3\}, P_2 = \{2\}, P_3 = \{2,3,7\} \quad \Rightarrow \quad C = \{2\}, \ U\{2,3,7\}.$$

3. По формулам (1.5.3) и (1.5.4) найдем НОД и НОК:

$$\text{НОД}(12,16,42) = 2^1 = 2;$$

$$\text{НОД}(12,16,42) = 2^4 \cdot 3^1 \cdot 7^1 = 336.$$

Ответ: $\text{НОД}(12,16,42) = 2$,
$\text{НОК}(12,16,42) = 336$. ■

1.6. Сравнения по модулю

Множество целых чисел бесконечно. Однако отношение делимости целых чисел позволяет разбить это множество на конечное число классов. Например, отношение делимости на число 2 разбивает все целые числа на числа четные и нечетные. Этот простой пример допускает следующее обобщение.

Опр. 1.6.1 Два целых числа a и b, называются **сравнимыми по модулю** $m \in \mathbb{N}$, если они при делении на m имеют один и тот же остаток.

Отношение сравнимости чисел обозначается как

$$a \equiv b \pmod{m}.$$

Свойства сравнения по модулю

I. Если числа a и b сравнимы по модулю m, то модуль m делит их разность, причем верно и обратное:

$$a \equiv b \pmod{m} \quad \Leftrightarrow \quad m|(a-b). \qquad (1.6.1)$$

II. Отношение сравнения по модулю есть отношение эквивалентности:

$a \equiv a \pmod{m}$, (рефлективность)

$a \equiv b \pmod{m} \ \Leftrightarrow \ b \equiv a \pmod{m}$, (симметричность)

$a \equiv b \pmod{m}, \ b \equiv c \pmod{m} \ \Rightarrow \ a \equiv c \pmod{m}$. (транзитивность)

III. Если $a \equiv b \pmod m$ и $c \equiv d \pmod m$, то справедливы следующие сравнения:

$$a + c \equiv b + d \pmod m, \quad (1.6.2)$$
$$a - c \equiv b - d \pmod m, \quad (1.6.3)$$
$$a \cdot c \equiv b \cdot d \pmod m. \quad (1.6.4)$$

IV. Если $a \equiv b \pmod m$ и $P(x)$ – некоторый многочлен с целочисленными коэффициентами, то

$$P(a) \equiv P(b) \pmod m. \quad (1.6.5)$$

V. Обе части сравнения можно поделить на их общий делитель, если он является взаимнопростым с модулем:

$$da \equiv db \pmod m, \ \text{НОД}(d, m) = 1 \quad \Rightarrow \quad a \equiv b \pmod m.$$

VI. Обе части сравнения и модуль можно поделить на их общий делитель:

$$da \equiv db \pmod{dm} \Rightarrow a \equiv b \pmod m.$$

VII. Если $a \equiv b \pmod m$, то $\text{НОД}(a, m) = \text{НОД}(b, m)$.

VIII. Если $a \equiv b \pmod m$ и $d|m$, то $a \equiv b \pmod d$.

Пример 1.6.1. Имеет ли уравнение
$x^2 - 5y^2 = 3$
целые решения?

Решение

Пусть (a, b) некоторое целое решение:

$$a^2 - 5b^2 = 3.$$

Тогда, так как $a^2 - 3 = 5b^2$, то $a^2 \equiv 3 (\text{mod } 5)$.

Все целые числа разбиваются на группы чисел, в каждой из которых все числа сравнимы по модулю 5 только либо с $0, 1, 2, 3$ или 4. Проанализируем квадраты этих чисел:

$$0^2 = 0,$$
$$1^2 = 1,$$
$$2^2 = 4,$$
$$3^2 = 9 \equiv 4 (\text{mod } 5),$$
$$4^2 = 16 \equiv 1 \pmod 5.$$

Таким образом, ни один из квадратов целого числа a не может быть сравним с числом 3 по модулю 5, значит наше предположение о существовании целочисленного решения заданного уравнения неверно.

Ответ: уравнение целочисленных решений не имеет. ■

1.7. Классы вычетов

Согласно свойству II отношение сравнения по фиксированному модулю m есть отношение эквивалентности, а значит, все множество целых чисел разбивается на конечное число непересекающихся классов эквивалентности.

Опр. 1.7.1 Все числа, сравнимые по заданному модулю m, образуют **класс вычетов по модулю m.** При этом любое число a из класса называется **вычетом по модулю m.**

Из определения следует, что класс вычетов образуют все числа, которые при делении на число m дают один и тот же остаток r. Безусловно, при заданном модуле m имеется ровно m различных остатков, а значит, и классов вычетов, которые будем обозначать чертой сверху:

$\bar{0}, \bar{1}, \bar{2}, \dots, \overline{m-1}.$

Опр. 1.7.2 Множество всех чисел, принадлежащих разным классам вычетов, называется **полной системой вычетов.**

В качестве представителя класса вычетов можно выбирать любое число, Так полными системами вычетов по модулю 5 являются:

$\{0,1,2,3,4\}, \{1,2,3,4,5\}, \{-2,-1,0,1,2\}$ и др.

Теорема 1.7.1

Если $\text{НОД}(a,m) = 1$ и x пробегает полную систему вычетов по модулю m, то числа $ax + b$, где $b \in \mathbb{Z}$, также пробегают полную систему вычетов по модулю m.

Согласно свойству VII числа, принадлежащие одному классу вычетов, имеют с модулем m один и тот же делитель. Рассмотрим только те классы вычетов, для которых $\text{НОД}(a,m) = 1$, то есть которые взаимнопросты с модулем.

Опр. 1.7.3 Множество всех чисел, принадлежащих различным классам вычетов, которые взаимнопросты с модулем m, называется **приведенной системой вычетов**.

Пример 1.7.1. Пусть $m = 24$. Тогда полная система вычетов может быть записана как

$$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23\},$$

при этом множество

$$\{1, 5, 7, 11, 13, 17, 19, 23\}$$

является приведенной системой.

■

Теорема 1.7.2

Если $\text{НОД}(a, m) = 1$ и x пробегает приведенную систему вычетов по модулю m, то числа $ax + b$, где $b \in \mathbb{Z}$, также пробегают приведенную систему вычетов по модулю m.

Приведенные системы вычетов, впервые рассмотренные Л. Эйлером, дают возможность работать с классами вычетов не только по простым, но и по составным модулям.

1.8. Функция Эйлера

Опр. 1.8.1 **Функцией Эйлера** $\varphi(m)$ называется число классов в приведенной системе вычетов по модулю m.

Для небольших аргументов значения функции Эйлера можно определить непосредственно, выписывая явный вид приведенной системы.

Пример 1.8.1. Некоторые значения функции Эйлера:

$$\begin{aligned} m = 2 &\Rightarrow \{1\} \Rightarrow \varphi(2) = 1, \\ m = 3 &\Rightarrow \{1, 2\} \Rightarrow \varphi(3) = 2, \\ m = 4 &\Rightarrow \{1, 3\} \Rightarrow \varphi(3) = 2, \\ m = 24 &\Rightarrow \{1, 5, 7, 11, 13, 17, 19, 23\} \Rightarrow \varphi(24) = 8. \end{aligned}$$

■

В общем случае вычисление значений функции Эйлера основано на использовании следующих результатов.

Теорема 1.8.1

Если аргумент функции Эйлера $m = p$ – простое число, то справедливы соотношения:

$$\varphi(p) = p - 1, \quad (1.8.1)$$

$$\varphi(p^k) = p^k - p^{k-1}, \quad \forall k \in \mathbb{N}. \quad (1.8.2)$$

Теорема 1.8.2 (*свойство мультипликативности*)

Если a и b взаимнопростые числа, то имеет место соотношение

$$\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b). \quad (1.8.3)$$

Теорема 1.8.3

Для функции Эйлера справедлива формула:

$$\varphi(a) = a \prod_{p|a} \left(1 - \frac{1}{p}\right), \quad (1.8.4)$$

где произведение производится по всем различным простым делителям числа a.

Теорема 1.8.4 (*теорема Эйлера*)

Для любого целого числа a, взаимнопростого с модулем m, выполняется сравнение:

$$a^{\varphi(m)} \equiv 1 \pmod{m}. \quad (1.8.5)$$

Следствие (*малая теорема Ферма*)

Если $\text{НОД}(a, p) = 1$, где p – простое число, то

$$a^{p-1} \equiv 1 \pmod{p}. \quad (1.8.6)$$

Пример 1.8.1. Найти $\varphi(100)$.

Решение

Предварительно разложим число 100 на простые сомножители: $100 = 2^2 5^2$.

Тогда по формуле (1.8.4) находим:

$$\varphi(100) = 100 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{5}\right) = 100 \cdot \frac{1}{2} \cdot \frac{4}{5} = 40.$$

Ответ: 40. ■

Пример 1.8.2. Найти последние две цифры числа 2^{100}.

Решение

Заметим, что последние две цифры любого целого числа совпадают с его вычетом по модулю 100. Поэтому, по-существу, требуется найти

$$x \equiv 2^{100} \pmod{100}.$$

Поделим обе части сравнения и модуль на 4 (общий делитель):

$$\frac{x}{4} \equiv 2^{98} \pmod{25}.$$

Далее непосредственно находим:

$$2^{10} = 1024 \equiv -1 \pmod{25}; \quad 2^8 = 256 \equiv 6 \pmod{25},$$

поэтому

$$2^{98} \equiv (-1)^9 \cdot 6 \pmod{25} = -6 \pmod{25}.$$

Таким образом, получаем

$$\frac{x}{4} \equiv -6 \pmod{25} \Rightarrow x \equiv -24 \pmod{100} \Rightarrow x \equiv 76 \pmod{100}.$$

Ответ: 76. ■

1.9. Сравнения первой степени

Опр. 1.9.1 **Сравнением первой степени** называется сравнение вида

$$ax \equiv b \pmod{m}. \qquad (1.9.1)$$

Здесь требуется найти все различные классы вычетов $\bar{x}$ по модулю m, удовлетворяющих сравнению (1.9.1).

Теорема 1.9.1

Сравнение первой степени разрешимо тогда и только тогда, когда $\text{НОД}(a,m)$ делит b, причем количество решений совпадает с $\text{НОД}(a,m)$.

Следствие

Если $\text{НОД}(a,m) = 1$, то сравнение первой степени имеет единственное решение.

Решение сравнений, по-существу, связано с его преобразованием к простейшему виду с использованием свойств сравнений. Цель преобразований – получить перед неизвестным x коэффициент равный 1.

Пример 1.9.1. Решить сравнение

$$38x \equiv 4 \pmod{26}.$$

Решение

В первую очередь уменьшим коэффициенты сравнения, заменяя их наименьшими представителями соответствующего класса вычетов по модулю 26:

$$38x \equiv 4 \pmod{26} \quad \Rightarrow \quad 12x \equiv 4 \pmod{26}.$$

Заметим, что $\text{НОД}(12,4) = 2$ и $2|(b = 4)$. Поэтому согласно теореме 1.9.1 сравнение разрешимо и имеет два решения.

Коэффициенты и модуль кратны 2. После деления на 2 получим:

$$6x \equiv 2 \pmod{13}.$$

Далее, используя свойства сравнений и заменяя коэффициенты представителями их класса вычетов, приводим сравнение к простейшему виду:

$$6x \equiv 2 \pmod{13} \Rightarrow 12x \equiv 4 \pmod{13} \Rightarrow -x \equiv 4 \pmod{13} \Rightarrow$$
$$\Rightarrow x \equiv -4 \pmod{13} \Rightarrow x \equiv 9 \pmod{13}.$$

Возвращаясь к исходному модулю, находим два решения:

$$x_1 \equiv 9 \pmod{26}, \qquad x_2 \equiv (9 + 13) \pmod{26} \equiv 22 \pmod{26}.$$

Ответ: $\{9 \pmod{26},\ 22 \pmod{26}\}$. ■

Следует отметить тесную связь между линейными диофантовыми уравнениями и сравнениями первой степени, что позволяет применять эффективные методы теории вычетов к решению диофантовых уравнений. Рассмотрим в качестве примера решение диофантового уравнения из задачи 1.4.1.

Пример 1.9.2. Решить диофантовое уравнение

$$12x + 7y = 43.$$

Решение

Перепишем уравнение в виде

$$12x - 43 = -7y.$$

Таким образом, переменная x принадлежит классу вычетов, который является решением следующего сравнения:

$$12x \equiv 43 \pmod 7.$$

Используя свойства сравнений, находим

$$12x \equiv 43 \pmod 7 \Rightarrow 5x \equiv 1 \pmod 7 \Rightarrow 15x \equiv 3 \pmod 7 \Rightarrow$$
$$\Rightarrow x \equiv 3 \pmod 7.$$

В качестве частного решения выберем наименьшее положительное целое: $x = 3$. Подставляя это значение в исходное уравнение, находим вторую переменную:

$7y = 43 - 12 \cdot 3 = 7 \Rightarrow y = 1.$

Пара чисел $(3, 1)$ является частным решением заданного диофантового уравнения (именно она является решением задачи 1.4.1). Общее решение уравнения записывается в виде (1.4.6):

$$x = 3 - 7t, y = 1 + 12t, \text{ где } t \in \mathbb{Z}.$$

Ответ: $(x, y) = \{(3 - 7t, 1 + 12t) | \ t \in \mathbb{Z}\}$. ■

1.10. Китайская теорема об остатках

Рассмотрим задачу о поиске множества целых чисел, которые удовлетворяют одновременно нескольким сравнениям. Простейшая система сравнений имеет вид

$$\begin{cases} x \equiv a_1 \pmod{m_1}, \\ x \equiv a_2 \pmod{m_2}, \\ \ldots\ldots\ldots\ldots\ldots \\ x \equiv a_k \pmod{m_k}. \end{cases} \qquad (1.10.1)$$

В случае взаимно простых модулей решение этой системы может быть найдено с помощью так называемой *китайской теоремы об остатках.*

Теорема 1.10.1 (*китайская теорема об остатках*)

Если модули сравнений $m_1, m_2, \ldots, m_k$ в системе (1.10.1) попарно просты, то система разрешима и решение может быть представлено в виде

$$x \equiv x_0 (\mathrm{mod}\, M), \qquad (1.10.2)$$

где

$$x_0 = M_1 b_1 + M_2 b_2 + \cdots + M_k b_k,$$
$$M = \text{НОК}(m_1, m_2, \ldots, m_k) = m_1 m_2 \ldots m_k,$$
$$M_l = M / m_l, \quad 1 \le l \le k,$$

а числа b_l являются частными решениями сравнений

$$M_l b_l \equiv a_l \ (\mathrm{mod}\, m_l), \quad 1 \le l \le k.$$

Пример 1.10.1. Решить систему сравнений

$$\begin{cases} x \equiv 3 (\mathrm{mod}\ \ 7), \\ x \equiv 2 (\mathrm{mod}\ 11), \\ x \equiv 1 (\mathrm{mod}\ 13). \end{cases}$$

Решение

Модули сравнений $7, 11, 13$ попарно просты, поэтому решение системы можно искать с помощью китайской теоремы об остатках.

Последовательно находим:

$$M = 7 \cdot 11 \cdot 13 = 1001;$$
$$M_1 = 11 \cdot 13 = 143, \ M_2 = 7 \cdot 13 = 91, \ M_3 = 7 \cdot 11 = 77.$$

Далее решаем вспомогательные сравнения и находим числа b_l, как некоторые частные решения (например, наименьшие по модулю):

$$M_1 b_1 \equiv a_1 \ (\mathrm{mod}\, m_1) \ \Rightarrow \ 143 b_1 \equiv 3 (\mathrm{mod}\, 7) \ \Rightarrow \ b_1 = 1;$$
$$M_2 b_2 \equiv a_2 \ (\mathrm{mod}\, m_2) \ \Rightarrow \ 91 b_2 \equiv 2 (\mathrm{mod}\, 11) \ \Rightarrow \ b_2 = -3;$$
$$M_3 b_3 \equiv a_3 \ (\mathrm{mod}\, m_3) \ \Rightarrow \ 77 b_3 \equiv 1 (\mathrm{mod}\, 13) \ \Rightarrow \ b_3 = -1.$$

Наконец, вычисляем число x_0 и записываем решение исходной системы в виде класса вычетов (1.10.2):

$$x_0 = 143 \cdot 1 + 91 \cdot (-3) + 77 \cdot (-1) = -207;$$
$$x \equiv -207 \ (\mathrm{mod}\, 1001) \equiv 794 \ (\mathrm{mod}\, 1001).$$

Ответ: $x \equiv 794 \ (\mathrm{mod}\, 1001)$. ■

ГЛАВА 2

КРИПТОГРАФИЯ И СОВРЕМЕННЫЕ КРИПТОСИСТЕМЫ

2.1. Основные понятия и методы криптографии

Криптография – это дисциплина, которая занимается разработкой методов преобразования информации с целью ее защиты от незаконного использования.

Шифрование – процесс применения шифра-преобразования к защищаемой информации.

Шифротекст (или *криптограмма*) – зашифрованное сообщение.

Дешифрование – процесс обратный шифрованию, заключающийся в восстановлении исходной информации.

Современная криптография является областью знаний, связанной с решением таких проблем безопасности как

- конфиденциальность;
- целостность;
- аутентификация;
- невозможность отказа от авторства.

Шифр – семейство обратимых преобразований, каждое из которых определяется некоторым параметром, называемым *ключом*, а также порядком применения данного преобразования, называемым *режимом шифрования*. Каждое преобразование однозначно определяется ключом и описывается *некоторым криптографическим алгоритмом*. Один и тот же криптографический алгоритм может применяться для шифрования в различных режимах. Выбор конкретного решения зависит от ситуации.

Следует отметить, что ключи и алгоритмы шифрования и дешифрования могут отличаться друг от друга. Пару алгоритмов шифрования и дешифрования называют *криптосистемой*, а реализующие их устройства или приспособления – *шифротехникой*.

Рассмотрим некоторые типы шифров, которые принято относить к *классическим шифрам*. Они различаются по типу преобразования, осуществляемого с открытым текстом.

Шифр замены

Шифром замены называется шифр, при котором фрагменты открытого текста заменяются их эквивалентами в шифротексте. Это простейший и наиболее популярный класс шифров. Известными историческими примерами являются:

- шифр Цезаря;
- “цифирная азбука” Петра 1;
- “Великий шифр” Россиньоля;
- “пляшущие человечки” А. Конан-Дойля.

Определим математическую модель шифра замены.

Будем считать, что открытые и шифрованные тексты являются словами в алфавитах A и B, причем мощности (число символов) алфавитов равны n и m, соответственно.

Далее, обозначим через A^* и B^* множества слов конечной длины в алфавитах A и B. Тогда исходный текст X и шифрованный тест Y будут подмножествами A^* и B^*:

$$X \subseteq A^*, \qquad Y \subseteq B^*.$$

Перед шифрованием текст разбивается на фрагменты, которые называются *шифровеличинами*. При шифровании шифровеличины заменяются эквивалентами, которые принято называть *шифрообозначениями*. Безусловно, они являются подмножествами или элементами множеств A^* и B^*.

Пусть $U = \{u_1, u_2, \dots, u_N\}$ – множество всех возможных шифровеличин, а $V = \{v_1, v_2, \dots, v_M\}$ – множество всех возможных щифрообозначений. Требование однозначности дешифрования будет выполнено, если мощности множеств будут удовлетворять неравенствам

$$N \geq n, \qquad M \geq m, \qquad M \geq N.$$

Из последнего неравенства следует, что множество шифрообозначений можно разбить на N непересекающихся подмножеств:

$$V = \bigcup_{i=1}^{N} V_i^{(\alpha)}.$$

Здесь верхний индекс α нумерует различные разбиения. В результате имеем семейство биекций:

$$\varphi^{(\alpha)}: U \to \{V_1^{(\alpha)}, V_2^{(\alpha)}, \dots, V_N^{(\alpha)}\},$$

где

$$\varphi^{(\alpha)}(u_i) = V_i^{(\alpha)}, i = \overline{1, N}.$$

В случае $N = M$ получаем однозначное разбиение.

Криптоанализ одноалфавитных шифров замены основан на изучении частоты появления отдельных букв или их сочетаний (биграмм, триграмм и т.п.) в данном языке. Таблицы таких частот составлены для всех известных языков. Классические примеры такого криптоанализа, основанного на исследовании частот знаков в шифротекстах, можно встретить в литературе (рассказы Э. По “Золотой жук” и А. Конан-Дойля “Пляшущие человечки”).

Шифр перестановки

Шифром перестановки называется шифр, в котором буквы открытого текста лишь переставляются местами.

Одним из примеров шифров перестановки является *шифросистема Виженера*. Шифрование здесь осуществляется по таблице, представляющей собой квадратную матрицу порядка $n \times n$, где n – число символов алфавита. Каждая строка таблицы получается из предыдущей строки с помощью циклического сдвига на один символ в выбранном изначально направлении (влево или вправо). Обычно в алфавит включают дополнительно специальный символ ␣, соответствующий пробелу.

Далее выбирается ключевое слово или фраза.

Алгоритм шифрования состоит из нескольких этапов:

1) под каждой буквой исходного сообщения последовательно подписываются буквы ключа, возможно с повторением;
2) каждая буква шифротекста находится по таблице как буква, стоящая на пересечении столбца и строки, которые последовательно определяются по буквам исходного текста и ключа, соответственно.

Дешифрование производится в обратном порядке, а именно в строке, соответствующей очередной букве ключа, находим букву шифротекста, на которую указывает буква ключа. Тогда буква исходного текста восстанавливается как первая буква столбца, содержащего найденную букву шифротекста.

Помимо таблиц изменять порядок букв можно с помощью специально изготовленных трафаретов, классическим примером которых является *решетка Кардано*. При наложении на лист бумаги открытыми остаются лишь некоторые позиции. Сообщение вписывается в отверстия трафарета. При расшифровке на текст шифротекста, накладывается трафарет, после чего считывается текст сообщения. Возможны различные комбинации применения трафаретов, например, с поворотом и др.

2.2. RSA криптосистема

Статья Диффи и Хеллмана, вышедшая в 1976 году, перевернула представления о криптографических системах, заложив основы криптографии с открытым ключом. Разработанный впоследствии алгоритм Диффи-Хеллмана позволял двум сторонам получить общий секретный ключ, используя незащищенный канал связи. Однако этот алгоритм не решал проблему аутентификации. Без дополнительных средств пользователи не могли достоверно знать, с кем они сгенерировали ключ.

Изучив эту статью, трое ученых Рональд Ривест, Ади Шамир и Леонард Адлеман из Массачусетского технологического института (США) приступили к поискам математического алгоритма, который позволял бы реализовать идею, сформулированную Диффи и Хеллманом. После изучения более 40 возможных вариантов они остановились на алгоритме, в основе которого лежала процедура разложения натурального числа на простые сомножители. Этот алгоритм в дальнейшем получил название RSA криптосистемы (по первым буквам фамилий авторов алгоритма).

Интересно, что в августе 1977 года в колонке «Математические игры» Мартина Гарднера в научно-популярном журнале Scientific America с разрешения Рональда Ривеста появилось первое описание RSA криптосистемы. Читателям было предложено расшифровать английскую фразу, зашифрованную описанным алгоритмом. В качестве открытых параметров системы были использованы число $n = 11438 \ldots 541$, имеющее 129 знаков и известное как RSA-129, и простое число $e = 9007$. За расшифровку была обещана награда в $100\$$. По заявлению Ривеста для разложения числа RSA-129 на простые сомножители потребовалось бы $40 \cdot 10^{12}$ лет. Однако приблизительно через 15 лет, а именно, 3 сентября 1993 года было объявлено о старте проекта распределенных вычислений с координацией через электронную почту по нахождению сомножителей числа RSA-129 с целью решения головоломки. На протяжении полугода более 600 добровольцев из 20 стран жертвовали процессорным временем работы своих 1600 персональных компьютеров. В результате искомое разложение было найдено, а сообщение расшифровано. Полученную награду победители пожертвовали в *Фонд свободного программного обеспечения*.

Полное описание алгоритма было опубликовано в 1978 году, а патент на изобретение был выдан в 1983 году.

В 1989 году RSA криптосистема начинает использоваться в зарождающейся сети Интернет, а с 1990 года и Министерством обороны США.

Алгоритм RSA криптосистемы

1. Исходный текст перевести в числовую форму.
Метод перевода считается известным. В результате текст представляется в виде одного большого числа x.
2. Выбрать основное число алгоритма N, которое представляет собой произведение двух больших простых чисел

$$N = p \cdot q, \tag{2.2.1}$$

причем $p, q \nmid x$ и

$$0 < x < N.$$

3. Вычислить значение функции Эйлера для числа N:

$$\varphi(N) = \varphi(pq) = \varphi(p)\varphi(q) = (p-1)(q-1). \tag{2.2.2}$$

4. Выбрать некоторое число e, которое является взаимнопростым с числом $\varphi(N)$ (2.2.2):
$\text{НОД}(e, \varphi(N)) = 1.$
Обычно в качестве этого числа выбирается простое число с небольшим количеством цифр, например, из класса чисел Ферма $\{17, 257, 65537\}$.
5. Найти число d, которое является взаимно обратным с e по модулю $\varphi(N)$:

$$d \cdot e \equiv 1 \bmod \varphi(N). \tag{2.2.3}$$

Заметим, что это линейное сравнение имеет единственное решение. Пара $\{e, N\}$ представляет собой открытый, а пара $\{d, N\}$ закрытый RSA ключ. Число d держится в секрете. Чтобы найти d, надо определить модуль сравнения (2.2.3) – $\varphi(N)$, для вычисления которого по формуле (2.2.2), необходимо знать разложение числа N на простые сомножители (2.2.1). В свою очередь, алгоритм разложения числа на множители не является полиномиальным, и для больших чисел представляет собой чрезвычайно сложную вычислительную задачу.

6. Зашифровать сообщение x по формуле

$$y = E[x] \equiv x^e \bmod N. \qquad (2.2.4)$$

Важно, что отправитель А посылает зашифрованное сообщение получателю В *по открытому каналу*.

7. После получения шифротекста y дешифрование производится по формуле

$$x = D[y] \equiv y^d \bmod N. \qquad (2.2.5)$$

Действительно, согласно теореме Эйлера 1.8.4 в предположении, что число x не делится на числа p и q, следовательно, $\text{НОД}(x, N) = 1$, имеем

$x^{\varphi(N)} \equiv 1 \bmod N.$

Таким образом,

$y^d \bmod N \equiv x^{ed} \bmod N \equiv x^{k\varphi(N)+1} \bmod N \equiv x \bmod N.$

ГЛАВА 3

ГРУППЫ, КОЛЬЦА, ПОЛЯ

3.1. Основные понятия общей алгебры

Всякую функцию типа

$$\varphi : \underbrace{M \times M \times \ldots \times M}_{n \text{ раз}} \to M$$

будем называть n-арной операцией, определенной на множестве M. При этом число аргументов n называется ***арностью*** операции. В частности, при $n = 2$ имеем бинарную операцию

$$\varphi : M \times M \to M \;\Rightarrow\; w = \varphi(u, v).$$

Опр. 3.1.1 Множество M вместе с заданной на нем совокупностью операций $\Omega = \{\varphi_1, \varphi_2, \ldots, \varphi_m\}$ называется ***алгеброй*** $A =< M, \Omega >$. При этом само множество M называется ***носителем алгебры***, а совокупность операций Ω – ***сигнатурой алгебры***.

Множество $M' \subseteq M$ называется *замкнутым* относительно некоторой операции φ, определенной на M, если значения φ на аргументах из M' сами принадлежат M', т.е.

$$\varphi(M') \in M'.$$

Если M' замкнуто относительно всех операций из сигнатуры алгебры $\Omega = \{\varphi_1, \varphi_2, \ldots, \varphi_m\}$, то M' называется ***подалгеброй*** алгебры A.

Пример 3.1.1. Для алгебры $A =< \boldsymbol{R}, \{\cdot, +\} > \Rightarrow M = \boldsymbol{R},\ \Omega = \{\cdot, +\}$.
Так как обе операции бинарные, то тип алгебры $A(2,2)$. Такая алгебра называется полем действительных чисел.

Очевидно, что $A' =< \boldsymbol{Z}, \{\cdot, +\} >$ есть подалгебра A. ■

Пример 3.1.2. Пусть задано некоторое множество M, а $B(M)$ – его булеан. Тогда алгебра $B =< B(M); \cup, \cap, \bar{} >$ имеет сигнатуру $\Omega = \{\cup, \cap, \bar{}\}$, а ее тип $(2,2,1)$. Данная алгебра называется *булевой алгеброй множеств или алгеброй Кантора.*

■

Если M – конечное множество, то бинарные операции могут быть заданы таблицами.

Пример 3.1.3. Рассмотрим квадрат с вершинами в точках A_1, A_2, A_3, A_4 и повороты вокруг центра квадрата, переводящие вершины друг в друга. Зафиксируем некоторое направление поворота как положительное. Существует всего 4 различных поворота, переводящих вершины в себя, а именно, повороты на 0, $\frac{\pi}{2}$, π, $\frac{3\pi}{2}$ радиан. Таким образом, получаем алгебру с носителем $M = \{A_1, A_2, A_3, A_4\}$ и 4 унарными операциями-поворотами $\Omega = \{\lambda, \beta, \gamma, \delta\}$. Таблица имеет вид:

	α	β	γ	δ
A_1	A_1	A_2	A_3	A_4
A_2	A_2	A_3	A_4	A_1
A_3	A_3	A_4	A_1	A_2
A_4	A_4	A_1	A_2	A_3

Тип алгебры (1, 1, 1, 1). У этой алгебры нет подалгебр.

■

Пример 3.1.4. Рассмотрим множество поворотов $\Omega = \{\lambda, \beta, \gamma, \delta\}$ из предыдущего примера с бинарной операцией: $\circ$ – композицией преобразований. Тогда $A = <\Omega; \circ>$ есть алгебра поворотов с носителем Ω и сигнатурой, состоящей из одной операции $\{\circ\}$. Тип алгебры (2). Ее таблица Кэли имеет вид:

$\circ$	α	β	γ	δ
α	α	β	γ	δ
β	β	γ	δ	α
γ	γ	δ	α	β
δ	δ	α	β	γ

Множество $\{\alpha, \gamma\}$ образует подалгебру алгебры $<\Omega; \circ>$:

$\circ$	α	γ
α	α	γ
γ	γ	α

■

Далее рассмотрим различные алгебры с одной операцией.

Опр. 3.1.2 Алгебра вида $< M, f_2 >$, где f_2 – некоторая бинарная операция $f_2 : M^2 \to M$ называется ***группоидом***. Если f_2 – операция типа умножения, то группоид называется *мультипликативным*, а если тип сложения – ***аддитивным***.

Для бинарной операции удобно ввести некоторые общие обозначения:

$$af_2b \equiv a * b .$$

Опр. 3.1.3 Группоид называется *коммутативным*, если

$$a*b = b*a , \qquad (3.1.1)$$

и *ассоциативным*, если

$$a*(b*c) = (a*b)*c . \qquad (3.1.2)$$

Важным примером ассоциативного группоида является множество отображений с композицией. Примером некоммутативного группоида является множество матриц с операцией – матричное умножение. Пример не ассоциативного группоида – булеан $B(U)$ с декартовым произведением $\times$.

Опр. 3.1.4 Элемент e группоида $< M; * >$ называется ***единичным*** для операции $*$, если выполняются равенства

$$a*e = e*a = a . \qquad (3.1.3)$$

Для мультипликативных группоидов e есть 1, а для аддитивных – 0.

Опр. 3.1.4 Группоид с ассоциативной операцией $*$ называется ***полугруппой***, а полугруппа с единицей называется ***моноидом***.

Пример 3.1.5. Рассмотрим следующие группоиды на множестве $\mathbb{Z}$:

1) $< \boldsymbol{Z}; + >$ – полугруппа,
т.к. $(a+b)+c = a+(b+c)$ для любых чисел из $\mathbb{Z}$.

2) $< \boldsymbol{Z}; - >$ – группоид, но не полугруппа,
т.к. $(a-b)-c \neq a-(b-c)$ и нет ассоциативности. ■

Важным примером полугрупп с точки зрения приложений является следующая алгебраическая система.

Пусть имеется множество символов $S = \{s_1, s_2, ...\}$, которые назовем ***алфавитом***. Тогда некоторая упорядоченная совокупность символов образует ***слово***. Для удобства вводится в качестве отдельного символа пробел ␣. Рассмотрим множество всех символов S^*. Введем над символами следующую бинарную операцию:

$$U \circ V = UV . \qquad (3.1.4)$$

Ее называют ***конкатенацией*** (другие названия - сцепление, приписывание, слияние). Очевидно, что эта операция–слияние не коммутативна, но ассоциативна. Следовательно, наш группоид $< S^*, \circ >$ является полугруппой. Она называется ***свободной полугруппой***. Безусловно, можно выделить не все слова, а только их часть $L \subseteq S^*$. Такое подмножество удобно называть ***языком***.

Понятие языка можно ввести на любом множестве, в частности, на двухэлементном множестве $\{0,1\}$. На языке можно вводить различные грамматики типа $a^n b^m$, $b^n a b^m$ и т.п. Развитие такой алгебраической теории приводит нас к ***теории автоматов***.

Всякую полугруппу можно получить из свободных полугрупп путем задания так называемых определяющих соотношений:

$$a^2 = a, \quad ab = ba \quad \text{и т.п.}$$

Из любого слова, используя определяющие соотношения, можно получить эквивалентные слова.

Намного более сложной является обратная задача – установление эквивалентности двух слов. Эта задача приводит к ***теории алгоритмов***.

3.2. Группы и подгруппы

Опр. 3.2.1 Пусть G - алгебра с одной бинарной операцией $\circ$. Тогда алгебра G называется ***группой***, если выполняются следующие условия:

G_1: $a \circ (b \circ c) = (a \circ b) \circ c, \quad \forall a, b, c \in G;$

G_2: $\exists e \Rightarrow a \circ e = e \circ a = a, \quad \forall a \in G;$

G_3: $\forall a \ \exists a^{-1} \Rightarrow a^{-1} \circ a = a \circ a^{-1} = e.$

В случае, если групповая операция обладает дополнительно свойством коммутативности:

$$a \circ b = b \circ a, \quad \forall a, b \in G,$$

то группа называется *коммутативной* или *абелевой*.

С целью упрощения записи часто символ групповой операции опускают:

$$a \circ b \equiv ab.$$

Общие свойства групп

I. Любая группа содержит только один единичный элемент e.

II. Для любого элемента группы a существует только один обратный элемент a^{-1}.

III. В группе выполняется *правило сокращения*:
$ab = ac \Leftrightarrow b = c.$

IV. Теорема перегруппировки. Пусть g_k некоторый элемент группы G. Тогда множество элементов $g_k G$ совпадает с G:
$g_k G = G.$

Пример 3.2.1. Множество целых чисел $\mathbb{Z}$ образуют абелеву группу относительно операции сложения:

$$a \circ b \equiv a + b.$$

Здесь $e \equiv 0$, а $a^{-1} = -a$. ■

Пример 3.2.2. Полная система классов вычетов по простому модулю p является абелевой группой относительно как операции сложения (*аддитивная группа* $\mathbb{Z}_p$), так и умножения (*мультипликативная группа* $\mathbb{Z}_p^*$). ■

Пример 3.2.3. Полная система классов вычетов по составному модулю m является аддитивной группой $\mathbb{Z}_m$. Мультипликативной группой она не является, так как не все элементы обратимы (нарушается условие G_3). Однако уже *приведенная* система классов вычетов (причем по любому модулю) представляет собой мультипликативную группу $\mathbb{Z}_m^*$. ■

Опр. 3.2 Число элементов n конечной группы G называется ее ***порядком*** (обозначается как $|G|$):

$$|G| = n.$$

Пример 3.2.4. Для аддитивной и мультипликативной групп, которые можно образовать из классов вычетов по модулю m имеем:

$$|\mathbb{Z}_m| = m, \quad (3.2.1)$$

$$|\mathbb{Z}_m^*| = \varphi(m). \quad (3.2.2)$$

■

Конечные группы малых порядков удобно задавать с помощью таблиц Кэли.

Опр. 3.2.3 Подмножество H группы G, которое само образует группу относительно общей групповой операции $\circ$, называется ***подгруппой***.

У любой группы G всегда есть две подгруппы – пустое множество $\varnothing$ и сама группа G. Эти подгруппы называются *несобственными*, а все остальные – *собственными*.

Пусть a – некоторый элемент группы G. Действуя элементом на себя, приходим к понятию степени:

$$\underbrace{a \circ a \circ \ldots \circ a}_{m \text{ раз}} = a^m. \quad (3.2.3)$$

Можно показать, что в случае конечных групп всегда найдется натуральное число l такое, что

$$a^l = e. \quad (3.2.4)$$

Опр. 3.2.4 Наименьшее число l, для которого справедливо соотношение (3.2.4), называется ***порядком элемента*** a.

Следует отметить, что элементы бесконечных групп могут не иметь конечного порядка.

Теорема 3.2.1

Пусть элемент a группы G имеет порядок l. Тогда множество элементов $\{a, a^2, a^3, \ldots, a^l\}$ образует подгруппу группы G.

Таким образом, любой элемент группы порождает подгруппу.

Опр. 3.2.5 Пусть H подгруппа группы G, и $g \in G$. Тогда множество элементов Hg называется ***правым смежным классом***, а gH ***левым смежным классом***, которые порождаются подгруппой H и элементом g.

Теорема 3.2.2

Все смежные классы одного типа, порождаемые одной подгруппой H задают разбиение группы.

Действительно, любой элемент группы попадает в какой-нибудь смежный класс, например, порождаемый самим этим элементом. Остается только показать, что любые два смежных класса, имеющих общий элемент, совпадают.

Пример 3.2.5. Пусть $G = \mathbb{Z}$. Тогда $2\mathbb{Z}$ - подгруппа четных чисел, а $2\mathbb{Z} + 1$ – смежный класс нечетных чисел. Отметим, что этот смежный класс подгруппу не образует, так как не содержит единичного элемента (конкретно – числа 0) аддитивной группы $\mathbb{Z}$. ■

Опр. 3.2.6 Число смежных классов конечной группы G по подгруппе H называется ***индексом подгруппы*** H и обозначается как $[G:H]$ и $[H:G]$ для левых и правых смежных классов.

В соответствии с теоремой 3.2.1 имеет место следующее разложение группы G по подгруппе H:

$G = H \cup g_1H \cup g_2H \cup \ldots \cup g_kH.$

Оно задает определенное отношение эквивалентности для элементов группы. Аналогичное разбиение может быть записано и для правых смежных классов.

Теорема 3.2.3. 5*теорема Лагранжа*)

Порядок любой подгруппы H конечной группы G является делителем порядка группы G, причем

$$|G| = |H| \cdot [G:H] = |H| \cdot [H:G]. \qquad (3.2.3)$$

Следствие 1

Число левых и правых смежных классов группы G по одной подгруппе H равны.

Следствие 2

Всякая конечная группа простого порядка p не имеет собственных подгрупп.

Следствие 3

Для любого элемента a конечной группы G справедливо соотношение

$$a^{|G|} = e. \qquad (3.2.4)$$

Доказательство теоремы основано на проверке того факта, что все смежные классы (одного типа) по некоторой подгруппе H содержат одинаковое количество элементов группы.

3.3. Нормальные подгруппы и фактор-группы

Опр. 3.3.1 Два элемента a и b группы G называются ***сопряженными***, если найдется элемент группы g такой, что будет выполняться равенство

$$a = gbg^{-1}. \qquad (3.3.1)$$

Теорема 3.3.1

Отношение сопряжения элементов есть отношение эквивалентности:
$a = gbg^{-1} \Rightarrow a \sim b.$

Для доказательства теоремы необходимо проверить рефлексивность, симметричность и транзитивность отношения сопряженности элементов группы. Так для проверки свойства рефлексивности достаточно положить $g = e$. Далее находим:
$eae^{-1} = ae = a.$

Симметричность следует из обратимости всех элементов группы:

$$a = gbg^{-1} \Rightarrow b = g^{-1}a(g^{-1})^{-1} = \tilde{g}a\tilde{g}^{-1}, \text{ где } \tilde{g} = g^{-1}.$$

Аналогично проверяется и транзитивность:

$$b = g_1ag_1^{-1},\ c = g_2bg_2^{-1} \Rightarrow$$
$$\Rightarrow c = g_2(g_1ag_1^{-1})g_2^{-1} = (g_2g_1)a(g_2g_1)^{-1} = g_3ag_3^{-1}.$$

Как известно, всякое отношение эквивалентности разбивает множество на непересекающиеся классы. Таким образом, отношение сопряженности разбивает группу на *классы сопряженных элементов*.

Теорема 3.3.2

Если элемент a сопряжен элементу b, то и элемент a^k сопряжен элементу b^k.

Следствие

Сопряженные элементы имеют один порядок.

Пример 3.3.1. Рассмотрим группу подстановок третьего порядка S_3 с композицией подстановок в качестве групповой операции. Введем следующие обозначения для элементов группы:

$$\pi_1 = (1\,2\,3), \pi_2 = (2\,1\,3), \pi_3 = (1\,3\,2), \pi_4 = (3\,2\,1), \pi_5 = (3\,1\,2), \pi_6 = (2\,3\,1).$$

Разложим элементы по циклам:

$$\pi_1 = e, \pi_2 = (1\,2)\,(3), \pi_3 = (1)(2\,3), \pi_4 = (2)(1\,3), \pi_5 = (1\,3\,2), \pi_6 = (1\,2\,3).$$

Далее находим:

$$\pi_1^1 = e, \qquad \pi_2^2 = \pi_3^2 = \pi_4^2 = e, \qquad \pi_5^3 = \pi_6^3 = e.$$

Таким образом, группа S_3 разбивается на сопряженные классы:

$$S_3 = \{\pi_1\} \cup \{\pi_2, \pi_3, \pi_4\} \cup \{\pi_5, \pi_6\}.$$

■

Пусть H некоторая подгруппа группы G. Вообще говоря, элементы подгруппы H могут и не быть сопряженными друг с другом. В этом случае левые и правые смежные классы по подгруппе H не будут совпадать:

$$gHg^{-1} \neq H \;\Rightarrow\; gH \neq Hg.$$

Опр. 3.3.2 Подгруппа H называется ***нормальной подгруппой*** группы G (обозначается как $H \lhd G$), если выполняется равенство

$$gHg^{-1} = H. \qquad (3.3.2)$$

Заметим, что для нормальной подгруппы левые и правые смежные классы совпадают:

$$gH = Hg. \qquad (3.3.3)$$

Поэтому для абелевых (коммутирующих) групп все подгруппы автоматически являются нормальными.

Опр. 3.3.3 Группа G называется ***простой***, если она не имеет нормальных подгрупп.

Пример 3.3.1. Рассмотрим группу S_3 (см. пример 3.3.1). Множество $H = \{\pi_1, \pi_5, \pi_6\}$ образует подгруппу S_3, в чем нетрудно убедиться, построив для S_3 таблицу Кэли:

$\circ$	π_1	π_2	π_3	π_4	π_5	π_6
π_1	π_1	π_2	π_3	π_4	π_5	π_6
π_2	π_2	π_1	π_5	π_6	π_3	π_4
π_3	π_3	π_6	π_1	π_5	π_4	π_2
π_4	π_4	π_5	π_6	π_1	π_2	π_3
π_5	π_5	π_4	π_2	π_3	π_6	π_1
π_6	π_6	π_5	π_4	π_2	π_1	π_5

$\Rightarrow$

$\circ$	π_1	π_5	π_6
π_1	π_1	π_5	π_6
π_5	π_5	π_6	π_1
π_6	π_6	π_1	π_5

По таблице определяем левые и правые смежные классы для элементов, не входящих в подгруппу H (для элементов из H левые и правые смежные классы совпадают с H):

$$\pi_2 H = \pi_3 H = \pi_4 H = \{\pi_2, \pi_3, \pi_4\},$$
$$H\pi_2 = H\pi_3 = H\pi_4 = \{\pi_2, \pi_3, \pi_4\}.$$

Таким образом, левые и правые смежные классы совпадают для всех элементов группы, а значит, подгруппа $H = \{\pi_1, \pi_5, \pi_6\}$ является нормальной: $H \lhd S_3$.

■

Пусть группа G не является простой, и H – ее нормальная подгруппа. Рассмотрим совокупность смежных классов группы G по подгруппе H.

Теорема 3.3.3

Множество всех смежных классов группы G по нормальной подгруппе H с бинарной операцией

$$(g_i H) \circ (g_j H) = (g_i g_j) H \qquad (3.3.4)$$

образует группу (называемую *фактор-группой* G/H) с единичным элементом $e = H$ и порядком $|G/H| = |H|$.

Проверим корректность (однозначную определенность) операции (3.3.4). Для представителей смежных классов $g_i h_1$ и $g_j h_2$, используя ассоциативность групповой операции и тот факт, что для нормальной подгруппы левые и правые смежные классы совпадают, а значит, всегда найдется элемент h_1' такой, что $h_1 g_j = g_j h_1'$, последовательно находим:

$$(g_i h_1)(g_j h_2) = g_i (h_1 g_j) h_2 = g_i (g_j h_1') h_2 = (g_i g_j) h_3.$$

В силу произвольности выбора представителей смежных классов делаем вывод, что операция (3.3.4), определенная на множестве смежных классов, корректна. Для завершения доказательства теоремы осталось проверить выполнение аксиом $G_1 - G_3$.

3.4. Гомоморфизм и изоморфизм групп

Важнейшими понятиями общей алгебры являются гомоморфизм и изоморфизм, которые являются обобщениями таких понятий как равенство, тождество, эквивалентность. Они позволяют свести задачу изучения свойств алгебр к изучению свойств только специального набора алгебр. Рассмотрим эти понятия на примере групп.

Опр. 3.4.1 Однозначное отображение f группы G в группу G', при котором для любых двух элементов a и b из G выполняется равенство

$$f(ab) = f(a)f(b) \qquad (3.4.1)$$

называется ***гомоморфизмом*** группы G в группу G'.

Свойства гомоморфизма групп

I. При гомоморфизме единичный элемент e отображается в единичный элемент e'.

II. При гомоморфизме взаимнообратные элементы g и g^{-1} отображаются во взаимнообратные элементы g' и g'^{-1}.

III. При гомоморфизме все элементы группы G, отображающиеся в единичный элемент e', образуют нормальную подгруппу $H \lhd G$.

Опр. 3.4.2 Множество всех элементов группы G, отображающихся при гомоморфизме $f: G \to G'$ в единичный элемент e', называется ***ядром гомоморфизма*** $\ker f$:

$$\ker f = \{g \in G | f(g) = e'\}.$$

Согласно свойству III ядро любого гомоморфизма образует нормальную подгруппу исходной группы.

Пример 3.4.1. Невырожденные матрицы одного порядка n образуют группу (обозначается как $GL(n, R)$) с групповой операцией – матричное умно-

жение. Тогда, сопоставляя каждой матрице $A \in GL(n,R)$ ее определитель $\det A \neq 0$, получим гомоморфизм:

$$f: GL(n,R) \to R/\{0\},$$

где $R/\{0\}$ – мультипликативная группа действительных чисел. Действительно, согласно свойству мультипликативности определителей имеем

$$\det(AB) = \det A \det B,$$

что соответствует характеризующему гомоморфизм соотношению (3.4.1). Поскольку в группе $R/\{0\}$ единичный элемент $e \equiv 1$, то ядро гомоморфизма состоит из всех матриц с определителем равным 1:

$$\ker f = \{A \in GL(n,R) | \det A = 1\}.$$

Эти же матрицы образуют нормальную подгруппу группы $GL(n,R)$.

■

Опр. 3.4.3 | *Взаимно однозначный* гомоморфизм f группы G в группу G', называется ***изоморфизмом***. Группы G и G', между которыми можно установить некоторый изоморфизм $f: G \leftrightarrow G'$ называются ***изоморфными***: $G \cong G'$.

Ядро любого изоморфизма состоит только из одного единичного элемента $\ker f = \{e\}$. Свойства элементов изоморфных групп полностью совпадают. Изоморфные группы отличаются только природой своих элементов и определением групповых операций.

Имеют место следующие фундаментальные теоремы.

Теорема 3.4.1 (*о гоморфизме*)

Пусть f – гомоморфизм группы G на всю группу G' (*эпиморфизм*), а $\ker f$ его ядро. Тогда группа G' изоморфна фактор-группе по ядру $\ker f$:

$$G' \cong G/\ker f.$$

Теорема 3.4.2 (*теорема Кэли*)

Любая конечная группа G порядка n изоморфна группе перестановок $n-$го порядка S_n.

Теорема Кэли указывает на исключительность групп S_n как эталонных при изучении свойств конечных групп.

3.5. Симметрические группы

Пусть M – некоторое конечное множество порядка n. Перенумеруем его элементы, тем самым установив взаимно однозначное отображение (биекцию) множества M в множество первых n натуральных чисел $X = \{1, 2, \dots, n\}$.

Далее рассмотрим множество биекций $\pi: X \to X$, называемых *подстановками порядка* n:

$$\pi = \begin{pmatrix} 1 & 2 & 3 \dots n \\ i_1 & i_2 & i_3 \dots i_n \end{pmatrix} \equiv (i_1\ i_2 \dots\ i_n), \text{ где } i_k = \pi(k). \qquad (3.5.1)$$

Повторные отображения позволяют естественным образом ввести на множестве подстановок бинарную операцию – *композицию*:

$\pi_1 \circ \pi_2 \equiv \pi_1\pi_2$

(*выполняется слева направо*) и наделить это множество алгебраической структурой с характерными свойствами:

- композиция подстановок *ассоциативна*:
$$\pi_1(\pi_2\pi_3) = (\pi_1\pi_2)\pi_3;$$
- *тождественная подстановка* $\pi(k) = k, \forall k = \overline{1,n}$, может рассматриваться как единичный элемент:
$$e = (1\ 2 \dots n);$$
- для любой подстановки $\pi = (i_1\ i_2 \dots\ i_n)$ существует единственная ей *обратная подстановка* π^{-1}:
$$\pi^{-1} = \begin{pmatrix} i_1 & i_2 & i_3 \cdots & i_n \\ 1 & 2 & 3 \cdots & n \end{pmatrix} \Rightarrow \pi \circ \pi^{-1} = e.$$

Таким образом, все подстановки одного порядка с композицией образуют группу.

Опр. 3.5.1 Группа подстановок порядка n называется ***симметрической группой*** S_n.

Порядок симметрической группы равен числу всех различных подстановок $n-$го порядка:

$$|S_n| = n! \qquad (3.5.2)$$

Рассмотрим специальный класс подстановок.

Опр. 3.5.2 Подстановки вида $1 \to 2 \to \cdots \to k \to 1$, то есть
$$\pi(l) = l + 1,\ \forall l < k; \quad \pi(k) = 1,$$
называются ***циклом*** σ длины k.

Циклы принято обозначать круглыми скобками:

$$\sigma = (1\ 2\ 3 \ldots k) \equiv \begin{pmatrix} 1 & 2 & 3 & \ldots & k-1 & k \\ 2 & 3 & 4 & \ldots & k & 1 \end{pmatrix}.$$

Опр. 3.5.3 Два цикла называются *независимыми*, если они не имеют общих элементов.

Очевидно, что независимые циклы перестановочны:

$$\sigma_1\sigma_2 = \sigma_2\sigma_1. \qquad (3.5.3)$$

Опр. 3.5.4. Цикл длины 2 называется ***транспозицией***.

Теорема 3.5.1

Любая подстановка единственным образом разложима в произведение независимых циклов:

$$\pi = \sigma_1\sigma_2 \ldots \sigma_k. \qquad (3.5.4)$$

Пример 3.5.1. Разложить подстановку $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 2 & 5 & 1 \end{pmatrix}$ в произведение независимых циклов.

Решение

Стартуем с 1 и определяем первый цикл σ_1:

$$1 \to \pi(1) = 4 \to \pi(4) = 5 \to \pi(5) = 1 \ \Rightarrow\ \sigma_1 = (1\ 4\ 5).$$

Далее выбираем любое число, не входящее в σ_1, например, 2, и определяем следующий цикл:

$$2 \to \pi(2) = 3 \to \pi(3) = 2 \ \Rightarrow\ \sigma_2 = (2\ 3).$$

Таким образом, искомое разложение имеет вид:

$$\pi = \sigma_1\sigma_2 = (1\ 4\ 5)(2\ 3).$$ ■

Теорема 3.5.2

Любая подстановка является произведением транспозиций.

В теореме 3.5.2 единственность представления не предполагается. Однако общее количество транспозиций позволяет ввести важное классифицирующие подстановки понятие.

Опр. 3.5.5 Подстановка π называется ***четной***, если она представима в виде композиции четного числа транспозиций, и ***нечетной***, если число транспозиций нечетно.

При $n > 1$ количества четных и нечетных подстановок совпадают и равны $n!/2$.

Теорема 3.5.3

Все четные подстановки образуют подгруппу группы S_n.

Действительно, тождественная подстановка e относится к классу четных подстановок. Для любой транспозиции τ имеем:

$$\tau^2 = e \;\Rightarrow\; \tau^{-1} = \tau,$$

а значит,

$$\pi = \tau_1\tau_2 \dots \tau_m \;\Rightarrow\; \pi^{-1} = \tau_m^{-1}\tau_{m-1}^{-1} \dots \tau_1^{-1} = \tau_m\tau_{m-1} \dots \tau_1.$$

Опр. 3.5.6 Подгруппа четных подстановок группы S_n называется ***знакопеременной подгруппой*** и обозначается как A_n.

Композиция τA_n, где $\tau = (1\ 2)$, совпадает с множеством всех нечетных подстановок и одновременно определяет смежный класс по подгруппе A_n. Таким образом, для симметрической группы S_n справедливо разбиение:

$$S_n = A_n \cup \tau A_n.$$

3.6. Циклические группы

Опр. 3.6.1 Группа G называется ***циклической***, если она порождается одним элементом a:
$G = \{a, a^2, a^3, \dots, a^n = e\} \equiv < a >$.
Элемент a называется ***порождающим*** (группу) ***элементом.***

Из определения следует, что циклической может быть только *конечная абелева* группа. Название группы «циклическая» указывает на наличие в группе естественных циклов:

$$a^m = a^{m+n} \qquad (3.6.1)$$

для $\forall m$. Здесь n – порядок группы.

Пример 3.6.1. Классы вычетов по любому модулю m образуют аддитивную циклическую группу $\mathbb{Z}_m$ порядка m. Порождающим элементом является класс $\bar{1}$.

■

Свойства циклических групп

1. Любая подгруппа циклической группы также является циклической, причем она порождается любым своим элементом $g \neq e$.

2. В циклической группе $< a >$ порядка n элемент a^k порождает подгруппу порядка
$l = \frac{n}{d}$, где $d = \text{НОД}(n, k)$.

3. Для любого делителя d порядка n циклической группы $< a >$ группа содержит только одну подгруппу порядка $l = n/d$.

4. Циклическая группа $< a >$ порядка n содержит ровно $\varphi(n)$ образующих элементов. Причем элемент a^k будет образующим только, если $\text{НОД}(n, k) = 1$.

Пример 3.6.2. Пусть $G = < a >$ - циклическая группа порядка 6 и a ее образующий элемент. Тогда имеем

$$\varphi(6) = 6\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) = 2.$$

Следовательно, согласно свойству 4, группа содержит 2 образующих элемента, а именно, $g_1 = a$ и $g_2 = a^5$. В качестве проверки выпишем все различные степени второго элемента:

$$\{a^5, a^{10}, a^{15}, a^{20}, a^{25}, a^{30}\} = \{a^5, a^4, a^3, a^2, a, e\} = G,$$

так как $a^6 = e$.

■

3.7. Кольца и поля

Перейдем к рассмотрению алгебраических систем с двумя бинарными операциями.

Опр. 3.7.1 ***Кольцом*** называется алгебраическая система $< M; +, * >$ с двумя бинарными операциями $+$ *(«сложение»)* и $*$ *(«умножение»),* которые удовлетворяют следующим условиям:

K_1: $< M; + >$ – абелева группа;

K_2: $< M; * >$ – моноид (полугруппа с единицей);

K_3: справедливы законы дистрибутивности:

$$a * (b + c) = a * b + a * c, \qquad (3.7.1)$$

$$(a+b)*c = a*c + b*c. \qquad (3.7.2)$$

Кольцо называется *коммутативным*, если дополнительно

$$a*b = b*a. \qquad (3.7.3)$$

Пример 3.7.1. Рассмотрим множество целых чисел $\mathbb{Z}$ с арифметическими операциями сложения и умножения. Тогда $<\mathbb{Z}; +, \times>$ есть коммутативное кольцо. ■

Пример 3.7.2. Рассмотрим множество *всех* квадратных матриц $M_{n\times n}$ одного порядка n с операциями сложения и умножения матриц. Тогда эта алгебраическая система образует некоммутативное кольцо. ■

Принято нулевой элемент аддитивной группы $< M; +>$ называть ***нулем*** (обозначается как 0), а единичный элемент моноида $< M; *>$ ***единицей*** (обозначается как 1).

Заметим, что, так как множество M относительно операции «сложения» $+$ есть аддитивная группа, то для каждого элемента a из M имеется «обратный элемент». Этот элемент называется *противоположным* и обозначается как $-a$. Что касается второй операции «умножения» $\times$, то в общем случае для колец существование обратного элемента a^{-1} не предполагается. Законы дистрибутивности (3.6.1) и (3.6.2) позволяют корректно согласовывать выполнения двух операций.

Общими для колец являются следующие результаты.

Лемма 1

В любом кольце $< M; +, *>$ нуль аддитивной группы $< M; +>$ является нулем и для моноида $< M; *>$:

$$0*b = b*0 = 0. \qquad (3.7.4)$$

Лемма 2

Для любых элементов a и b произвольного кольца $< M; +, *>$ справедливо соотношение

$$(-a)*(-b) = a*b. \qquad (3.7.5)$$

Данные результаты являются прямым следствием групповой структуры системы $< M; +>$, а именно, наличие единственного еди-

ничного элемента 0, обратимости (существование единственного противоположного a элемента $-a$) и закона сокращения:

$$a + x = a \quad \Rightarrow \quad x = 0;$$
$$a + x = 0 \quad \Rightarrow \quad x = -a;$$
$$a + x = b + x \quad \Rightarrow \quad a = b.$$

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

$\times$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	1	$\bar{2}$	3
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{0}$	$\bar{2}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Опр. 3.7.2 Два ненулевых элемента a и b кольца $< M; +, * >$ называются ***делителями нуля***, если их произведение есть нуль кольца:

$$a * b = 0. \qquad (3.7.6)$$

В случае конечных колец небольшого порядка основные операции над их элементами удобно задавать в виде таблиц. Важнейшим примером конечных колец являются кольца классов вычетов по модулю m:

$$\mathbb{Z}_m = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{m-1}\}.$$

Пример 3.7.3. Рассмотрим кольцо $\mathbb{Z}_4$. Таблицы, определяющие операции сложения и умножения между элементами кольца, имеют вид:

В частности, находим

$$\bar{2} + \bar{2} = \bar{0}, \qquad \bar{2} \times \bar{2} = \bar{0}.$$

Таким образом, в кольце $\mathbb{Z}_4$ *«дважды два»* равно не четырем, а нулю, и кольцо содержит делитель нуля – класс $\bar{2}$.

■

В числовых кольцах $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ делителей нуля нет. Другими словами, если $xy = 0$, то либо $x = 0$, либо $y = 0$.

Примерами колец с делителями нуля являются кольца

- квадратных вырожденных матриц;
- классы вычетов с составными модулями.

Опр. 3.7.3 | ***Областью целостности*** называется коммутативное кольцо с единицей без делителей нуля.

Лемма 3

В области целостности выполняется закон сокращения:

$$a * b = a * c \Leftrightarrow b = c, \quad \text{для } \forall a \neq 0. \qquad (3.7.7)$$

В кольце K с единицей естественно выделить множество обратимых элементов, которые по аналогии с определением 3.7.2, по-существу, являются делителями единицы:

$$a * a^{-1} = a^{-1} * a = 1. \qquad (3.7.8)$$

Однако в кольцах, содержащих делители нуля, не все элементы обратимы. Действительно, если $a * b = 0$, причем $a, b \neq 0$, то в случае существования элемента a^{-1} мы бы имели

$$a^{-1} * (a * b) = a^{-1} * 0 \Rightarrow (a^{-1} * a) * b = 0 \Rightarrow 1 * b = 0 \Rightarrow b = 0,$$

что противоречит исходному предположению о существовании делителей нуля ($b \neq 0$).

Пример 3.7.4. Для элементов кольца $\mathbb{Z}_4$ (пример 3.7.3) непосредственно из «таблицы умножения» находим:

$$\bar{1} \times \bar{1} = \bar{1} \Rightarrow \bar{1}^{-1} = \bar{1},$$
$$\bar{3} \times \bar{3} = \bar{1} \Rightarrow \bar{3}^{-1} = \bar{3}.$$

Элемент $\bar{2}$ ни с одним элементом кольца в произведении класс $\bar{1}$ не дает, для него в кольце нет обратного элемента $\bar{2}^{-1}$, а значит, он необратим. При этом, как следует из примера 3.6.3, элемент $\bar{2}$ является делителем нуля.

■

Теорема 3.7.1

Все *обратимые элементы* кольца $K =< M; +, * >$ с единицей образуют группу $G(K)$ по умножению $*$.

Особый интерес с точки зрения приложений представляют собой кольца, для которых в группу обратимых элементов входят все элементы кольца

Опр. 3.7.4 | ***Полем*** P называется коммутативное кольцо с единицей (*область целостности*), в котором все элементы за исключением нуля обратимы.

По-существу, в поле *все ненулевые* элементы образуют мультипликативную группу. Важнейшими примерами бесконечных полей являются поля рациональных $\mathbb{Q}$, действительных $\mathbb{R}$ и комплексных $\mathbb{C}$ чисел.

Особый интерес представляют собой конечные поля.

Теорема 3.7.2

Всякая конечная область целостности является полем.

Именно конечность области целостности обуславливает обратимость всех ее элементов.

Теорема 3.7.3

Кольцо классов вычетов $\mathbb{Z}_m$ является полем тогда и только тогда, когда модуль $m = p$ – простое число.

Опр. 3.7.5 Поле классов вычетов по простому модулю $\mathbb{Z}_p$ называется ***полем Галуа порядка p*** и обозначается как

$$GF(p) \equiv \mathbb{Z}_p.$$

3.8. Подкольца и идеалы

Опр. 3.8.1. Подмножество S кольца K называется его ***подкольцом***, если оно замкнуто относительно определенных в кольце K операций сложения $+$ и умножения $*$, и само образует кольцо относительно этих операций.

Введем для колец аналог нормальной подгруппы группы G.

Опр. 3.8.2 Подкольцо H кольца K называется ***идеалом (***или ***двусторонним идеалом)*** этого кольца, если для любых элементов $h \in H$ и $a \in K$ элементы $a * h$ и $h * a$ принадлежат подкольцу H.

Пример 3.8.1. Множество целых чисел $\mathbb{Z}$ является подкольцом поля рациональных чисел $\mathbb{Q}$, но не идеалом, так как, например,

$$2 \cdot \frac{1}{5} = \frac{2}{5} \notin \mathbb{Z}.$$ ■

Всякое кольцо K содержит, по крайней мере, два идеала: множество $\{0\}$ и само кольцо K. Эти идеалы называются *несобственными,* а все другие – *собственными.*

Теорема 3.8.1

Любой элемент a коммутативного кольца K порождает идеал вида $< a >= \{a * x \mid x \in K\}$.

Теорема является следствием свойств дистрибутивности, ассоциативности и коммутативности операций $+$ и $*$, определяющих алгебраическую структуру кольца K.

Пример 3.8.2. Рассмотрим кольцо целых чисел $\mathbb{Z}$. Тогда согласно теореме 3.8.1 числа, кратные некоторому целому числу m образуют идеал, который обозначается как $m\mathbb{Z}$.

■

Опр. 3.8.3

Идеал H коммутативного кольца K называется ***главным идеалом***, если в кольце найдется элемент a, который порождает этот идеал: $< a > = H$.

Если коммутативное кольцо K не является полем, то среди его элементов найдется хотя бы один необратимый ненулевой элемент a. Но тогда идеал, порождаемый этим элементом, не содержит 1, а значит, не может совпадать со всем кольцом K и в любом случае является собственным. Таким образом, мы приходим к следующему отличительному свойству полей.

Теорема 3.8.2

Любое поле P не имеет собственных идеалов.

Рассмотрим кольцо K с единицей. Единица порождает циклическую подгруппу аддитивной группы кольца. Эта циклическая подгруппа автоматически будет подкольцом. Действительно,

$$\underbrace{(1+1+\cdots+1)}_{m} * \underbrace{(1+1+\cdots+1)}_{n} = \underbrace{(1+1+\cdots+1)}_{mn}.$$

Опр. 3.8.4 ***Характеристикой*** кольца K называется порядок его аддитивной подгруппы $< 1, + >$, порождаемой единицей кольца 1:

$$char\ K = | < 1, + > |. \qquad (3.8.1)$$

В случае, когда подгруппа $< 1, + >$ бесконечна, то говорят, что *кольцо имеет характеристику* 0.

Пример 3.8.3. Характеристика кольца вычетов по модулю m равна m:

$$char\ \mathbb{Z}_m = m.$$

■

Теорема 3.8.3

Характеристика кольца, являющегося областью целостности, равна 0 или простому числу p.

Опр. 3.8.5 ***Центром*** C кольца K называется множество его элементов, которые коммутируют со всеми элементами x кольца:

$$C = \{a \mid a * x = x * a, \quad \forall x \in K\}.$$

Очевидно, что центр коммутативного кольца K совпадает с самим кольцом: $C = K$.

Теорема 3.8.4

Центр любого кольца является его подкольцом.

Пример 3.8.4. Пусть M_n – кольцо квадратных матриц порядка n. Центр этого кольца состоит из всех матриц, кратных единичной матрице E:

$$C = \{\lambda E\}.$$

■

По аналогии с фактор-группой, порождаемой нормальной подгруппой группы G, любой идеал H кольца K порождает фактор-кольцо K/H. При этом умножение соответствующих классов смежности вводится по правилу:

$$(a + H) * (b + H) = (a * b) + H. \qquad (3.8.2)$$

Пример 3.8.5. Рассмотрим идеал $m\mathbb{Z}$ (множество целых чисел кратных m) кольца $\mathbb{Z}$. Тогда фактор-кольцо $\mathbb{Z}/m\mathbb{Z}$, по-существу представляет собой класс вычетов по модулю m:

$$\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}_m.$$

■

Фактор-кольца наследуют не все свойства колец. Так кольцо целых чисел $\mathbb{Z}$ делителей нуля не имеет, а, например, его фактор-кольцо $\mathbb{Z}/6\mathbb{Z} = \mathbb{Z}_6$ имеет уже два делителя нуля.

3.9. Гомоморфизм и изоморфизм колец

Опр. 3.9.1 Пусть $< K; +, \times >$ и $< K'; \oplus, \otimes >$ − кольца. Тогда отображение $f: K \to K'$ называется ***гомоморфизмом колец***, если оно сохраняет порядок характеризующих структуру колец операций:

$$f(a + b) = f(a) \oplus f(b), \quad (3.9.1)$$

$$f(a \times b) = f(a) \otimes f(b). \quad (3.9.2)$$

Для колец с единицей дополнительно

$$f(1) = 1'. \quad (3.9.3)$$

Лемма 1

Пусть f – гомоморфизм колец $f: K \to K'$. Тогда

$$f(0) = 0', \quad (3.9.4)$$

$$f(-a) = -f(a). \quad (3.9.5)$$

В случае если элемент $a \in K$ обратим, то

$$f(a^{-1}) = f(a)^{-1}. \quad (3.9.6)$$

Понятия − *ядро, образ, эпиморфизм (сюръекция), мономорфизм (инъекция), изоморфизм* и другие имеют для колец тот же смысл, что и для групп.

Опр. 3.9.2. ***Ядром гомоморфизма*** $f: K \to K'$ называется множество всех элементов кольца K, которые отображаются в нуль кольца K':

$$\ker f = \{a \in K | f(a) = 0'\}.$$

Лемма 2

Ядро $\ker f$ гомоморфизма $f: K \to K'$ является подкольцом кольца K'.

Лемма является следствием основных свойств гомоморфных отображений (3.9.1) и (3.9.2).

Опр. 3.9.3 | ***Изоморфизмом (биекцией) колец*** K и K' называется любой их взаимно однозначный *(биективный)* гомоморфизм.

Отношение изоморфизма колец обозначается как $K \cong K'$. Изоморфные кольца имеют одну алгебраическую структуру и отличаются только природой своих элементов и определением базовых операций.

Пример 3.9.1. Рассмотрим отображение $f: \mathbb{Z} \to \mathbb{Z}_m$. Это отображение является гомоморфизмом кольца целых чисел $\mathbb{Z}$ в класс вычетов $\mathbb{Z}_m$ по модулю m, Оно очевидно сюръективно, но не инъективно (каждый класс содержит счетное множество чисел), а поэтому не биективно. Ядро гомоморфизма f состоит из всех целых чисел кратных m: $\ker f = m\mathbb{Z}$ (пример 3.8.5).

■

Теорема 3.9.1

Пусть $f: K \to K'$ – гомоморфизм кольца K в кольцо K' и $\ker f$ – его ядро. Тогда кольцо K' изоморфно фактор-кольцу $K/\ker f$.

3.10. Линейные системы над полем P

Стандартная теория линейных систем с действительными коэффициентами и методы их решения основаны на алгоритмах выполнения арифметических операций. При этом никак не учитывается специфика поля действительных чисел $\mathbb{R}$, его особенности и отличия, например, от поля рациональных чисел $\mathbb{Q}$. Это наводит на мысль, что все известные в теории линейных систем результаты можно естественным образом обобщить и на другие поля, в том числе и конечные.

Пример 3.10.1. Пусть задана однородная система линейных уравнений следующего вида:

$$AX = 0, \text{ где } A = \|a_{ij}\| = \begin{Vmatrix} 1 & 2 & 3 & 4 \\ -10 & 13 & 14 & 15 \\ 12 & -9 & 14 & 15 \\ 12 & 13 & -8 & 15 \end{Vmatrix}.$$

Прямые вычисления дают:

$$\det A = 2^3 \cdot 11^3.$$

Следовательно, если $a_{ij}, x_k \in P$, где P – некоторое поле характеристики 0 или $l \neq 2,11$ (в этом случае коэффициенты и неизвестные рассматриваются как классы вычетов), то система является невырожденной и имеет единственное нулевое решение:

$$X = 0.$$

Положим $P = \mathbb{Z}_2$. Тогда $\operatorname{char} P = 2$, и, используя сравнения по модулю $m = 2$, матрицу A можно преобразовать к виду:

$$A = \begin{Vmatrix} 1 & 2 & 3 & 4 \\ -10 & 13 & 14 & 15 \\ 12 & -9 & 14 & 15 \\ 12 & 13 & -8 & 15 \end{Vmatrix} = \begin{Vmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \end{Vmatrix} \pmod 2.$$

Очевидно, что ранг системы в этом случае равен 2 и система допускает 2 линейно независимых решения, например:

$$X_1 = (1,0,1,0) \quad \text{и} \quad X_2 = (0,1,0,1).$$

Заметим, что здесь (и в дальнейшем) используются упрощенные обозначения и все числа надо понимать как соответствующие классы вычетов $\overline{0}, \overline{1}, \ldots$.

Положим $P = \mathbb{Z}_{11}$. Тогда $\operatorname{char} P = 11$, и, используя сравнения по модулю $m = 11$, для матрицы A имеем:

$$A = \begin{Vmatrix} 1 & 2 & 3 & 4 \\ -10 & 13 & 14 & 15 \\ 12 & -9 & 14 & 15 \\ 12 & 13 & -8 & 15 \end{Vmatrix} = \begin{Vmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{Vmatrix} \pmod{11}.$$

Теперь ранг матрицы коэффициентов A равен $\operatorname{rg} A = 1$, и система допускает уже 3 линейно независимых решения, например:

$X_1 = (9,1,0,0)$; $X_2 = (8,0,1,0)$; $X_3 = (7,0,0,4)$.

Таким образом, ответ существенно зависит от поля P, над которым рассматривается система, но ее анализ ничем не отличается от стандартного.

■

Конечные поля, например поле Галуа $GF(p)$, широко используются в теории кодирования. Так для передачи сообщения

МИРУ МИР

в принципе достаточно повторения четырех элементарных сообщений:

М $= \{0,0\}$, И $= \{1,0\}$, Р $= \{0,1\}$, У $= \{1,1\}$.

Их можно интерпретировать как вектор-строки двумерного линейного пространства над полем $P = \mathbb{Z}_2 = \{0,1\}$. Во время передачи сигналов в канале связи может произойти сбой:

$$0 \leftrightarrow 1.$$

В результате адресат может получить неверное сообщение, например:

РИМУ РИМ.

Согласно теореме Шеннона за счет увеличения длины элементарных сообщений (что эффективно приведет к уменьшению скорости передачи сигналов) влияние помех может быть устранено.

Предположим, что при передаче сигналов возможно искажение одного символа из пяти переданных. Зафиксируем в линейном пространстве $\mathcal{L} = \mathbb{Z}_2^5$ подмножество

$$S_0 = \{\text{М}(0,0,1,1,0), \text{И}(1,0,0,1,1), \text{Р}(0,1,1,0,1), \text{У}(1,1,0,0,1)\}.$$

Подмножество S_0 состоит из так называемых *кодовых векторов*. Составим таблицу возможных искажений:

Кодовые векторы	0 0 1 1 0	1 0 0 1 1	0 1 1 0 1	1 1 0 0 0
Кодовые векторы с одним искажением	0 0 0 1 0	0 0 0 1 1	0 0 1 0 1	0 1 0 0 0
	0 0 1 0 0	1 0 0 0 1	0 1 0 0 1	1 0 0 0 0
	0 0 1 1 1	1 0 0 1 0	0 1 1 0 0	1 1 1 0 0
	0 1 1 1 0	1 0 1 1 1	0 1 1 1 1	1 1 0 0 1
	1 0 1 1 0	1 1 0 1 1	1 1 1 0 1	1 1 0 1 0

Отметим, что количество возможных наборов

$$2^5 = 32 > 4 \cdot 5 = 20,$$

и множество искаженных векторов из разных столбцов не пересекаются. Поэтому возможно правильное декодирование истинного сообщения при наличии одной ошибки.

Переходя к пространству $\mathcal{L} = \mathbb{Z}_2^n$ размерности n можно сконструировать аналогичный код, способный безошибочно передавать, например, весь русский алфавит, то есть любой текст. Чтобы декодирование не свелось к длительному простому перебору, подмножество S_0 строится специальным образом. При этом используются свойства конечных полей $\mathbb{F}_p$ (полей Галуа характеристики p).

3.11. Кольцо многочленов

Пусть K – некоторое коммутативное кольцо.

Опр. 3.11.1 ***Многочленом (полиномом)*** степени m одного аргумента x над коммутативным кольцом K называется выражение вида

$$P_m(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_m x^m, \quad (3.11.1)$$

где $a_k \in K\ \forall k = \overline{0,m}$, причем $a_m \neq 0$. При этом форма (3.11.1) записи многочлена называется *стандартной* или *канонической.*

Стандартный многочлен однозначно определяется своими коэффициентами, которые можно рассматривать как координаты многочлена в базисе одночленов $\mathcal{B} = \{1, x, x^2, \dots, x^m\}$:

$P_m = (a_0, a_1, \dots, a_m)$.

Чтобы все коэффициенты были равноправными, необходимо допустить возможность обращения в 0 и старшего коэффициента a_m. При этом нулевой многочлен будет иметь нулевые координаты

$P_m(x) \equiv 0 = (0, 0, \dots, 0)$.

Степень многочлена, заданного своими координатами, определяется по максимальному номеру отличной от нуля компоненты:

$(a_0, a_1, \dots, a_k, 0, \dots, 0) \Rightarrow \deg P(x) = k$.

Опр. 3.11.2 Два многочлена $P_m(x)$ и $Q_n(x)$ равны друг другу, если имеют одну и ту же каноническую форму.

Лемма (*критерий равенства многочленов)*

Многочлены $P_m(x)$ и $Q_n(x)$ равны тогда и только тогда, когда

1) равны их степени: $m = n$;
2) равны все их соответствующие коэффициенты: $a_k = b_k, \forall k$.

Сложение многочленов определяется как операция приведения подобных, то есть сложение коэффициентов при одинаковых степенях аргумента x. Умножение в силу коммутативности кольца K определяется по законам обычной алгебры. При этом для степени результирующего многочлена имеем

$$\deg\big(P(x) + Q(x)\big) \leq \max\{\deg P, \deg Q\},$$

$$\deg\big(P(x)Q(x)\big) = \deg P(x) + \deg Q(x). \qquad (3.11.2)$$

Множество всех многочленов над коммутативным кольцом K с введенными операциями сложения и умножения образуют кольцо многочленов $\mathcal{K}(x)$. Причем многочлены нулевой степени, то есть константы, образуют кольцо изоморфное кольцу K – *кольцо коэффициентов*.

Многочлены, определенные над полем P, обладают дополнительными свойствами.

Теорема 3.11.1

Над любым полем P кольцо многочленов $K(x)$ является областью целостности, причем в кольце $K(x)$ обратимыми являются только ненулевые константы.

Доказательство теоремы, по-существу, повторяет алгоритм деления многочленов.

Опр. 3.11.3 Многочлен $P(x)$ в кольце многочленов $K(x)$ называется ***приводимым***, если найдутся два многочлена $p(x)$ и $q(x)$ такие, что

$$P(x) = p(x)q(x), \qquad (3.11.3)$$

в противном случае многочлен называется ***неприводимым***.

Приводимость многочленов существенно зависит от поля, над которым рассматривается многочлен.

Пример 3.11.1. Пусть $P(x) = x^2 - 2$. Многочлен $P(x)$ неприводим над полем рациональных чисел $P = \mathbb{Q}$ и полем классов вычетов $\mathbb{Z}_3$ по модулю 3. Однако он приводим над полем действительных чисел $P = \mathbb{R}$:

$x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$,

и полем классов вычетов $\mathbb{Z}_7$ по модулю 7:

$x^2 - 2 = (x + 3)(x + 4)$.

■

Рассмотрим многочлены над коммутативным кольцом K, которое представляет собой область целостности с единицей.

Опр. 3.11.4 Элемент $c \in K$ называется ***корнем*** или ***нулем многочлена*** $P(x)$, если

$$P(c) = 0. \qquad (3.11.4)$$

Теорема 3.11.2 (*теорема Безу*)

Элемент $c \in K$ является корнем многочлена $P(x)$ тогда и только тогда, когда двучлен $x - c$ делит многочлен $P(x)$ в кольце K.

Доказательство теоремы, по-существу, повторяет доказательство теоремы Безу в обычной алгебре, где кольцо K есть поле действительных чисел $K = \mathbb{R}$.

Деление многочленов на двучлен над любым кольцом K удобно выполнять с использованием *схемы Горнера*.

Пример 3.11.2. Поделить многочлен $P(x) = 2x^2 + 5x - 3$ на двучлен $q(x) = x + 2$ над полем:

$a)$ $\mathbb{Q}$;

б) $GF(5)$ $(\mathbb{Z}_5)$.

Решение

Используя схему Горнера, находим:

$a)$

	2	5	-3
-2	2	1	-5

$\Rightarrow \frac{2x^2+5x-3}{x+2} = 2x + 1 - \frac{5}{x+2}.$

Заданный многочлен $P(x)$ над полем рациональных чисел $\mathbb{Q}$ на двучлен $q(x) = x + 2$ нацело не делится: остаток от деления равен -5.

Дискриминант многочлена равен $D = 25 + 24 = 49$, и многочлен имеет два рациональных корня:

$$x_1 = \frac{1}{2}, x_2 = -3.$$

б) В случае поля Галуа $GF(5)$, которое совпадает с полем $\mathbb{Z}_5$, коэффициенты можно заменить любыми представителями классов вычетов, которым коэффициенты принадлежат. Таким образом, имеем:

$P(x) = 2x^2 + 5x - 3 \equiv 2x^2 + 2.$

Далее выполняем деление (по схеме Горнера):

	2	0	2
-2	2	1	0

$\Rightarrow \frac{2x^2+5x-3}{x+2} = 2x + 1.$

Таким образом, над полем $GF(5)$ заданный многочлен раскладывается на множители:

$$P(x) = 2x^2 + 5x - 3 = (x + 2)(2x + 1)$$

и имеет два корня $x_1 = -2 \equiv 3 \; mod \; 5$ и $x_2 = 2 \; mod \; 5$.

■

Опр. 3.11.5 Элемент $c \in K$ называется ***корнем кратности k*** многочлена $P(x)$, если многочлен $P(x)$ делится на многочлен $(x - c)^k$ и не делится на многочлен $(x - c)^{k+1}$. Корни кратности 1 называются *простыми корнями*.

Теорема 3.11.3

Пусть кольцо K – коммутативная область целостности, $P(x) \not\equiv 0$ – многочлен над K, а $c_1, c_2, \dots, c_l$ – его корни кратности $k_1, k_2, \dots, k_l$, соответственно. Тогда многочлен единственным образом раскладывается на множители

$$P(x) = (x - c_1)^{k_1}(x - c_2)^{k_2} \dots (x - c_l)^{k_l} q(x), \quad (3.11.5)$$

где $q(c_k) \neq 0,\ \forall k = \overline{1, l}$, причем

$k_1 + k_2 + \dots + k_l \leq \deg P(x)$.

Следует заметить, что без предположения о целостности кольца (отсутствии делителей нуля) теорема неверна – нарушится единственность разложения.

Пример 3.11.3. Рассмотрим многочлен $P_3(x) = x^3$ над кольцом $\mathbb{Z}_8$. Данное кольцо не является областью целостности и имеет два делителя нуля, а именно, классы 2 и 4.

Далее находим: $P_3(0) = P_3(2) = P_3(4) = P_3(6) = 0\ (mod\ 8)$. Таким образом, многочлен имеет 4 (!) различных корня и несколько форм разложений на множители:

$P_3(x) = x^3 = x(x-4)^2 = (x-2)(x^2+x+4) = (x-6)(x^2-x+4)$.

■

Теорема 3.11.4

Два многочлена $P(x)$ и $Q(x)$ над кольцом K, являющимся коммутативной областью целостности, степени $\leq n$, принимающие равные значения при подстановке $n+1$ различных элементов из K, тождественно равны:

$P(x) = Q(x)$.

Опр. 3.11.6 Поле P называется ***алгебраически замкнутым***, если любой многочлен из кольца многочленов $\mathcal{P}(x)$ (то есть над полем P) представим в виде разложения на линейные множители.

Другими словами поле P – замкнуто, если над этим полем неприводимыми являются только многочлены первой степени.

Лемма

Если каждый многочлен над полем P имеет, по крайней мере, один корень, то поле P является алгебраически замкнутым.

Теорема 3.11.5 (*основная теорема алгебры*)

Поле комплексных чисел $\mathbb{C}$ является алгебраически замкнутым.

Согласно основной теореме алгебры *всякий* многочлен $P_n(z)$ над полем комплексных чисел $\mathbb{C}$ имеет ровно n корней (с учетом их кратностей), а значит, может быть представлен в виде

$$P_n(z) = a(z - c_1)^{k_1}(z - c_2)^{k_2} \dots (z - c_l)^{k_l}, \qquad (3.11.6)$$

где

$$k_1 + k_2 + \dots + k_l = n. \qquad (3.11.7)$$

Рассмотрим кольцо многочленов над полем действительных чисел $\mathbb{R}$. Поле $\mathbb{R}$ не является алгебраически замкнутым, так как, например, многочлен $P_2(x) = x^2 + 1$ не имеет действительных корней. Тем не менее, для кольца многочленов над полем $\mathbb{R}$ имеет место следующий общий результат.

Теорема 3.11.6

Всякий многочлен $P(x)$ над полем действительных чисел $\mathbb{R}$ на линейные множители и квадратные трехчлены (с отрицательными дискриминантами).

Пример 3.11.4. Для многочлена $P_4(x) = x^4 + 1$ находим:

$$x^4 + 1 = x^4 + 2x^2 + 1 - 2x^2 = (x^2 + 1)^2 - \left(\sqrt{2}x\right)^2 =$$
$$= \left(x^2 - \sqrt{2}x + 1\right)\left(x^2 + \sqrt{2}x + 1\right).$$

■

Литература

1. Нестеренко, Ю. В. Теория чисел / Ю. В. Нестеренко. – М. : Издательский центр «Академия», 2008. – 272 с.
2. Кострикин, А.И. Введение в алгебру. / А. И. Кострикин. – М. : Наука, 1977.
3. Биркгоф, Г. Современная прикладная алгебра ; пер. с англ. / Г. Биркгоф, Т. Барти. – М. : Мир, 1976.
4. Виноградов, И. М. Основы теории чисел / И. М. Виноградов. – 9-е изд., перераб. – М. : Наука, 1981.
5. Курош, А. Г. Курс высшей алгебры / Курош А. Г. – СПб. : Издательство «Лань», 2008. – 432 с.
6. Ленг, С. Алгебра ; пер. с англ./ С. Ленг. – М. : Мир, 1968.
7. Харин, Ю. С. Математические и компьютерные основы криптологии / Ю. С. Харин. Минск : Новое знание, 2003.

ОГЛАВЛЕНИЕ

Бабич Александр Антонович

ВЫСШАЯ АЛГЕБРА

Пособие
по курсу «Математика. Геометрия и алгебра»
для студентов специальности 1-40 04 01 «Информатика
и технологии программирования»
дневной формы обучения

Подписано к размещению в электронную библиотеку
ГГТУ им. П. О. Сухого в качестве электронного
учебно-методического документа 18.11.20.

Рег. № 93Е.
http://www.gstu.by