

Министерство образования Республики Беларусь
Учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

Факультет компьютерных систем и сетей

Кафедра высшей математики

ПРИКЛАДНАЯ МАТЕМАТИКА

*Рекомендовано учебно-методическим объединением по образованию
в области информатики и радиоэлектроники в качестве пособия
для специальности 6-05-0611-02 «Информационная безопасность»*

*Рекомендовано учебно-методическим объединением
по профессионально-техническому обучению
в качестве пособия для студентов, обучающихся по специальности
6-05-0719-01 «Инженерно-педагогическая деятельность»*

Минск БГУИР 2026

УДК 512.5(075.8)
ББК 22.144я73
П75

Авторы:

М. А. Глецевич, С. С. Каянович, О. Н. Малышева, А. Н. Семеняко

Рецензенты:

кафедра «Высшая математика» Белорусского
национального технического университета
(протокол № 8 от 24.03.2025)

заведующий кафедрой математических методов в экономике
учреждения образования
«Белорусский государственный экономический университет»
кандидат физико-математических наук, доцент Ю. Л. Ратушева

Прикладная математика : пособие / М. А. Глецевич, С. С. Каянович,
П75 **О. Н. Малышева, А. Н. Семеняко. – Минск : БГУИР, 2026. – 172 с. : ил.**
ISBN 978-985-543-904-3.

Содержит необходимые материалы для проведения лабораторных работ по специальному курсу «Прикладная математика». В соответствии с программой пособие разделено на пять модулей: «Основы теории чисел», «Основы теории групп», «Исторические и современные криптосистемы», «Кольца. Идеалы колец», «Конечные поля». Каждый модуль включает в себя краткие теоретические сведения, подробные решения типовых заданий, тест для самопроверки приобретенных знаний, содержащий ключ с ответами, и индивидуальные задания для лабораторных работ.

УДК 512.5(075.8)
ББК 22.144я73

ISBN 978-985-543-904-3

© УО «Белорусский государственный университет
информатики и радиоэлектроники», 2026

СОДЕРЖАНИЕ

Введение	5
Модуль № 1. Основы теории чисел	7
Теоретические сведения по теме «Основы теории чисел»	7
Типовые задания по теме «Основы теории чисел» с образцами решений	27
Тест для самопроверки по теме «Основы теории чисел»	40
Индивидуальные задания для лабораторной работы № 1 «Основы теории чисел»	42
Модуль № 2. Основы теории групп	47
Теоретические сведения по теме «Основы теории групп»	47
Типовые задания по теме «Основы теории групп» с образцами решений	58
Тест для самопроверки по теме «Основы теории групп»	69
Индивидуальные задания для лабораторной работы № 2 «Основы теории групп»	72
Модуль № 3. Исторические и современные критосистемы	77
Теоретические сведения по теме «Исторические и современные критосистемы»	77
Типовые задания по теме «Исторические и современные критосистемы» с образцами решений	102
Тест для самопроверки по теме «Исторические и современные критосистемы»	108
Индивидуальные задания для лабораторной работы № 3 «Исторические и современные критосистемы»	112
Модуль № 4. Кольца. Идеалы колец	122
Теоретические сведения по теме «Кольца. Идеалы колец»	122
Типовые задания по теме «Кольца. Идеалы колец» с образцами решений	131
Тест для самопроверки по теме «Кольца. Идеалы колец»	137
Индивидуальные задания для лабораторной работы № 4 «Кольца. Идеалы колец»	140
Модуль № 5. Конечные поля	145
Теоретические сведения по теме «Конечные поля»	145
Типовые задания по теме «Конечные поля» с образцами решений	149
Тест для самопроверки по теме «Конечные поля»	161
Индивидуальные задания для лабораторной работы № 5 «Конечные поля»	164

Приложение 1. Таблицы порядковых номеров букв белорусского, русского и английского алфавитов	167
Приложение 2. Функции математического пакета Wolfram Mathematica, рекомендуемые для использования при выполнении лабораторных работ	168
Список использованных источников	169

ВВЕДЕНИЕ

С развитием информационных технологий и их стремительно возрастающей ролью во всех сферах деятельности человека постоянно растет и актуальность надежного шифрования информации, устойчивого ко всевозможным атакам. При подготовке специалистов в области информационной безопасности крайне важно заложить математический фундамент современных криптографических систем, поскольку именно он позволяет понимать оптимальные условия применения криптосистем, а также их уязвимости и способы свести эти уязвимости к минимуму. Кроме того, постоянно возрастает потребность в разработке новых методов шифрования, а такая разработка невозможна без свободного владения основополагающими принципами шифрования и кодирования, которые базируются на понятиях таких математических дисциплин, как основы теории групп, модулярная алгебра и ряд разделов абстрактной алгебры. Каждая из перечисленных дисциплин включает в себя значительный объем теоретического материала, достаточного сложного для изучения на нематематических специальностях.

Целью настоящего пособия является предоставление основной информации по указанным разделам математики, необходимой при подготовке студентов БГУИР специальностей «Инженерно-педагогическая деятельность» и «Информационная безопасность», а также предложение заданий, позволяющих закрепить приобретенные знания, развить навык их применения к практическим задачам и уяснить связь математического аппарата с принципами шифрования в современных криптосистемах.

В соответствии с учебной программой дисциплины «Прикладная математика» данное пособие разделено на пять модулей, каждый из которых содержит краткие теоретические сведения по теме модуля, типовые задания с образцами решения, тест с ключами для самопроверки обучающихся, а также индивидуальные задания для лабораторных работ.

В первом модуле рассматриваются основные вопросы теории чисел и модулярной алгебры: делимость целых чисел, простые числа, сравнимость чисел по модулю и классы вычетов, а также операции над классами вычетов и решение сравнений и систем сравнений.

Во втором модуле внимание уделяется основам теории групп. Изучающих дисциплину знакомят с определениями бинарной алгебраической операции, группы, подгруппы, смежных классов по подгруппе, циклических групп, приводятся основные теоремы, отражающие их свойства. Приведены определения подстановки, цикла и транспозиции, их основные свойства и действия над ними.

Третий модуль посвящен историческим и современным криптосистемам. Обзор многовековой истории шифрования включает в себя изложение принципов шифра Цезаря, решетки Кардано, криптосистемы Тритемиуса, постолбцовой транспозиции и некоторых других шифров. Пошагово описываются этапы шифрования и дешифрования при использовании современных криптосистем RSA и Эль-Гамала.

В четвертом модуле рассматриваются понятия колец и идеалов колец, их свойства и конкретные примеры этих алгебраических структур. Особое внимание уделяется кольцам полиномов, их корням и понятию приводимых и неприводимых полиномов.

Пятый модуль направлен на ознакомление обучающихся с конечными полями, их основными свойствами, структурой и способами построения, а также с простейшими вычислениями в конечных полях.

Структура каждого модуля предполагает, что работа студента с данным пособием будет наиболее эффективной, если он будет последовательно переходить от одной части модуля к другой. Теоретическая часть включает в себя необходимый минимум определений и теорем, почти в каждом случае сопровождающихся конкретным примером, достаточно наглядным и простым (при условии, что будут актуализированы знания дисциплин высшей математики, полученные при изучении линейной алгебры и теории многочленов). Далее приводится детализированное решение типовых заданий лабораторных работ, которое опирается на информацию из теоретического раздела. Внимательное изучение образцов решений задач позволит обучающемуся самостоятельно выполнить все индивидуальные задания соответствующей лабораторной работы. Перед тем как переходить к этим заданиям, авторы рекомендуют проверить, насколько хорошо усвоены новые понятия, и закрепить навык работы с ними, пройдя тест по теме модуля. Каждый тест снабжен ключом.

Пособие завершается двумя приложениями, которые содержат таблицы для криптографического шифрования алфавитов русского, белорусского и английского языка, а также список функций компьютерного пакета Wolfram Mathematica, рекомендованных для использования при выполнении лабораторных работ.

МОДУЛЬ № 1. ОСНОВЫ ТЕОРИИ ЧИСЕЛ

ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ ПО ТЕМЕ «ОСНОВЫ ТЕОРИИ ЧИСЕЛ»¹

§ 1. Делимость целых чисел

Определение 1.1. *Множеством целых чисел, обозначаемым символом $\mathbb{Z}$, называют множество $\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \dots\}$.*

Очевидно, множество целых чисел замкнуто относительно операций сложения и умножения, т. е. сумма $a + b$, разность $a - b$, произведение ab двух целых чисел a и b являются числами целыми. Иначе обстоит дело с делением $a : b = \frac{a}{b}$, так как частное от деления $a : b$ далеко не всегда является целым (здесь $a, b \in \mathbb{Z}$, $b \neq 0$).

В дальнейшем будем рассматривать только целые числа и обозначать их буквами латинского алфавита.

Определение 1.2. *Если частное от деления числа a на число b есть целое число q , то этот факт обозначают $a : b = q$ или $a = bq$ и говорят « a делится на b », « a кратно b » или « b делит a », « b – делитель числа a ».*

Тот факт, что целое число a делится на целое число b , обозначают следующим образом: $a : b$. Если в упорядоченной паре целых чисел (a, b) b является делителем числа a , то говорят, что (a, b) принадлежит отношению² делимости, а знак $:$ – знак отношения делимости.

Лемма 1.1 (транзитивность отношения делимости). *Если a кратно c , c кратно b , то a кратно b .*

Лемма 1.2. *Пусть есть равенство $a_1 + a_2 + \dots + a_m = b_1 + b_2 + \dots + b_n$ и относительно произвольных $m + n - 1$ слагаемых известно, что они кратны c . Тогда и оставшееся $(m + n)$ -е слагаемое кратно c .*

Иными словами, если каждое слагаемое кратно c , то и сумма кратна c .

Теорема 1.1 (о делении с остатком). *Для любых целых чисел a и b , $b \neq 0$, существует единственная пара q и r целых чисел, $0 \leq r < |b|$, такая, что $a = bq + r$.*

Определение 1.3. *Если число a представлено в виде $a = bq + r$; $0 \leq r < |b|$, то число q называют **неполным частным** при условии $r \neq 0$ (**частным** (или **полным частным**) – при $r = 0$), а число r – **остатком** от деления a на b .*

Приведем примеры деления целых чисел с остатком, демонстрирующие различные случаи.

¹ При подготовке данного раздела использовались следующие источники: [1, 5, 6, 13, 16, 21].

² Подробно про общее понятие бинарного отношения как подмножества декартового произведения двух множеств см. [1]

Пример 1.1. При значениях $a = 30$, $b = -7$ имеем равенство $30 = (-7) \cdot (-4) + 2$ и неравенства $(-7) \cdot (-4) < 30$; $(-7) \cdot (-5) > 30$. Неполное частное равно -4 , остаток равен 2 : $0 \leq 2 < |-7|$.

Пример 1.2. При значениях $a = -30$, $b = 4$ имеем равенство $-30 = 4 \cdot (-8) + 2$ и неравенства $4 \cdot (-8) < -30$; $4 \cdot (-7) > -30$. Неполное частное равно -8 , остаток равен 2 : $0 \leq 2 < |4|$.

Пример 1.3. При значениях $a = -55$, $b = -54$ имеем равенство $-55 = (-54) \cdot 2 + 53$ и неравенства $(-54) \cdot 2 < -55$; $(-54) \cdot 1 > -55$. Неполное частное равно 2 , остаток равен 53 : $0 \leq 53 < |-54|$.

Замечание. В двух рассмотренных выше примерах 1.1 и 1.3 число b было отрицательным. Поменяв одновременно знаки у чисел b и q и сохранив при этом равенство $a = bq + r$, можно и в этих примерах добиться того, чтобы число b было положительным. Еще заметим, что при конкретных a и b числа q и r находятся делением уголком числа a на число b .

§ 2. Наибольший общий делитель. Алгоритм Евклида. Взаимно простые числа

1. Простые и составные числа

В дальнейшем будем рассматривать *только положительные делители* чисел.

Определение 1.4. Если целые числа $a_1, a_2, \dots, a_n$ делятся на целое число δ , то δ называют их **общим делителем**. Наибольший из всех общих делителей этих чисел называется их **наибольшим общим делителем** и обозначается $\text{НОД}(a_1, a_2, \dots, a_n)$.

Кроме указанного выше, для наибольшего общего делителя будем применять и обозначение $d(a_1, a_2, \dots, a_n)$, для произвольного общего делителя – обозначение $\delta(a_1, a_2, \dots, a_n)$ или $\text{ОД}(a_1, a_2, \dots, a_n)$.

Определение 1.5. Целое число $p > 1$ называется **простым**, если оно имеет ровно два (положительных) делителя: единицу и самого себя. Целое число, большее 1, имеющее кроме единицы и самого себя другие положительные делители, называется **составным**. Если $\text{НОД}(a_1, a_2, \dots, a_n) = 1$, то числа $a_1, a_2, \dots, a_n$ называются **взаимно простыми**. Если каждое из чисел $a_1, a_2, \dots, a_n$ взаимно просто с каждым другим из них, то числа $a_1, a_2, \dots, a_n$ называются **попарно простыми**.

Очевидно, что числа попарно простые будут и взаимно простыми. В случае двух чисел, $n = 2$, понятия «попарно простые» и «взаимно простые» совпадают.

2. Общие делители двух чисел. Алгоритм Евклида

Лемма 1.3. Если a кратно b , то множество общих делителей чисел a и b совпадает с множеством делителей числа b , в частности $d(a, b) = b$.

Лемма 1.4. Если $a = bq + c$, то множество общих делителей чисел a и b совпадает с множеством общих делителей чисел b и c , в частности $d(a, b) = d(b, c)$.

▷ Из равенства $a = bq + c$ следует: всякий общий делитель чисел a и b является делителем и числа c , т. е. общим делителем b и c ; из него же следует: всякий общий делитель чисел b и c является делителем и числа a , т. е. общим делителем a и b (лемма 1.2). Таким образом, множество всех общих делителей чисел a и b совпадает с множеством всех общих делителей чисел b и c . Отсюда следует вывод: $d(a, b) = d(b, c)$. ◀

Для вычисления наибольшего общего делителя (НОД) применяется **алгоритм Евклида**. Алгоритм назван в честь греческого математика Евклида (III век до н. э.), который впервые описал его в VII и X книгах «Начал». В самом простом случае алгоритм Евклида применяется к паре положительных целых чисел и на каждом шаге формирует новую пару, которая состоит из меньшего числа и остатка от деления большего числа на меньшее. Принцип действия алгоритма основан на утверждении теоремы 1.2.

Теорема 1.2. НОД положительных целых чисел a и b ($a > b$) равен последнему отличному от нуля остатку следующей цепочки равенств:

$$\bar{a} = \bar{b}q_1 + \underline{r_1};$$

$$\bar{b} = \underline{\bar{r}_1}q_2 + \underline{r_2};$$

$$\bar{r_1} = \underline{\bar{r}_2}q_3 + \underline{r_3};$$

...

$$\bar{r_{n-2}} = \underline{\bar{r_{n-1}}}q_n + \underline{r_n};$$

$$\bar{r_{n-1}} = \underline{\bar{r_n}}q_{n+1} + \underline{0},$$

т. е. $d(a, b) = r_n$. Здесь $0 < r_1 < b$, $0 < r_2 < r_1$, $0 < r_3 < r_2$, ..., $0 < r_n < r_{n-1}$.

▷ Каждое равенство цепочки из теоремы 1.2 и неравенства вида $0 < r_{j+1} < r_j$, $j = 1, \dots, n-1$ имеют место в силу теоремы 1.1. В каждом равенстве цепочки пара чисел с черточками сверху имеет НОД такой же, какой имеет пара чисел с черточками внизу (лемма 1.4), при этом число, входящее в каждую из этих двух пар, имеет две черточки: одну сверху, одну внизу. В силу указанной леммы 1.4 справедливы равенства:

$$d(a, b) = d(b, r_1) = d(r_1, r_2) = \dots = d(r_{n-2}, r_{n-1}) = d(r_{n-1}, r_n) = d(r_n, 0) = r_n.$$

Цепочка равенств заканчивается, когда получается $r_{n+1} = 0$. Последнее неизбежно, так как цепочка b, r_1, r_2 и т. д., как цепочка убывающих целых, не может содержать более чем b положительных чисел. ◀

Пример 1.4 (вычисления НОД двух натуральных чисел). Вычислить $\text{НОД}(8281, 3234) = d(8281, 3234)$ с помощью алгоритма Евклида.

$$1) \quad 8281 = \underline{3234} \cdot 2 + \underline{1813}; \quad 3234 = \underline{1813} \cdot 1 + \underline{1421}; \quad 1813 = \underline{1421} \cdot 1 + \underline{392}; \\ 1421 = \underline{392} \cdot 3 + \underline{245}; \quad 392 = \underline{245} \cdot 1 + \underline{147}; \quad 245 = \underline{147} \cdot 1 + \underline{98}; \quad 147 = \underline{98} \cdot 1 + \underline{49}; \\ 98 = \underline{49} \cdot 2 + \underline{0}.$$

Отсюда следует, что $d(8281, 3234) = 49$. Для получения вышезаписанных равенств, начиная со второго, выполнялось деление уголком чисел, подчеркнутых в предыдущем равенстве. Первое равенство получалось делением уголком заданных чисел.

$$\begin{array}{r} \underline{8281} \overline{) 3234} \\ \underline{6468} \\ 1813 \end{array} \quad 2; \quad \begin{array}{r} \underline{3234} \overline{) 1813} \\ \underline{1813} \\ 1421 \end{array} \quad 1; \quad \begin{array}{r} \underline{1813} \overline{) 1421} \\ \underline{1421} \\ 392 \end{array} \quad 1; \text{ и т. д.}$$

Обратное прохождение по цепочке равенств алгоритма Евклида подтверждает справедливость теоремы.

Теорема 1.3 (о представлении НОД(a, b) через числа a и b). Если $d = \text{НОД}(a, b)$, то существуют такие целые u и v , что выполняется соотношение

$$d = au + bv.$$

Последнее равенство называют *соотношением Безу* для НОД целых чисел a и b .

Пример нахождения соотношения Безу для НОД(8281, 3234).

$$\begin{aligned} 49 &= 147 + 98(-1) = 147 + (245 + 147(-1))(-1) = 147 \cdot 2 + 245 \cdot (-1) = \\ &= (392 + 245 \cdot (-1)) \cdot 2 + 245 \cdot (-1) = 392 \cdot 2 + 245 \cdot (-3) = 392 \cdot 2 + \\ &+ (1421 + 392 \cdot (-3)) \cdot (-3) = 392 \cdot 11 + 1421 \cdot (-3) = (1813 + 1421 \cdot (-1)) \cdot 11 + \\ &+ 1421 \cdot (-3) = 1813 \cdot 11 + 1421 \cdot (-14) = 1813 \cdot 11 + (3234 + 1813 \cdot (-1)) \cdot (-14) = \\ &= 1813 \cdot 25 + 3234 \cdot (-14) = (8281 + 3234 \cdot (-2)) \cdot 25 + 3234 \cdot (-14) = \\ &= 8281 \cdot 25 + 3234 \cdot (-64), \quad \text{т. е. } 49 = 8281 \cdot 25 + 3234 \cdot (-64). \end{aligned}$$

В приведенном выше примере необходимо выполнить алгоритм Евклида дважды – сначала в прямом, а затем в обратном направлении.

Предложим еще один способ, который не требует обратной прогонки алгоритма – **расширенный алгоритм Евклида**. Этот способ основан на том, чтобы на каждом i -м шаге алгоритма Евклида для нахождения НОД(a, b) получившийся остаток r_i представить в виде линейной комбинации a и b с целочисленными коэффициентами u_i и v_i :

$$1\text{-й шаг: } a = bq_1 + r_1 \Rightarrow r_1 = a - q_1b \Rightarrow r_1 = au_1 + bv_1, \text{ где } u_1 = 1, v_1 = -q_1$$

$$\begin{aligned} 2\text{-й шаг: } b &= r_1q_2 + r_2 \Rightarrow r_2 = b - r_1q_2 = [\text{подставим } r_1 \text{ из 1-го шага}] = \\ &= b - (au_1 + bv_1)q_2 = a(-q_2u_1) + b(1 - q_2v_1) \Rightarrow \\ &\Rightarrow r_2 = au_2 + bv_2, \text{ где } u_2 = 0 - q_2u_1, v_2 = 1 - q_2v_1 \end{aligned}$$

$$\begin{aligned} 3\text{-й шаг: } r_1 &= r_2q_3 + r_3 \Rightarrow \\ &\Rightarrow r_3 = r_1 - r_2q_3 = [\text{подставим } r_1 \text{ и } r_2 \text{ из 1-го и 2-го шагов}] = \\ &= au_1 + bv_1 - (au_2 + bv_2)q_3 = a(u_1 - q_3u_2) + b(v_1 - q_3v_2) \Rightarrow \\ &\Rightarrow r_3 = au_3 + bv_3, \text{ где } u_3 = u_1 - q_3u_2, v_3 = v_1 - q_3v_2 \end{aligned}$$

$$\begin{aligned}
k\text{-й шаг: } r_{k-2} = r_{k-1}q_k + r_k &\Rightarrow r_k = r_{k-2} - r_{k-1}q_k = [\text{подставим } r_{k-2} \text{ и } r_{k-1}] = \\
&= au_{k-2} + bv_{k-2} - (au_{k-1} + bv_{k-1})q_k = a(u_{k-2} - q_k u_{k-1}) + b(v_{k-2} - q_k v_{k-1}) \Rightarrow \\
&\Rightarrow r_k = au_k + bv_k, \text{ где } u_k = u_{k-2} - q_k u_{k-1}, v_k = v_{k-2} - q_k v_{k-1}.
\end{aligned}$$

Таким образом, положив $u_0 = 0, v_0 = 1, u_1 = 1, v_1 = -q_1$, где q_i – частное на i -м шаге, получим рекуррентные формулы для расчетов коэффициентов u_i и v_i :

$$u_i = u_{i-2} - q_i u_{i-1}, \quad v_i = v_{i-2} - q_i v_{i-1}, \quad i \geq 2.$$

На каждом шаге расширенного алгоритма Евклида рассчитываются остаток r_i , частное q_i и коэффициенты u_i и v_i . На шаге с последним ненулевым остатком u_i и v_i будут являться искомыми величинами u и v . (Пример использования расширенного алгоритма Евклида см. в параграфе 6 и решении типовых задач.)

Замечание. Если числа a и b взаимно простые, то соотношение Безу приобретает вид $au + bv = 1$.

Теорема 1.4 (критерий взаимной простоты целых чисел). *Целые числа a и b являются взаимно простыми тогда и только тогда, когда существуют такие целые u и v , для которых выполняется равенство $au + bv = 1$.*

Лемма 1.5 (следствие из теоремы 1.4). *Если произведение ab целых чисел делится на целое число c и $d(a, c) = 1$, то b делится на c .*

Определение 1.6. *Общим кратным целых чисел $a_1, a_2, \dots, a_n$ называется всякое целое число, которое кратно каждому из $a_1, a_2, \dots, a_n$, т. е. делится на каждое из этих чисел без остатка. Наименьшее из всех общих кратных этих чисел называется их **наименьшим общим кратным** и обозначается*

$$\text{НОК}(a_1, a_2, \dots, a_n).$$

Свойство НОК и НОД двух чисел. Для любых двух целых чисел a и b верно равенство $\text{НОК}(a, b) \cdot \text{НОД}(a, b) = a \cdot b$.

§ 3. Простые числа. Основная теорема арифметики

1. Простые числа и их нахождение

Очевидно: если число $a > 1$ составное, то его можно представить в виде $a = b \cdot c$, где хотя бы одно из двух чисел b, c принадлежит отрезку $[2, \sqrt{a}]$, поскольку в противном случае $b \cdot c > \sqrt{a} \cdot \sqrt{a} = a$ и равенство $a = b \cdot c$ не выполнится (здесь все числа целые, больше единицы). Также очевидно, что наименьший натуральный делитель натурального числа является числом простым, следовательно, *наименьший натуральный делитель обязательно является простым числом из отрезка $[2, \sqrt{a}]$* . Можно заключить, что при проверке, является ли простым некоторое заданное число m , достаточно выяснить простым перебором, делится ли m на какое-либо простое число из отрезка $[2, \sqrt{m}]$. Если среди простых

чисел, принадлежащих этому отрезку, делителей числа m не нашлось, то проверять делимость m на числа большие $\sqrt{m}$ нет необходимости – можно утверждать, что число m простое.

Теорема 1.5 (о количестве простых чисел). *Простых чисел бесконечно много.*

Иначе говоря, множество простых чисел не ограничено сверху.

Для нахождения простых чисел, не превосходящих данного натурального числа, существует способ, называемый **решето Эратосфена**. Этот способ назван в честь его создателя – древнегреческого математика Эратосфена Киренского, который предложил процедуру фильтрации списка чисел от 2 до n с целью выявления и зачеркивания всех составных чисел в нем.

Поясним подробнее эту процедуру.

Для того чтобы отыскать все простые числа, не превосходящие n , выписываем по порядку все натуральные числа от 1 до n

$$1, 2, 3, \dots, n$$

и далее «просеиваем» это множество, предварительно вычеркнув из него 1 (1 по определению простым числом не является), в направлении увеличения его элементов, оставляя простые числа и вычеркивая составные.

На первом шаге процедуры наименьшее в списке простое число есть 2. Его оставляем, а числа, кратные 2, вычеркиваем. Очевидно, первым вычеркнутым является $4 = 2^2$.

На втором шаге переходим к наименьшему невычеркнутому числу. Оно равно 3 и является простым, следовательно, оставляем его. Вычеркиваем все числа, кратные 3, которые еще не было вычеркнуты на первом шаге. Первым вычеркиваемым на этот раз будет число $9 = 3^2$, так как 6 уже было вычеркнуто как кратное 2.

На третьем шаге наименьшее из невычеркнутых чисел – это простое число 5. Оставляем его и вычеркиваем все числа, кратные 5, которые еще не были вычеркнуты ранее. Теперь первым вычеркиваемым является $25 = 5^2$, так как 10, 15, 20 уже вычеркнуты по причине кратности 2 или 3.

Рисунок 1 иллюстрирует действия решета Эратосфена при поиске простых чисел, не превосходящих 17.

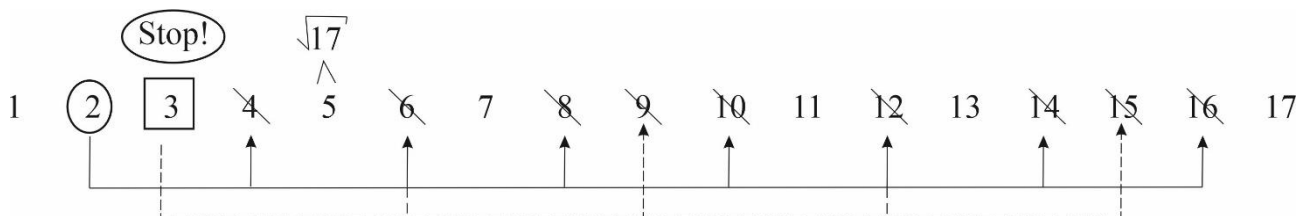


Рис. 1. Механизм «просеивания» через решето Эратосфена

Начальные шаги решета Эратосфена демонстрируют общие закономерности этого алгоритма. Во-первых, в начале каждого шага число m – наименьшее

из невычеркнутых чисел – обязательно является простым. Если бы оно было составным, то его наименьший делитель был бы среди простых чисел, не превосходящих $\sqrt{m}$. Все такие простые числа заведомо меньше m , и кратные этим простым уже вычеркнули на предыдущих шагах, но тогда бы и m было вычеркнуто. Следовательно, наименьшее невычеркнутое m составным быть не может. Во-вторых, на этом же шаге алгоритма наименьшее из вычеркиваемых составных чисел равно m^2 . Все составные числа l , меньшие m^2 , имеют простой делитель, не превосходящий $\sqrt{l}$. Так как $l < m^2$, то $\sqrt{l} < m$; т. е. каждое составное число l , меньшее m^2 , кратно некоторому простому числу, меньшему m . Но такие кратные числа уже вычеркнуты на предыдущих шагах. Следовательно, m^2 первое вычеркиваемое на данном шаге.

Из описанных общих закономерностей следует условие остановки алгоритма. Если на каком-либо шаге наименьшее невычеркнутое простое m равно $\sqrt{n}$, то первым вычеркиваемым будет число $m^2 = n$, завершающее список. Больше ничего вычеркнуть нельзя, остались только простые числа. Если же $\sqrt{n}$ не является простым числом, то на каком-либо шаге наименьшее невычеркнутое простое число m превысит $\sqrt{n}$. В таком случае первый кандидат на вычеркивание $m^2 > n$ и процесс вычеркивания также останавливается на наибольшем простом числе, меньшем $\sqrt{n}$. Таким образом, алгоритм продолжается до тех пор, пока наименьшее невычеркнутое число не превосходит $\sqrt{n}$. В примере использования решета Эратосфена для «просеивания» простых чисел, не превосходящих 17, показанном на рис. 1, алгоритм останавливается на втором шаге, так как $5 < \sqrt{17}$. Таким образом, после выполнения алгоритма остались невычеркнутыми только простые числа 5, 7, 11, 13, 17.

2. Основная теорема арифметики

Лемма 1.6. Совокупность ОД чисел a и b совпадает с совокупностью делителей их НОД.

Лемма 1.7. Для любого целого числа m справедливо равенство $d(am, bm) = d(a, b) \cdot m$, где $d(a, b) = \text{НОД}(a, b)$.

Лемма 1.8. Если $d(a, b) = 1$, то $d(ac, b) = d(c, b)$.

Лемма 1.9. Если каждое $a_1, a_2, \dots, a_m$ взаимно просто с каждым $b_1, b_2, \dots, b_n$, то и произведение $a_1 a_2 \dots a_m$ взаимно просто с произведением $b_1 b_2 \dots b_n$.

Лемма 1.10. Всякое целое a или взаимно просто с данным простым числом p , или делится на p .

Лемма 1.11. Если произведение нескольких сомножителей делится на данное простое p , то по крайней мере один из сомножителей делится на число p .

Теорема 1.6 (основная теорема арифметики). Каждое натуральное число $a > 1$ является или простым числом, или единственным образом (с точностью до перестановки сомножителей) представляется произведением степеней простых чисел

$$a = p_1^{n_1} \cdot p_2^{n_2} \cdot \dots \cdot p_m^{n_m},$$

где $p_1, p_2, \dots, p_m$ – различные простые числа, $n_1, n_2, \dots, n_m$ – натуральные числа. Такое представление называется **каноническим представлением** числа a , а также **каноническим разложением** числа, а сам процесс нахождения такого разложения называется **факторизацией** числа a .

Очевидно следующее следствие из этой теоремы.

Следствие 1.1. Пусть a имеет каноническое представление вида $a = p_1^{n_1} \cdot p_2^{n_2} \cdot \dots \cdot p_m^{n_m}$. Тогда множество всех делителей числа a составляют числа вида $p_1^{k_1} \cdot p_2^{k_2} \cdot \dots \cdot p_m^{k_m}$; $0 \leq k_1 \leq n_1, 0 \leq k_2 \leq n_2, \dots, 0 \leq k_m \leq n_m$.

§ 4. Сравнения

1. Основные понятия и свойства сравнений

Выше, в параграфах 1 и 2, рассматривалось деление целых чисел с остатком. Далее расширим это понятие до модулярной арифметики. Будем объединять целые числа во множества по признаку одинаковых **остатков от деления** их на данное целое положительное m , которое назовем **модулем**. Мы уже знаем, что каждому целому числу отвечает определенный остаток от деления его на число m (теорема 1.1).

Определение 1.7. Если два целых числа a и b при их делении на число m имеют один и тот же остаток r , то эти числа называются **равноостаточными по модулю m** или **сравнимыми по модулю m** .

Сравнимость чисел a и b по модулю m записывается так:

$$a \equiv b \pmod{m} \quad \text{или} \quad a \equiv b(m),$$

читается так: a **сравнимо с b по модулю m** .

Соотношение $a \equiv b \pmod{m}$ или $a \equiv b(m)$ называют **сравнением по модулю m** .

Теорема 1.7 (о сравнимости двух чисел). Целые числа a и b сравнимы по модулю m тогда и только тогда, когда справедливо хотя бы одно из следующих трех равносильных условий:

- 1) a и b имеют одинаковые остатки (один и тот же остаток) от деления на m ;
- 2) $(a - b)$ делится на m , т. е. существует такое целое q , что $a - b = mq$;
- 3) $a = b + mq$ для некоторого целого q .

Пример 1.5 (чисел, сравнимых по модулю 8). Выполнив деление некоторых целых чисел на 8 (чисел, имеющих от деления остаток 3)

$$\begin{array}{r} 3 \overline{)8} \\ 0 \overline{)0} \\ \hline 3 \end{array} ; \quad \begin{array}{r} 5 \overline{)8} \\ 8 \overline{)-1} \\ \hline 3 \end{array} ; \quad \begin{array}{r} 21 \overline{)8} \\ 24 \overline{)-3} \\ \hline 3 \end{array} ; \quad \begin{array}{r} 11 \overline{)8} \\ 8 \overline{)1} \\ \hline 3 \end{array} ,$$

видим, что $-21 \equiv -5 \pmod{8} \equiv 3 \pmod{8} \equiv 11 \pmod{8}$.

Свойства сравнений

С1. Два числа, сравнимые с третьим, сравнимы между собой (по тому же модулю).

С2. Сравнения можно складывать и вычитать, т. е. если $a \equiv b \pmod{m}$, $c \equiv h \pmod{m}$, то $(a \pm c) \equiv (b \pm h) \pmod{m}$.

Замечание. Далее для краткости вместо записи $a \equiv b \pmod{m}$ будем применять равносильную запись $a \equiv b \pmod{m}$.

С3. Слагаемое левой (правой) части сравнения можно переносить в другую часть, поменяв знак перед ним на противоположный.

С4. К каждой части сравнения можно прибавить любое число, кратное модулю (не обязательно одно и то же к обеим частям).

С5. Сравнения можно перемножать, что означает: если $a \equiv b \pmod{m}$, $c \equiv h \pmod{m}$, то $ac \equiv bh \pmod{m}$.

С6. Обе части сравнения можно возвести в одну и ту же натуральную степень, а также умножить на одно и то же целое: если $a \equiv b \pmod{m}$, то $a^n \equiv b^n \pmod{m} \forall n \in \mathbb{Z}$ и $ka \equiv kb \pmod{m} \forall k \in \mathbb{Z}$.

С7. Обе части сравнения можно разделить на взаимно простой с модулем их общий делитель: если $a \equiv b \pmod{m}$, $\text{ОД}(a, b) = \delta$ и $\text{НОД}(\delta, m) = 1$, то $\frac{a}{\delta} \equiv \frac{b}{\delta} \pmod{m}$.

С8. Обе части сравнения и модуль можно умножить на одно и то же целое и можно разделить на любой их общий делитель: если $a \equiv b \pmod{m}$ и $\text{ОД}(a, b, m) = \delta$, то $\frac{a}{\delta} \equiv \frac{b}{\delta} \pmod{\frac{m}{\delta}}$.

Свойство С8 можно сформулировать и таким образом: если в сравнении $a \equiv b \pmod{m}$ числа a, b, m имеют общий делитель δ , т. е. $a = \delta a_1$, $b = \delta b_1$, $m = \delta m_1$, то $a_1 \equiv b_1 \pmod{m_1}$.

С9. Если одна часть сравнения и модуль делятся на какое-либо число, то и другая часть сравнения должна делиться на то же число: если $a \equiv b \pmod{m}$ и $a : \delta, m : \delta$, то и $b : \delta$, если $a \equiv b \pmod{m}$ и $b : \delta, m : \delta$, то и $a : \delta$.

С10. К обеим частям сравнения можно добавить одно и то же число, т. е. если $a \equiv b \pmod{m}$, то $(a + c) \equiv (b + c) \pmod{m}$ для всякого целого c (c может быть и отрицательным).

2. Функция Эйлера

Определение 1.8. Функцией Эйлера или ϕ -функцией называется функция натурального аргумента $n > 1$, значение которой равно количеству натуральных чисел, не превосходящих n и взаимно простых с n . Функция Эйлера обозначается $\phi(n)$.

Пример 1.6. Найдем значение функции Эйлера для чисел 8 и 7. Числа, взаимно простые с 8 и не превосходящие его: 1, 3, 5, 7, следовательно, $\varphi(8) = 4$. Числа, взаимно простые с 7 и не превосходящие его: 1, 2, 3, 4, 5, 6, тогда $\varphi(7) = 6$.

Свойства функции Эйлера:

1. Если p – простое число, то $\varphi(p) = p - 1$.
2. Если p – простое число, то $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$, где $\alpha \in \mathbb{N}$, $\alpha > 1$.
3. Если a и b – взаимно простые числа, то $\varphi(ab) = \varphi(a)\varphi(b)$.
4. Если известно каноническое разложение числа $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$, где $\alpha_i \in \mathbb{N}$, $\alpha_i > 1$, $i = 1, \dots, s$, то

$$\varphi(n) = p_1^{\alpha_1-1} p_2^{\alpha_2-1} \dots p_s^{\alpha_s-1} (p_1 - 1)(p_2 - 1) \dots (p_s - 1).$$

Теорема 1.8 (теорема Эйлера). Если a и m – взаимно простые числа и $m > 1$, то $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Теорема 1.9 (малая теорема Ферма). Если a – натуральное число (не делится на p) и p – простое число, то $a^{p-1} \equiv 1 \pmod{p}$.

При всех целых a справедливо равенство

$$a^p \equiv a \pmod{p}.$$

Обратив внимание на свойство 1 функции Эйлера, не сложно увидеть, что малая теорема Ферма – частный случай теоремы Эйлера при простом модуле.

§ 5. Классы вычетов и операции над ними

Рассмотрим остатки от деления произвольного целого числа на данное целое положительное $m > 1$. При таком делении существуют m различных остатков $0, 1, 2, \dots, m-1$. Каждое целое число в зависимости от его остатка при делении на m может быть включено только в одно из подмножеств вида:

$$\begin{aligned}\bar{0} &= \{\dots, -2m, -m, 0, m, 2m, \dots\}, \\ \bar{1} &= \{\dots, -2m+1, -m+1, 1, m+1, 2m+1, \dots\}, \\ \bar{2} &= \{\dots, -2m+2, -m+2, 2, m+2, 2m+2, \dots\}, \dots, \\ \overline{m-1} &= \{\dots, -m-1, -1, m-1, 2m-1, \dots\}.\end{aligned}$$

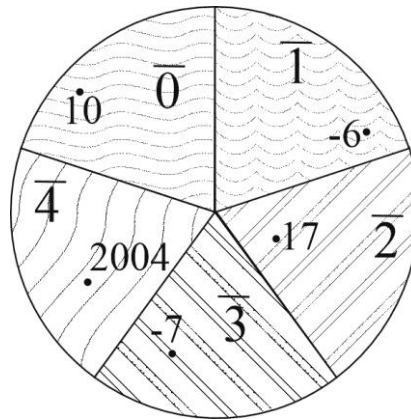
Анализируя элементный состав этих подмножеств целых чисел, замечаем следующее. Так как числа каждого отдельно взятого подмножества имеют один и тот же остаток от деления на число m , то они сравнимы по модулю m . Если же рассмотреть два разных подмножества, например $\bar{k}$ и $\bar{l}$, $\bar{k} \neq \bar{l}$, $\bar{k}, \bar{l} \in \{\bar{0}, \bar{1}, \dots, \overline{m-1}\}$, и взять в каждом из них произвольные элементы $k_1 \in \bar{k}$, $l_1 \in \bar{l}$, то взятые два элемента k_1 и l_1 не сравнимы по модулю m . Это означает, что подмножества $\bar{0}, \bar{1}, \dots, \overline{m-1}$ попарно не пересекаются.

Определение 1.8. *Классом вычетов по модулю m называют множество всех сравнимых друг с другом по модулю m чисел. Любое число из класса (представитель класса) называют **вычетом** по модулю m . Если число k является представителем некоторого класса, то этот класс вычетов обозначают $\bar{k}$. Множество $\{\bar{0}, \bar{1}, \dots, \overline{m-1}\}$ всех классов вычетов по модулю m обозначают: $\mathbb{Z}/m\mathbb{Z}$:*

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

Пример 1.7. Всем хорошо известны классы вычетов по модулю 2 – это четные ($\bar{0}$) и нечетные ($\bar{1}$) числа.

На рис. 2 отражено разбиение множества целых чисел на классы вычетов по модулю 5.



$$10 \in \bar{0}, -6 \in \bar{1}, 17 \in \bar{2}, -7 \in \bar{3}, 2004 \in \bar{4}$$

Рис. 2. Диаграмма классов вычетов $\mathbb{Z}/5\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$

Определение 1.9. *Полной системой вычетов (ПОВ) по модулю m называют множество из m вычетов, взятых по одному из каждого класса множества $\mathbb{Z}/m\mathbb{Z}$.*

Чаще всего в качестве полной системы вычетов выбирают наименьшие неотрицательные вычеты $0, 1, 2, \dots, m-1$.

Лемма 1.12. *Любые m чисел, попарно не сравнимые по модулю m , образуют полную систему вычетов по этому модулю.*

Лемма 1.13. *Если $d(a, m)=1$ и x пробегает полную систему вычетов по модулю m , то $ax + b$, где b – любое целое, тоже пробегает ПСВ по модулю m .*

Отметим, что класс вычетов полностью определяется одним своим представителем, так как если известно, что число k принадлежит некоторому классу, то согласно п. 3 теоремы 1.7 все остальные элементы этого класса можно отыскать как сравнимые с k числа по формуле $k + mq$, $q \in \mathbb{Z}$. Поэтому для обозначения класса вычетов достаточно указать один конкретный вычет. Если два класса обозначены сравнимыми между собой вычетами, то эти классы – **совпадающие (равные)** множества.

Лемма 1.14. Классы вычетов $\bar{k}$ и $\bar{l}$ по модулю m являются **равными** тогда и только тогда, если k сравнимо с l по модулю m : $\bar{k} = \bar{l}$, $\bar{k}, \bar{l} \in \mathbb{Z}/m\mathbb{Z} \Leftrightarrow k \equiv l(m)$. Таким образом, $\bar{k} = \overline{k + mq}$.

Пример 1.8. На множестве $\mathbb{Z}/5\mathbb{Z}$ верны равенства

$$\bar{6} = \overline{1+5} = \bar{1}, \bar{12} = \overline{2+2 \cdot 5} = \bar{2}.$$

Рассмотрим два класса $\bar{k}$ и $\bar{l}$ из множества $\mathbb{Z}/m\mathbb{Z}$, $\bar{k} \neq \bar{l}$. Выберем произвольным образом пару чисел: k_1 – вычет из класса $\bar{k}$ и l_1 – вычет из класса $\bar{l}$. Сумма $k_1 + l_1$ будет принадлежать классу вычетов $\bar{n}$ из $\mathbb{Z}/m\mathbb{Z}$, причем можно показать, что класс $\bar{n}$ не зависит от выбора чисел k_1 и l_1 . На основании этого свойства вводится операция сложения двух классов.

Определение 1.10. Суммой классов вычетов $\bar{k}$ и $\bar{l}$ называется единственный класс вычетов из $\mathbb{Z}/m\mathbb{Z}$, которому принадлежат все суммы вида $k_1 + l_1$, где $k_1 \in \bar{k}$, $l_1 \in \bar{l}$.

Также можно показать, что класс, которому принадлежит произведение чисел k_1 и l_1 , не зависит от выбора чисел k_1 и l_1 .

Определение 1.11. Произведением классов вычетов $\bar{k}$ и $\bar{l}$ называется единственный класс вычетов из $\mathbb{Z}/m\mathbb{Z}$, которому принадлежат все произведения вида $k_1 l_1$, где $k_1 \in \bar{k}$, $l_1 \in \bar{l}$.

Сумма и произведение классов вычетов определяются по следующим правилам:

1. Для того чтобы сложить два класса вычетов, необходимо выбрать представитель из каждого класса, сложить их и взять класс, к которому принадлежит полученная сумма.
2. Для того чтобы умножить один класс вычетов на другой, необходимо выбрать представитель из каждого класса, перемножить их и взять класс, к которому принадлежит полученное произведение.

Свойства операций сложения и умножения классов вычетов:

1. Коммутативность сложения и умножения:

$$\forall \bar{k}, \bar{l} \in \mathbb{Z}/m\mathbb{Z} \text{ имеет место } \bar{k} + \bar{l} = \bar{l} + \bar{k}, \bar{k} \cdot \bar{l} = \bar{l} \cdot \bar{k}.$$

2. Ассоциативность сложения и умножения:

$$\forall \bar{k}, \bar{l}, \bar{n} \in \mathbb{Z}/m\mathbb{Z} \text{ имеет место } (\bar{k} + \bar{l}) + \bar{n} = \bar{k} + (\bar{l} + \bar{n}), (\bar{k} \cdot \bar{l}) \cdot \bar{n} = \bar{k} \cdot (\bar{l} \cdot \bar{n}).$$

3. Существование нейтрального элемента относительно сложения и относительно умножения:

нейтральный элемент относительно сложения – класс $\bar{0}$:

$$\forall \bar{k} \in \mathbb{Z}/m\mathbb{Z} \text{ имеет место } \bar{k} + \bar{0} = \bar{0} + \bar{k} = \bar{k};$$

нейтральный элемент относительно умножения – класс $\bar{1}$:

$$\forall \bar{k} \in \mathbb{Z}/m\mathbb{Z} \text{ имеет место } \bar{k} \cdot \bar{1} = \bar{1} \cdot \bar{k} = \bar{k}.$$

4. *Существование противоположного элемента относительно сложения:*

$$\forall \bar{k} \in \mathbb{Z}/m\mathbb{Z} \exists (-\bar{k}): \quad \bar{k} + (-\bar{k}) = \bar{0}.$$

5. *Дистрибутивность сложения относительно умножения:*

$$\forall \bar{k}, \bar{l}, \bar{n} \in \mathbb{Z}/m\mathbb{Z} \text{ имеет место } (\bar{k} + \bar{l}) \cdot \bar{n} = \bar{k} \cdot \bar{n} + \bar{l} \cdot \bar{n}.$$

Следствие из четвертого свойства: на множестве классов вычетов $\mathbb{Z}/m\mathbb{Z}$ можно ввести **операцию вычитания** как дополнительную к операции сложения:

$$\forall \bar{k}, \bar{l} \in \mathbb{Z}/m\mathbb{Z} \text{ имеет место } \bar{k} - \bar{l} = \bar{k} + (-\bar{l}),$$

где $(-\bar{l})$ – класс, противоположный классу $\bar{l}$.

Правило вычитания классов вычетов аналогично правилу сложения: для того чтобы от одного класса вычетов отнять другой, необходимо выбрать представитель из каждого класса, от представителя первого класса отнять представитель второго и взять класс, к которому принадлежит полученная разность.

Операции сложения и умножения, введенные на множестве классов вычетов $\mathbb{Z}/m\mathbb{Z}$ и удовлетворяющие совокупности свойств 1–5, формируют из множества $\mathbb{Z}/m\mathbb{Z}$ алгебраическую структуру, которая называется **коммутативным кольцом с единицей**. В дальнейшем, говоря не просто «множество классов вычетов», а именно «кольцо классов вычетов», мы тем самым подчеркиваем, что определены операции умножения и сложения указанным выше образом. Более подробно о кольцах как об алгебраических структурах речь пойдет в четвертом модуле.

Определение 1.12. Класс $\bar{x} \in \mathbb{Z}/m\mathbb{Z}$ называется **обратным** к классу $\bar{a} \in \mathbb{Z}/m\mathbb{Z}$, если верно равенство $\bar{x} \cdot \bar{a} = \bar{1}$.

Класс, обратный к классу $\bar{a}$, обозначается $\bar{a}^{-1}$.

Пример 1.9. В кольце классов вычетов $\mathbb{Z}/5\mathbb{Z}$ верно равенство $\bar{2} \cdot \bar{3} = \bar{6} = \bar{1}$, значит, класс $\bar{2}$ является обратным к классу $\bar{3}$, и наоборот: $\bar{3}^{-1} = \bar{2}$, $\bar{2}^{-1} = \bar{3}$.

Определение 1.13. **Обратимый класс вычетов** – класс вычетов, к которому существует обратный.

Пример 1.10. В кольце $\mathbb{Z}/5\mathbb{Z}$ классы $\bar{2}$ и $\bar{3}$ являются обратимыми.

Является ли конкретный класс обратимым, зависит от его соотношения с модулем m кольца $\mathbb{Z}/m\mathbb{Z}$.

Теорема 1.10 (критерий обратимого класса). Для класса $\bar{k} \in \mathbb{Z}/m\mathbb{Z}$ существует обратный тогда и только тогда, когда k и m – взаимно простые числа.

Следствие. В кольце классов вычетов с простым модулем всякий ненулевой класс обратим.

Замечание. Так как в общем случае не всякий класс вычетов является обратимым, то **на множестве $\mathbb{Z}/m\mathbb{Z}$ не определена операция деления!** Нельзя делить класс вычетов на другой класс!

Свойства обратимых классов. Если класс $\bar{k} \in \mathbb{Z}/m\mathbb{Z}$ обратим, то:

- 1) обратный к нему класс $\bar{k}^{-1} \in \mathbb{Z}/m\mathbb{Z}$ определен единственным образом;
- 2) для любого ненулевого класса $\bar{l} \in \mathbb{Z}/m\mathbb{Z}$ произведение $\bar{k} \cdot \bar{l} \neq \bar{0}$;
- 3) для любых двух классов $\bar{l}_1, \bar{l}_2 \in \mathbb{Z}/m\mathbb{Z}$ равенство $\bar{k} \cdot \bar{l}_1 = \bar{k} \cdot \bar{l}_2$ имеет место тогда и только тогда, когда $\bar{l}_1 = \bar{l}_2$;
- 4) если в произведении $\bar{k} \cdot \bar{l}$ класс $\bar{l}$ пробегает всевозможные значения из $\mathbb{Z}/m\mathbb{Z}$, то и результат произведения также пробегает всевозможные значения из $\mathbb{Z}/m\mathbb{Z}$ без повторов, т. е. полную систему вычетов;
- 5) обратный класс $\bar{k}^{-1} \in \mathbb{Z}/m\mathbb{Z}$ также обратим, причем $(\bar{k}^{-1})^{-1} = \bar{k}$;
- 6) произведение обратимых классов также является обратимым классом.

Свойства необратимых классов. Если класс $\bar{k} \in \mathbb{Z}/m\mathbb{Z}$ необратим, то:

- 1) существует такой ненулевой класс $\bar{l} \in \mathbb{Z}/m\mathbb{Z}$, что произведение $\bar{k} \cdot \bar{l} = \bar{0}$;
- 2) существуют два не равных между собой класса $\bar{l}_1, \bar{l}_2 \in \mathbb{Z}/m\mathbb{Z}$, $\bar{l}_1 \neq \bar{l}_2$, таких, что $\bar{k} \cdot \bar{l}_1 = \bar{k} \cdot \bar{l}_2$.

Из свойств обратимых и необратимых классов следует важный вывод:

в равенстве $\bar{k} \cdot \bar{l}_1 = \bar{k} \cdot \bar{l}_2$ формально можно выполнить сокращение на класс $\bar{k}$ тогда и только тогда, когда класс $\bar{k}$ **обратим**, т. е. k взаимно просто с модулем m .

Способы нахождения обратных классов.

Один из способов нахождения класса, обратного к $\bar{k}$, следует из теоремы Эйлера:

$$k^{\varphi(m)} \equiv 1(m) \Leftrightarrow \overline{k^{\varphi(m)}} = \bar{1} \Leftrightarrow \overline{k \cdot k^{\varphi(m)-1}} = \bar{1} \Leftrightarrow \bar{k}^{-1} = \overline{k^{\varphi(m)-1}}.$$

Второй способ использует соотношение Безу для взаимно простых чисел k и m :

$$\begin{aligned} \text{НОД}(k, m) = 1 = m \cdot u + k \cdot v &\Leftrightarrow \bar{1} = \bar{m} \cdot \bar{u} + \bar{k} \cdot \bar{v} = \left[\bar{m} = \bar{0} \right] = \bar{k} \cdot \bar{v} \Leftrightarrow \\ &\Leftrightarrow \bar{k} \cdot \bar{v} = \bar{1} \Leftrightarrow (\bar{k})^{-1} = \bar{v}. \end{aligned}$$

С обратимыми классами тесно связано понятие приведенной системы вычетов.

Определение 1.14. *Приведенной системой вычетов по модулю m называют множество вычетов, взятых по одному из каждого класса, содержащего взаимно простые с модулем m числа, т. е. из каждого обратимого класса.*

Из определения приведенной системы вычетов и функции Эйлера следует, что число элементов в приведенной системе вычетов по модулю m равно $\varphi(m)$.

§ 6. Решение сравнений

В этом параграфе будем рассматривать сравнения, содержащие неизвестные, и начнем со сравнений с одним неизвестным. В общем случае такие сравнения имеют вид:

$$f(x) \equiv 0 \pmod{m}; \quad f(x) = a_0 x^n + a_1 x^{n-1} + \dots + a_n,$$

где $a_0, a_1, \dots, a_n$ – целые числа.

1. О количестве решений сравнения

Если в сравнении $a_0 x^n + a_1 x^{n-1} + \dots + a_n \equiv 0 \pmod{m}$ a_0 не делится на m , то n называется *степенью сравнения*.

Решить сравнение – значит найти все значения x , ему удовлетворяющие, или доказать, что их нет.

Определение 1.15. Два сравнения, которым удовлетворяют одни и те же значения x , называют *равносильными*.

Если сравнению $a_0 x^n + a_1 x^{n-1} + \dots + a_n \equiv 0 \pmod{m}$ удовлетворяет какое-либо $x = x_1$, то тому же сравнению будут удовлетворять и все числа, сравнимые с числом x_1 по модулю m . Действительно, пусть $y_1 \equiv x_1 \pmod{m}$ (в более краткой записи $y_1 \equiv x_1(m)$). Тогда $y_1 = x_1 + mq$ (теорема 1.7, условие 3). Поэтому

$$\begin{aligned} f(y_1) &= a_0(x_1 + mq)^n + a_1(x_1 + mq)^{n-1} + \dots + a_n = a_0 x_1^n + a_1 x_1^{n-1} + \dots + a_n + mA = \\ &= f(x_1) + mA, \end{aligned}$$

где A есть выражение, получаемое после раскрытия скобок $(x_1 + mq)^{n-j}$ по формуле бинома Ньютона и вынесения множителя m за скобки из слагаемых, оставшихся после записи $f(x_1)$. Отсюда следует: если значение x_1 удовлетворяет рассматриваемому сравнению, то и значение y_1 ему удовлетворяет (свойство сравнений С4).

Итак, если сравнению $a_0 x^n + a_1 x^{n-1} + \dots + a_n \equiv 0 \pmod{m}$ удовлетворяет какое-либо $x = x_1$, то тому же сравнению будут удовлетворять и все числа, сравнимые с числом x_1 по модулю m . Весь этот класс чисел будем рассматривать как *одно решение*. При таком соглашении $a_0 x^n + a_1 x^{n-1} + \dots + a_n \equiv 0 \pmod{m}$ будет иметь столько решений, сколько вычетов полной системы ему удовлетворяет.

Пример 1.11. Решить сравнение $x^3 + x + 2 \equiv 0 \pmod{11}$.

Полная система вычетов в нашем примере есть 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10. Из них сравнению удовлетворяют числа 5, 7, 10. Таким образом, рассматриваемое в примере сравнение имеет три решения:

$$x \equiv 5(11), \quad x \equiv 7(11), \quad x \equiv 10(11).$$

2. Сравнения первой степени

Заметим, что сравнение первой степени $ax - b \equiv 0(m)$ можно привести к виду

$$ax \equiv b(m).$$

Рассмотрим несколько примеров.

Случай 1. Решить сравнение

$$35x \equiv 7(\text{mod}12).$$

Перебрав полную систему вычетов $0, 1, \dots, 10, 11$, найдем *ровно одно* число: $x = 5$, удовлетворяющее нашему сравнению, поскольку выполняется равенство $35 \cdot 5 = 12 \cdot 14 + 7$. Итак, сравнение в случае 1 имеет одно решение:

$$x \equiv 5(12).$$

При этом значении x число $35x$ сравнимо с числом 7 по модулю 12 .

Случай 2. Решить сравнение

$$15x \equiv 10(\text{mod}21).$$

Перебрав полную систему вычетов $0, 1, \dots, 20$, убедимся, что ни при одном значении x из этого множества число $15x$ не будет сравнимо с числом 10 по модулю 21 . Это сравнение не имеет решений.

Случай 3. Решить сравнение

$$15x \equiv 12(\text{mod}21).$$

Пробегаая полную систему вычетов случая 2, найдем три числа: $x = 5$, $x = 12$, $x = 19$, при которых $15x$ сравнимо с двенадцатью по модулю 21 . Это означает, что сравнение случая 3 имеет три решения:

$$x \equiv 5(21), \quad x \equiv 12(21), \quad x \equiv 19(21).$$

Эти примеры служат иллюстрацией следующей теоремы.

Теорема 1.11. Пусть $\text{НОД}(a, m) = d$. Сравнение $ax \equiv b(\text{mod} m)$ не имеет решений, если b не делится на НОД чисел a и m , т. е. на число d . При b , кратном d , сравнение имеет d решений вида

$$x_1, \quad x_1 + m_1, \quad x_1 + 2m_1, \quad \dots, \quad x_1 + (d - 1)m_1,$$

где $m_1 = m / d$.

3. Решение сравнений с помощью классов вычетов по модулю m

Согласно определениям классов вычетов по модулю m и решения сравнения, любое сравнение с одной или несколькими неизвестными можно записать в виде уравнения в кольце классов вычетов. Так, сравнение вида $ax \equiv b(m)$ равносильно уравнению $\bar{a} \cdot \bar{x} = \bar{b}$ в кольце классов вычетов $\mathbb{Z}/m\mathbb{Z}$, где $\bar{a}, \bar{x}, \bar{b} \in \mathbb{Z}/m\mathbb{Z}$.

Воспользовавшись свойствами операции умножения и свойствами обратимых и необратимых классов, можно доказать следующую теорему:

Теорема 1.12. Уравнение вида $\bar{a} \cdot \bar{x} = \bar{b}$ имеет единственное решение тогда и только тогда, когда класс вычетов $\bar{a}$ обратим, причем $\bar{x} = \bar{a}^{-1} \cdot \bar{b}$.

Пример 1.12. Решить сравнение

$$71x \equiv 47(\text{mod}103).$$

Это сравнение равносильно уравнению $\overline{71} \cdot \overline{x} = \overline{47}$ в кольце классов вычетов $\mathbb{Z}/103\mathbb{Z}$. Так как $\text{НОД}(71, 103) = 1$, то класс $\overline{71}$ обратим. Найдем обратный к нему, используя расширенный алгоритм Евклида нахождения коэффициентов соотношения Безу (подробное применение алгоритма см. в образцах решения типовых заданий лабораторной работы). Соотношение Безу для чисел 103 и 71 выглядит следующим образом: $1 = 20 \cdot 103 + (-29) \cdot 71$.

Это соотношение является верным и для классов в кольце $\mathbb{Z}/103\mathbb{Z}$, откуда имеем:

$$\overline{1} = \overline{20} \cdot \overline{103} + \overline{(-29)} \cdot \overline{71} = \left[\overline{103} = \overline{0}, \overline{-29} = \overline{74 + 103 \cdot (-1)} = \overline{74} \right] = \overline{74} \cdot \overline{71}.$$

Так как $\overline{74} \cdot \overline{71} = \overline{1}$, по определению обратного класса имеем $\overline{71}^{-1} = \overline{74}$. Тогда искомый класс $\overline{x} = \overline{71}^{-1} \cdot \overline{47} = \overline{74} \cdot \overline{47} = \overline{74 \cdot 47} = \overline{3478} = \overline{103 \cdot 33 + 79} = \overline{79}$.

Если же в уравнении $\overline{a} \cdot \overline{x} = \overline{b}$ в кольце классов вычетов $\mathbb{Z}/m\mathbb{Z}$ класс $\overline{a}$ необратим, то можно либо перейти от уравнения к сравнению и анализировать его, как показано в п. 2, либо, если $\text{НОД}(a, b) > 1$, перейти к совокупности уравнений в классах вычетов. Подробно на последнем способе останавливаться не будем, так как он не имеет по сравнению с первым никаких преимуществ.

Важно! Умножение уравнения $\overline{a} \cdot \overline{x} = \overline{b}$ на класс $\overline{k}$ приводит к равносильному уравнению тогда и только тогда, когда класс $\overline{k}$ – обратимый.

4. Системы сравнений первой степени

При решении системы уравнений в кольце классов вычетов $\mathbb{Z}/m\mathbb{Z}$, уравнения которой задаются в виде $\overline{a}_1 \cdot \overline{x}_1 + \overline{a}_2 \cdot \overline{x}_2 + \dots + \overline{a}_n \cdot \overline{x}_n = \overline{b}_k$, можно использовать два подхода. В первом переходят на язык сравнений и затем используют равносильные преобразования, чтобы получить одно сравнение с одной неизвестной. Во втором подходе все преобразования проводятся в кольце классов вычетов. Для обоих подходов важно, чтобы все преобразования приводили к равносильным системам, поэтому необходимо использовать свойства сравнений и операций над классами вычетов. На основании этих свойств в обоих случаях может применяться метод Гаусса, позволяющий при обратном ходе каждый раз решать одно сравнение первой степени с одним неизвестным (одно уравнение в классах вычетов), что было изучено в пп. 2 и 3. Однако при реализации его прямого хода коэффициенты при неизвестных могут значительно возрасти. Во избежание этого можно попытаться исключать неизвестные способом, пригодным только для конкретной решаемой системы. Кроме того, при преобразованиях уравнений системы необходимо избегать умножения сравнений на число (класс), не являющееся взаимно простым с модулем, иначе можно получить лишние решения (см. подробный разбор этого случая в образцах решения типовых заданий лабораторных работ).

Пример 1.13. В кольце классов вычетов $\mathbb{Z}/19\mathbb{Z}$ решить систему уравнений

$$\begin{cases} \overline{14} \cdot \bar{x} + \overline{12} \cdot \bar{y} = \bar{5}; \\ \overline{11} \cdot \bar{x} + \overline{14} \cdot \bar{y} = \bar{2}. \end{cases}$$

Записываем $\begin{cases} 14x + 12y \equiv 5(19); \\ 11x + 14y \equiv 2(19); \end{cases} \quad \begin{cases} 12y + 14x \equiv 5(19); \\ 14y + 11x \equiv 2(19). \end{cases}$

$$\left(\begin{array}{cc|c} 12 & 14 & 5(19) \\ 14 & 11 & 2(19) \end{array} \right) \cdot \begin{matrix} (-7) \\ 6 \end{matrix} \rightsquigarrow \left(\begin{array}{cc|c} 12 & 14 & 5(19) \\ 0 & -32 & -23(19) \end{array} \right) \sim \left(\begin{array}{cc|c} 12 & 14 & 5(19) \\ 0 & 6 & 15(19) \end{array} \right).$$

Решаем сравнение $6x \equiv 15(19)$, $2x \equiv 5(19)$. Это сравнение, как мы уже знаем, имеет одно решение. Это решение есть $x \equiv 12(19)$. Первая строка последней матрицы приводит к сравнению $12y + 14 \cdot 12 \equiv 5(19)$, $12y + 168 \equiv 5(19)$, $12y + 19 \cdot 8 + 16 \equiv 5(19)$, $12y + 16 \equiv 5(19)$, $12y \equiv -11(19)$, $12y \equiv 8(19)$, $3y \equiv 2(19)$, $y \equiv 7(19)$.

Таким образом, решением в $\mathbb{Z}/19\mathbb{Z}$ будет $\bar{x} = \overline{12}$, $\bar{y} = \overline{7}$.

Пример 1.14. В кольце классов вычетов $\mathbb{Z}/14\mathbb{Z}$ решить систему уравнений

$$\begin{cases} \overline{13} \cdot \bar{x} + \bar{5} \cdot \bar{y} = \overline{11}; \\ \bar{7} \cdot \bar{x} + \overline{11} \cdot \bar{y} = \overline{13}. \end{cases}$$

На языке сравнений имеем $\begin{cases} 13x + 5y \equiv 11(14) \\ 7x + 11y \equiv 13(14) \end{cases}$.

$$\left(\begin{array}{cc|c} 13 & 5 & 11(14) \\ 7 & 11 & 13(14) \end{array} \right) \cdot \begin{matrix} (-7) \\ 13 \end{matrix} \rightsquigarrow \left(\begin{array}{cc|c} 13 & 5 & 11(14) \\ 0 & 108 & 92(14) \end{array} \right) \sim \left(\begin{array}{cc|c} 13 & 5 & 11(14) \\ 0 & 54 & 46(7) \end{array} \right).$$

Решаем сравнение $54y \equiv 46(7)$, $27y \equiv 23(7)$. $6y \equiv 2(7)$, $3y \equiv 1(7)$. Находим два числа $y_1 = 5$, $y_1 + m_1 = 5 + 7 = 12$. Действительно, решая сравнение $108y \equiv 92(14)$, получаем $10y \equiv 8(14)$, $y = 5$ и $y = 12$.

При каждом из этих значений решаем сравнение $13x + 5y \equiv 11(14)$.

При $y = 5$: $13x + 25 \equiv 11(14)$, $13x + 11 \equiv 11(14)$, $x = 0$.

При $y = 12$: $13x + 60 \equiv 11(14)$, $13x + 4 \equiv 11(14)$, $13x \equiv 7(14)$, $x = 7$.

Итак, одно решение есть $\bar{x} = \bar{0}$, $\bar{y} = \bar{5}$; другое – $\bar{x} = \bar{7}$, $\bar{y} = \bar{12}$.

Пример 1.15. В кольце $\mathbb{Z}/12\mathbb{Z}$ решить систему уравнений

$$\begin{cases} \bar{x} + \bar{5} \cdot \bar{y} = \overline{11}; \\ \bar{7} \cdot \bar{x} + \overline{11} \cdot \bar{y} = \bar{1}. \end{cases}$$

Запишем расширенную матрицу системы, элементами которой являются классы:

$$\left(\begin{array}{cc|c} \bar{1} & \bar{5} & \overline{11} \\ \bar{7} & \overline{11} & \bar{1} \end{array} \right).$$

Выполним элементарные преобразования над строками этой матрицы, избегая умножения на классы, вычеты которых не взаимно простые с модулем 12. Получим матрицу равносильной системы:

$$\left(\begin{array}{cc|c} \bar{1} & \bar{5} & \bar{11} \\ \bar{7} & \bar{11} & \bar{1} \end{array}\right) \cdot (-\bar{7}) \nearrow \sim \left(\begin{array}{cc|c} \bar{1} & \bar{5} & \bar{11} \\ \bar{0} & \bar{-24} & \bar{-76} \end{array}\right) \sim \left(\begin{array}{cc|c} \bar{1} & \bar{5} & \bar{11} \\ \bar{0} & \bar{0} & \bar{8} \end{array}\right).$$

Здесь использовали равенство классов $\bar{-24} = \bar{-2} \cdot \bar{12} = \bar{0}$, $\bar{-76} = \bar{8} + (-\bar{7}) \cdot \bar{12} = \bar{8}$.

Выписав по последней строке матрицы уравнение $\bar{0} \cdot \bar{y} = \bar{8}$, видим, что уравнение решений не имеет, так как умножение на нулевой класс всегда дает класс $\bar{0}$. Следовательно, система решений не имеет.

Пример 1.16. В кольце $\mathbb{Z}/12\mathbb{Z}$ решить систему уравнений

$$\begin{cases} \bar{x} + \bar{5} \cdot \bar{y} = \bar{3}; \\ \bar{7} \cdot \bar{x} + \bar{11} \cdot \bar{y} = \bar{9}. \end{cases}$$

Аналогично предыдущему примеру преобразуем матрицу системы в кольце классов вычетов $\mathbb{Z}/12\mathbb{Z}$:

$$\left(\begin{array}{cc|c} \bar{1} & \bar{5} & \bar{3} \\ \bar{7} & \bar{11} & \bar{9} \end{array}\right) \cdot (-\bar{7}) \nearrow \sim \left(\begin{array}{cc|c} \bar{1} & \bar{5} & \bar{3} \\ \bar{0} & \bar{-24} & \bar{-12} \end{array}\right) \sim \left(\begin{array}{cc|c} \bar{1} & \bar{5} & \bar{3} \\ \bar{0} & \bar{0} & \bar{0} \end{array}\right).$$

Так как последняя строка матрицы целиком состоит из нулей, то исходная система уравнений равносильна уравнению $\bar{x} + \bar{5} \cdot \bar{y} = \bar{3}$, из которого выразим класс $\bar{x}$:

$$\bar{x} = \bar{3} - \bar{5} \cdot \bar{y}.$$

Нет каких-либо ограничений на класс $\bar{y}$, поэтому подставим вместо $\bar{y}$ все возможные классы из кольца $\mathbb{Z}/12\mathbb{Z}$. Так как класс $\bar{5}$ является обратимым, то по свойствам обратимых классов и операций над классами, $\bar{x}$ также пробежит все возможные классы из кольца $\mathbb{Z}/12\mathbb{Z}$:

$$\begin{aligned} \bar{y}_1 = \bar{0} &\Rightarrow \bar{x}_1 = \bar{3} - \bar{5} \cdot \bar{y} = \bar{3}, \\ \bar{y}_2 = \bar{1} &\Rightarrow \bar{x}_2 = \bar{3} - \bar{5} \cdot \bar{1} = \bar{-2} = \bar{10}, \\ \bar{y}_3 = \bar{2} &\Rightarrow \bar{x}_3 = \bar{3} - \bar{5} \cdot \bar{2} = \bar{-7} = \bar{5}, \\ \bar{y}_4 = \bar{3} &\Rightarrow \bar{x}_4 = \bar{3} - \bar{5} \cdot \bar{3} = \bar{-12} = \bar{0}, \\ \bar{y}_5 = \bar{4} &\Rightarrow \bar{x}_5 = \bar{3} - \bar{5} \cdot \bar{4} = \bar{-17} = \bar{7}, \\ \bar{y}_6 = \bar{5} &\Rightarrow \bar{x}_6 = \bar{3} - \bar{5} \cdot \bar{5} = \bar{-22} = \bar{2}, \\ \bar{y}_7 = \bar{6} &\Rightarrow \bar{x}_7 = \bar{3} - \bar{5} \cdot \bar{6} = \bar{-27} = \bar{9}, \\ \bar{y}_8 = \bar{7} &\Rightarrow \bar{x}_8 = \bar{3} - \bar{5} \cdot \bar{7} = \bar{-32} = \bar{4}, \\ \bar{y}_9 = \bar{8} &\Rightarrow \bar{x}_9 = \bar{3} - \bar{5} \cdot \bar{8} = \bar{-37} = \bar{11}, \\ \bar{y}_{10} = \bar{9} &\Rightarrow \bar{x}_{10} = \bar{3} - \bar{5} \cdot \bar{9} = \bar{-42} = \bar{6}, \end{aligned}$$

$$\bar{y}_{11} = \bar{10} \Rightarrow \bar{x}_{11} = \bar{3} - \bar{5} \cdot \bar{10} = \overline{-47} = \bar{1},$$

$$\bar{y}_{12} = \bar{11} \Rightarrow \bar{x}_{12} = \bar{3} - \bar{5} \cdot \bar{11} = \overline{-52} = \bar{8}.$$

Таким образом, получили 12 различных решений – столько, сколько элементов в кольце классов вычетов $\mathbb{Z}/12\mathbb{Z}$.

Проанализируем представленные здесь примеры. В примере 1.13 определитель матрицы системы, составленной из классов вычетов в кольце $\mathbb{Z}/19\mathbb{Z}$:

$$\Delta = \begin{vmatrix} \bar{14} & \bar{12} \\ \bar{11} & \bar{14} \end{vmatrix} = \bar{14} \cdot \bar{14} - \bar{11} \cdot \bar{12} = \overline{196} - \overline{132} = \overline{64} = \bar{7}.$$

Получили ненулевой класс, который по свойствам колец вычетов по простому модулю обратим. Система имеет единственное решение.

В примере 1.14 определитель матрицы системы равен $\bar{10}$ – необратимый класс в кольце классов вычетов $\mathbb{Z}/14\mathbb{Z}$. Система имеет несколько решений.

В примерах 1.15 и 1.16 матрица системы одна и та же, ее определитель равен $\bar{0}$. Для этих систем в зависимости от столбца свободных членов решения либо не существовало, либо количество решений совпадало с числом элементов кольца вычетов. Все четыре примера служат иллюстрацией следующего утверждения:

Утверждение. Если определитель системы уравнений в кольце классов вычетов по модулю m является *обратимым классом*, то система имеет единственное решение, которое можно отыскать методом, аналогичным правилу Крамера, заменяя в нем деление на определитель матрицы умножением на обратный к нему класс. Если определитель системы уравнений в кольце классов вычетов по модулю m является *необратимым классом*, то система может иметь несколько решений либо не иметь вовсе.

Пример использования метода, аналогичного правилу Крамера, см. в образцах решения типовых заданий лабораторных работ.

Безусловно, вопрос о существовании и количестве решений систем уравнений в кольце классов вычетов является довольно интересным и требует подробного исследования в общем виде. Но настоящее пособие не ставит этого своей целью, а лишь использует решение таких систем уравнений как хороший способ познакомить читателя с особенностями действий над классами, т. е. модулярной алгебры.

ТИПОВЫЕ ЗАДАНИЯ ПО ТЕМЕ «ОСНОВЫ ТЕОРИИ ЧИСЕЛ» С ОБРАЗАЦАМИ РЕШЕНИЙ

Задание 1. Найти НОД и НОК чисел $a = 7700, b = 360$, воспользовавшись:

а) алгоритмом Евклида; б) канонической факторизацией (каноническим разложением) чисел.

Решение

а) Применим алгоритм Евклида и для удобства шаги алгоритма будем записывать в таблицу. Как видим из таблицы, после вычисления в столбце «Остаток» значения в столбцах «Делимое» и «Делитель» следующей строки заполняются автоматически переносом (см. стрелки).

- 1) $7700 = 360 \cdot 21 + 140$;
- 2) $360 = 140 \cdot 2 + 80$;
- 3) $140 = 80 \cdot 1 + 60$;
- 4) $80 = 60 \cdot 1 + 20$;
- 5) $60 = 20 \cdot 3 + 0$.

Номер шага	Делимое	Делитель	Остаток
1	7700	360	140
2	360	140	80
3	140	80	60
4	80	60	20
5	60	20	0

Алгоритм останавливается сразу, как только остаток равен нулю, а последний отличный от нуля остаток равен НОД(7700, 360):

$$\text{НОД}(7700, 360) = 20.$$

Зная НОД(7700, 360), вычислим НОК(7700, 360), используя соотношение $\text{НОД}(a, b) \cdot \text{НОК}(a, b) = a \cdot b$:

$$\text{НОК}(7700, 360) = \frac{7700 \cdot 360}{\text{НОД}(7700, 360)} = 138600.$$

б) Найдем разложения на простые множители за несколько шагов: на каждом шаге будем выписывать справа от числа один из его простых делителей, а под числом – частное от деления. На последнем шаге частным является 1:

7700	5	360	5
1540	5	72	2
308	2	36	2
154	2	18	2
77	7	9	3
11	11	3	3
1		1	

Запишем канонические факторизации (разложения) этих чисел с учетом повторяющихся простых делителей:

$$a = 7700 = 2^2 \cdot 5^2 \cdot 7 \cdot 11,$$

$$b = 360 = 2^3 \cdot 3^2 \cdot 5.$$

Для того чтобы вычислить НОД(a, b), перемножим *наименьшие* из входящих в оба разложения степени общих простых делителей:

$$\text{НОД}(a, b) = 2^2 \cdot 5 = 20.$$

Для того чтобы вычислить НОК(a, b), перемножим *наибольшие* из входящих в оба разложения степени всех простых делителей:

$$\text{НОК}(a, b) = 2^3 \cdot 3^2 \cdot 5^2 \cdot 7 \cdot 11 = 138600. \blacktriangle$$

Замечание. В приведенном примере задача факторизации обоих чисел не является сложной, поскольку сами числа невелики и на каждом шаге легко установить простые делители, пользуясь признаками делимости на 2, 3, 5. В случае больших чисел, содержащих 7 и более символов в записи, найти каноническое разложение гораздо сложнее. Приведем пример: легко видеть, что делителем числа 10830434878 является 2, в частном от деления получим 5415217439. Это число не обладает очевидными признаками делимости, и при факторизации такого большого числа целесообразно проверять, является ли оно простым. В данном случае получено простое число, в чем можно убедиться, например, перебором простых делителей, не превосходящих $\sqrt{5415217439}$ (см. решето Эратосфена). Их количество составляет 7265, при этом заранее необходимо выписать все, что приводит к низкой скорости работы алгоритма перебора. По этой причине указанный алгоритм не используется для факторизации больших чисел. Для решения этой задачи в настоящее время разработан ряд более быстрых алгоритмов экспоненциальной и субэкспоненциальной сложности, но вопрос о существовании полиномиального алгоритма факторизации чисел для классического компьютера остается открытым (хотя такой алгоритм разработан для квантового компьютера).

Задание 2. С помощью расширенного алгоритма Евклида найти целые числа u, v удовлетворяющие соотношению Безу: $au + bv = \text{НОД}(a, b)$ для целых чисел $a = 5187; b = 1520$.

Решение

Δ *Способ 1.* Вначале вычислим НОД(5187, 1520) по алгоритму Евклида, как это было сделано в задании 1, пункт «а».

- 1) $5187 = 1520 \cdot 3 + 627$;
- 2) $1520 = 627 \cdot 2 + 266$;
- 3) $627 = 266 \cdot 2 + 95$;
- 4) $266 = 95 \cdot 2 + 76$;
- 5) $95 = 76 \cdot 1 + 19$;
- 6) $76 = 19 \cdot 4 + 0$.

Номер шага	Делимое	Делитель	Остаток
1	5187	1520	627
2	1520	627	266
3	627	266	95
4	266	95	76
5	95	76	19
6	76	19	0

Таким образом, $\text{НОД}(5187, 1520) = 19$. Проведем алгоритм Евклида в обратном направлении – снизу вверх по таблице, на каждом шаге выражая остаток через делимое и делитель. Начнем с последнего ненулевого остатка, равного $\text{НОД}(5187, 1520)$:

$$19 = 95 - 76 \cdot 1.$$

Двигаясь на шаг вверх по таблице, замечаем, что предыдущим остатком в прямом ходе алгоритма Евклида является 76, выразим его из строки 4 и подставим в равенство, полученное ранее:

$$19 = 95 - 76 = 95 - (266 + 95 \cdot (-2)) = 266 \cdot (-1) + 95 \cdot 3.$$

Продолжая движение вверх по таблице, видим, что остаток на третьем шаге прямого хода – число 95. Поэтому надо предварительно раскрыть скобки и определить множитель при 95. Затем выражаем 95 из строки 3 и подставляем его в предыдущее равенство с последующим приведением подобных:

$$19 = 266 \cdot (-1) + 95 \cdot 3 = 266 \cdot (-1) + (627 + 266 \cdot (-2)) \cdot 3 = 266 \cdot (-7) + 627 \cdot 3.$$

Аналогичным образом проводим вычисления на последних двух шагах, последовательно выражая из строк 2 и 1 остатки 266 и 627:

$$19 = 266 \cdot (-7) + 627 \cdot 3 = (1520 - 627 \cdot 2) \cdot (-7) + 627 \cdot 3 = 1520 \cdot (-7) + 627 \cdot 17 = 1520 \cdot (-7) + (5187 - 1520 \cdot 3) \cdot 17 = 5187 \cdot 17 + 1520 \cdot (-58).$$

Таким образом,

$$19 = 5187 \cdot 17 + 1520 \cdot (-58) \Rightarrow u = 17, v = -58.$$

Способ 2. На каждом i -м шаге алгоритма Евклида будем представлять остаток r_i в виде линейной комбинации 5187 и 1520 с целочисленными коэффициентами u_i и v_i , пользуясь рекуррентными формулами:

$$u_i = u_{i-2} - q_i u_{i-1}, \quad v_i = v_{i-2} - q_i v_{i-1}, \quad i \geq 2,$$

положив в них $u_0 = 0, v_0 = 1, u_1 = 1, v_1 = -q_1$, где q_i – частное на i -м шаге. Тогда на шаге с последним ненулевым остатком u_i и v_i будут являться искомыми величинами u и v . Результаты расчетов занесем в таблицу 1. Для примера выпишем подробные вычисления u_3 и v_3 :

$$u_1 = 1, u_2 = -2, q_3 = 2 \Rightarrow u_3 = u_1 - q_3 u_2 = 1 - 2 \cdot (-2) = 5$$

$$v_1 = -3, v_2 = 7, q_3 = 2 \Rightarrow v_3 = v_1 - q_3 v_2 = -3 - 2 \cdot 7 = -17$$

Таблица 1

Расширенный алгоритм Евклида

Номер шага	Делимое	Делитель	Остаток	Частное	u_i	v_i
0					0	1
1	5187	1520	627	3	1	-3
2	1520	627	266	2	-2	7
3	627	266	95	2	5	-17
4	266	95	76	2	-12	41
5	95	76	<u>19</u>	1	<u>17</u>	<u>-58</u>
6	76	19	0	4		

Из строки 5 выписываем сразу и НОД(5187, 1520), и соотношение Безу:
 $\text{НОД}(5187, 1520) = 19 = 5187 \cdot 17 + 1520 \cdot (-58) \Rightarrow u = 17, v = -58. \blacktriangle$

Задание 3. Найти остаток от деления 2025^{1989} на 37.

Решение

Δ Переформулируем задание на языке сравнений: найдем наименьшее положительное число, сравнимое с 2025^{1989} по модулю 37. Так как основание 2025 больше модуля, то вначале найдем остаток от деления 2025 на 37:

$$2025 \equiv 27 \pmod{37}.$$

Тогда по свойству сравнений $a \equiv b \pmod{m} \Rightarrow a^n \equiv b^n \pmod{m}$ имеем

$$2025^{1989} \equiv 27^{1989} \pmod{37} = (3^3)^{1989} \pmod{37} = 3^{5967} \pmod{37}.$$

Проблема с большим основанием решена, необходимо разобраться с большой степенью. Так как 37 – простое число, и 3 не делится на 37, то применима малая теорема Ферма: для простого p и a , не делящегося на p , справедливо $a^{p-1} \equiv 1 \pmod{p}$. Тогда

$$3^{36} \equiv 1 \pmod{37}.$$

Представим 5967 в соответствии с теоремой о делении с остатком:

$$5967 = 165 \cdot 36 + 27, \text{ тогда } 3^{5967} = 3^{165 \cdot 36 + 27} = 3^{165 \cdot 36} \cdot 3^{27} = (3^{36})^{165} \cdot 3^{27}.$$

Применим свойства сравнений $a \equiv b \pmod{m} \Rightarrow a^n \equiv b^n \pmod{m}$ и $a \equiv b \pmod{m} \Rightarrow ka \equiv kb \pmod{m} \forall k \in \mathbb{Z}$:

$$3^{36} \equiv 1 \pmod{37} \Rightarrow (3^{36})^{165} \cdot 3^{27} \equiv 3^{27} \pmod{37}.$$

Осталось найти остаток от деления 3^{27} на 37. Эту задачу будем решать пошагово, на каждом шаге используя свойство сравнений $a \equiv b \pmod{m} \Rightarrow a^n \equiv b^n \pmod{m}$ при $n = 2$:

$$3^2 = 9 \equiv 9 \pmod{37};$$

$$3^4 = 81 \equiv 7 \pmod{37};$$

$$3^8 \equiv 7^2 \pmod{37} = 49 \pmod{37} \equiv 12 \pmod{37};$$

$$3^{16} \equiv 12^2 \pmod{37} = 144 \pmod{37} \equiv 33 \pmod{37}.$$

Зная числа, сравнимые со степенями 3 по модулю 37, представим 3^{27} в виде произведения этих степеней и воспользуемся свойством сравнений $a \equiv b \pmod{m}, c \equiv d \pmod{m} \Rightarrow a \cdot c \equiv b \cdot d \pmod{m}$:

$$3^{27} = 3^{16+8+3} = 3^{16} \cdot 3^8 \cdot 3^3 \equiv 33 \cdot 12 \cdot 27 \pmod{37} = 10692 \pmod{37} \equiv 36 \pmod{37}.$$

Таким образом, $2025^{1989} \equiv 3^{27} \pmod{37} \equiv 36 \pmod{37}$ или, иными словами, остаток от деления 2025^{1989} на 37 равен 36. $\blacktriangle$

Замечание. Описанный выше процесс нахождения остатка от деления 3^{27} на 37 называется также возведением 3 в двадцать седьмую степень по модулю 37,

а использованный алгоритм возведения относится к классу алгоритмов быстрого возведения в степень и называется «справа налево». Это название обусловлено тем, что степень записывается в двоичной системе счисления в виде 0 и 1, и биты степени просматриваются от младшего к старшему.

Задание 4. Построить таблицы сложения в кольце классов вычетов: а) $\mathbb{Z}/5\mathbb{Z}$; б) $\mathbb{Z}/8\mathbb{Z}$.

Решение

а) Кольцо классов вычетов по модулю 5 состоит из элементов $\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}$. Запишем их в таблицу, свободные ячейки которой будем заполнять результатами сложения классов, стоящих в начале соответствующих строки и столбца.

$\oplus$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$					
$\bar{1}$					
$\bar{2}$					
$\bar{3}$					
$\bar{4}$					

Напомним, что каждый класс полностью определяется одним своим представителем (вычетом), поэтому достаточно найти один из представителей класса суммы. Для того чтобы найти представитель суммы двух классов, надо сложить представители этих классов. Для записи класса суммы, как и для любого класса, используется наименьший неотрицательный вычет, поэтому если сумма представителей классов превышает модуль или равна ему, то искомый класс обозначаем остатком от деления этой суммы на модуль (по определению сумма и полученный остаток принадлежат одному классу):

$$\bar{1} + \bar{2}: 1 + 2 = 3 \Rightarrow \bar{1} + \bar{2} = \bar{3};$$

$$\bar{1} + \bar{4}: 1 + 4 = 5, 5 \equiv 0 \pmod{5} \Rightarrow \bar{1} + \bar{4} = \bar{0};$$

$$\bar{3} + \bar{4}: 3 + 4 = 7, 7 \equiv 2 \pmod{5} \Rightarrow \bar{3} + \bar{4} = \bar{2}.$$

$\oplus$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$					
$\bar{1}$			$\bar{1} + \bar{2}$		$\bar{1} + \bar{4}$
$\bar{2}$		$\bar{1} + \bar{2}$			
$\bar{3}$					$\bar{3} + \bar{4}$
$\bar{4}$		$\bar{1} + \bar{4}$		$\bar{3} + \bar{4}$	



$\oplus$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$					
$\bar{1}$			$\bar{3}$		$\bar{0}$
$\bar{2}$		$\bar{3}$			
$\bar{3}$					$\bar{2}$
$\bar{4}$		$\bar{0}$		$\bar{2}$	

Запишем в таблицу результат всех остальных вычислений.

$\oplus$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$

б) Составляем таблицу аналогично пункту «а».

$\oplus$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{6}$	$\bar{6}$	$\bar{7}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{7}$	$\bar{7}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$

Замечание. Обратите внимание на то, что для таблиц обоих пунктов характерно следующее:

- результаты пробегают в каждой строке полную систему вычетов без повторов;

- в каждой строке встречается нулевой класс – это означает, что для любого класса вычетов, вне зависимости от свойств модуля, найдется **противоположный элемент**, т. е. класс, дающий в сумме с выбранным класс $\bar{0}$.

Симметрия заполнения таблицы отражает свойство коммутативности операции сложения классов вычетов. ▲

Задание 5. Построить таблицу умножения в кольце классов вычетов: а) $\mathbb{Z}/5\mathbb{Z}$; б) $\mathbb{Z}/8\mathbb{Z}$. В каждом пункте найти пары взаимно обратных относительно умножения элементов.

Решение

а) Ячейки таблицы умножения классов будем заполнять аналогично задаанию 4:

$\otimes$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$					
$\bar{1}$					
$\bar{2}$					
$\bar{3}$					$\bar{3} \cdot \bar{4}$
$\bar{4}$				$\bar{3} \cdot \bar{4}$	

Для того чтобы найти представитель произведения двух классов, надо перемножить представители этих классов. Если произведение превышает модуль, то, как и в случае со сложением, класс произведения обозначаем остатком от деления произведения представителей на модуль:

$$\bar{1} \cdot \bar{3} : 1 \cdot 3 = 3 \Rightarrow \bar{1} \cdot \bar{3} = \bar{3};$$

$$\bar{3} \cdot \bar{4} : 3 \cdot 4 = 12, 12 \equiv 2 \pmod{5} \Rightarrow \bar{3} \cdot \bar{4} = \bar{2}.$$

Соответствующие ячейки в таблице заполняются следующим образом.

$\otimes$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$					
$\bar{1}$				$\bar{1} \cdot \bar{3}$	
$\bar{2}$					
$\bar{3}$		$\bar{1} \cdot \bar{3}$			$\bar{3} \cdot \bar{4}$
$\bar{4}$				$\bar{3} \cdot \bar{4}$	



$\otimes$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$					
$\bar{1}$				$\bar{3}$	
$\bar{2}$		$\bar{3}$			
$\bar{3}$					$\bar{2}$
$\bar{4}$				$\bar{2}$	

Запишем в таблицу результат всех остальных вычислений.

$\otimes$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Взаимно обратные относительно умножения элементы $\mathbb{Z}/m\mathbb{Z}$ кольца классов вычетов – это взаимно обратные классы. По определению произведение взаимно обратных классов равно $\bar{1}$, поэтому найдем в ячейках таблицы результат $\bar{1}$ и выпишем пары соответствующих сомножителей:

$(\bar{1}, \bar{1})$ – класс $\bar{1}$ взаимно обратный самому себе, $(\bar{2}, \bar{3}), (\bar{4}, \bar{4})$ – класс $\bar{4}$ взаимно обратный самому себе. Как видим из таблицы, все ненулевые классы имеют обратные.

б) Составляем таблицу аналогично пункту «а»:

$\otimes$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{6}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{6}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{6}$	$\bar{1}$	$\bar{4}$	$\bar{7}$	$\bar{2}$	$\bar{5}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{0}$	$\bar{4}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{2}$	$\bar{7}$	$\bar{4}$	$\bar{1}$	$\bar{6}$	$\bar{3}$
$\bar{6}$	$\bar{0}$	$\bar{6}$	$\bar{4}$	$\bar{2}$	$\bar{0}$	$\bar{6}$	$\bar{4}$	$\bar{2}$
$\bar{7}$	$\bar{0}$	$\bar{7}$	$\bar{6}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Выпишем пары взаимно обратных элементов, аналогично пункту «а»:

$(\bar{1}, \bar{1}), (\bar{3}, \bar{3}), (\bar{5}, \bar{5}), (\bar{7}, \bar{7})$ – лишь некоторые ненулевые классы имеют

обратные, причем в данном случае все они оказались взаимно обратными самим себе.

Замечание. На примере полученных таблиц обратите внимание на свойства обратимых и необратимых классов вычетов, сформулированных в теоретическом разделе:

- ненулевой класс имеет обратный только в том случае, если он взаимно простой с модулем. Таким образом, в пункте «а» с простым модулем все ненулевые классы имеют обратные;

- результаты произведения пробегают в строке полную систему вычетов без повторов только в том случае, если сомножитель в этой строке взаимно простой с модулем, т. е. является обратимым классом. Таким образом, для простого модуля в пункте «а» полная система вычетов пробегается в каждой строке;

- два ненулевых класса могут дать в произведении нулевой класс, только если модуль – составное число (таблица пункта «б»);

- если представитель класса не является взаимно простым с модулем, т. е. класс необратим, то в его строке результаты произведений формируют циклическую структуру. Это также является одним из общих свойств колец, речь о котором пойдет в модуле 4 «Кольца. Идеалы колец»;

- аналогично заданию 4, симметрия заполнения таблицы отражает свойство коммутативности операции умножения классов вычетов. ▲

Задание 6. Вычислить значения функции Эйлера: а) $\varphi(7)$, б) $\varphi(21)$, в) $\varphi(360)$.

Решение

Вычислим значения функции Эйлера, пользуясь ее свойствами.

а) Так как 7 – простое число, то применим свойство функции Эйлера от простого аргумента p : $\varphi(p) = p - 1 \Rightarrow \varphi(7) = 7 - 1 = 6$.

б) Так как 21 раскладывается в произведение простых сомножителей $21 = 3 \cdot 7$, то применим свойство функции Эйлера от произведения взаимно простых сомножителей:

$$\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b) \Rightarrow \varphi(21) = \varphi(3 \cdot 7) = \varphi(3) \cdot \varphi(7) = 2 \cdot 6 = 12.$$

в) Для 360 запишем каноническое разложение (см. задание 1): $360 = 2^3 \cdot 3^2 \cdot 5$.

Зная каноническое разложение аргумента, можно рассчитать значение функции Эйлера согласно формуле:

$$\varphi(p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}) = p_1^{\alpha_1-1} p_2^{\alpha_2-1} \dots p_s^{\alpha_s-1} (p_1-1)(p_2-1) \dots (p_s-1).$$

Применяя эту формулу, получим

$$\varphi(360) = \varphi(2^3 \cdot 3^2 \cdot 5) = 2^{3-1} \cdot 3^{2-1} \cdot 5^{1-1} \cdot (2-1) \cdot (3-1) \cdot (5-1) = 4 \cdot 3 \cdot 1 \cdot 1 \cdot 3 \cdot 4 = 144. \blacktriangle$$

Задание 7. Решить системы уравнений в соответствующих кольцах классов

вычетов: а) $\begin{cases} \bar{2} \cdot \bar{x} + \bar{8} \cdot \bar{y} = \bar{6}, \\ \bar{3} \cdot \bar{x} + \bar{7} \cdot \bar{y} = \bar{10} \end{cases}$ в $\mathbb{Z}/13\mathbb{Z}$; б) $\begin{cases} \bar{x} + \bar{8} \cdot \bar{y} + \bar{3} \cdot \bar{z} = \bar{4}, \\ \bar{3} \cdot \bar{x} + \bar{y} + \bar{2} \cdot \bar{z} = \bar{3}, \\ \bar{2} \cdot \bar{x} + \bar{5} \cdot \bar{y} + \bar{4} \cdot \bar{z} = \bar{1} \end{cases}$ в $\mathbb{Z}/24\mathbb{Z}$;

в) $\begin{cases} \bar{5} \cdot \bar{x} + \bar{3} \cdot \bar{y} = \bar{11}, \\ \bar{7} \cdot \bar{x} + \bar{5} \cdot \bar{y} = \bar{7} \end{cases}$ в $\mathbb{Z}/18\mathbb{Z}$.

а) *Способ 1.* Запишем систему на языке сравнений: $\begin{cases} 2x + 8y \equiv 6(13) \\ 3x + 7y \equiv 10(13) \end{cases}$.

Заметим, что обе части первого сравнения можно разделить на их общий делитель 2, так как он взаимно прост с модулем 13, получим равносильную систему сравнений:

$$\begin{cases} x + 4y \equiv 3(13); \\ 3x + 7y \equiv 10(13). \end{cases}$$

Составим матрицу системы сравнений и проведем элементарные преобразования над строками:

$$\left(\begin{array}{cc|c} 1 & 4 & 3(13) \\ 3 & 7 & 10(13) \end{array} \right) \cdot (-3) \nearrow \sim \left(\begin{array}{cc|c} 1 & 4 & 3(13) \\ 0 & -5 & 1(13) \end{array} \right) \sim \left(\begin{array}{cc|c} 1 & 4 & 3(13) \\ 0 & 8 & 1(13) \end{array} \right).$$

Решаем сравнение $8y \equiv 1(13)$. Так как модуль – простое число, то оно будет иметь только одно решение, которое можно подобрать из полной системы вычетов: $y \equiv 5(13)$. Подставив это решение в первую строку последней матрицы придем к сравнению $x + 4 \cdot 5 \equiv 3(13)$, проведем ряд равносильных преобразований:

$$x + 4 \cdot 5 \equiv 3(13) \Leftrightarrow x + 20 \equiv 3(13) \Leftrightarrow x + 7 \equiv 3(13) \Leftrightarrow x \equiv -4(13) \Leftrightarrow x \equiv 9(13).$$

Таким образом, решением в $\mathbb{Z}/13\mathbb{Z}$ будет пара классов вычетов $\bar{x} = \bar{9}$, $\bar{y} = \bar{5}$.

Способ 2. Так как числа 2 и 13 взаимно простые, то класс $\bar{2}$ обратим и допустимо формальное сокращение на $\bar{2}$ первого уравнения системы, при этом получим равносильную систему:

$$\begin{cases} \bar{x} + \bar{4} \cdot y = \bar{3}; \\ \bar{3} \cdot x + \bar{7} \cdot \bar{y} = \bar{10}. \end{cases}$$

Будем решать систему уравнений, не переходя на язык сравнений. Запишем расширенную матрицу системы, элементами которой являются классы, и проведем над строками этой матрицы элементарные преобразования, получая каждый раз матрицу равносильной системы (все ненулевые классы в данном кольце обратимы):

$$\left(\begin{array}{cc|c} \bar{1} & \bar{4} & \bar{3} \\ \bar{3} & \bar{7} & \bar{10} \end{array} \right) \cdot (-\bar{3}) \nearrow \sim \left(\begin{array}{cc|c} \bar{1} & \bar{4} & \bar{3} \\ 0 & \bar{-5} & \bar{1} \end{array} \right) \sim \left(\begin{array}{cc|c} \bar{1} & \bar{4} & \bar{3} \\ 0 & \bar{8} & \bar{1} \end{array} \right).$$

Здесь использовали равенство классов $\bar{-5} = \overline{-5+13} = \bar{8}$. Эти преобразования выглядят точно так же, как и в решении первым способом. По второй строке матрицы выпишем уравнение

$$\bar{8} \cdot \bar{y} = \bar{1}.$$

Так как деление в кольце классов вычетов не определено, то необходимо умножить обе части уравнения на элемент, обратный к классу $\bar{8}$. Поскольку 8 и 13 взаимно простые, то класс $\bar{8}$ обратим. Чтобы не искать его с помощью таблицы умножения, найдем соотношение Безу для чисел 13 и 8:

$$\text{НОД}(13, 8) = 1 = 40 - 39 = (-3) \cdot 39 + 5 \cdot 8.$$

В данном случае коэффициенты легко подбираются, но в общем случае можно использовать расширенный алгоритм Евклида. Запишем соотношение Безу для классов:

$$\bar{1} = (-\bar{3}) \cdot \bar{13} + \bar{5} \cdot \bar{8} = [\bar{13} = \bar{0}] = \bar{5} \cdot \bar{8}.$$

Отсюда следует, что обратным к классу $\bar{8}$ является класс $\bar{5}$. Умножим на этот класс обе части уравнения $\bar{8} \cdot \bar{y} = \bar{1}$:

$$(\bar{5} \cdot \bar{8}) \bar{y} = \bar{5} \Leftrightarrow \bar{y} = \bar{5}.$$

Выразим класс $\bar{x}$, подставив в первое уравнение системы $\bar{y} = \bar{5}$:

$$\bar{x} + \bar{4} \cdot \bar{5} = \bar{3} \Leftrightarrow \bar{x} = \bar{3} - \bar{20} = \overline{-17} = \bar{9}.$$

Таким образом, решением в $\mathbb{Z}/13\mathbb{Z}$ будет пара классов вычетов $\bar{x} = \bar{9}$, $\bar{y} = \bar{5}$.

Замечание. Второй способ может показаться более громоздким, но только лишь за счет того, что в нем подробно описано нахождение обратного класса.

$$\text{б) Способ 1. На языке сравнений} \quad \begin{cases} x + 8y + 3z = 4(24); \\ 3x + y + 2z = 3(24); \\ 2x + 5y + 4z = 1(24). \end{cases}$$

Прямой ход метода Гаусса

$$\begin{aligned}
& \xrightarrow{(-3) \cdot \begin{pmatrix} 1 & 8 & 3 & | & 4(24) \\ 3 & 1 & 2 & | & 3(24) \\ 2 & 5 & 4 & | & 1(24) \end{pmatrix} \cdot (-2)} \sim \begin{pmatrix} 1 & 8 & 3 & | & 4(24) \\ 0 & -23 & -7 & | & -9(24) \\ 0 & -11 & -2 & | & -7(24) \end{pmatrix} \cdot (-11) \cdot 23 \sim \\
& \sim \begin{pmatrix} 1 & 8 & 3 & | & 4(24) \\ 0 & -23 & -7 & | & -9(24) \\ 0 & 0 & 31 & | & -62(24) \end{pmatrix} \sim \begin{pmatrix} 1 & 8 & 3 & | & 4(24) \\ 0 & -23 & -7 & | & -9(24) \\ 0 & 0 & 1 & | & -2(24) \end{pmatrix} \sim \begin{pmatrix} 1 & 8 & 3 & | & 4(24) \\ 0 & -23 & -7 & | & -9(24) \\ 0 & 0 & 1 & | & 22(24) \end{pmatrix}.
\end{aligned}$$

Решаем сравнение $z \equiv 22(24)$, $z = 22$. Далее получаем $-23y - 7z \equiv -9(24)$, $y - 7z \equiv -9(24)$, $y - 154 \equiv 15(24)$, $y + 14 \equiv 15(24)$, $y \equiv 1(24)$, $y = 1$. Решаем сравнение $x + 8 \cdot 1 + 3 \cdot 22 \equiv 4(24)$, $x + 2 \equiv 4(24)$, $x \equiv 2(24)$, $x = 2$.

Итак, решением в $\mathbb{Z}/24\mathbb{Z}$ будет $\bar{x} = \bar{2}$, $\bar{y} = \bar{1}$, $\bar{z} = \bar{22}$.

Способ 2. Вычислим определитель системы в заданном кольце классов вычетов:

$$\Delta = \begin{vmatrix} \bar{1} & \bar{8} & \bar{3} \\ \bar{3} & \bar{1} & \bar{2} \\ \bar{2} & \bar{5} & \bar{4} \end{vmatrix} = \overline{-31} = \overline{-31 + 2 \cdot 24} = \overline{17}.$$

Так как 17 и 24 – взаимно простые, то существует единственный обратный к $\overline{17}$ класс, а система уравнений имеет единственное решение. Его можно найти методом, аналогичным правилу Крамера, в котором деление на определитель системы заменяется умножением на класс, обратный к нему. Вычислим определители, поочередно заменяя столбец матрицы системы на столбец свободных членов:

$$\Delta_x = \begin{vmatrix} \bar{4} & \bar{8} & \bar{3} \\ \bar{3} & \bar{1} & \bar{2} \\ \bar{1} & \bar{5} & \bar{4} \end{vmatrix} = \overline{-62} = \overline{-62 + 3 \cdot 24} = \overline{10}, \quad \Delta_y = \begin{vmatrix} \bar{1} & \bar{4} & \bar{3} \\ \bar{3} & \bar{3} & \bar{2} \\ \bar{2} & \bar{1} & \bar{4} \end{vmatrix} = \overline{-31} = \overline{-31 + 2 \cdot 24} = \overline{17},$$

$$\Delta_z = \begin{vmatrix} \bar{1} & \bar{8} & \bar{4} \\ \bar{3} & \bar{1} & \bar{3} \\ \bar{2} & \bar{5} & \bar{1} \end{vmatrix} = \overline{62} = \overline{62 - 2 \cdot 24} = \overline{14}.$$

Найдем класс, обратный к классу $\overline{17}$, используя соотношение Безу:

$$\bar{1} = \bar{5} \cdot \bar{24} + (\bar{-7}) \cdot \bar{17} = [\bar{24} = \bar{0}, \bar{-7} = \bar{17}] = \bar{17} \cdot \bar{17} \Rightarrow \Delta^{-1} = \overline{17}.$$

Вычислим искомые классы:

$$\bar{x} = \Delta_x \cdot \Delta^{-1} = \overline{10} \cdot \overline{17} = \overline{170} = \overline{2 + 24 \cdot 7} = \bar{2},$$

$$\bar{y} = \Delta_y \cdot \Delta^{-1} = \overline{17} \cdot \overline{17} = \bar{1},$$

$$\bar{z} = \Delta_z \cdot \Delta^{-1} = \overline{14} \cdot \overline{17} = \overline{238} = \overline{22 + 24 \cdot 9} = \bar{22}.$$

Итак, решением в $\mathbb{Z}/24\mathbb{Z}$ будет $\bar{x} = \bar{2}$, $\bar{y} = \bar{1}$, $\bar{z} = \bar{22}$.

в) Вычислим определитель данной системы: $\Delta = \begin{vmatrix} \bar{5} & \bar{3} \\ \bar{7} & \bar{5} \end{vmatrix} = \bar{4}$. Так как

$\text{НОД}(18, 4) = 2 > 1$ и класс $\bar{4}$ необратим, то система может иметь несколько решений или может не иметь ни одного. Проведем элементарные преобразования над строками расширенной матрицы:

$$\left(\begin{array}{cc|c} \bar{5} & \bar{3} & \bar{11} \\ \bar{7} & \bar{5} & \bar{7} \end{array} \right) \cdot \begin{matrix} (-\bar{7}) \\ \cdot \bar{5} \end{matrix} \rightsquigarrow \left(\begin{array}{cc|c} \bar{5} & \bar{3} & \bar{11} \\ \bar{0} & \bar{4} & \bar{12} \end{array} \right).$$

Решим уравнение $\bar{4}y = \bar{12}$. Поскольку обратного класса к $\bar{4}$ не существует, то перепишем его на языке сравнений:

$$4y \equiv 12(18) \Rightarrow 2y \equiv 6(9).$$

Здесь обе части сравнения и модуль сократили на $\text{НОД}(4, 18) = 2$. Таким образом, у исходного сравнения два решения.

Так как 2 и 9 – взаимно простые числа, то далее сокращаем обе части сравнения на 2, не меняя модуля и получая равносильное сравнение:

$$2y \equiv 6(9) \Leftrightarrow y \equiv 3(9).$$

Возвращаемся к решениям сравнения по модулю 18, к полученному у прибавляя 9, пока не превысим 18, и получаем два решения в кольце $\mathbb{Z}/18\mathbb{Z}$:

$$y \equiv 3(9) \Rightarrow y_1 \equiv 3(18), y_2 \equiv 3 + 9 = 12(18) \Rightarrow \bar{y}_1 = \bar{3}, \bar{y}_2 = \bar{12}.$$

Подставим $y_1 = \bar{3}$ в первое уравнение системы: $\bar{5} \cdot \bar{x} + \bar{3} \cdot \bar{3} = \bar{11} \Leftrightarrow \bar{5} \cdot \bar{x} = \bar{11} - \bar{9} \Leftrightarrow \bar{5} \cdot \bar{x} = \bar{2}$.

Это уравнение решим, найдя обратный к классу $\bar{5}$ из соотношения Безу:

$$\bar{1} = \bar{36} - \bar{35} = \bar{18} \cdot \bar{2} + (-\bar{7}) \cdot \bar{5} = [\bar{18} = \bar{0}, -\bar{7} = \bar{11}] = \bar{5} \cdot \bar{11} \Rightarrow \bar{5}^{-1} = \bar{11}.$$

$$\text{Тогда } \bar{5} \cdot \bar{x}_1 = \bar{2} \Rightarrow \bar{x}_1 = \bar{2} \cdot \bar{11} = \bar{22} = \bar{4}.$$

$$\text{Аналогичным образом найдем } \bar{y}_2 = \bar{12} \Rightarrow \bar{x}_2 = \bar{13}.$$

Таким образом, система имеет два решения в кольце классов вычетов $\mathbb{Z}/18\mathbb{Z}$ ($\bar{x}_1 = \bar{4}; \bar{y}_1 = \bar{3}$) и ($\bar{x}_2 = \bar{13}; \bar{y}_2 = \bar{12}$).

Замечание. Если определитель системы не является взаимно простым с модулем, то при проведении элементарных преобразований над строками системы необходимо избегать умножения на числа, являющиеся делителями модуля. Приведем пример. Если умножить второе уравнение исходной системы на $\bar{3}$ с целью последующего исключения неизвестной y , получим систему

$$\begin{cases} \bar{5}x + \bar{3}y = \bar{11}; \\ \bar{21}x + \bar{15}y = \bar{21}, \end{cases} \Leftrightarrow \begin{cases} \bar{5}x + \bar{3}y = \bar{11}; \\ \bar{3}x + \bar{15}y = \bar{3}. \end{cases}$$

При переходе ко второй системе использовали равенство классов $\overline{21} = \overline{18 + 3} = \overline{3}$. Можно убедиться непосредственной проверкой, что решениями этой системы являются пары классов $(\overline{4}; \overline{3}), (\overline{4}; \overline{9}), (\overline{4}; \overline{15}), (\overline{13}; \overline{0}), (\overline{13}; \overline{6}), (\overline{13}; \overline{12})$, и, таким образом, полученная система не является равносильной исходной. Это происходит по той причине, что существует два ненулевых класса $\overline{6}$ и $\overline{12}$, в произведении с $\overline{3}$ дающих $\overline{0}$: $\overline{6} \cdot \overline{3} = \overline{18} = \overline{0}$, $\overline{12} \cdot \overline{3} = \overline{36} = \overline{0}$. Поэтому справедлива цепочка уравнений:

$$\overline{21} \cdot \overline{x} + \overline{15} \cdot \overline{y} = \overline{21} \Leftrightarrow \overline{21} \cdot \overline{x} + \overline{15} \cdot \overline{y} - \overline{21} = \overline{0} \Leftrightarrow \overline{3} \cdot (\overline{7} \cdot \overline{x} + \overline{5} \cdot \overline{y} - \overline{7}) = \overline{0} \Leftrightarrow$$

$$\begin{cases} \overline{7} \cdot \overline{x} + \overline{5} \cdot \overline{y} - \overline{7} = \overline{0}; \\ \overline{7} \cdot \overline{x} + \overline{5} \cdot \overline{y} - \overline{7} = \overline{6}; \\ \overline{7} \cdot \overline{x} + \overline{5} \cdot \overline{y} - \overline{7} = \overline{12}. \end{cases}$$

Последние два уравнения совокупности дают лишние решения.

То же самое замечание справедливо и для решения системы при переходе на язык сравнений. ▲

**ТЕСТ ДЛЯ САМОПРОВЕРКИ ПО ТЕМЕ
«ОСНОВЫ ТЕОРИИ ЧИСЕЛ»**

Вопрос 1. Пусть $a = 3^2 \cdot 5^2 \cdot 11$, $b = 2 \cdot 3^2 \cdot 5^3$. Найти $\frac{\text{НОК}(a;b)}{\text{НОД}(a;b)}$.

- A) 990;
- B) 55;
- C) 550;
- D) 110;
- E) 22.

Вопрос 2. Для начала каждого предложения A–D подберите его окончание так, чтобы получилось верное утверждение. Ответ запишите в виде сочетания букв и цифр, соблюдая алфавитную последовательность букв. Некоторые данные правого столбца могут использоваться несколько раз или не использоваться вообще.

Начало предложения	Окончание предложения
A. Остаток от деления (-13) на 3 равен ...	1) 480
B. Максимальное количество пар взаимно простых чисел из набора 1, 2, 3, 6, 7 равно ...	2) 7
C. Степень сравнения $48x^3 - 24x^2 + 3x + 1 \equiv 0 \pmod{12}$ равна...	3) -1
D. Произведение $\text{НОК}(40, 12) \cdot \text{НОД}(40, 12)$ равно ...	4) 3
	5) 1
	6) 2
	7) 8

Вопрос 3. Найти остаток от деления 343^{42} на 17:

- A) 5;
- B) 8;
- C) 9;
- D) 4;
- E) 1.

Вопрос 4. Найти $\varphi(7) + \varphi(44)$, где $\varphi(n)$ – функция Эйлера.

Вопрос 5. В кольце классов вычетов $\mathbb{Z}/21\mathbb{Z}$ найти класс, равный $\bar{3} \cdot \bar{8} + \bar{7} \cdot \bar{5}$.

Вопрос 6. Из перечисленных ниже пар в кольце $\mathbb{Z}/25\mathbb{Z}$ выбрать пару взаимно обратных элементов:

- A) $(\bar{18}; \bar{8})$;
- B) $(\bar{11}; \bar{12})$;
- C) $(\bar{23}; \bar{6})$;

- D) $(\overline{9}; \overline{6})$;
 E) $(\overline{18}; \overline{7})$.

Вопрос 7. В кольце $\mathbb{Z}/602\mathbb{Z}$ найти класс, обратный к классу $\overline{11}$.

Вопрос 8. Укажите числа, для которых сравнение $a \equiv b \pmod{m}$ верно:

- A) $a = 47, b = 13, m = 7$;
 B) $a = 22, b = 13, m = 5$;
 C) $a = 73, b = 29, m = 11$;
 D) $a = 19, b = 8, m = 3$;
 E) $a = 67, b = 7, m = 9$.

Вопрос 9. Одним из решений сравнения $123x \equiv 51 \pmod{15}$ является:

- A) $15 \cdot t + 7, t \in \mathbb{Z}$;
 B) $15 \cdot t + 13, t \in \mathbb{Z}$;
 C) $15 \cdot t + 1, t \in \mathbb{Z}$;
 D) $15 \cdot t + 5, t \in \mathbb{Z}$;
 E) $15 \cdot t + 11, t \in \mathbb{Z}$.

Вопрос 10*. Сколько решений имеет сравнение $24x \equiv 48 \pmod{84}$?

- A) 1;
 B) 0;
 C) 84;
 D) 12;
 E) 24.

Ключ к тесту:

<i>Номер вопроса</i>	<i>Ответ</i>
1	D
2	A6B7C5D1
3	B
4	26
5	17
6	E
7	219
8	C
9	A
10	D

ИНДИВИДУАЛЬНЫЕ ЗАДАНИЯ ДЛЯ ЛАБОРАТОРНОЙ РАБОТЫ № 1 «ОСНОВЫ ТЕОРИИ ЧИСЕЛ»

1. Найти НОД(a, b) и НОК(a, b), воспользовавшись: а) алгоритмом Евклида; б) канонической факторизацией чисел.

2. С помощью расширенного алгоритма Евклида найти целые u, v , удовлетворяющие соотношению Безу: $au + bv = \text{НОД}(a, b)$.

3. Найти остаток от деления данного числа на заданное простое число.

4. Построить таблицы сложения в кольце: а) $\mathbb{Z}/k\mathbb{Z}$; б) $\mathbb{Z}/n\mathbb{Z}$.

5. Построить таблицы умножения в кольце: а) $\mathbb{Z}/k\mathbb{Z}$; б) $\mathbb{Z}/n\mathbb{Z}$.

В кольцах $\mathbb{Z}/k\mathbb{Z}$ и $\mathbb{Z}/n\mathbb{Z}$ найти пары взаимно обратных относительно умножения элементов.

6. Вычислить $\varphi(k)$, $\varphi(n)$ для k, n из четвертого задания, $\varphi(a)$ – для целого a из первого задания.

7. Решить систему уравнений в кольце классов вычетов: а) $\mathbb{Z}/p\mathbb{Z}$; б) $\mathbb{Z}/s\mathbb{Z}$; в) $\mathbb{Z}/n\mathbb{Z}$.

Вариант 1

1–2. $a = 1139$, $b = 3267$.

3. Остаток от деления 1998^{2001} на 29.

4–6. $k = 11$; $n = 24$.

7. $p = 11$; $s = 25$.

$$\begin{array}{lll} \text{а) } \begin{cases} \overline{2}x + \overline{4}y = \overline{10}; \\ \overline{x} + \overline{6}y = \overline{8}; \end{cases} & \text{б) } \begin{cases} \overline{5}x + \overline{4}y + \overline{3}z = \overline{4}; \\ \overline{6}x + \overline{5}y + \overline{2}z = \overline{3}; \\ \overline{9}x + \overline{8}y + \overline{15}z = \overline{6}; \end{cases} & \text{в) } \begin{cases} \overline{13}x + \overline{5}y = \overline{11}; \\ \overline{7}x + \overline{11}y = \overline{13}. \end{cases} \end{array}$$

Вариант 2

1–2. $a = 5901$, $b = 4801$.

3. Найти остаток от деления 2005^{2003} на 17.

4–6. $k = 13$; $n = 18$.

7. $p = 13$; $s = 49$.

$$\begin{array}{lll} \text{а) } \begin{cases} \overline{3}x + \overline{6}y = \overline{12}; \\ \overline{4}x + \overline{6}y = \overline{4}; \end{cases} & \text{б) } \begin{cases} \overline{3}x + \overline{2}y + z = \overline{10}; \\ \overline{4}x + y + \overline{2}z = \overline{12}; \\ \overline{5}x + \overline{3}y + z = \overline{14}; \end{cases} & \text{в) } \begin{cases} \overline{13}x + \overline{5}y = \overline{11}; \\ \overline{7}x + \overline{11}y = \overline{13}. \end{cases} \end{array}$$

Вариант 3

1–2. $a = 6042$, $b = 3648$.

3. Найти остаток от деления 2001^{2005} на 17.

4–6. $k = 23$; $n = 12$.

7. $p = 23$; $s = 24$.

$$\text{а) } \begin{cases} \overline{17}x + \overline{3}y = \overline{2}; \\ \overline{5}x + \overline{16}y = \overline{11}; \end{cases} \quad \text{б) } \begin{cases} \overline{3}x + y + \overline{2}z = \overline{3}; \\ \overline{2}x + \overline{5}y + \overline{4}z = \overline{1}; \\ x + \overline{8}y + \overline{3}z = \overline{4}; \end{cases} \quad \text{в) } \begin{cases} \overline{13}x + \overline{5}y = \overline{11}; \\ \overline{7}x + \overline{11}y = \overline{13}. \end{cases}$$

Вариант 4

1–2. $a = 2397$, $b = 4317$.

3. Найти остаток от деления 2004^{2998} на 19.

4–6. $k = 17$; $n = 21$.

7. $p = 17$; $s = 25$.

$$\text{а) } \begin{cases} \overline{13}x + \overline{7}y = \overline{2}; \\ \overline{6}x + \overline{8}y = \overline{15}; \end{cases} \quad \text{б) } \begin{cases} x + y + \overline{3}z = \overline{2}; \\ \overline{4}x + y + \overline{6}z = \overline{5}; \\ \overline{8}x + \overline{3}y + \overline{2}z = \overline{3}; \end{cases} \quad \text{в) } \begin{cases} \overline{13}x + \overline{5}y = \overline{11}; \\ \overline{7}x + \overline{11}y = \overline{13}. \end{cases}$$

Вариант 5

1–2. $a = 9183$, $b = 3389$.

3. Найти остаток от деления 1999^{2005} на 23.

4–6. $k = 19$; $n = 26$.

7. $p = 19$; $s = 49$.

$$\text{а) } \begin{cases} \overline{14}x + \overline{12}y = \overline{5}; \\ \overline{11}x + \overline{14}y = \overline{2}; \end{cases} \quad \text{б) } \begin{cases} x + y + z = \overline{3}; \\ \overline{2}x + \overline{5}y + \overline{3}z = \overline{1}; \\ \overline{3}x + \overline{2}y + \overline{2}z = \overline{8}; \end{cases} \quad \text{в) } \begin{cases} \overline{13}x + \overline{5}y = \overline{11}; \\ \overline{7}x + \overline{11}y = \overline{13}. \end{cases}$$

Вариант 6

1–2. $a = 5361$, $b = 1962$.

3. Найти остаток от деления 1998^{2001} на 19.

4–6. $k = 13$; $n = 27$.

7. $p = 13$; $s = 28$.

$$\text{a) } \begin{cases} \overline{5}x + \overline{7}y = \overline{12}; \\ \overline{4}x + \overline{9}y = \overline{10}; \end{cases} \quad \text{б) } \begin{cases} x + \overline{2}y + z = \overline{2}; \\ \overline{3}x + \overline{3}y + \overline{2}z = \overline{6}; \\ \overline{2}x + \overline{24}y + z = \overline{9}; \end{cases} \quad \text{в) } \begin{cases} \overline{13}x + \overline{5}y = \overline{11}; \\ \overline{7}x + \overline{11}y = \overline{13}. \end{cases}$$

Вариант 7

1–2. $a = 7964$, $b = 1698$.

3. Найти остаток от деления 1997^{2004} на 17.

4–6. $k = 7$; $n = 28$.

7. $p = 19$; $s = 49$;

$$\text{a) } \begin{cases} \overline{5}x + \overline{3}y = \overline{6}; \\ \overline{4}x + \overline{3}y = \overline{5}; \end{cases} \quad \text{б) } \begin{cases} x + \overline{2}y + \overline{4}z = \overline{1}; \\ x + \overline{4}y + \overline{6}z = \overline{0}; \\ \overline{2}x + \overline{8}y + \overline{4}z = \overline{47}; \end{cases} \quad \text{в) } \begin{cases} \overline{13}x + \overline{5}y = \overline{11}; \\ \overline{7}x + \overline{11}y = \overline{13}. \end{cases}$$

Вариант 8

1–2. $a = 8348$, $b = 5591$.

3. Найти остаток от деления 1996^{2003} на 11.

4–6. $k = 29$; $n = 12$.

7. $p = 29$; $s = 35$;

$$\text{a) } \begin{cases} \overline{15}x + \overline{24}y = \overline{17}; \\ \overline{14}x + \overline{13}y = \overline{15}; \end{cases} \quad \text{б) } \begin{cases} x + y + \overline{2}z = \overline{2}; \\ \overline{2}x + y + \overline{4}z = \overline{1}; \\ \overline{5}x + \overline{4}y + \overline{7}z = \overline{4}; \end{cases} \quad \text{в) } \begin{cases} \overline{13}x + \overline{5}y = \overline{11}; \\ \overline{7}x + \overline{11}y = \overline{13}. \end{cases}$$

Вариант 9

1–2. $a = 16254$, $b = 1290$.

3. Найти остаток от деления 2006^{1998} на 19.

4–6. $k = 23$; $n = 14$.

7. $p = 23$; $s = 35$;

$$\text{a) } \begin{cases} \overline{15}x + \overline{10}y = \overline{17}; \\ \overline{18}x + \overline{19}y = \overline{20}; \end{cases} \quad \text{б) } \begin{cases} \overline{3}x + \overline{4}y + z = \overline{1}; \\ x + y + z = \overline{2}; \\ \overline{2}x + \overline{34}y + \overline{2}z = \overline{7}; \end{cases} \quad \text{в) } \begin{cases} \overline{13}x + \overline{5}y = \overline{11}; \\ \overline{7}x + \overline{11}y = \overline{13}. \end{cases}$$

Вариант 10

1–2. $a = 6377$, $b = 9568$.

3. Найти остаток от деления 2010^{1999} на 17 числа.

4–6. $k = 31$; $n = 12$.

7. $p = 31$; $s = 38$;

$$\text{a) } \begin{cases} \overline{25}x + \overline{29}y = \overline{30}; \\ \overline{14}x + \overline{8}y = \overline{27}; \end{cases} \quad \text{б) } \begin{cases} x + \overline{34}y + \overline{3}z = \overline{5}; \\ \overline{2}x + \overline{31}y + \overline{2}z = \overline{3}; \\ \overline{3}x + \overline{30}y + \overline{4}z = \overline{9}; \end{cases} \quad \text{в) } \begin{cases} \overline{13}x + \overline{5}y = \overline{11}; \\ \overline{7}x + \overline{11}y = \overline{13}. \end{cases}$$

Вариант 11

1–2. $a = 7955$, $b = 2315$.

3. Найти остаток от деления 2005^{1999} на 19.

4–6. $k = 17$; $n = 30$.

7. $p = 17$; $s = 36$;

$$\text{a) } \begin{cases} \overline{15}x + \overline{8}y = \overline{16}; \\ \overline{14}x + \overline{13}y = \overline{7}; \end{cases} \quad \text{б) } \begin{cases} x + \overline{34}y + z = \overline{7}; \\ x + \overline{33}y + \overline{35}z = \overline{2}; \\ \overline{5}x + \overline{27}y + \overline{30}z = \overline{1}; \end{cases} \quad \text{в) } \begin{cases} \overline{13}x + \overline{5}y = \overline{11}; \\ \overline{7}x + \overline{11}y = \overline{13}. \end{cases}$$

Вариант 12

1–2. $a = 1688$, $b = 1826$.

3. Найти остаток от деления 1995^{2004} на 16.

4–6. $k = 29$; $n = 9$.

7. $p = 29$; $s = 49$;

$$\text{a) } \begin{cases} \overline{5}x + \overline{7}y = \overline{16}; \\ \overline{21}x + \overline{25}y = \overline{17}; \end{cases} \quad \text{б) } \begin{cases} x + y + z = \overline{6}; \\ \overline{2}x + y + \overline{48}z = \overline{1}; \\ \overline{3}x + \overline{5}y + \overline{46}z = \overline{1}; \end{cases} \quad \text{в) } \begin{cases} \overline{13}x + \overline{5}y = \overline{11}; \\ \overline{7}x + \overline{11}y = \overline{13}. \end{cases}$$

Вариант 13

1–2. $a = 2411$, $b = 6187$.

3. Найти остаток от деления 2011^{1999} на 17.

4–6. $k = 17$; $n = 22$.

7. $p = 17$; $s = 25$;

$$\text{a) } \begin{cases} \overline{14}x + \overline{4}y = \overline{11}; \\ \overline{12}x + \overline{15}y = \overline{13}; \end{cases} \quad \text{б) } \begin{cases} x + \overline{22}y + \overline{8}z = \overline{5}; \\ \overline{2}x + \overline{18}y + \overline{9}z = \overline{1}; \\ \overline{3}x + \overline{19}y + \overline{7}z = \overline{4}; \end{cases} \quad \text{в) } \begin{cases} \overline{13}x + \overline{5}y = \overline{11}; \\ \overline{7}x + \overline{11}y = \overline{13}. \end{cases}$$

Вариант 14

1–2. $a = 3562$, $b = 3128$.

3. Найти остаток от деления 2005^{2004} на 19.

4–6. $k = 19$; $n = 14$.

7. $p = 19$; $s = 40$;

$$\text{a) } \begin{cases} \overline{14}x + \overline{18}y = \overline{17}; \\ \overline{2}x + \overline{10}y = \overline{4}; \end{cases} \quad \text{б) } \begin{cases} x + \overline{33}y + \overline{4}z = \overline{4}; \\ \overline{2}x + \overline{34}y + \overline{3}z = \overline{6}; \\ \overline{4}x + \overline{31}y + \overline{2}z = \overline{7}; \end{cases} \quad \text{в) } \begin{cases} \overline{13}x + \overline{5}y = \overline{11}; \\ \overline{7}x + \overline{11}y = \overline{13}. \end{cases}$$

Вариант 15

1–2. $a = 7409$, $b = 6793$.

3. Найти остаток от деления 2005^{2002} на 29.

4–6. $k = 23$; $n = 16$.

7. $p = 23$; $s = 49$;

$$\text{a) } \begin{cases} \overline{4}x + \overline{8}y = \overline{13}; \\ \overline{12}x + \overline{19}y = \overline{7}; \end{cases} \quad \text{б) } \begin{cases} x + y + \overline{2}z = \overline{1}; \\ \overline{4}x + \overline{6}y + \overline{3}z = \overline{2}; \\ \overline{8}x + \overline{4}y + \overline{8}z = \overline{3}. \end{cases} \quad \text{в) } \begin{cases} \overline{13}x + \overline{5}y = \overline{11}; \\ \overline{7}x + \overline{11}y = \overline{13}. \end{cases}$$

МОДУЛЬ № 2. ОСНОВЫ ТЕОРИИ ГРУПП

ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ ПО ТЕМЕ «ОСНОВЫ ТЕОРИИ ГРУПП»¹

§ 1. Группы и подгруппы. Циклические группы

Рассмотрим множество A , природу элементов которого не будем конкретизировать, поскольку ими могут быть, например, числа, матрицы, отображения. В дальнейшем будем рассматривать некоторое абстрактное множество A с элементами произвольной природы.

Определение 2.1. *Бинарной алгебраической операцией на множестве A называют правило, по которому каждой упорядоченной паре элементов (a, b) множества A ставится в соответствие единственный вполне определенный элемент этого множества c .*

Пример 2.1. На числовых множествах действительных чисел $\mathbb{R}$ и комплексных чисел $\mathbb{C}$ бинарными операциями будут операции сложения, вычитания и умножения их элементов.

Пример 2.2. На множестве свободных векторов пространства $\mathbb{R}^3$ заданы операции скалярного и векторного произведения векторов. Скалярное произведение не является алгебраической операцией, так как ее результатом является число, не принадлежащее исходному множеству векторов, в то время как векторное произведение, результатом которого будет вектор этого же пространства, является бинарной алгебраической операцией.

Бинарную алгебраическую операцию на множестве A будем далее обозначать символом « $\circ$ »:

$$a \circ b = c,$$

где $a, b, c \in A$.

Определение 2.2. *Группой называется множество G элементов произвольной природы, на котором задана бинарная алгебраическая операция, называемая также групповой операцией и удовлетворяющая следующим аксиомам:*

1) *ассоциативность групповой операции:*

$$\forall a, b, c \in G \text{ имеет место } a \circ (b \circ c) = (a \circ b) \circ c;$$

2) *существование нейтрального элемента:*

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

3) *существование для всякого элемента a обратного, или симметричного, к нему элемента:*

$$\forall a \in G \quad \exists a^{-1} \in G : a \circ a^{-1} = a^{-1} \circ a = e.$$

Для обозначения групповой операции вместо символа « $\circ$ » используют либо точку, либо знак сложения (+). В первом случае групповую операцию называют

¹ При подготовке данного раздела использовались следующие источники: [5, 6, 15, 16, 21].

умножением, саму группу – мультипликативной, нейтральный элемент обозначают 1, а обратный к элементу a обозначают a^{-1} . Во втором случае групповую операцию называют операцией сложения, группу – аддитивной, нейтральный элемент обозначают 0, а обратный к элементу a называют противоположным и обозначают $-a$. Эти определения представлены в таблице 2.

Таблица 2

Типы групп по групповой операции

Обозначение групповой операции	Название групповой операции	Название группы	Нейтральный элемент	Симметричный элемент к a
+	Сложение	Аддитивная	0 – нуль	$-a$ – противоположный
·	Умножение	Мультипликативная	1 – единица	a^{-1} – обратный

Замечание. Для обозначения группы G с указанной групповой операцией « $\circ$ » будем использовать запись $(G, \circ)$, тогда $(G, +)$ – группа с операцией сложения, а $(G, \cdot)$ – группа с операцией умножения.

Пример 2.3. Множество действительных чисел $\mathbb{R}$ является группой относительно операции сложения. Это аддитивная группа. Однако относительно операции умножения то же множество нельзя назвать группой: наличие элемента нуль, не имеющего обратного, нарушает выполнение третьей аксиомы определения группы. Исключив нуль из множества действительных чисел, получим множество $\mathbb{R}/\{0\}$, являющееся мультипликативной группой.

Пример 2.4. Операция сложения классов вычетов по модулю n удовлетворяет всем аксиомам групповой операции, следовательно, множество $\mathbb{Z}/n\mathbb{Z}$ классов вычетов по модулю n образует аддитивную группу. Будем обозначать ее $(\mathbb{Z}/n\mathbb{Z}, +)$.

По количеству элементов группы делятся на конечные и бесконечные.

Определение 2.3. *Порядком конечной группы G называется число элементов в группе. Порядок группы обозначается $|G|$.*

Пример 2.5. Аддитивная группа $(\mathbb{R}, +)$ является бесконечной группой, так как содержит бесконечное число членов. Группа $(\mathbb{Z}/n\mathbb{Z}, +)$ содержит n классов вычетов, следовательно, она является конечной, а ее порядок равен n .

По свойствам групповой операции группы делятся на коммутативные и некоммутативные.

Определение 2.4. *Коммутативная, или абелева, группа – это группа G , бинарная алгебраическая операция которой коммутативна:*

$$\forall a, b \in G \text{ имеет место } a \circ b = b \circ a.$$

Пример 2.6. Группы $(\mathbb{Z}/n\mathbb{Z}, +)$ и $(\mathbb{R}, +)$ являются абелевыми группами в силу коммутативности операции сложения.

Пример 2.7. Несмотря на разделение групп на мультипликативные и аддитивные, групповая операция не обязательно должна быть стандартной операцией

сложения или стандартной операцией умножения. Рассмотрим множество линейных функций, определенных на всем множестве действительных чисел:

$$M = \{f(x) = ax + b \mid a, b \in \mathbb{R}, a \neq 0, -\infty < x < +\infty\}.$$

Введем операцию над элементами этого множества как композицию функций:

$$\forall f(x), g(x) \in M \quad f \circ g = f(g(x)).$$

Убедимся, что эта операция является бинарной алгебраической операцией, т. е. композиция линейных функций также является линейной функцией. Пусть $f(x) = ax + b$, а $g(x) = cx + d$. Тогда:

$$\begin{aligned} f \circ g &= f(g(x)) = f(cx + d) = a(cx + d) + b = acx + ad + b = \\ &= \begin{bmatrix} ac = m = \text{const}, m \neq 0 \\ ad + b = n = \text{const} \end{bmatrix} = \\ &= mx + n \in M. \end{aligned}$$

Согласно общим свойствам отображений, частным случаем которых являются рассматриваемые линейные функции, композиция отображений обладает свойством ассоциативности.

В качестве нейтрального элемента выберем функцию $e(x) = x$:

$$\begin{aligned} \forall g \in M \quad e \circ g &= e(g(x)) = e(cx + d) = cx + d = g; \\ g \circ e &= g(e(x)) = g(x) = g. \end{aligned}$$

Каждая линейная функция является взаимно однозначной. Как известно, для каждой взаимно однозначной функции существует обратная ей. Так, для функции $f(x) = ax + b$ обратной будет являться функция $f^{-1}(x) = (x - b) / a$:

$$\begin{aligned} \forall f \in M \quad f \circ f^{-1} &= f(f^{-1}) = f\left(\frac{1}{a}x - \frac{b}{a}\right) = a\left(\frac{1}{a}x - \frac{b}{a}\right) + b = x = e; \\ f^{-1} \circ f &= f^{-1}(f) = f^{-1}(ax + b) = \frac{1}{a}(ax + b) - \frac{b}{a} = x = e. \end{aligned}$$

Таким образом, все три аксиомы групповой операции выполнены, следовательно, рассматриваемое множество линейных функций образует группу относительно операции композиции функций. Очевидно, что эта операция не является непосредственным умножением $f(x)$ на $g(x)$. Тем не менее описанная группа считается мультипликативной.

Определение 2.5. *Подгруппой H группы G называется непустое подмножество группы G , являющееся группой относительно той же операции, которая определена в группе G .*

Пример 2.8. Множество действительных чисел $\mathbb{R}$ является группой относительно сложения, ее подмножество $\mathbb{Z}$ целых чисел – также группа относительно сложения, следовательно, является подгруппой аддитивной группы $(\mathbb{R}, +)$.

Замечание. Существует ряд понятий и свойств, общих для мультипликативных и аддитивных групп. Не ограничивая общности рассуждений, в данном мо-

дуле везде далее будем использовать мультипликативную запись групповой операции и называть операцию произведением. Естественно, что в аддитивных группах операция будет сложением, а симметричный элемент будет являться противоположным к данному.

Теорема 2.1 (критерий подгруппы). *Для того чтобы непустое подмножество H группы G являлось ее подгруппой необходимо и достаточно, чтобы выполнялись два условия: 1) произведение любых двух элементов подмножества H также должно принадлежать этому подмножеству: $\forall a, b \in H \Rightarrow a \cdot b \in H$; 2) для любого элемента подмножества H обратный к нему также должен принадлежать подмножеству H : $\forall a \in H \Rightarrow a^{-1} \in H$.*

Пример 2.9. Рассмотрим аддитивную группу целых чисел $(\mathbb{Z}, +)$. Ее подмножество чисел, состоящее из чисел, кратных некоторому числу n , задается как $\{qn \mid q \in \mathbb{Z}\}$ и образует ее подгруппу. Проверим выполнение критерия подгруппы. Действительно, для любых двух чисел, кратных n , их сумма также кратна n :

$$\forall q_1, q_2 \in \mathbb{Z} \quad q_1 n + q_2 n = q_3 n \in \{qn \mid q \in \mathbb{Z}\}.$$

Очевидно, что число, противоположное кратному n , также кратно n . Таким образом, все условия критерия подгруппы выполнены, и подмножество $\{qn \mid q \in \mathbb{Z}\}$ является подгруппой группы $(\mathbb{Z}, +)$.

Из определения подгруппы следует, что подгруппами являются сама группа G и ее нейтральный элемент $H = \{e\}$. Эти две подгруппы называются **тривиальными или несобственными**.

Определение 2.6. Собственная подгруппа H группы G – подгруппа, не совпадающая ни с G , ни с $\{e\}$.

Определение 2.7. Рассмотрим мультипликативную группу G и ее элемент a , n – целое число. Введем обозначения

$$a^n = \begin{cases} 1, n = 0 \\ \underbrace{a \cdot a \cdot \dots \cdot a}_{n \text{ множителей}}, n > 0 \\ (a^{-n})^{-1}, n < 0. \end{cases}$$

Элемент a^n , обозначенный таким образом, будем называть **n -й степенью элемента a** .

Замечание. В случае аддитивной группы под n -й степенью элемента a будем понимать

$$a^n = \begin{cases} 0, n = 0 \\ \underbrace{a + a + \dots + a}_{n \text{ слагаемых}}, n > 0 \\ -(a^{-n}), n < 0. \end{cases}$$

Определение 2.8. Порядком элемента a группы G называется наименьшее натуральное число n , такое, что $a^n = 1$. Если такого числа n не существует, то говорят, что элемент a имеет бесконечный порядок.

Пример 2.10. В аддитивной группе $(\mathbb{Z}/3\mathbb{Z}, +)$ элемент $\bar{1}$ имеет порядок 3, так как $\bar{1} + \bar{1} + \bar{1} = \bar{3} = \bar{0}$.

Теорема 2.2. Множество всевозможных целых степеней элемента a группы G $\{a^n | n \in \mathbb{Z}\}$ образует абелеву подгруппу группы G . Эта подгруппа называется **циклической, порожденной элементом a** .

Циклическая подгруппа, порожденная элементом a , обозначается $\langle a \rangle$:

$$\langle a \rangle = \{a^n | a \in G, n \in \mathbb{Z}\}.$$

Теорема 2.3. Циклическая подгруппа, порожденная элементом a конечного порядка n , содержит n элементов.

Иными словами, если порядок элемента конечен, то он порождает циклическую подгруппу того же порядка.

Пример 2.11. В аддитивной группе $(\mathbb{Z}/10\mathbb{Z}, +)$ элемент $\bar{2}$ имеет порядок 5: $\bar{2} + \bar{2} + \bar{2} + \bar{2} + \bar{2} = \bar{10} = \bar{0}$, циклическая подгруппа, порожденная этим элементом, содержит пять элементов:

$$\langle a \rangle = \{\bar{2}, \bar{2} + \bar{2} = \bar{4}, \bar{2} + \bar{2} + \bar{2} = \bar{6}, \bar{2} + \bar{2} + \bar{2} + \bar{2} = \bar{8}, \bar{2} + \bar{2} + \bar{2} + \bar{2} + \bar{2} = \bar{10}\}.$$

Определение 2.9. Циклическая группа G – группа, которая содержит такой элемент a , что порожденная им циклическая подгруппа совпадает с G : $\langle a \rangle = G$. Такой элемент называется **генератором группы**.

Пример 2.12. Аддитивная группа $(\mathbb{Z}/n\mathbb{Z}, +)$ является циклической, так как каждый ее элемент может быть представлен в виде степени элемента $\bar{1}$, не превосходящей n :

$$\bar{k} = \underbrace{\bar{1} + \bar{1} + \dots + \bar{1}}_{k \text{ слагаемых}}.$$

Таким образом, класс $\bar{1}$ является генератором группы $(\mathbb{Z}/n\mathbb{Z}, +)$.

Свойства циклических групп:

- 1) всякая циклическая группа является абелевой;
- 2) каждая подгруппа циклической группы есть циклическая группа;
- 3) элемент a^k в циклической группе $\langle a \rangle$ порядка m порождает подгруппу порядка $m / \text{НОК}(m, n)$;

- 4) конечная циклическая группа $\langle a \rangle$ порядка m имеет $\varphi(m)$ генераторов группы, где $\varphi(m)$ – функция Эйлера от m .

Определить, является ли группа циклической, в общем случае можно, лишь отыскав непосредственной проверкой ее генератор. Для произвольно взятой группы это трудоемкий процесс. Однако для некоторых частных случаев групп его можно не проводить, так как для них указаны достаточные условия их циклическости.

Определение 2.10. Мультипликативная группа кольца классов вычетов $\mathbb{Z}/n\mathbb{Z}$ – множество обратимых классов вычетов с введенной на нем операцией умножения классов. Обозначается $\mathbb{Z}/n\mathbb{Z}^*$.

Пример 2.13. Мультипликативную группу кольца вычетов $\mathbb{Z}/6\mathbb{Z}$ образуют два обратимых класса $\bar{1}$ и $\bar{5}$. Других обратимых классов вычетов нет:

$$\mathbb{Z}/6\mathbb{Z}^* = \{\bar{1}, \bar{5}\}.$$

Теорема 2.4. Если $n = p^k$, где $p \neq 2$ и является простым, k – натуральное число, или $n = 2^k$, где k равно 1 или 2, то мультипликативная группа $\mathbb{Z}/n\mathbb{Z}^*$ является циклической.

Обобщая изложенные в этом параграфе определения и свойства групп, можно заключить, что каждую группу (подгруппу) можно охарактеризовать по четырем категориям: тип групповой операции, число элементов, коммутативность групповой операции, цикличность. За исключением связи аддитивных и циклических групп с абелевыми (всякая циклическая группа абелева, и всякая аддитивная группа абелева), эти категории являются независимыми. Схематичное изображение всех типов групп представлены на рис. 3.

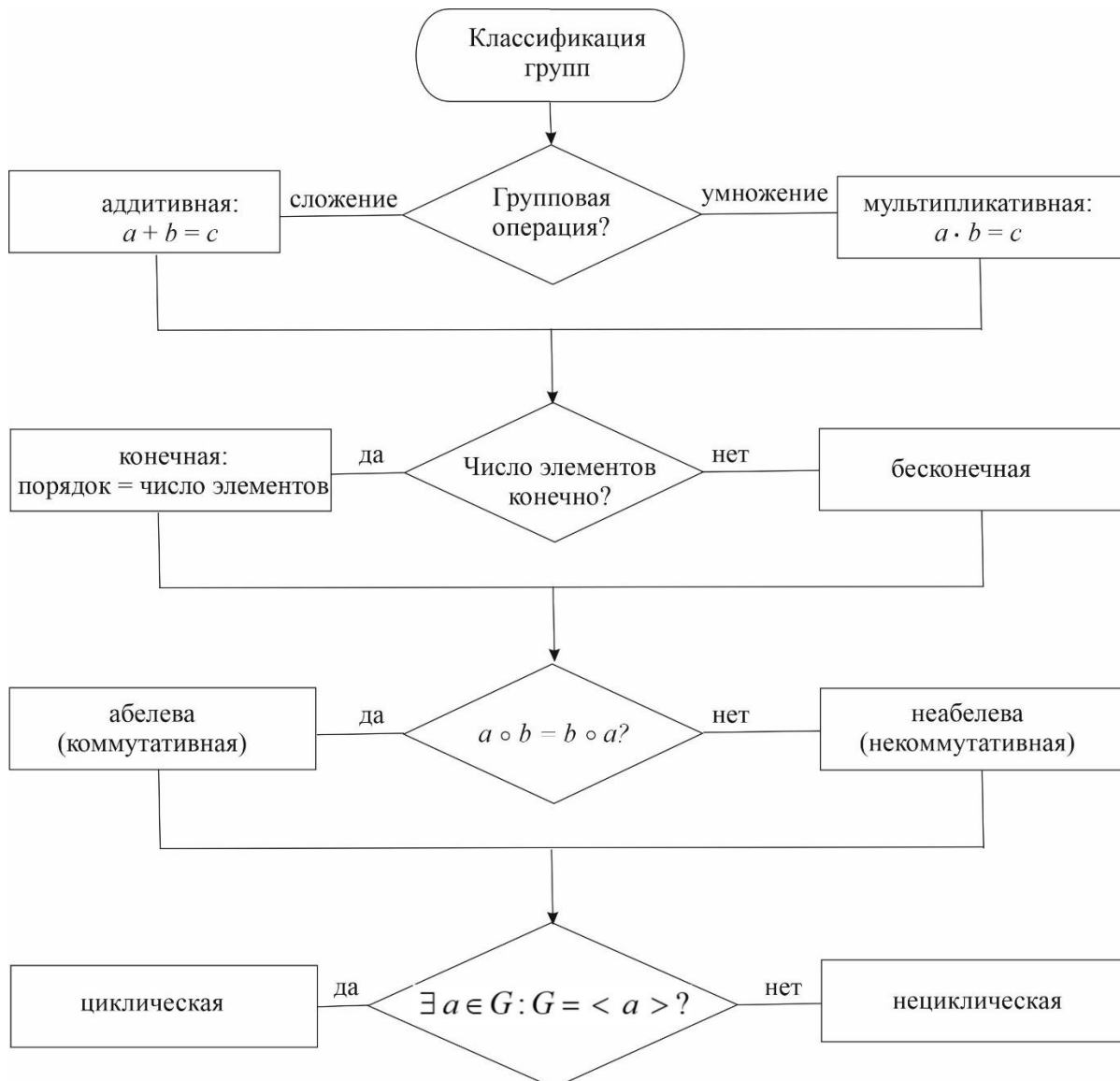


Рис. 3. Схема классификации групп по различным признакам

Любая группа (подгруппа) может быть охарактеризована по каждой категории. Например, группа $(\mathbb{Z}/n\mathbb{Z}, +)$ – аддитивная, конечная, абелева и циклическая.

§ 2. Подстановки. Симметрические группы

Рассмотрим конечное множество Ω из n элементов произвольной природы. Каждому из элементов присвоим его порядковый номер, и в дальнейшем будем различать элементы по их порядковым номерам: $\Omega = \{1, \dots, n\}$.

Определение 2.11. *Подстановка на конечном множестве Ω – взаимно однозначное отображение множества Ω в самого себя, т. е. правило, по которому каждому элементу множества Ω (прообразу) ставится в соответствие вполне определенный элемент этого же множества (образ), причем для любых двух различных прообразов их образы также различны.*

Замечание. Образ и прообраз могут совпадать.

Поскольку множество Ω конечно, то одним из способов задания подстановки является непосредственное перечисление пар «прообраз – образ». Это перечисление записывается в виде двух строк, в верхней указываются элементы множества Ω , упорядоченные по возрастанию номера, в нижней строке под каждым элементом записывается соответствующий ему образ.

Пример 2.14. Рассмотрим подстановку f на множестве из пяти элементов:

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

Из этой записи видим, что образом элемента 1 является элемент 4. Также говорят, что подстановка f переводит 1 в 4 и пишут $f(1) = 4$.

Зафиксируем число элементов n множества Ω и рассмотрим всевозможные подстановки на таком множестве. Введем операцию умножения двух подстановок как композицию соответствующих отображений: $(gf)(i) = g(f(i))$.

Пример 2.15. Найти произведение подстановок gf , если

$$f = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}; \quad g = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

Для каждого элемента вычислим его образ при композиции gf :

$$gf(1) = g(f(1)) = g(3) = 1;$$

$$gf(2) = g(f(2)) = g(1) = 3;$$

$$gf(3) = g(f(3)) = g(2) = 2.$$

Запишем полученные результаты в виде двух строк:

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

Операция умножения подстановок обладает свойством ассоциативности (но в общем случае не обладает свойством коммутативности). Нейтральным элементом на множестве подстановок является тождественная подстановка e , переводящая каждый элемент в самого себя: $e(i) = i$. Поскольку всякая подстановка – взаимно однозначное отображение, то из общих свойств отображений следует, что для любой подстановки f найдется такая подстановка f^{-1} , что $f^{-1}f = ff^{-1} = e$,

т. е. для любой подстановки существует обратная к ней f^{-1} . Из наличия групповых свойств элементов множества подстановок вытекает следующая теорема.

Теорема 2.5. *Множество подстановок на заданном конечном множестве n элементов образует группу относительно операции умножения. Эта группа называется симметрической на n элементах и обозначается S_n .*

Порядок симметрической группы S_n равен $n!$

Каждая подстановка f порождает конечную циклическую подгруппу $\langle f \rangle$. Порядок этой подгруппы и подстановки, входящие в эту подгруппу, можно получить, разложив подстановку на циклы.

Определение 2.12. *Циклом длины k называется подстановка вида*

$$f_k = \begin{pmatrix} i & f(i) & \dots & f^k(i) \\ f(i) & f^2(i) & \dots & i \end{pmatrix},$$

где f – некоторая подстановка из группы S_n . Также говорят, что элементы $i, f(i), \dots, f^k(i)$ являются Γ_f -эквивалентными.

Цикл также обозначается одной строкой $(i \ f(i) \ \dots \ f^k(i))$.

Определение 2.13. *Транспозицией называется цикл длиной 2.*

Пример 2.16. Выписать цикл, содержащий элемент 4, из подстановки

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 9 & 5 & 3 & 1 & 7 & 4 & 2 & 8 \end{pmatrix}.$$

В данном примере $i = 4$. Найдем по двустрочной таблице следующие образы:

$$f(i) = f(4) = 3;$$

$$f^2(i) = f^2(4) = f(3) = 5;$$

$$f^3(4) = f(5) = 1;$$

$$f^4(4) = f(1) = 6;$$

$$f^5(4) = f(6) = 7;$$

$$f^6(4) = f(7) = 4.$$

Таким образом, мы получили для $i = 4$ $f^k(i) = f^6(i) = i$, значит, цикл замкнулся. Поскольку $k = 6$, то полученный цикл имеет длину 6. Выпишем его в виде подстановки, опуская те элементы, на которые цикл действует тождественно (не вошедшие в цепочку $4 \rightarrow 3 \rightarrow 5 \rightarrow 1 \rightarrow 6 \rightarrow 7 \rightarrow 4$):

$$\begin{pmatrix} 4 & 3 & 5 & 1 & 6 & 7 \\ 3 & 5 & 1 & 6 & 7 & 4 \end{pmatrix} = (435167).$$

Как правило, выписывая из подстановки цикл, начинают с наименьшего номера, поэтому тот же цикл записывают как (167435) .

Можно показать, что каждый элемент множества Ω входит только в один цикл, и, таким образом, множество Ω разбивается с помощью подстановки f на непересекающиеся классы. Каждый такой класс состоит из элементов, входящих в один цикл, и называется **f -орбитой**.

Определение 2.14. *Независимые, или непересекающиеся, циклы – это циклы, не содержащие общих элементов.*

Поскольку каждый цикл – частный случай подстановки, циклы также можно умножать друг на друга по общим правилам умножения подстановок. При записи произведения циклов, как правило, не указывают циклы длиной 1, поскольку такой цикл соответствует тождественной подстановке. Произведение независимых циклов обладает свойством коммутативности.

Теорема 2.6. *Каждая подстановка f раскладывается в произведение независимых циклов длиной не менее двух. Это разложение определено однозначно с точностью до порядка следования независимых циклов.*

Теорема 2.7. *Любую подстановку f можно представить в виде произведения транспозиций. Любые два разложения данной подстановки в произведения транспозиций содержат либо четное число сомножителей, либо нечетное.*

Определение 2.15. *Четная (нечетная) подстановка f – это подстановка, разложение которой в произведение транспозиций содержит четное (нечетное) количество сомножителей.*

§ 3. Смежные классы по подгруппе. Теорема Лагранжа

Рассмотрим собственную подгруппу H группы G .

Определение 2.16. *Левым смежным классом по подгруппе H называется подмножество $aH \subset G$ всех произведений вида $a \cdot h$, где a – фиксированный элемент группы G , h – любой элемент из подгруппы H : $aH = \{ah \mid h \in H\}$. Правым смежным классом называется подмножество $Ha \subset G$, где a – фиксированный элемент группы G , такое, что $Ha = \{ha \mid h \in H\}$.*

Пример 2.17. В примере 2.9, сопровождающем теорему 2.1, было показано, что подмножество $H = \{h = qn \mid q \in \mathbb{Z}\}$ целых чисел, кратных заданному числу n , является подгруппой аддитивной группы $(\mathbb{Z}, +)$. Выберем фиксированное целое число k и построим левый смежный класс по подгруппе H . Этот смежный класс образуют всевозможные суммы вида $k + qn$, $q \in \mathbb{Z}$. Несложно убедиться, что все элементы данного смежного класса попарно сравнимы между собой по модулю n , и при этом все числа, сравнимые по модулю n с числом k , попали в этот класс. Из этого следует, что смежный класс kH совпал с классом вычетов $\bar{k}$.

В случае если левый класс aH совпадает с правым классом Ha , т. е. $aH = Ha$, такой класс называют **двусторонним**. В частности, всякий смежный класс в абелевой группе является двусторонним.

Теорема 2.8. *Пусть H – собственная подгруппа группы G . Тогда два левых смежных класса aH и bH равны между собой тогда и только тогда, когда произведение $a^{-1}b$ принадлежит подгруппе H . Для равенства двух правых смежных классов Ha и Hb необходимо и достаточно, чтобы ba^{-1} принадлежало подгруппе H .*

Теорема 2.9. Пусть H – собственная подгруппа группы G . Тогда любые два левых (правых) смежных класса либо совпадают, либо не пересекаются.

Теорема 2.10. Группа G является объединением непересекающихся смежных классов группы G по собственной подгруппе H .

С остальными свойствами смежных классов можно ознакомиться в пособии [20].

Представление конечной группы G в виде объединения непересекающихся левых (правых) смежных классов G по H называют *разложением Лагранжа*.

Пример 2.18. Множество целых чисел является объединением классов вычетов по модулю n . Как было показано выше, класс вычетов можно рассматривать как смежный класс по подгруппе чисел, кратных n , тогда можно также сказать, что аддитивная группа целых чисел $\mathbb{Z}$ является объединением смежных классов по подгруппе $H = \{h = qn | q \in \mathbb{Z}\}$.

Определение 2.17. *Фактор-множеством (левым) группы G по подгруппе H называется множество левых смежных классов и обозначается через G/H .*

Пример 2.19. Множество классов вычетов по модулю n является фактор-множеством аддитивной группы целых чисел $\mathbb{Z}$ по подгруппе H чисел, кратных числу n .

Определение 2.18. *Мощность множества G/H называется индексом подгруппы H и обозначается через $[G : H]$. В частности, индекс подгруппы H равен числу левых смежных классов, если это число конечно.*

Теорема 2.11 (Лагранжа). Если H – подгруппа группы G , то порядок группы равен произведению порядка подгруппы H на ее индекс: $|G| = |H| \cdot [G : H]$.

Следствие 1. Порядок подгруппы делит порядок конечной группы.

Следствие 2. Порядок любого элемента группы делит порядок конечной группы.

Следствие 3. Если порядок группы является простым числом, то эта группа является циклической.

В приведенных выше примерах была показана параллель между смежными классами и классами вычетов как частным случаем смежных классов. Операция сложения – это групповая операция аддитивной группы чисел, на которой построено множество классов вычетов. Как известно, на множестве классов вычетов также определена операция сложения, относительно которой это множество образует группу. Всегда ли можно построить группу на множестве G/H смежных классов по подгруппе H группы G , т. е. всегда ли можно задать ту же операцию над смежными классами, что задана над элементами группы G ? Вообще говоря, ответ отрицательный, но если потребовать от подгруппы H дополнительных условий, то на множестве G/H можно ввести групповую операцию группы G .

Определение 2.19. Подгруппа H группы G называется *нормальной подгруппой* или *нормальным делителем* группы G , если для любого элемента g группы G и любого элемента h подгруппы H элемент $g^{-1}hg \in H$.

Нормальная подгруппа H обозначается $H \triangleleft G$.

Теорема 2.12 (критерий нормальной подгруппы). *Подгруппа H является нормальной подгруппой группы G тогда и только тогда, когда любой левый смежный класс aH по подгруппе совпадает с правым смежным классом Ha , т. е. является двусторонним.*

Из критерия нормальной подгруппы следует, что любая подгруппа абелевой группы является нормальной.

Благодаря введению нормальной подгруппы как подгруппы с определенными характеристиками, становится возможным определить групповую операцию над смежными классами по заданной нормальной подгруппе H .

Определение 2.20. *Произведением двух левых смежных классов aH и bH по нормальной подгруппе H произвольной группы G называется смежный класс abH .*

Таким образом, на множестве смежных классов по нормальной подгруппе задана операция умножения. Можно показать, что ее результат – смежный класс abH не зависит от выбора представителей классов aH и bH .

Замечание. В общем случае под умножением смежных классов понимают ту же операцию, что определена над элементами группы G , поскольку результат операции над смежными классами полностью определяется операцией над их представителями – элементами группы G . Поэтому операцию над смежными классами называют **индуцированной на фактор-множестве G/H** .

Теорема 2.13. *Если H – нормальная подгруппа произвольной группы G , то G/H – множество всех левых смежных классов по подгруппе H является группой относительно операции умножения. Эта группа называется **фактор-группой G по H** .*

Для фактор-группы смежный класс $eH = H$ служит нейтральным элементом, а обратным к смежному классу aH является смежный класс $a^{-1}H$.

Пример 2.20. Как было указано выше, множество классов вычетов по модулю n – это фактор-множество аддитивной группы целых чисел $(\mathbb{Z}, +)$ по подгруппе H чисел, кратных n . В силу того, что группа $(\mathbb{Z}, +)$ является абелевой, указанная подгруппа H – нормальная подгруппа. Также известно, что определена операция сложения классов вычетов (смотри модуль 1, § 5) через сложение представителей двух классов. Иными словами, на фактор-множестве группы $(\mathbb{Z}, +)$ по нормальной подгруппе H задана индуцированная операция сложения. Тогда согласно теореме 2.13, фактор-множество классов вычетов образует **фактор-группу** относительно индуцированной операции сложения.

ТИПОВЫЕ ЗАДАНИЯ ПО ТЕМЕ «ОСНОВЫ ТЕОРИИ ГРУПП» С ОБРАЗЦАМИ РЕШЕНИЙ

Задание 1. Выяснить, является ли группой множество с заданной операцией:

А) многочлены степени n от неизвестной x с действительными коэффициентами и операцией сложения;

Б) положительные действительные числа с операцией « $\circ$ », заданной следующим образом: $\forall a, b \in \mathbb{R}^+ \quad a \circ b = a^2 b^2$;

В) степени данного действительного числа a , $a \neq 0, \pm 1$, с целыми показателями относительно операции умножения;

Г) многочлены степени не выше n (включая нуль) от неизвестной x с действительными коэффициентами и операцией сложения.

Решение

А) Вначале проверим, является ли заданная операция бинарной алгебраической, т. е. всегда ли результат ее действия принадлежит исходному множеству. Многочлены степени n от неизвестного x с действительными коэффициентами образуют множество:

$$\{a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \mid a_i \in \mathbb{R}, i = 0, 1, \dots, n, a_n \neq 0\}.$$

Рассмотрим сумму двух многочленов степени n , старшие коэффициенты которых противоположны: $a_n = -a_n$. Тогда их сумма является многочленом степени меньшей n , а значит, исходному множеству не принадлежит. Следовательно, указанная операция на данном множестве не является бинарной алгебраической, а само множество многочленов степени n с действительными коэффициентами относительно операции сложения не является группой.

Б) В первую очередь убедимся, что результат операции принадлежит указанному множеству: действительно, $\forall a, b \in \mathbb{R}^+ \quad a^2 b^2 \in \mathbb{R}^+$. Следовательно, определенная операция является бинарной алгебраической операцией. Проверим ассоциативность операции « $\circ$ »:

$$\forall a, b, c \in \mathbb{R}^+ \quad (a \circ b) \circ c = [a \circ b = d \in \mathbb{R}^+] = d \circ c = d^2 c^2 = [d = a^2 b^2] = = a^4 b^4 c^2;$$

$$\forall a, b, c \in \mathbb{R}^+ \quad a \circ (b \circ c) = [b \circ c = h \in \mathbb{R}^+] = a \circ h = a^2 h^2 = [h = b^2 c^2] = = a^2 b^4 c^4.$$

Не трудно заметить, что для произвольных $a, b, c \in \mathbb{R}^+ \quad (a \circ b) \circ c \neq a \circ (b \circ c)$. Свойством ассоциативности заданная бинарная алгебраическая операция « $\circ$ » не обладает.

Следовательно, указанное множество с введенной операцией « $\circ$ » не является группой.

В) Элементы указанного множества G находятся по формуле $a^n, n \in \mathbb{Z}$. Проверим, является ли введенная на G операция умножения бинарной алгебраической:

$$\forall n, m \in \mathbb{Z} \quad a^n \cdot a^m = a^{n+m} \in G, \text{ так как } \forall n, m \in \mathbb{Z} \quad n + m \in \mathbb{Z}.$$

Действительно, заданная операция на множестве G является бинарной алгебраической.

Ассоциативность операции умножения очевидна:

$$\forall n, m, k \in \mathbb{Z} \quad (a^n \cdot a^m) \cdot a^k = a^{(n+m)+k} = a^{n+m+k} = a^n \cdot (a^m \cdot a^k).$$

В качестве нейтрального элемента множества G выберем $a^0 = 1$. Действительно, для любого элемента множества $a^n \in G$ имеет место равенство $a^n \cdot a^0 = a^0 \cdot a^n = a^n$.

Так как $\forall n \in \mathbb{Z} \quad (-n) \in \mathbb{Z}$, то для любого элемента a^n во множестве G найдется и обратный к нему $(a^n)^{-1} = a^{-n} \in G$, в произведении с которым a^n дает нейтральный элемент: $a^n \cdot a^{-n} = a^{-n} \cdot a^n = a^0$.

Таким образом, выполнены все требования групповой операции, и заданное множество относительно умножения является группой.

Г) В отличие от пункта «А» для элементов множества многочленов степени не выше n с действительными коэффициентами (включая нуль) нет требования, чтобы коэффициент при степени n (или какой-либо еще) был отличен от нуля. При сложении двух многочленов степени не выше n всегда получим многочлен также степени не выше n , следовательно, на этом множестве операция сложения является бинарной алгебраической. По свойствам суммы многочленов она также является ассоциативной. Нейтральным элементом является многочлен $h(x) = 0$ (многочлен нулевой степени). Тогда для каждого многочлена степени не выше n найдется противоположный ему:

для любого $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0, a_i \in \mathbb{R}, i = 0, 1, \dots, n$ существует многочлен $g(x) = (-a_n) x^n + (-a_{n-1}) x^{n-1} + \dots + (-a_1) x + (-a_0)$, такой, что $f(x) + g(x) = 0 \quad \forall x \in \mathbb{R}$.

Следовательно, множество действительных многочленов степени не выше n (включая нуль) от неизвестного x относительно операции сложения является группой. ▲

Задание 2а. Вычислить коммутатор $h = g^{-1} f^{-1} g f$ для данных подстановок f и g :

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 2 & 5 & 7 & 8 & 9 & 1 & 3 & 6 \end{pmatrix} \text{ и } g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 4 & 3 & 7 & 6 & 9 & 1 & 8 & 5 \end{pmatrix}.$$

Решение

Предварительно вычислим подстановки, обратные к f и g . Если подстановка f переводит 1 в 4, то обратная к ней f^{-1} — 4 в 1, и так для всех элементов:

$$\begin{array}{cccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ f^{-1} & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow \\ 4 & 2 & 5 & 7 & 8 & 9 & 1 & 3 & 6 \end{array}$$

Так как аргументы, на которые действует f^{-1} , должны быть в первой строке, то для записи f^{-1} надо первую и вторую строки в записи f поменять местами, а затем упорядочить столбцы по возрастанию:

$$f^{-1} = \begin{pmatrix} 4 & 2 & 5 & 7 & 8 & 9 & 1 & 3 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 2 & 8 & 1 & 3 & 9 & 4 & 5 & 6 \end{pmatrix}.$$

Аналогичным образом получим g^{-1} – обратную к g :

$$g^{-1} = \begin{pmatrix} 2 & 4 & 3 & 7 & 6 & 9 & 1 & 8 & 5 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 1 & 3 & 2 & 9 & 5 & 4 & 8 & 6 \end{pmatrix}.$$

Приступим к вычислению коммутатора $h = g^{-1} f^{-1} g f$. Действия подстановок проводятся в порядке справа налево, на первом шаге действует самая правая подстановка f . Например:

$$\begin{aligned} (g^{-1} f^{-1} g f)(1) &= (g^{-1} f^{-1} g)(f(1)) = (g^{-1} f^{-1} g)(4) = (g^{-1} f^{-1})(g(4)) = \\ &= (g^{-1} f^{-1})(7) = g^{-1}(f^{-1}(7)) = g^{-1}(4) = 2. \end{aligned}$$

Проведем вычисления для всех элементов. Слева от стрелок указываем, какую подстановку применяем:

$$\begin{array}{cccccccccc} & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ f & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ & 4 & 2 & 5 & 7 & 8 & 9 & 1 & 3 & 6 \\ g & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ & 7 & 4 & 6 & 1 & 8 & 5 & 2 & 3 & 9 \\ f^{-1} & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ & 4 & 1 & 9 & 7 & 5 & 3 & 2 & 8 & 6 \\ g^{-1} & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ & 2 & 7 & 6 & 4 & 9 & 3 & 1 & 8 & 5 \end{array}$$

В конечном итоге имеем (выписываем первую строку и последнюю из всех преобразований):

$$g^{-1} f^{-1} g f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 7 & 6 & 4 & 9 & 3 & 1 & 8 & 5 \end{pmatrix}. \blacktriangle$$

Задание 26. Разложить в произведение циклов и транспозиций подстановку $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 2 & 5 & 7 & 8 & 9 & 1 & 3 & 6 \end{pmatrix}$. Определить ее четность.

Решение

Данная подстановка переводит 1 в 4, 4 в 7, а 7 – опять в 1. Таким образом, $f(1) = 4$, $f(4) = f(f(1)) = f^2(1) = 7$, $f(7) = f(f(4)) = f^3(1) = 1$, т. е., действуя на элемент 1 подстановкой f несколько раз, проходим цикл $1 \xrightarrow{f} 4 \xrightarrow{f} 7 \xrightarrow{f} 1$

$$\begin{pmatrix} 1 & f(1) & f^2(1) \\ f(1) & f^2(1) & 1 \end{pmatrix} = \begin{pmatrix} 1 & 4 & 7 \\ 4 & 7 & 1 \end{pmatrix}.$$

Подстановка, которая действует на элементы 1, 4, 7 описанным выше образом, а на все остальные – тождественно, согласно определению 2.12, называется циклом длиной 3 и обозначается (147). Также говорят, что элементы 1, 4, 7 являются Γ_f -эквивалентными.

Далее, видим, что подстановка f переводит 3 в 5, 5 в 8, а 8 опять в 3. Аналогично предыдущему случаю записываем цикл (358) – цикл длиной 3. Подстановка f также содержит цикл (69) – такой цикл длиной 2 называется *транспозицией*. Элемент 2 также образует цикл из одного элемента, совпадающий с тождественной подстановкой, при разложении ее не указывают. Таким образом, разложение в произведение циклов и транспозиций подстановки f имеет вид $f = (147)(358)(69)$. Циклы в разложении не пересекаются, поэтому порядок записи не важен.

Разложим цикл (147) в произведение транспозиций. Для этого запишем цикл в более развернутом виде

$$\begin{pmatrix} 1 & 4 & 7 \\ 4 & 7 & 1 \end{pmatrix}$$

и за несколько шагов от первой строки перейдем к последней, помня, что на каждом шаге можно совершать только одну транспозицию, т. е. менять местами одну пару элементов:

$$\begin{array}{ccc} 1 & 4 & 7 \\ (14) & \downarrow & \downarrow & \downarrow \\ & 4 & 1 & 7 \\ (17) & \downarrow & \downarrow & \downarrow \\ & 4 & 7 & 1 \end{array}$$

Слева от стрелок указаны применяемые транспозиции, выписывая которые снизу вверх, получим искомое разложение цикла: $(147) = (17)(14)$. Обратим внимание, что транспозиции пересекаются (обе имеют элемент 1), поэтому важен их порядок записи: правее всех должна быть записана транспозиция, действующая первой. Отметим также, что предложенное здесь разложение не единственно, например можно представить $(147) = (14)(47)$.

Аналогичным образом разложим в произведение транспозиций цикл (358): $(358) = (38)(35)$.

Разложение в произведение транспозиций подстановки f имеет вид:
 $f = (147)(358)(69) = (17)(14)(38)(35)(69)$.

Это разложение включает пять транспозиций – нечетное число, значит, и подстановка f является нечетной. ▲

Задание 2в. Вычислить произведение циклов и транспозиций $(6235)(274)(13)(8295)$.

Решение

Найдем результат композиции циклов и транспозиций аналогично пункту а, первым применяя цикл, записанный справа (он переводит 8 в 2, 2 в 9, 9 в 5, и 5 в 8, на все остальные элементы действует тождественно):

	1	2	3	4	5	6	7	8	9
(8295)	↓	↓	↓	↓	↓	↓	↓	↓	↓
	1	9	3	4	8	6	7	2	5
(13)	↓	↓	↓	↓	↓	↓	↓	↓	↓
	3	9	1	4	8	6	7	2	5
(274)	↓	↓	↓	↓	↓	↓	↓	↓	↓
	3	9	1	2	8	6	4	7	5
(6235)	↓	↓	↓	↓	↓	↓	↓	↓	↓
	5	9	1	3	8	2	4	7	6

Итог:

$$(6235)(274)(13)(8295) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 9 & 1 & 3 & 8 & 2 & 4 & 7 & 6 \end{pmatrix}.$$

Заметим, для того чтобы узнать, как заданное произведение циклов и транспозиций действует только на один элемент, нет необходимости выписывать все преобразования. Достаточно лишь «отслеживать» преобразования этого элемента, читая композицию справа налево. Например, элемент 8 самым правым циклом переводится в 2. 2 входит как аргумент в третий справа цикл, который переводит его в 7. Далее 7 нигде не встречается. Таким образом, композиция циклов и транспозиций переводит 8 в 7. ▲

Задание 3. Выписать циклическую группу, порожденную подстановкой f . Указать ее порядок. Найти f^{1000} .

Решение

Циклическая группа, порожденная некоторым элементом, состоит из всевозможных целых степеней этого элемента. Вычислим степени подстановки f , т. е. будем несколько раз действовать этой подстановкой:

	1	2	3	4	5	6	7	8	9
f	↓	↓	↓	↓	↓	↓	↓	↓	↓
	4	2	5	7	8	9	1	3	6
f^2	↓	↓	↓	↓	↓	↓	↓	↓	↓
	7	2	8	1	3	6	4	5	9
f^3	↓	↓	↓	↓	↓	↓	↓	↓	↓
	1	2	3	4	5	9	7	8	6
f^4	↓	↓	↓	↓	↓	↓	↓	↓	↓
	4	2	5	7	8	6	1	3	9
f^5	↓	↓	↓	↓	↓	↓	↓	↓	↓
	7	2	8	1	3	9	4	5	6
f^6	↓	↓	↓	↓	↓	↓	↓	↓	↓
	1	2	3	4	5	6	7	8	9

После действия f^6 получили тождественную подстановку e , дальнейшие степени новых результатов не дадут, их не вычисляем. Таким образом, $f^6 = e$, и по определению, порядок подстановки f равен 6, а циклическая группа $\langle f \rangle$ включает шесть элементов. Выпишем эти подстановки:

$$\begin{aligned}
 f &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 2 & 5 & 7 & 8 & 9 & 1 & 3 & 6 \end{pmatrix}; & f^2 &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 2 & 8 & 1 & 3 & 6 & 4 & 5 & 9 \end{pmatrix}; \\
 f^3 &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 2 & 3 & 4 & 5 & 9 & 7 & 8 & 6 \end{pmatrix}; & f^4 &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 2 & 5 & 7 & 8 & 6 & 1 & 3 & 9 \end{pmatrix}; \\
 f^5 &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 2 & 8 & 1 & 3 & 9 & 4 & 5 & 6 \end{pmatrix}; & f^6 &= e.
 \end{aligned}$$

В форме записи последовательного действия различных степеней подстановки f видно, что при повторном действии подстановки Γ_f -эквивалентные элементы движутся по своим циклам, иначе говоря, f -орбитам (для примера циклы (147) и (69) выделены пунктиром). Заметим, что для того чтобы получить тождественную подстановку, каждый элемент должен один или несколько раз пройти полностью свой цикл, поэтому порядок подстановки f равен НОК длин всех входящих в него циклов: $\text{НОК}(2, 3) = 6$.

Вычислим f^{1000} . Так как $f^6 = e$, то представим $1000 = 6 \cdot 166 + 4$, тогда

$$f^{1000} = f^{6 \cdot 166 + 4} = (f^6)^{166} \cdot f^4 = e^{166} \cdot f^4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 2 & 5 & 7 & 8 & 6 & 1 & 3 & 9 \end{pmatrix}. \blacktriangle$$

Задание 4. Рассмотрим аддитивную группу $V_5 = M_{1 \times 5}(\mathbb{Z}/2\mathbb{Z})$, элементами которой являются всевозможные строки-матрицы с пятью координатами из

кольца $\mathbb{Z}/2\mathbb{Z}$, а групповой операцией – покомпонатное сложение по модулю два. (Далее при записи классов из кольца $\mathbb{Z}/2\mathbb{Z}$ знак черты сверху будем опускать.)

1. Сколько в этой группе элементов?

2. Пусть H_1 и H_2 – следующие подмножества элементов группы V_5 :

$$H_1 = \left\{ \underbrace{(0 \ 0 \ 0 \ 0 \ 0)}_{\bar{0}}, \underbrace{(0 \ 1 \ 1 \ 0 \ 0)}_{e_1} \right\},$$

$$H_2 = \left\{ \underbrace{(0 \ 0 \ 0 \ 0 \ 0)}_{\bar{0}}, \underbrace{(0 \ 1 \ 1 \ 0 \ 0)}_{e_1}, \underbrace{(1 \ 1 \ 0 \ 1 \ 0)}_{e_2} \right\}.$$

Являются ли H_1 и H_2 подгруппами группы V_5 ? В случае положительного ответа выяснить, циклическая ли это подгруппа, в случае отрицательного – достроить до подгруппы.

Решение

1. Поскольку каждая из пяти координат может независимо от других принимать лишь два значения, то порядок группы V_5 (число ее элементов) равен $2^5 = 32$.

2. Рассмотрим подмножество из двух элементов H_1 и проверим критерий подгруппы (теорема 2.1). Очевидно, что нейтральным элементом аддитивной группы V_5 является $\bar{0} = (0 \ 0 \ 0 \ 0 \ 0)$. Поскольку при сложении по модулю два $0 + 0 = 0 \pmod{2}$ и $1 + 1 = 0 \pmod{2}$, то как элемент $\bar{0}$, так и элемент e_1 является противоположным к самому себе, так как в сумме с собой дают нейтральный элемент: $\bar{0} + \bar{0} = \bar{0}$, $e_1 + e_1 = \bar{0}$. Следовательно, выполнено первое условие критерия подгруппы: H_1 к любому своему элементу включает противоположный. Кроме того, $e_1 + \bar{0} = e_1 \in H_1$, и выполняется второе условие критерия подгруппы: для любых двух элементов подгруппы результат групповой операции принадлежит подгруппе. Следовательно, H_1 – подгруппа группы V_5 .

Все элементы подгруппы можно представить в виде степеней элемента e_1 (под степенью n пониманием результат выполнения групповой операции с одним и тем же элементом, в данном случае – сложение e_1 с самим собой):

$$H_1 = \{e_1, e_1^2\} = [e_1^2 = e_1 + e_1 = \bar{0}] = \{e_1, \bar{0}\}.$$

Тогда подгруппа является циклической H_1 , генератором подгруппы является элемент e_1 , обозначают $H_1 = \langle e_1 \rangle$. Так как $e_1^2 = \bar{0}$, порядок элемента e_1 равен двум.

Подмножество H_2 также состоит из элементов, противоположных самим себе. Однако второе условие критерия подгруппы не выполняется:

$$e_1 + e_2 = (0 \ 1 \ 1 \ 0 \ 0) + (1 \ 1 \ 0 \ 1 \ 0) = (1 \ 0 \ 1 \ 1 \ 0) \notin H_2.$$

Следовательно, H_2 подгруппой не является.

Построим подмножество H_3 , дополнив H_2 элементом $e_3 = e_1 + e_2$. Он является противоположным самому себе, и таким образом для H_3 выполняется первое условие критерия подгруппы. Кроме того, справедливы равенства:

$$e_1 + e_2 = e_3 \in H_3,$$

$$e_1 + e_3 = e_1 + (e_1 + e_2) = (e_1 + e_1) + e_2 = e_2 \in H_3,$$

$$e_2 + e_3 = e_2 + (e_1 + e_2) = e_2 + (e_2 + e_1) = (e_2 + e_2) + e_1 = e_1 \in H_3,$$

$$e_i + \bar{0} = e_i \in H_3, i = 1, 2, 3.$$

Таким образом, для любых двух элементов H_3 результат групповой операции принадлежит H_3 – второе условие критерия подгруппы. Получили, что H_3 – подгруппа группы V_5 .

Каждый элемент этой подгруппы, отличный от единицы, имеет порядок два, а следовательно, не может являться генератором подгруппы. Поэтому H_3 является нециклической.

H_3 представляет собой частный случай **четверной группы Клейна**. ▲

Задание 5. Выпишите таблицу смежных классов группы V_5 по подгруппе

$$H_3 = \left\{ \underbrace{(0 \ 0 \ 0 \ 0 \ 0)}_{\bar{0}}, \underbrace{(0 \ 1 \ 1 \ 0 \ 0)}_{e_1}, \underbrace{(1 \ 1 \ 0 \ 1 \ 0)}_{e_2}, \underbrace{(1 \ 0 \ 1 \ 1 \ 0)}_{e_3} \right\}.$$

Решение

Для построения смежного класса по подгруппе aH_3 выбираем любой элемент группы $a \in V_5$ и находим результаты групповой операции с каждым из элементов подгруппы H_3 (табл. 3). Вначале, как правило, выбирают нейтральный элемент группы $\bar{0}$, таким образом, среди смежных классов один всегда совпадает с самой подгруппой:

$$\bar{0} + H_3 = H_3.$$

Затем для построения следующего смежного класса выбираем еще один элемент группы V_5 , не вошедший ни в один ранее построенный смежный класс, иначе нового класса не получим. Смежные классы по подгруппам в V_5 используются для декодирования в теории линейных кодов, и с точки зрения прикладной значимости для построения нового класса в группе V_5 выбирают матрицу-строку a с минимально возможным числом единиц, так называемый **лидер класса** (см. [38]). Исходя из этих соображений, для второго смежного класса возьмем в качестве лидера элемент $(1 \ 0 \ 0 \ 0 \ 0)$, для третьего – $(0 \ 1 \ 0 \ 0 \ 0)$ и т. д. Заполним таблицу смежных классов.

Смежные классы по подгруппе H_3

№ п/п	Класс $a + H_3$	$a + \bar{0}$	$a + e_1$	$a + e_2$	$a + e_3$
1	$\bar{0} + H_3 = H_3$	(00000)	(01100)	(11010)	(10110)
2	$(10000) + H_3$	(10000)	(11100)	(01010)	(00110)
3	$(01000) + H_3$	(01000)	(00100)	(10010)	(11110)
4	$(00010) + H_3$	(00010)	(01110)	(11000)	(10100)
5	$(00001) + H_3$	(00001)	(01101)	(11011)	(10111)
6	$(10001) + H_3$	(10001)	(11101)	(01011)	(00111)
7	$(00011) + H_3$	(00011)	(01111)	(11001)	(10101)
8	$(00101) + H_3$	(00101)	(01001)	(11111)	(10011)

Обратите внимание, что при построении четвертого смежного класса в качестве лидера не могли выбрать $(0 \ 0 \ 1 \ 0 \ 0)$, так как этот элемент уже вошел в третий класс. Указанные выше два условия выбора лидера – наименьшее число единиц в записи и невключение в предыдущие классы – оставляют свободу действий, и столбец элементов a может быть сформирован и иным образом. Тем не менее при любом способе заполнения этого столбца количество смежных классов получится всегда одним и тем же, так как определено следствием из теоремы Лагранжа и равно частному от деления порядка группы на порядок подгруппы: $32 : 4 = 8$. Кроме того, выбор лидера при разбиении группы на смежные классы по фиксированной подгруппе не влияет на состав получившихся подмножеств, т. е. разбиение на смежные классы единственно. ▲

Задание 6. Выпишите все элементы мультипликативной группы кольца: а) $\mathbb{Z}/23\mathbb{Z}$; б) $\mathbb{Z}/28\mathbb{Z}$. Сравнить количество этих элементов с $\varphi(23)$ и $\varphi(28)$ соответственно. Проверить, является ли эта группа относительно умножения циклической? Если ответ положительный, указать один из генераторов группы.

Решение

По определению групповая операция мультипликативной группы – умножение. Тогда мультипликативная группа кольца вычетов $\mathbb{Z}/m\mathbb{Z}$, обозначаемая $(\mathbb{Z}/m\mathbb{Z})^*$, состоит из всех обратимых классов. Действительно, выполняются все три аксиомы группы. Во-первых, операция умножения обратимых классов обладает свойством ассоциативности. Во-вторых, среди обратимых классов в любом кольце вычетов есть класс $\bar{1}$, такой что для любого $\bar{a} \in \mathbb{Z}/m\mathbb{Z}$ имеет место $\bar{1} \cdot \bar{a} = \bar{a} \cdot \bar{1} = \bar{a}$. Отсюда следует, что класс $\bar{1}$ – нейтральный относительно групповой операции элемент. В-третьих, по определению обратимого класса он имеет обратный относительно умножения класс, который также является обратимым.

Количество элементов в группе $(\mathbb{Z}/m\mathbb{Z})^*$ согласно критерию обратимого класса совпадает с числом классов, взаимно простых с модулем, которое равно $\varphi(m)$.

а) Мультипликативная группа кольца $\mathbb{Z}/23\mathbb{Z}$ состоит из всех ненулевых классов в силу простого модуля 23: $G = \mathbb{Z}/23\mathbb{Z}^* = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}, \bar{8}, \bar{9}, \bar{10}, \bar{11}, \bar{12}, \bar{13}, \bar{14}, \bar{15}, \bar{16}, \bar{17}, \bar{18}, \bar{19}, \bar{20}, \bar{21}, \bar{22}\}$.

Количество элементов группы $\mathbb{Z}/23\mathbb{Z}^*$, т. е. ее порядок $|G|$, равно 22.

$\varphi(23) = 23 - 1 = 22$, что совпадает с порядком $\mathbb{Z}/23\mathbb{Z}^*$.

Так как модуль $\mathbb{Z}/23\mathbb{Z}$ – простое число, то в силу теоремы 2.4 группа $\mathbb{Z}/23\mathbb{Z}^*$ является циклической. По свойствам циклической конечной группы порядка g она имеет $\varphi(g)$ генераторов группы, определить которые можно непосредственным перебором. В группе $\mathbb{Z}/23\mathbb{Z}^*$ таким образом имеется $\varphi(22) = 10$ генераторов группы. Обращаем внимание, что не всякий элемент циклической группы может быть ее генератором! Элемент может быть генератором группы, только если его порядок совпадет с порядком группы. Начнем проверку с элемента $\bar{2}$ и выпишем циклическую подгруппу, состоящую из степеней этого элемента (вычисления останавливаем, как только $2^k = 1$):

$$\langle \bar{2} \rangle = \{ \bar{2}, \bar{2}^2 = \bar{4}, \bar{2}^3 = \bar{8}, \bar{2}^4 = \bar{16}, \bar{2}^5 = \bar{32} = \bar{9}, \bar{2}^6 = \bar{2} \cdot \bar{9} = \bar{18}, \\ \bar{2}^7 = \bar{2} \cdot \bar{18} = \bar{36} = \bar{13}, \bar{2}^8 = \bar{2} \cdot \bar{13} = \bar{26} = \bar{3}, \bar{2}^9 = \bar{2} \cdot \bar{3} = \bar{6}, \bar{2}^{10} = \bar{2} \cdot \bar{6} = \bar{12}, \bar{2}^{11} = \bar{2} \cdot \bar{12} = \bar{24} = \bar{1} \}.$$

Так как $\bar{2}^{11} = \bar{1}$, то порядок элемента $\bar{2}$ равен 11, и этот элемент не является генератором группы $\mathbb{Z}/23\mathbb{Z}^*$: как видно из вычислений, циклическая подгруппа $\langle \bar{2} \rangle$ включает в себя не все элементы группы $\mathbb{Z}/23\mathbb{Z}^*$.

Для того чтобы не проверять по порядку все оставшиеся элементы группы $\mathbb{Z}/23\mathbb{Z}^*$ (их 20), воспользуемся следствиями из теоремы Лагранжа и заранее исключим некоторые элементы из рассмотрения. Заметим, что циклическая подгруппа $\langle \bar{2} \rangle$ сама является конечной группой порядка 11. По следствию из теоремы Лагранжа порядок любого элемента конечной группы является делителем порядка группы. Из этого следует, что элементы $\bar{3}, \bar{4}, \bar{6}, \bar{8}, \bar{9}, \bar{12}, \bar{13}, \bar{16}, \bar{18}$ могут иметь лишь порядок 11, а значит, не могут быть генераторами группы $\mathbb{Z}/23\mathbb{Z}^*$. Поэтому следующий элемент, который целесообразно проверить на генератор группы, – это элемент $\bar{5}$:

$$\langle \bar{5} \rangle = \{ \bar{5}, \bar{5}^2 = \bar{25} = \bar{2}, \bar{5}^3 = \bar{5} \cdot \bar{2} = \bar{10}, \bar{5}^4 = \bar{5} \cdot \bar{10} = \bar{50} = \bar{4}, \bar{5}^5 = \bar{5} \cdot \bar{4} = \bar{20}, \\ \bar{5}^6 = \bar{5} \cdot \bar{20} = \bar{100} = \bar{8}, \bar{5}^7 = \bar{5} \cdot \bar{8} = \bar{40} = \bar{17}, \bar{5}^8 = \bar{5} \cdot \bar{17} = \bar{85} = \bar{16}, \bar{5}^9 = \bar{5} \cdot \bar{16} = \bar{80} = \bar{11}, \\ \bar{5}^{10} = \bar{5} \cdot \bar{11} = \bar{55} = \bar{9}, \bar{5}^{11} = \bar{5} \cdot \bar{9} = \bar{45} = \bar{22}, \bar{5}^{12} = \bar{5} \cdot \bar{22} = \bar{110} = \bar{18}, \\ \bar{5}^{13} = \bar{5} \cdot \bar{18} = \bar{90} = \bar{21}, \bar{5}^{14} = \bar{5} \cdot \bar{21} = \bar{105} = \bar{13}, \bar{5}^{15} = \bar{5} \cdot \bar{13} = \bar{65} = \bar{19},$$

$$\begin{aligned} \bar{5}^{16} &= \bar{5} \cdot \bar{19} = \overline{95} = \bar{3}, \bar{5}^{17} = \bar{5} \cdot \bar{3} = \overline{15}, \bar{5}^{18} = \bar{5} \cdot \overline{15} = \overline{75} = \bar{6}, \bar{5}^{19} = \bar{5} \cdot \bar{6} = \overline{30} = \bar{7}, \\ \bar{5}^{20} &= \bar{5} \cdot \bar{7} = \overline{35} = \overline{12}, \bar{5}^{21} = \bar{5} \cdot \overline{12} = \overline{60} = \overline{14}, \bar{5}^{22} = \bar{5} \cdot \overline{14} = \overline{70} = \bar{1} \}. \end{aligned}$$

Как видим, порядок элемента $\bar{5}$ равен 22, все элементы $\mathbb{Z}/23\mathbb{Z}^*$ содержатся в $\langle \bar{5} \rangle$, следовательно, $\mathbb{Z}/23\mathbb{Z}^* = \langle \bar{5} \rangle$ и класс $\bar{5}$ является генератором группы.

б) Мультипликативная группа кольца $\mathbb{Z}/28\mathbb{Z}$ состоит из всех обратимых классов (взаимно простых с модулем):

$$G = \mathbb{Z}/28\mathbb{Z}^* = \{\bar{1}, \bar{3}, \bar{5}, \bar{9}, \bar{11}, \bar{13}, \bar{15}, \bar{17}, \bar{19}, \bar{23}, \bar{25}, \bar{27}\}.$$

Количество элементов группы $\mathbb{Z}/28\mathbb{Z}^*$, т. е. ее порядок $|G|$ равен 12.

$\varphi(28) = 12$, что совпадает с порядком $\mathbb{Z}/28\mathbb{Z}^*$.

В данном случае модуль 28 не является простым числом, и более того, не удовлетворяет ни одному из условий критерия цикличности мультипликативных групп $\mathbb{Z}/m\mathbb{Z}^*$ (теорема 2.4). Следовательно, группа $\mathbb{Z}/28\mathbb{Z}^*$ циклической не является. ▲

Задание 7. Выписать смежные классы $\mathbb{Z}/28\mathbb{Z}^* / \langle \bar{9} \rangle$.

Решение

Выпишем циклическую подгруппу, порожденную классом 9:

$$\langle \bar{9} \rangle = \{ \bar{9}, \bar{9}^2 = \overline{81} = \overline{25}, \bar{9}^3 = \bar{9} \cdot \overline{25} = \overline{225} = \bar{1} \}.$$

Ее порядок $|H| = 3$. Индекс подгруппы для конечных групп, равный числу смежных классов по подгруппе, согласно следствию из теоремы Лагранжа, считается следующим образом:

$$|G : H| = |G| / |H| = 12 / 3 = 4.$$

Аналогично заданию 5, для построения смежного класса по подгруппе aH выбираем любой элемент группы $a \in G$ и находим результаты групповой операции с каждым из элементов подгруппы H . Вначале выберем нейтральный элемент группы $e = 1$, получим класс, совпадающий с самой подгруппой ($\forall h \in H e \cdot h = h$): $\bar{1}H = \{ \bar{9}, \overline{25}, \bar{1} \}$. Для построения следующего смежного класса необходимо выбрать любой элемент группы, не включенный в ранее построенные классы. Построим смежный класс $\bar{3}H$:

$$\bar{3}H = \{ \bar{9} \cdot \bar{3} = \overline{27}, \overline{25} \cdot \bar{3} = \overline{75} = \overline{19}, \bar{1} \cdot \bar{3} = \bar{3} \} = \{ \overline{27}, \overline{19}, \bar{3} \}.$$

Далее, смежный класс $\bar{5}H$:

$$\bar{5}H = \{ \bar{9} \cdot \bar{5} = \overline{45} = \overline{17}, \overline{25} \cdot \bar{5} = \overline{125} = \overline{13}, \bar{1} \cdot \bar{5} = \bar{5} \} = \{ \overline{17}, \overline{13}, \bar{5} \}.$$

Смежный класс $\bar{11}H$:

$$\bar{11}H = \{ \bar{9} \cdot \bar{11} = \overline{99} = \overline{15}, \overline{25} \cdot \bar{11} = \overline{275} = \overline{23}, \bar{1} \cdot \bar{11} = \bar{11} \} = \{ \overline{15}, \overline{23}, \bar{11} \}.$$

Больше не осталось ни одного элемента группы, не попавшего ни в один из смежных классов – получено 4 класса, как и требовалось. Обращаем внимание, что смежные классы не пересекаются. ▲

ТЕСТ ДЛЯ САМОПРОВЕРКИ ПО ТЕМЕ «ОСНОВЫ ТЕОРИИ ГРУПП»

Вопрос 1. Выбрать множества, являющиеся группами относительно указанных операций:

а) $(P_n[x], +)$ – множество многочленов степени не выше n с действительными коэффициентами;

б) $(\mathbb{C} \setminus \{0\}, \times)$ – множество комплексных чисел, отличных от нуля;

в) $(V_3, +)$ – множество трехмерных векторов с действительными координатами;

г) $(\mathbb{Z}/m\mathbb{Z}, \times)$ – множество классов вычетов по модулю m ;

д) $(\mathbb{Q}, \times)$ – множество рациональных чисел.

А) а, в, д;

В) в, г, д;

С) б, в, г;

Д) а, б, в;

Е) б, г, д.

Вопрос 2. Вычислить произведение подстановок $p^{-1} \cdot s$, если

$$p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 5 & 4 & 6 & 1 \end{pmatrix} \text{ и } s = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix}.$$

А) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 6 & 4 & 5 & 3 & 2 \end{pmatrix};$

В) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 6 & 5 & 3 & 4 & 2 \end{pmatrix};$

С) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 4 & 2 & 1 & 6 \end{pmatrix};$

Д) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 5 & 6 & 1 & 2 \end{pmatrix};$

Е) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 2 & 3 & 1 & 6 \end{pmatrix}.$

Вопрос 3. Вычислить произведение циклов и транспозиций

$(32896)(16)(72)(8651)(37852)$. В ответе указать число, в которое переходит число 8.

А) 3;

В) 7;

С) 1;

Д) 2;

Е) 9.

Вопрос 4. Выписать циклическую группу $\langle C \rangle$, порожденную матрицей $C = \begin{pmatrix} 2 & 2 \\ 2 & 1 \end{pmatrix}$ с элементами из кольца $\mathbb{Z}/3\mathbb{Z}$. В ответе указать C^{103} .

A) $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix};$

B) $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix};$

C) $\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix};$

D) $\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix};$

E) $\begin{pmatrix} 2 & 2 \\ 2 & 1 \end{pmatrix}.$

Вопрос 5. Группа G с заданной на ней операцией умножения называется:

A) мультипликативной;

B) абелевой;

C) коммутативной;

D) аддитивной;

E) несобственной.

Вопрос 6. Выписать все элементы мультипликативной группы $\mathbb{Z}/18\mathbb{Z}^*$. В ответе указать их количество:

A) 12;

B) 9;

C) 18;

D) 2;

E) 6.

Вопрос 7. Пусть $G = \mathbb{Z}/15\mathbb{Z}^*$, $H = \langle \overline{11} \rangle$ – циклическая подгруппа группы G , порожденная элементом $\overline{11}$. Найти порядок H :

A) 4;

B) 3;

C) 8;

D) 2;

E) 5.

Вопрос 8. Выбрать группы, которые НЕ являются циклическими:

- A) $\mathbb{Z}/13\mathbb{Z}^*$;
- B) $\mathbb{Z}/4\mathbb{Z}^*$;
- C) $\mathbb{Z}/6\mathbb{Z}^*$;
- D) $\mathbb{Z}/12\mathbb{Z}^*$;
- E) $\mathbb{Z}/15\mathbb{Z}^*$.

Вопрос 9. Является ли группой множество всех положительных действительных чисел с операцией $m \circ n = m^n$?

Вопрос 10. Содержит ли группа $\mathbb{Z}/25\mathbb{Z}^*$ нециклическую подгруппу?

Вопрос 11*. Является ли нормальной подгруппа $\langle f \rangle$, порожденная подстановкой $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$ в группе S_4 ?

Ключ к тесту:

Номер вопроса	Ответ
1	D
2	C
3	A
4	D
5	A
6	E
7	D
8	C, D, E
9	Нет
10	Нет
11	Нет

ИНДИВИДУАЛЬНЫЕ ЗАДАНИЯ ДЛЯ ЛАБОРАТОРНОЙ РАБОТЫ № 2 «ОСНОВЫ ТЕОРИИ ГРУПП»

1. Выяснить, является ли группой указанное множество с заданной операцией.
2. Для заданных подстановок f и g выполнить следующие действия:
 - а) Вычислить коммутатор $h = g^{-1}f^{-1}gf$.
 - б) Разложить в произведение циклов и транспозиций подстановку f . Определить ее четность.
 - в) Вычислить произведение указанных циклов и транспозиций.
3. Выписать циклическую группу $\langle f \rangle$, порожденную подстановкой f из второго задания. Указать ее порядок. Найти f^{1000} .
4. Дополнить подмножество векторов $\bar{0}(00000)$, $\bar{a}$, $\bar{b}$ четвертым вектором так, чтобы они образовали подгруппу относительно сложения в группе V_5 всех векторов с координатами из $\mathbb{Z}/2\mathbb{Z}$. Ответ обосновать.
5. Выписать таблицу смежных классов группы V_5 по построенной подгруппе.
6. Выписать все элементы мультипликативной группы кольца: а) $\mathbb{Z}/k\mathbb{Z}$; б) $\mathbb{Z}/m\mathbb{Z}$. Сравнить количество этих элементов с $\varphi(k)$ и $\varphi(m)$ соответственно. Являются ли эти группы относительно умножения циклическими? Если ответ положительный, указать один из генераторов группы.
7. Выписать смежные классы мультипликативной группы указанного кольца по циклической подгруппе заданного элемента l : $(\mathbb{Z}/n\mathbb{Z})^*/\langle l \rangle$.

Вариант 1

1. Множество целых чисел с операцией вычитания.
2. а. $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 9 & 5 & 6 & 8 & 4 & 1 & 3 & 7 \end{pmatrix}; g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 1 & 8 & 6 & 9 & 7 & 3 & 2 & 5 \end{pmatrix};$
2. в. $(7 \ 1 \ 8 \ 5)(4 \ 6 \ 3)(8 \ 2)(9 \ 1 \ 3 \ 5)$.
4. $\bar{a}(10101)$, $\bar{b}(10011)$.
6. $k = 17$; $m = 32$.
7. $(\mathbb{Z}/32\mathbb{Z})^*/\langle 17 \rangle$.

Вариант 2

1. Множество всех положительных вещественных чисел с операцией деления.
2. а. $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 6 & 9 & 1 & 7 & 8 & 5 & 2 & 4 \end{pmatrix}; g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 1 & 8 & 6 & 9 & 7 & 3 & 2 & 5 \end{pmatrix};$

2. в. $(3 \ 1 \ 9 \ 5)(4 \ 2 \ 3)(8 \ 9)(7 \ 1 \ 6 \ 5)$.
 4. $\bar{a}(10110), \bar{b}(11001)$.
 6. $k = 19; m = 30$.
 7. $(\mathbb{Z}/19\mathbb{Z})^*/\langle 7 \rangle$.

Вариант 3

1. Множество целых чисел с операцией $m * n = mn + m$.
 2. а. $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 9 & 8 & 3 & 1 & 4 & 2 & 6 & 7 \end{pmatrix}; g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 1 & 8 & 6 & 9 & 7 & 3 & 2 & 5 \end{pmatrix};$
 2. в. $(4 \ 2 \ 6 \ 9)(5 \ 2 \ 7)(7 \ 9)(7 \ 3 \ 8 \ 1)$.
 4. $\bar{a}(10110), b(10101)$.
 6. $k = 13; m = 34$.
 7. $(\mathbb{Z}/34\mathbb{Z})^*/\langle 19 \rangle$.

Вариант 4

1. Множество целых чисел с операцией $m * n = m + 2n$.
 2. а. $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 6 & 2 & 8 & 1 & 3 & 4 & 7 & 5 \end{pmatrix}; g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 1 & 8 & 6 & 9 & 7 & 3 & 2 & 5 \end{pmatrix};$
 2. в. $(2 \ 4 \ 9 \ 5)(1 \ 3 \ 7)(5 \ 8)(7 \ 1 \ 3 \ 6)$.
 4. $\bar{a}(11000), b(10110)$.
 6. $k = 11; m = 27$.
 7. $(\mathbb{Z}/27\mathbb{Z})^*/\langle 17 \rangle$.

Вариант 5

1. Множество целых чисел с операцией умножения.
 2. а. $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 4 & 5 & 6 & 7 & 8 & 9 & 2 & 1 \end{pmatrix}; g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 1 & 8 & 6 & 9 & 7 & 3 & 2 & 5 \end{pmatrix};$
 2. в. $(9 \ 1 \ 3 \ 5)(6 \ 2 \ 8)(2 \ 9)(7 \ 1 \ 4 \ 8)$.
 4. $\bar{a}(11011), b(11100)$.
 6. $k = 18; m = 31$.
 7. $(\mathbb{Z}/31\mathbb{Z})^*/\langle 26 \rangle$.

Вариант 6

1. Множество вещественных чисел с операцией деления.
 2. а. $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 6 & 5 & 1 & 7 & 2 & 3 & 4 & 8 \end{pmatrix}; g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 1 & 8 & 6 & 9 & 7 & 3 & 2 & 5 \end{pmatrix};$

2. в. $(7 \ 3 \ 9 \ 5)(4 \ 1 \ 3)(8 \ 6)(9 \ 1 \ 2 \ 5)$.
 4. $\bar{a}(11011), b(10101)$.
 6. $k = 29; m = 16$.
 7. $(\mathbb{Z}/16\mathbb{Z})^* / \langle 7 \rangle$.

Вариант 7

1. Множество комплексных чисел с операцией $z_1 \otimes z_2 = \sqrt{z_1 z_2}$.
 2. а. $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 8 & 1 & 6 & 3 & 7 & 4 & 5 & 2 \end{pmatrix}; g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 1 & 8 & 6 & 9 & 7 & 3 & 2 & 5 \end{pmatrix}$;
 2. в. $(9 \ 1 \ 4 \ 5)(3 \ 2 \ 7)(3 \ 6)(7 \ 2 \ 6 \ 8)$.
 4. $\bar{a}(11001), b(10110)$.
 6. $k = 17; m = 26$.
 7. $(\mathbb{Z}/26\mathbb{Z})^* / \langle 7 \rangle$.

Вариант 8

1. Множество комплексных чисел с операцией деления.
 2. а. $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 8 & 7 & 5 & 9 & 3 & 6 & 1 & 2 \end{pmatrix}; g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 1 & 8 & 6 & 9 & 7 & 3 & 2 & 5 \end{pmatrix}$;
 2. в. $(4 \ 2 \ 9 \ 5)(7 \ 9 \ 3)(6 \ 1)(8 \ 6 \ 5 \ 1)$.
 4. $\bar{a}(11000), b(10110)$.
 6. $k = 7; m = 24$.
 7. $(\mathbb{Z} / 24\mathbb{Z})^* / \langle 17 \rangle$.

Вариант 9

1. Матрицы порядка n с целыми элементами относительно умножения.
 2. а. $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 6 & 5 & 1 & 7 & 2 & 8 & 4 & 3 \end{pmatrix}; g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 1 & 8 & 6 & 9 & 7 & 3 & 2 & 5 \end{pmatrix}$;
 2. в. $(9 \ 1 \ 3 \ 5)(4 \ 2 \ 3)(5 \ 7)(9 \ 1 \ 6 \ 8)$.
 4. $\bar{a}(11001), b(10110)$.
 6. $k = 11; m = 21$.
 7. $(\mathbb{Z}/21\mathbb{Z})^* / \langle 11 \rangle$.

Вариант 10

1. Матрицы порядка n с целыми элементами и определителем, равным единице, относительно умножения.

$$2. \text{ а. } f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 5 & 6 & 1 & 7 & 2 & 8 & 4 & 3 \end{pmatrix}; g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 1 & 8 & 6 & 9 & 7 & 3 & 2 & 5 \end{pmatrix};$$

$$2. \text{ в. } (8 \ 1 \ 9 \ 5)(1 \ 2 \ 3)(7 \ 9)(4 \ 1 \ 6 \ 5).$$

$$4. \bar{a}(10110), \bar{b}(01111).$$

$$6. k = 31; m = 20.$$

$$7. (\mathbb{Z}/20\mathbb{Z})^*/\langle 17 \rangle.$$

Вариант 11

1. Положительные действительные числа, если операция определяется задана выражением $a \circ b = a^b$.

$$2. \text{ а. } f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 5 & 6 & 7 & 1 & 2 & 8 & 4 & 3 \end{pmatrix}; g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 1 & 8 & 6 & 9 & 7 & 3 & 2 & 5 \end{pmatrix};$$

$$2. \text{ в. } (4 \ 1 \ 9 \ 5)(7 \ 2 \ 3)(2 \ 6)(3 \ 1 \ 6 \ 8).$$

$$4. \bar{a}(01001), \bar{b}(10110).$$

$$6. k = 14; m = 37.$$

$$7. (\mathbb{Z}/37\mathbb{Z})^*/\langle 3 \rangle.$$

Вариант 12

1. Многочлены степени n от неизвестной x с действительными коэффициентами относительно умножения.

$$2. \text{ а. } f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 6 & 5 & 1 & 7 & 4 & 8 & 2 & 3 \end{pmatrix}; g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 1 & 8 & 6 & 9 & 7 & 3 & 2 & 5 \end{pmatrix};$$

$$2. \text{ в. } (8 \ 1 \ 9 \ 5)(9 \ 2 \ 3)(6 \ 7)(7 \ 2 \ 4 \ 5).$$

$$4. \bar{a}(11001), \bar{b}(01111).$$

$$6. k = 17; m = 25.$$

$$7. (\mathbb{Z}/25\mathbb{Z})^*/\langle 7 \rangle.$$

Вариант 13

1. Все комплексные числа верхней полуплоскости относительно умножения.

$$2. \text{ а. } f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 6 & 2 & 1 & 7 & 5 & 8 & 4 & 3 \end{pmatrix}; g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 1 & 8 & 6 & 9 & 7 & 3 & 2 & 5 \end{pmatrix};$$

$$2. \text{ в. } (1 \ 6 \ 9 \ 5)(2 \ 4 \ 7)(3 \ 9)(6 \ 1 \ 7 \ 8).$$

$$4. \bar{a}(00110), b(01001).$$

$$6. k = 17; m = 27.$$

$$7. (\mathbb{Z}/27\mathbb{Z})^*/\langle 10 \rangle.$$

Вариант 14

1. Комплексные числа правой полуплоскости относительно умножения.

2. а. $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 6 & 5 & 1 & 7 & 2 & 4 & 8 & 3 \end{pmatrix}; g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 1 & 8 & 6 & 9 & 7 & 3 & 2 & 5 \end{pmatrix};$

2. в. $(2 \ 1 \ 7 \ 3)(4 \ 9 \ 3)(4 \ 7)(5 \ 2 \ 6 \ 9).$

4. $\bar{a}(11100), \bar{b}(00111).$

6. $k = 13; m = 22.$

7. $(\mathbb{Z}/22\mathbb{Z})^*/\langle 7 \rangle.$

Вариант 15

1. Комплексные числа нижней полуплоскости относительно умножения.

2. а. $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 6 & 5 & 1 & 7 & 2 & 4 & 8 & 3 \end{pmatrix}; g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 1 & 8 & 6 & 9 & 7 & 3 & 2 & 5 \end{pmatrix};$

2. в. $(8 \ 3 \ 9 \ 5)(4 \ 1 \ 3)(7 \ 9)(6 \ 1 \ 2 \ 5).$

4. $\bar{a}(00111), \bar{b}(01001).$

6. $k = 15; m = 29.$

7. $(\mathbb{Z}/29\mathbb{Z})^*/\langle 10 \rangle.$

МОДУЛЬ № 3. ИСТОРИЧЕСКИЕ И СОВРЕМЕННЫЕ КРИПТОСИСТЕМЫ

ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ ПО ТЕМЕ «ИСТОРИЧЕСКИЕ И СОВРЕМЕННЫЕ КРИПТОСИСТЕМЫ»¹

§ 1. Историческая криптография

Развитие человеческой цивилизации привело сначала к появлению письменности, а впоследствии к необходимости защиты информации от несанкционированного доступа. Возникли разного рода системы защиты информации, содержащие способы ее шифрования и дешифрования.

Искусство защиты информации путем ее преобразования в нечитаемый для постороннего формат имеет долгую и богатую историю, тесно переплетенную с развитием цивилизаций и технологий. Рассмотрим наиболее популярные исторические криптографические системы.

1. Шифр Цезаря

Шифр назван в честь римского полководца Гая Юлия Цезаря (12 июля 100 г. до н. э. – 15 марта 44 г. до н. э.), использовавшего его для секретной переписки со своими легатами. Это вид шифра-подстановки, в котором каждый символ в открытом тексте заменяется символом, отстоящим от исходного левее или правее по алфавиту на некоторое постоянное число позиций (замена на фиксированное число позиций по циклу). Например, в шифре со сдвигом вправо на 3, буква А (первая) заменяется на букву Г (четвертая), Б (вторая) на Д (пятая) и т. д.

Иными словами, замена производится в соответствии с таблицей, которая в русском варианте имеет следующий вид:

А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О
Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С

П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В

Тогда, чтобы прочесть зашифрованное сообщение нужно составить обратное соответствие, т. е. для буквы во второй строке нужно найти записанную над ней букву в первой.

Пример 3.1. Знаменитая фраза Цезаря на русском языке «ПРИШЕЛ, УВИДЕЛ, ПОБЕДИЛ», исторически известная на латинском языке как «VENI, VEDI, VICI», зашифрована с помощью вышеприведенной таблицы следующим образом:

ТУЛЫИО ЦЕЛЖЗО ТСДЗЖЛО

и легко может быть дешифрована с помощью обратной подстановки.

¹ При подготовке данного раздела использовались следующие источники: [16, 21, 23, 28, 37].

Заметим, что шифр Цезаря входит в класс шифров, называемых *«подстановка»* или *«простая замена»*. Это такие шифры, в котором каждая буква алфавита заменяется буквой, цифрой, символом или какой-нибудь их комбинацией.

Поскольку шифр Цезаря сохраняет статистические свойства исходного текста, то частотность букв становится известной и атакующий дешифратор может легко определить, какой ключ был использован для шифрования. Свойство шифра Цезаря сохранять буквенные зависимости в исходном тексте является его главным недостатком.

2. Криптосистема Тритемиуса

Данная система шифрования впервые была опубликована в 1518 г. в трактате «Полиграфия», принадлежащем перу религиозного деятеля аббата Иоганна Тритемия (1 февраля 1462 – 13 декабря 1516). Это была первая печатная работа по криптологии. Система Тритемиуса представляет собой дальнейшее усовершенствование системы шифрования Цезаря и базируется на идее применения *девизов*. Смысл шифрования состоит в следующем: в следующей строке под текстом подписывается некоторое слово – девиз (в дальнейшем его стали называть ключом) с повторением, затем рассчитывается постолбцовая сумма порядковых алфавитных номеров букв текста и девиза (ключа по новой терминологии), в результате формируется шифротекст.

Пример 3.2. Зашифруем строку из стихотворения Андрея Белого «Я помню вас и ваши речи» с помощью девиза «Воспоминание», который является названием стихотворения. Как сказано выше, для этого выпишем две строки – строку текста и строку ключа с повторением. Сверху и снизу добавим по строке номеров соответствующих букв в русском алфавите. Получим следующую таблицу:

33	17	16	14	15	32	3	1	19	10	3	1	26	10	18	6	25	10
Я	П	О	М	Н	Ю	В	А	С	И	В	А	Ш	И	Р	Е	Ч	И
В	О	С	П	О	М	И	Н	А	Н	И	Е	В	О	С	П	О	М
3	16	19	17	16	14	10	15	1	15	10	6	3	16	19	17	16	14

Для получения шифротекста суммируем числа каждого столбца полученной таблицы (порядковый номер букв русского алфавита см. в приложении 1). Если сумма чисел оказывается больше 33 (число букв русского алфавита), то вычитаем из этой суммы 33. После этих вычислений от числа переходим к букве, соответствующей этому номеру. Так, в первом столбце получаем число $33 + 3 = 36$, и, поскольку это число больше количества букв в русском алфавите, отсюда вычитаем 33 и получаем $36 - 33 = 3$, т. е. букву «В». Продолжив процедуру, получим следующее зашифрованное сообщение:

В	Я	Б	Э	Э	Л	Л	О	Т	Б	Л	Ё	Ы	Ш	Г	Х	Ж	Ц
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

Очевидно, что дешифрование как обратный процесс возможно только при знании девиза.

Предлагаем читателю расшифровать самостоятельно криптотекст Тритемиуса на белорусском языке:

ВЭАПЕЎАЕЁНРЫЗВОВТФЕШШЖЬЕХЬНАЮЕОВПАБЭДЭЯТЁШБФЭЦ
Девизом этого сообщения будет слово БЕЛАРУСЫ.

В 1585 г. был опубликован большой «Трактат о шифрах», принадлежавший французскому послу в Риме Блезу де Виженеру (5 апреля 1523 – 19 февраля 1596). Для обеспечения секретности дипломатической почты он внес небольшое практическое усовершенствование в криптосистему Тритемиуса, которое позволило процедуру шифрования – дешифрования осуществлять почти автоматически. Роль шифровальной машины у Виженера играет квадратная таблица с алфавитом.

Сверху таблицы жирным шрифтом написан алфавит для шифруемого текста, слева в столбец также жирным шрифтом записан алфавит для ключа. Первая строка основного тела таблицы заполнена алфавитом начиная с буквы Б, следующая сдвигается на один символ влево, то есть начинается на В, и так далее. Возвращаясь к примеру 3.2, найдем в верхней строке таблицы букву Я, в левом столбце букву В и на их пересечении увидим букву В. Эту же процедуру можно проделать с остальными буквами сообщения и заметить, насколько упростился и ускорился процесс шифровки и дешифровки текста.

Приведем таблицы Виженера для русского, белорусского и английского алфавита (табл. 4–6).

Таблица 4

Таблица Виженера для русского алфавита

	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я
а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а
б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б
в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в
г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г
д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д
е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е
ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё
ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж
з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з
и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и
й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й

[illegible]

Таблица 5

Таблица Виженера для белорусского алфавита

	а	б	в	г	д	е	ё	ж	з	і	й	к	л	м	н	о	п	р	с	т	у	ў	ф	х	ц	ч	ш	ы	ь	э	ю	я
а	б	в	г	д	е	ё	ж	з	і	й	к	л	м	н	о	п	р	с	т	у	ў	ф	х	ц	ч	ш	ы	ь	э	ю	я	а
б	в	г	д	е	ё	ж	з	і	й	к	л	м	н	о	п	р	с	т	у	ў	ф	х	ц	ч	ш	ы	ь	э	ю	я	а	б
в	г	д	е	ё	ж	з	і	й	к	л	м	н	о	п	р	с	т	у	ў	ф	х	ц	ч	ш	ы	ь	э	ю	я	а	б	в
г	д	е	ё	ж	з	і	й	к	л	м	н	о	п	р	с	т	у	ў	ф	х	ц	ч	ш	ы	ь	э	ю	я	а	б	в	г
д	е	ё	ж	з	і	й	к	л	м	н	о	п	р	с	т	у	ў	ф	х	ц	ч	ш	ы	ь	э	ю	я	а	б	в	г	д
е	ё	ж	з	і	й	к	л	м	н	о	п	р	с	т	у	ў	ф	х	ц	ч	ш	ы	ь	э	ю	я	а	б	в	г	д	е
ё	ж	з	і	й	к	л	м	н	о	п	р	с	т	у	ў	ф	х	ц	ч	ш	ы	ь	э	ю	я	а	б	в	г	д	е	ё
ж	з	і	й	к	л	м	н	о	п	р	с	т	у	ў	ф	х	ц	ч	ш	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж
з	і	й	к	л	м	н	о	п	р	с	т	у	ў	ф	х	ц	ч	ш	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з
і	й	к	л	м	н	о	п	р	с	т	у	ў	ф	х	ц	ч	ш	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	і
й	к	л	м	н	о	п	р	с	т	у	ў	ф	х	ц	ч	ш	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	і	й

[illegible]

Таблица 6

Таблица Виженера для английского алфавита

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a
b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b
c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c
d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d
e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e
f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f
g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g
h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h
i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i
j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	g
k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k

l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l
m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m
n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n
o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p
q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q
r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r
s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s
t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t
u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u
v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v
w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w
x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x
y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y
z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z

Такая **криптосистема с девизом** применялась в военном деле на протяжении 400 лет как абсолютно надежная и недешифруемая. Отдельные страницы бессмертной книги Ярослава Гашека «Похождения бравого солдата Швейка» свидетельствуют об успешном применении криптосистемы Тритемиуса вплоть до начала XX века.

Однако слишком долгое применение одного и того же ключа может дать возможность противнику найти закономерности и взломать криптосистему. Проблему повышения секретности ключей преодолевали двумя путями: создание длинных ключей и частая их смена. При этом решение проблемы выбора новых ключей и их передачи было гениально простым. Участники переписки стали использовать идентичные экземпляры одного и того же издания конкретной книги. Новый ключ сообщался по номеру страницы и абзаца этой книги. Естественно, два числа, переданные почтой или публикацией в рекламном отделе газеты, вряд ли дадут содержательную информацию противнику.

3. Постолбцовая транспозиция

Шифр «Маршрутная транспозиция» и его вариант «постолбцовая транспозиция» относится к классу шифров **транспозиции**, которые изменяют порядок символов в сообщении. В данную матрицу размером $m \times n$ вписывается сообщение по строкам. Получение шифротекста состоит в последовательном выписывании букв первого, второго и последующих столбцов. Аналогичным образом работает «построковая транспозиция».

Пример 3.3. Текст, состоящий из 30 букв, записан построчно змейкой в таблицу или матрицу размером 5×6

<i>М</i>	<i>И</i>	<i>Н</i>	<i>С</i>	<i>К</i>	<i>С</i>
<i>А</i>	<i>Ц</i>	<i>И</i>	<i>Л</i>	<i>О</i>	<i>Т</i>
<i>Р</i>	<i>Е</i>	<i>С</i>	<i>П</i>	<i>У</i>	<i>Б</i>
<i>Е</i>	<i>Б</i>	<i>И</i>	<i>К</i>	<i>И</i>	<i>Л</i>
<i>Л</i>	<i>А</i>	<i>Р</i>	<i>У</i>	<i>С</i>	<i>Ь</i>

Шифрованный текст получается последовательной записью столбцов этой таблицы в строку, также змейкой (первый столбец слева вниз, второй снизу вверх и т. д.):

МАРЕЛ АБЕЦИ НИСИР УКПЛС КОУИС ЬЛБТС

При дешифровке запись восстанавливают обратной змейкой, начиная с последнего символа.

Другой вариант записи текста по более естественному маршруту состоит в последовательном выписывании столбцов.

<i>М</i>	<i>И</i>	<i>Н</i>	<i>С</i>	<i>К</i>	<i>С</i>
<i>Т</i>	<i>О</i>	<i>Л</i>	<i>И</i>	<i>Ц</i>	<i>А</i>
<i>Р</i>	<i>Е</i>	<i>С</i>	<i>П</i>	<i>У</i>	<i>Б</i>
<i>Л</i>	<i>И</i>	<i>К</i>	<i>И</i>	<i>Б</i>	<i>Е</i>
<i>Л</i>	<i>А</i>	<i>Р</i>	<i>У</i>	<i>С</i>	<i>Ь</i>

→ *МТРЛЛ ИОЕИА НЛСКР СИПИУ КЦУБС САБЕЬ*

Попробуйте прочитать еще одно сообщение на белорусском языке, шифрованное методом «построчковой транспозиции», учитывая, что порядок записи строк по столбцам меняется на противоположный, а фраза читается змейкой:

УЛОВНА РІАМЬК АЖЕЖЕО ДВЫВЫП

Одной из более сложных вариаций шифрования является маршрутная транспозиция с применением девизов. Ее суть в том, что после записи текста в таблицу столбцы таблицы переставляются особым образом, прежде чем выписывать шифротекст. Такая перестановка столбцов связана с алфавитным порядком следования букв в девизе.

Пример 3.4. Усложним шифровку по первой таблице примера 3.3, применив к ней девиз «Немига». Согласно порядку следования букв в русском алфавите буквам этого девиза присваиваются соответственно следующие номера: 6, 3, 5, 4, 2, 1. В этом порядке и выписываем столбцы первой шифровки примера 3.3:

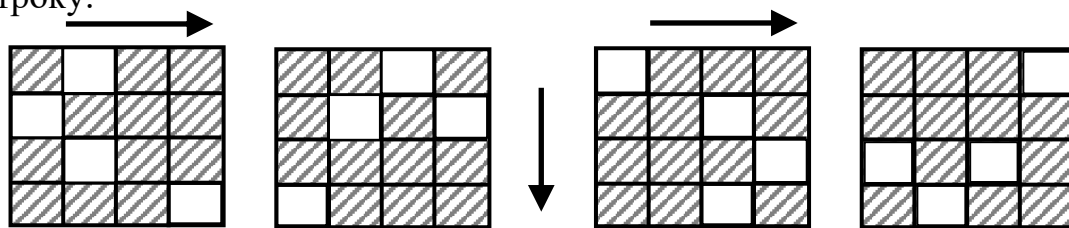
СТБЛЬ РИСИН КОУИС УКПЛС ИЦЕБА ЛЕРАМ

4. Криптосистема Кардано

Джироламо Кардано (24 сентября 1501 – 21 сентября 1576) – знаменитый итальянский математик, механик, врач, философ. Кардано – выдающийся мате-

матик, нашедший регулярный метод решения кубических уравнений по назван-
ным в его честь формулам Кардано. «Карданный вал» автомобиля как механиче-
ское устройство также является его изобретением. Наконец, Кардано придумал
свой вариант кодирования информации с использованием поворачивающегося
трафарета. Трафарет или *решетка Кардано* чаще всего изготавливается в
форме квадратной (иногда прямоугольной) карточки-таблицы, часть ячеек в ко-
торой вырезана и через которые наносится шифротекст. Иногда пустые поля
текста заполняются другим текстом для маскировки сообщений под обычные
послания.

Говоря подробнее, передаваемое сообщение должно содержать $4m * k$ букв.
Изготавливается трафарет из прямоугольного листа клетчатой бумаги размером
 $2m * 2k$ клеток. В трафарете вырезают $m * k$ клеток так, чтобы при наложении
его на такой же чистый лист бумаги четырьмя возможными способами (повора-
чивая его по или против часовой стрелки) его вырезы полностью покрывали всю
площадь листа. Ниже на рисунке показано размещение трафарета при его враще-
нии по часовой стрелке. Адресату заранее известен порядок этих четырех воз-
можных положений. Буквы сообщения последовательно вписываются в вырезы
трафарета – самый естественный вариант – по строкам, в каждой строке слева
направо. Заполненная таблица записывается последовательно – каждый столбец
в строку.



Проиллюстрируем на примере создание криптотекста из строки стихотво-
рения Николая Гумилёва «И сам я себя обманул» с помощью приведенной ре-
шетки.

	И		
С			
	А		
			М

	И	Я	
С	С		Е
	А		
Б			М

Я	И	Я	
С	С	О	Е
	А		Б
Б		М	М

Я	И	Я	А
С	С	О	Е
Н	А	У	Б
Б	Л	М	М

Преобразовав столбцы в строки, получаем:

ЯСНБ ИСАЛ ЯОУМ АЕБМ

Пример 3.5. Прочитайте записанное с помощью приведенного выше трафарета и в указанном выше порядке следующее краткое, но несомненно важное сообщение:

-ГМЗ БВУН РФАА ГУЛИ

В случае использования прямоугольного трафарета его вращение по или против часовой стрелки не подходит для шифрования, поэтому применяется последовательность симметричных отражений относительно горизонтальной и вертикальной средних линий. При этом необходимо, чтобы трафарет содержал четное число строк и столбцов. Такой способ применим и для квадратных решеток Кардано.

5. Аффинная система подстановок Цезаря

Аффинная система подстановок Цезаря базируется на модулярной арифметике. В системе шифрования Цезаря использовались только аддитивные свойства кольца классов вычетов по модулю m , т. е. множества $\mathbb{Z}/m\mathbb{Z}$. Однако элементы множества $\mathbb{Z}/m\mathbb{Z}$ можно также умножать по модулю m . Применяя одновременно операции сложения и умножения по модулю m над элементами множества $\mathbb{Z}/m\mathbb{Z}$, можно получить систему подстановок, которую называют аффинной системой подстановок Цезаря.

Суть этого метода шифрования состоит в следующем: каждая буква алфавита (преобразованная в число от 0 до $m - 1$, где m – число букв в алфавите) шифруется с помощью аффинной функции

$$E_{a,b}: \mathbb{Z}/m\mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z}, \quad E_{a,b}(t) = at + b(\text{mod } m),$$

$0 \leq a, b < m$, $\text{НОД}(a, m) = 1$, где t – числовое значение буквы некоторого алфавита (от 0 до $m-1$), m – размер алфавита, a и b – ключи шифрования (целые числа), a должно быть взаимно простым с m , чтобы существовало обратное преобразование, $\text{mod } m$ – операция взятия остатка по модулю m .

Например, английский алфавит содержит 26 букв, значит, в качестве параметра a может быть выбрано только число, взаимно простое с 26. Таких чисел всего двенадцать: 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23 и 25. Число b , в свою очередь, может принимать любое значение в интервале от 0 до 25, что в итоге дает нам $12 * 26 = 312$ вариантов возможных ключей.

Пример 3.6. Рассмотрим применение аффинного преобразования сообщения HELLO на английском языке. Пусть $m = 26$, $a = 3$, $b = 5$. Требование взаимной простоты чисел m и a выполнено, так как $\text{НОД}(3, 26) = 1$. Преобразуем буквы английского алфавита в числа по правилу: каждой букве ставится в соответствие число, равное ее порядковому номеру в алфавите, уменьшенному на единицу, т. е. букве «а» соответствует число 0 и т. д. Рассчитываем взаимное соответствие букв английского алфавита и их закодированных аналогов и заносим в нижеприведенную таблицу числовых кодов букв:

t	0	1	2	3	4	5	6	7	8	9	10	11	12	13
$3t + 5 \bmod 26$	5	8	11	14	17	20	23	0	3	6	9	12	15	18

t	14	15	16	17	18	19	20	21	22	23	24	25
$3t + 5 \bmod 26$	21	24	1	4	7	10	13	16	19	22	25	2

Проведя обратное преобразование закодированных чисел в буквы с использованием приведенной выше таблицы, получаем следующее соответствие для букв открытого текста и шифротекста:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
F	I	L	O	R	U	X	A	D	G	J	M	P	S	V	Y	B	E	H	K	N	Q	T	W	Z	C

Тогда исходное сообщение HELLO преобразуется в шифротекст ARMMV.

Предлагаем читателю самостоятельно составить процесс дешифрования сообщения, закодированного при помощи аффинной системы подстановок Цезаря.

Достоинством аффинной системы кодирования информации является удобное управление ключами, поскольку ключи шифрования и дешифрования представляются в компактной форме в виде пары чисел (a, b) . Недостатки аффинной системы подстановок аналогичны недостаткам системы шифрования Цезаря.

Аффинная система подстановок использовалась на практике несколько веков назад, а сегодня ее применение ограничивается большей частью иллюстрациями основных криптологических подходов.

6. Криптосистема Хилла

В 1929 году американский математик Лестер Сандерс Хилл опубликовал алгебраический метод, обобщающий аффинную подстановку Цезаря

$$E_{a,b}: \mathbb{Z}/m\mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z}, \quad E_{a,b}(t) = at + b(\bmod m)$$

и использующий не только сдвиг алфавитных символов, что обеспечивало шифр бóльшей криптостойкостью.

Изложим суть такого метода символьного кодирования, построенного на синтезе модульной арифметики и линейной алгебры. В его основе лежит линейное преобразование ***n -грамм*** – упорядоченных наборов из n чисел полной системы наименьших неотрицательных вычетов по модулю m . n -грамму обозначают как $\bar{x} = (x_1, x_2, \dots, x_n)$.

Напомним, что на множестве классов вычетов $\mathbb{Z}/m\mathbb{Z}$ определены операции сложения, вычитания и умножения по модулю m . Данное множество является примером кольца. Кольцо $\mathbb{R}$ представляет собой алгебраическую систему, в которой определены операции сложения, вычитания и умножения пар элементов. Эта алгебраическая система обладает рядом свойств:

- элементы кольца $\mathbb{R}$ образуют коммутативную группу относительно операции сложения; кроме того, существуют единичный и обратный элементы относительно операции сложения;
- умножение и сложение удовлетворяют ассоциативному и дистрибутивному законам.

Мультипликативное обратное α^{-1} элемента α кольца может существовать не всегда. Например, как было показано в разделе «Основы теории чисел», если модуль $m = 26$, то значения $2^{-1}(\text{mod } 26)$ и $13^{-1}(\text{mod } 26)$ не существуют.

Напомним, что если модуль m является простым числом p , то существует обратная величина любого ненулевого элемента t из $\mathbb{Z}/m\mathbb{Z}$ (при $m = p$).

Множество $\mathbb{Z}/p\mathbb{Z}$, где p – простое число, является примером алгебраической системы, называемой конечным полем. Ненулевые элементы $\mathbb{Z}/p\mathbb{Z}$ образуют мультипликативную группу.

Множество всех n -грамм $\bar{x} = (x_1, x_2, \dots, x_n)$ с компонентами из кольца $\mathbb{Z}/m\mathbb{Z}$ образует векторное пространство $Z_{m,n}$ над кольцом $\mathbb{Z}/m\mathbb{Z}$. Каждая n -грамма $\bar{x}$ называется вектором. В векторном пространстве $Z_{m,n}$ для векторов $\bar{x}$ определены операции покомпонентного сложения и вычитания по модулю m , а также скалярное умножение вектора на элемент t кольца $\mathbb{Z}/m\mathbb{Z}$. Сложение и скалярное умножение являются операциями, удовлетворяющими коммутативному, ассоциативному и дистрибутивному законам. Вектор $\bar{x}$ является линейной комбинацией векторов $\bar{x}^{(i)}$ с коэффициентами $t_i \in \mathbb{Z}/m\mathbb{Z}$, $1 \leq i \leq L$, если

$$\bar{x} = t_1 \bar{x}^{(1)} + t_2 \bar{x}^{(2)} + \dots + t_L \bar{x}^{(L)} (\text{mod } m).$$

Линейное преобразование T является отображением:

$$T: Z_{m,n} \rightarrow Z_{m,n}, T: \bar{x} \rightarrow \bar{y}, \bar{y} = T(\bar{x}),$$

которое удовлетворяет условию линейности

$$T(t * \bar{x} + s * \bar{y}) = t * T(\bar{x}) + s * T(\bar{y})$$

для всех s, t в $\mathbb{Z}/m\mathbb{Z}$ и $\bar{x}, \bar{y}$ в $Z_{m,n}$.

Линейное преобразование T может быть представлено матрицей размером $n \times n$ вида

$$T = \begin{bmatrix} \gamma_{1,1} & \gamma_{1,2} \cdots \gamma_{1,j} \cdots \gamma_{1,n} \\ \gamma_{2,1} & \gamma_{2,2} \cdots \gamma_{2,j} \cdots \gamma_{2,n} \\ \cdots & \cdots \\ \gamma_{i,1} & \gamma_{i,2} \cdots \gamma_{i,j} \cdots \gamma_{i,n} \\ \cdots & \cdots \\ \gamma_{n,1} & \gamma_{n,2} \cdots \gamma_{n,j} \cdots \gamma_{n,n} \end{bmatrix},$$

причем $y_i = \gamma_{i,1}x_1 + \gamma_{i,2}x_2 + \cdots + \gamma_{i,j}x_j + \cdots + \gamma_{i,n}x_n \pmod{m}$ или $y_i = \sum_{j=1}^n \gamma_{i,j}x_j \pmod{m}$, $1 \leq i \leq n$.

Базисом для векторного пространства $Z_{m,n}$ является набор векторов из $\{\bar{x}^{(i)}: 1 \leq i \leq n\}$, которые линейно независимы и порождают $Z_{m,n}$. Каждый базис для $Z_{m,n}$ содержит n линейно независимых векторов. Любой набор из n векторов, которые линейно независимы над $Z_{m,n}$, является базисом.

Пусть T является линейным преобразованием, описываемым матрицей T , причем $T: Z_{m,n} \rightarrow Z_{m,n}$.

Если векторы $\{\bar{x}^{(i)}: 1 \leq i \leq n\}$ линейно независимы над $Z_{m,n}$, тогда их образы $\{T(\bar{x}^{(i)}): 1 \leq i \leq n\}$ линейно независимы над $Z_{m,n}$ только в том случае, если определитель матрицы T , обозначаемый как $\det(T)$, не делится на любое простое p , которое делит m (т. е. число $\det(T)$ взаимно просто с m). В этом случае преобразование T называется обратимым (или невырожденным) линейным преобразованием, имеющим обратное преобразование T^{-1} :

$$T^{-1}: Z_{m,n} \rightarrow Z_{m,n}, TT^{-1} = T^{-1}T = I,$$

где I — единичная матрица. Кроме того, T^{-1} также является линейным преобразованием.

Пример 3.7. Зададим число $m = 26$ (число букв английского алфавита), матрицу преобразования

$$T = \begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix}$$

и вычислим определитель этой матрицы: $\det(T) = 9 \equiv 1 \pmod{2}$, $\det(T) = 9 \equiv 9 \pmod{13}$. Определитель является взаимно простым с модулем m , поэтому существует обратное преобразование T^{-1} и оно имеет вид

$$T^{-1} = \begin{pmatrix} 15 & 17 \\ 20 & 9 \end{pmatrix}.$$

Действительно,

$$TT^{-1} = T^{-1}T = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Пусть T является линейным преобразованием на $Z_{26,2}$ с матрицей $T = \begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix}$.

Используем это преобразование T для определения биграммной подстановки в английском алфавите $\{ABCDEFGH \dots XYZ\}$.

Сначала разобьем n -грамму открытого текста на биграммы, причем выберем n кратным 2, например 12-грамма PAYMOREMONEY делится на шесть биграмм:

PA YM OR EM ON EY.

Затем в каждой биграмме открытого текста заменим каждую букву ее числовым эквивалентом, равным номеру этой буквы в алфавите (полагаем, что нумерация букв в алфавите начинается с 1):

PA $\Leftrightarrow$ 16 1; YM $\Leftrightarrow$ 25 13; OR $\Leftrightarrow$ 15 18;

EM $\Leftrightarrow$ 5 13; ON $\Leftrightarrow$ 15 14; EY $\Leftrightarrow$ 5 25.

Преобразование биграмм $\bar{x}_j$ открытого текста в биграммы $\bar{y}_i$ шифротекста осуществляется в соответствии с уравнением $\bar{y}_j = T\bar{x}_j \pmod{26}$ или $\bar{y}_j = \begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix} x_j \pmod{26}$, где $\bar{x}_j$ и $\bar{y}_j$ – вектор-столбцы биграмм шифротекста и открытого текста соответственно.

Получаем:

$$\begin{aligned}\bar{y}_1 &= \begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix} \begin{pmatrix} 16 \\ 1 \end{pmatrix} \pmod{26} = \begin{pmatrix} 25 \\ 11 \end{pmatrix}, \\ \bar{y}_2 &= \begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix} \begin{pmatrix} 25 \\ 13 \end{pmatrix} \pmod{26} = \begin{pmatrix} 10 \\ 11 \end{pmatrix}, \\ \bar{y}_3 &= \begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix} \begin{pmatrix} 15 \\ 18 \end{pmatrix} \pmod{26} = \begin{pmatrix} 21 \\ 16 \end{pmatrix}, \\ \bar{y}_4 &= \begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix} \begin{pmatrix} 5 \\ 13 \end{pmatrix} \pmod{26} = \begin{pmatrix} 2 \\ 23 \end{pmatrix}, \\ \bar{y}_5 &= \begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix} \begin{pmatrix} 15 \\ 14 \end{pmatrix} \pmod{26} = \begin{pmatrix} 9 \\ 22 \end{pmatrix}, \\ \bar{y}_6 &= \begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix} \begin{pmatrix} 5 \\ 25 \end{pmatrix} \pmod{26} = \begin{pmatrix} 12 \\ 5 \end{pmatrix}.\end{aligned}$$

Заменяя в биграммах шифротекста числа на соответствующие буквы, получаем 12-грамму шифротекста: YK JK UP BW IV LE.

Для расшифрования биграмм $\bar{y}_j$ шифротекста и восстановления биграмм $\bar{x}_j$ открытого текста необходимо выполнить обратное преобразование T^{-1} согласно уравнению $\bar{x}_j = T^{-1}\bar{y}_j \pmod{26}$. В рассмотренном примере матрицы преобразования имели размер 2×2 и шифровались биграммы (пары) букв. Хотя буква Е может быть зашифрована по-разному в различных парах исходного сообщения, одна и та же пара, например ЕМ, будет шифроваться всегда одинаково на протяжении всего исходного текста.

Система Хилла является *одноалфавитной* в широком смысле слова.

Если систему Хилла использовать для шифрования русскоязычного сообщения, то число 26 (количество символов в алфавите) нужно заменить на 33.

§ 2. Современные криптосистемы

1. Криптосистема RSA

Название криптосистемы RSA является аббревиатурой от фамилий ее создателей – ученых Массачусетского технологического института Рональда Ривеста (Ronald Rivest), Ади Шамира (Adi Shamir) и Леонарда Адлемана (Leonard Adleman). Основные принципы этой системы были разработаны и опубликованы в 1977 г., применяется она и в настоящее время, например является базовой частью HTTPS-протокола. Алгоритм криптосистемы RSA относится к классу асимметричных алгоритмов шифрования, поскольку имеет два разных ключа для шифрования и расшифрования – открытый (публичный) и закрытый (приватный) соответственно.

Алгоритм. В работе с криптосистемой RSA можно выделить три этапа: создание ключа, шифрование сообщения и дешифровка сообщения.

Создание ключа

1. Выбрать произвольные простые числа p и q .

2. Найти их произведение – модуль n :

$$n = pq.$$

3. Вычислить функцию Эйлера от модуля:

$$\varphi(n) = (p-1)(q-1).$$

4. Выбрать случайное число e – *открытую экспоненту*, меньшее $\varphi(n)$ и взаимно простое с ним:

$$\text{НОД}(\varphi(n), e) = 1.$$

5. Найти число d – *секретную экспоненту*, обратное к e по модулю $\varphi(n)$:
 $ed \equiv 1 \pmod{\varphi(n)}.$

6. Предоставить набор чисел (n, e) в качестве *открытого ключа*, удалить всю информацию о $p, q, \varphi(n)$ и запомнить d в качестве *закрытого ключа*.

Адресат (Алиса) передает отправителю (Бобу) открытый ключ. Передача открытого ключа может осуществляться через посредника.

Шифрование

Боб шифрует свое числовое сообщение m , предварительно убедившись, что число $m < n$ и является взаимно простым с n . Для шифрования он возводит m в степень e по модулю n :

$$c = m^e \pmod{n}.$$

Боб отправляет Алисе зашифрованное сообщение. Передача возможна и через посредника, так как поскольку тот не имеет секретного ключа d , то и прочесть сообщение Боба не может.

Расшифровка

Алиса находит (вычисляет) зашифрованное сообщение m по формуле

$$m = c^d \pmod{n}.$$

На рис. 4 схематично представлены основные этапы передачи сообщений с использованием криптосистемы RSA.



Рис. 4. Схема передачи сообщения с помощью RSA

Обоснование криптосистемы RSA

Покажем, что указанная процедура шифрования и расшифрования задает корректную и однозначную передачу данных, т. е. Алиса может прочесть сообщение m Боба, имея открытый ключ (n, e) и закрытый ключ d . Покажем, что

$$c^d \pmod{n} = m.$$

Действительно, $c^d \pmod{n} = (m^e)^d \pmod{n} = m^{ed} \pmod{n}$. Поскольку $ed \equiv 1 \pmod{\phi(n)}$, то будем иметь $ed = 1 + l\phi(n)$, а это означает, что $c^d \pmod{n} = m^{1+l\phi(n)} \pmod{n}$. Тогда для взаимно простых чисел n и m справедлива теорема Эйлера, согласно которой $m^{\phi(n)} \equiv 1 \pmod{n}$, откуда следует, что $m^{l\phi(n)} \equiv 1 \pmod{n}$.

Таким образом, окончательно получаем:

$$c^d \pmod{n} = m^{1+l\phi(n)} \pmod{n} = m \cdot m^{l\phi(n)} \pmod{n} = m.$$

Полученное равенство доказывает, что алгоритм системы RSA является криптографическим, т. е. процедура расшифровки позволяет однозначно восстановить истинное сообщение.

Замечание. На пятом шаге создания ключей для нахождения секретной экспоненты d вместо функции Эйлера можно использовать *функцию Кармайкла*.

Функцию Кармайкла задают следующим образом: если известно каноническое разложение числа $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$, где p_i , $1 \leq i \leq s$ простые числа, α_k , $1 \leq k \leq s$ - натуральные степени, то значение функции Кармайкла вычисляется по формуле

$$\lambda(n) = \text{НОК}(\lambda(p_1^{\alpha_1}), \lambda(p_2^{\alpha_2}), \dots, \lambda(p_s^{\alpha_s})),$$

где

$$\lambda(p_i^{\alpha_i}) = \begin{cases} \varphi(p_i^{\alpha_i}), & \text{если } p_i \neq 2 \text{ или } p_i = 2 \text{ и } \alpha_i \leq 2, \\ \frac{1}{2}\varphi(p_i^{\alpha_i}), & \text{если } p_i = 2 \text{ и } \alpha_i \geq 3 \end{cases}.$$

Для функции, заданной таким образом, верна *теорема Кармайкла*.

Теорема Кармайкла. Если a взаимно просто с n , тогда $a^{\lambda(n)} \equiv 1 \pmod{n}$.

Удобство использования функции Кармайкла состоит в том, что при вычислении секретной экспоненты d как числа обратного к e по модулю $\lambda(n)$ можно получить меньшее значение, чем при использовании функции Эйлера, что в дальнейшем ускорит возведение в степень при расшифровке сообщения.

Пример 3.8. Зашифровать букву «и» с использованием криптосистемы RSA.

Вначале поставим в соответствие тексту число: каждой букве алфавита соответствует ее двузначный номер в алфавите. Таким образом, букве «и» соответствует число 10 (здесь и далее используем 33-х буквенный алфавит с буквой «ё», первым буквам соответствует номера вида 01, 02, ..., 09). Далее создадим ключ и зашифруем сообщение по указанному выше алгоритму. Шаги создания ключей и шифрования занесем в таблицу 7.

Таблица 7

Создание ключей и шифрование при использовании криптосистемы

№ шага	Действия	Примечание
1	Произвольно выбираем $p=13, q=19$	Создание ключей
2	Вычисляем $n=pq=13 \cdot 19=247$	
3	Находим $\varphi(n) = \varphi(247) = (13-1)(19-1) = 12 \cdot 18 = 216$	
4	Произвольно выбираем $e = 7$	
5	$7d \equiv 1 \pmod{216}$ с помощью расширенного алгоритма Евклида находим $d = 31$	
6	$(n, e) = (247, 7)$	
1	Вычисляем $c = m^e \pmod{n} = 10^7 \pmod{247} = 205$	Шифрование

Таким образом, адресат получит число 205.

Пример расшифровки сообщения подробно будет разобран в разделе типовых заданий с образцами решений.

2. Характеристики криптосистемы RSA

Оценим надежность криптосистемы RSA. Для того чтобы взломать шифр, необходимо знать секретную экспоненту d , для нахождения которой, в свою оче-

редь, требуется вычислить $\varphi(n)$, а следовательно, найти каноническое разложение числа n (модуля). При больших значениях n задача факторизации становится достаточно сложной. **Именно сложность задачи факторизации модуля n обеспечивает стойкость криптосистемы RSA.**

С другой стороны, это приводит к ряду ограничений и уязвимостей. Приведем некоторые из них.

1. При генерации ключа простые числа p и q должны быть выбраны случайным образом и независимо друг от друга и быть настолько большими, чтобы обеспечить требуемую длину ключей (в настоящий момент минимальные требования к длине ключа – 2048 бит).

2. Числа p и q должны быть такими, чтобы $\text{НОД}(p-1, q-1)$ был небольшим и, желательно, равным 2.

3. Числа p и q должны быть **сильно простыми** [27]. **Сильно простым** называется такое простое число r , что $r+1$ имеет большой простой делитель, $r-1$ имеет большой простой делитель s , такой, что число $s-1$ также обладает большим простым делителем.

4. Согласно теореме Винера, секретная экспонента d должна быть больше $\frac{1}{3}\sqrt[4]{n}$, в противном случае взломщик может установить d . Для повышения стойкости ко взлому и открытая экспонента e также должна быть большой. Эти требования к значениям d и e приводят к увеличению трудоемкости операции возведения в большую степень чисел m и c при шифровке и расшифровке сообщения.

В случае невыполнения одного из условий 1–3 имеются эффективные алгоритмы разложения n на простые множители, и шифр теряет свою стойкость ко взлому.

Для того чтобы избежать проблем с возведением в степень при выполнении условия 4, применяется китайская теорема об остатках.

3. Китайская теорема об остатках

Впервые китайская теорема об остатках была упомянута в арифметической формулировке в трактате древнекитайского математика Сунь Цзы между III и V веками н. э. Позже она встречается в полной форме в книге китайского математика Цинь Цзюшао «Математические рассуждения в 9 главах», датируемой 1247 годом.

Теорема (китайская теорема об остатках). Система сравнений с одним неизвестным x и попарно взаимно простыми модулями $m_1, m_2, \dots, m_k$:

$$\begin{cases} x \equiv b_1 \pmod{m_1}, \\ x \equiv b_2 \pmod{m_2}, \\ \dots \\ x \equiv b_k \pmod{m_k} \end{cases}$$

имеет единственное решение $x \equiv x_0 \pmod{m_1 m_2 \dots m_k}$,

где $x_0 = M_1 N_1 b_1 + M_2 N_2 b_2 + \dots + M_k N_k b_k$, $M_i = \frac{m_1 m_2 \cdot \dots \cdot m_k}{m_i}$, $N_i = M_i^{-1} (\text{mod } m_i)$,
 $i = 1, 2, \dots, k$.

Замечание. Класс чисел, сравнимых между собой по модулю $m_1 m_2 \cdot \dots \cdot m_k$, принимаем за одно решение.

Решение системы сравнений, данное в теореме, называют решением по алгоритму Гаусса.

Китайская теорема об остатках позволяет каждому целому числу x на отрезке от 0 до $(m_1 m_2 \cdot \dots \cdot m_k) - 1$ поставить во взаимно однозначное соответствие набор чисел $(b_1, b_2, \dots, b_k)$, где b_i является целым числом на отрезке от 0 до $m_i - 1$ включительно, $i = 1, 2, \dots, k$.

Определение 3.1. Набор чисел $(b_1, b_2, \dots, b_k)$, такой, что число x из отрезка от 0 до $(m_1 m_2 \cdot \dots \cdot m_k) - 1$ удовлетворяет системе

$$\begin{cases} x \equiv b_1 \pmod{m_1}, \\ x \equiv b_2 \pmod{m_2}, \\ \dots \\ x \equiv b_k \pmod{m_k}, \end{cases}$$

называется **CRT-представлением числа x** по модулю $m_1 m_2 \cdot \dots \cdot m_k$.

В термине «CRT-представление» CRT является аббревиатурой от «Chinese remainder theorem» («Китайская теорема об остатках»). То, что набор чисел $(b_1, b_2, \dots, b_k)$ является CRT-представлением числа x , будем обозначать как $x \leftrightarrow (b_1, b_2, \dots, b_k)$.

Пример 3.9. Найти CRT-представление числа 93 по модулю 140.

Разложим 140 в произведение попарно взаимно простых множителей:

$140 = 4 \cdot 5 \cdot 7$. Найдем остатки от деления 93 на 4, 5 и 7:

$$93 \equiv 1 \pmod{4},$$

$$93 \equiv 3 \pmod{5},$$

$$93 \equiv 2 \pmod{7}.$$

Таким образом, 93 удовлетворяет системе сравнений $\begin{cases} x \equiv 1 \pmod{4}, \\ x \equiv 3 \pmod{5}, \\ x \equiv 2 \pmod{7} \end{cases}$, следо-

вательно, его **CRT-представлением** является набор $(1, 3, 2)$. Обозначаем этот факт как $93 \leftrightarrow (1, 3, 2)$.

Следствие 1. Китайская теорема об остатках позволяет сделать вывод о том, что для числа x существует обратное к нему по модулю $m = m_1 m_2 \cdot \dots \cdot m_k$ число z , т. е. $xz \equiv 1 \pmod{m}$ тогда и только тогда, когда в CRT-представлении $(b_1, b_2, \dots, b_k)$ числа x каждое число b_i имеет обратное по соответствующему модулю m_i , причем $z = x^{-1} \pmod{m} \leftrightarrow (b_1^{-1} \pmod{m_1}, b_2^{-1} \pmod{m_2}, \dots, b_k^{-1} \pmod{m_k})$.

Следствие 2. Свойства сравнений и китайская теорема об остатках позволяют установить также взаимно однозначное соответствие между результатом операций над числами x и y и результатом операций над их CRT-представлениями. Эти соответствия для различных операций над числами $x \leftrightarrow (b_1, b_2, \dots, b_k)$ и $y \leftrightarrow (c_1, c_2, \dots, c_k)$ приведены ниже в таблице 8.

Таблица 8

Соответствие операций над числами и над их CRT-представлениями

Операция над x, y по модулю $m = m_1 m_2 \dots m_k$	CRT-представление результата операции
$x \pm y$	$(b_1 + c_1, b_2 + c_2, \dots, b_k + c_k)$
$x \cdot y$	$(b_1 \cdot c_1, b_2 \cdot c_2, \dots, b_k \cdot c_k)$
$x \cdot y^{-1}$	$(b_1 \cdot c_1^{-1}, b_2 \cdot c_2^{-1}, \dots, b_k \cdot c_k^{-1})$
x^k	$(b_1^n, b_2^n, \dots, b_k^n)$

С практической точки зрения суть следствий из китайской теоремы об остатках в следующем. Вместо того, чтобы выполнять операции по составному модулю над большими числами x и y , можно выполнять те же операции по простому модулю над их компонентами в CRT-представлении, а затем по полученному CRT-представлению восстановить искомое число. При этом хотя количество операций возрастает, все они совершаются над меньшими числами и по меньшему модулю, что существенно упрощает задачу. Именно поэтому для возведения в степень на этапах шифрования и расшифровки в алгоритмах RSA используется CRT-представление.

Особенностью применения CRT-представления в работе криптосистемы RSA является то, что модуль n раскладывается всего на два простых множителя. Следовательно, CRT-представление имеет только две компоненты и после их возведения в степень необходимо восстановить зашифрованное (расшифрованное) число по системе из двух сравнений. Для этого необязательно пользоваться алгоритмом Гаусса, можно найти решение с помощью **формул Гарнера**.

Пусть x удовлетворяет системе сравнений

$$\begin{cases} x \equiv a \pmod{p}, \\ x \equiv b \pmod{q}, \end{cases}$$

тогда

$$x = \left(\left((a - b)(q^{-1} \pmod{p}) \right) \pmod{p} \right) q + b$$

или

$$x = \left(\left((b - a)(p^{-1} \bmod q) \right) \bmod q \right) p + a.$$

При этом обе формулы дают одно и то же значение x .

Пример 3.10. Зашифровать слово «ма» в криптосистеме RSA, используя CRT-представление.

Переведем текст в число использованным в примере 3.8 способом, поставив каждой букве в соответствие ее номер в алфавите и записав эти номера подряд: «ма» = 1401.

Шаги создания ключей занесем в таблицу 9.

Таблица 9

Создание ключей при использовании криптосистемы RSA

№ шага	Действия	Примечание
1	Произвольно выбираем $p = 23, q = 61$	Создание ключей
2	Вычисляем $n = pq = 23 \cdot 61 = 1403$	
3	Находим $\varphi(n) = \varphi(1403) = (23 - 1)(61 - 1) = 1320$	
4	Произвольно выбираем $e = 853$	
5	$853d \equiv 1 \pmod{1403}$ с помощью расширенного алгоритма Евклида находим $d = 277$	
6	$(n, e) = (1403, 853)$	

Перейдем к шифрованию. Для создания шифра необходимо вычислить $c = m^e \pmod{n} = 1401^{853} \pmod{1403}$. Вначале проверим, можно ли уменьшить степень, воспользовавшись теоремой Кармайкла.

Так как $n = 1403 = 23 \cdot 61$, то $\lambda(n) = \lambda(23 \cdot 61) = \text{НОК}(\lambda(23), \lambda(61))$. Для чисел 23 и 61, согласно определению, значения функции Кармайкла $\lambda(23), \lambda(61)$ совпадают со значениями функции Эйлера $\varphi(23), \varphi(61)$:

$$\lambda(1403) = \text{НОК}(\lambda(23), \lambda(61)) = \text{НОК}(\varphi(23), \varphi(61)) = \text{НОК}(22, 60) = 660.$$

По теореме Кармайкла $a^{\lambda(n)} \equiv 1 \pmod{n}$ имеем:
 $1401^{\lambda(1403)} = 1401^{660} \equiv 1 \pmod{1403}$.

$$\text{Тогда } 1401^{853} = 1401^{660+193} = 1401^{660} \cdot 1401^{193} \equiv 1 \cdot 1401^{193} \pmod{1403}.$$

Заметим, что в данном случае применение теоремы Эйлера $a^{\varphi(n)} \equiv 1 \pmod{n}$ не позволяет упростить выражение, так как $\varphi(1403) = 1320$ превышает открытую экспоненту $e = 853$.

Далее для возведения в степень 193 числа 1401 по модулю 1403 будем использовать CRT-представление.

1. Найдем остатки от деления числа 1401 на $p = 23$ и $q = 61$:

$$1401 \equiv 21 \pmod{23},$$

$$1401 \equiv 59 \pmod{61}.$$

Тогда $1401 \leftrightarrow (21, 59)$, а $1401^{193} \leftrightarrow (21^{193}, 59^{193})$.

2. Вычислим $21^{193} \pmod{23}$ и $59^{193} \pmod{61}$. Вначале используем малую теорему Ферма для простых модулей $a^{p-1} \equiv 1 \pmod{p}$: $21^{22} \equiv 1 \pmod{23}$ и $59^{60} \equiv 1 \pmod{61}$, что позволит значительно упростить поставленную задачу:

$$21^{193} = 21^{22 \cdot 8 + 17} = (21^{22})^8 \cdot 21^{17} \equiv 1 \cdot 21^{17} \pmod{23},$$

$$59^{193} = 59^{60 \cdot 3 + 13} = (59^{60})^3 \cdot 59^{13} \equiv 1 \cdot 59^{13} \pmod{61}.$$

Для дальнейшего вычисления $21^{17} \pmod{23}$ и $59^{13} \pmod{61}$ будем использовать алгоритм быстрого возведения в степень (*бинарный метод справа налево*). При его реализации находим степени вида 2^k :

$$21^2 = 441 \equiv 4 \pmod{23};$$

$$21^4 \equiv 4^2 \pmod{23} = 16 \pmod{23};$$

$$21^8 \equiv 16^2 \pmod{23} \equiv 3 \pmod{23};$$

$$21^{16} \equiv 3^2 \pmod{23} = 9 \pmod{23}.$$

Представим степень 17 как сумму степеней двойки и воспользуемся свойством сравнений:

$$21^{17} = 21^{16+1} = 21^{16} \cdot 21 \equiv 9 \cdot 21 \pmod{23} \equiv 5 \pmod{23}.$$

Аналогичным образом выполним возведение в степень по модулю 61 числа 59:

$$59^2 = 3481 \equiv 4 \pmod{61};$$

$$59^4 \equiv 4^2 \pmod{61} = 16 \pmod{61};$$

$$59^8 \equiv 16^2 \pmod{61} \equiv 12 \pmod{61};$$

$$59^{16} \equiv 12^2 \pmod{61} \equiv 22 \pmod{61};$$

$$59^{13} = 59^{8+4+1} = 59^8 \cdot 59^4 \cdot 59 \equiv 12 \cdot 16 \cdot 59 \pmod{61} \equiv 43 \pmod{61}.$$

В итоге получено CRT-представление 1401^{193} по модулю 1403: $1401^{193} \leftrightarrow (11, 43)$

3. Восстановим по CRT-представлению число 1401^{193} по модулю 1403. Для этого будем использовать формулу Гарнера

$$c = ((b - a)(p^{-1} \pmod{q}) \pmod{q})p + a$$

при $a = 5$, $b = 43$, $p = 23$, $q = 61$.

Предварительно вычислим $p^{-1} \pmod{q} = 23^{-1} \pmod{61} = 8$.

Тогда $b - a = 43 - 5 = 38$, $((b - a)p^{-1} \pmod{q}) \pmod{q} = (38 \cdot 8) \pmod{61} = 60$,
 $c = 60 \cdot 23 + 5 = 1385$.

Итак, окончательный результат – шифр $c = 1401^{853} \pmod{1403} = 1385$.

Замечание. Если опустить этап понижения степени с помощью теоремы Кармайкла, а применять лишь малую теорему Ферма для компонент CRT-представления, то в результате также придем к необходимости вычислить $21^{17} \pmod{23}$ и $59^{13} \pmod{61}$.

Подробные примеры алгоритма расшифровки приведены в разделе типовых заданий с образцами решений.

4. Криптосистема Эль-Гамала

Данная система шифрования была создана во время обучения в аспирантуре американским криптографом родом из Египта Тахером Эль-Гамалем, опубликовавшем результаты своих исследований в 1985 году в статье «Криптосистема с открытым ключом и схема цифровой подписи на основе дискретных логарифмов». Криптосистема Эль-Гамала так же, как и криптосистема RSA, относится к асимметричным системам шифрования, и в настоящее время используется ее модификация на эллиптических кривых.

Алгоритм. Как и в случае с криптосистемой RSA, опишем три этапа использования криптосистемы Эль-Гамала: создание ключа, шифрование сообщения и расшифровка сообщения.

Создание ключа

1. Выбрать произвольное достаточно большое простое число P .
2. Найти число g – *генератор мультипликативной группы классов вычетов $(\mathbb{Z}/P\mathbb{Z})^*$* .
3. Выбрать случайным образом число x – *закрытый ключ*, меньший $P - 1$.
4. Найти число $y = g^x \pmod{P}$.
5. Предоставить набор чисел (P, g, y) в качестве *открытого ключа*.

Шифрование

1. Отправитель выбирает *рандомизатор* – случайное число r , $1 < r < P - 1$.
2. Генерирует открытый сеансовый ключ $C1 = g^r \pmod{P}$.
3. Находит число $y^r \pmod{P}$.
4. Шифрует сообщение m по формуле $C2 \equiv m y^r \pmod{P}$.

Отправитель посылает адресату *шифротекст* – пару чисел $(C1, C2)$.

Расшифровка

1. Адресат возводит открытый сеансовый ключ $C1$ в степень закрытого ключа x по модулю P : $K = C1^x \pmod{P}$.
2. Находит обратное к K по модулю P .
3. Вычисляет зашифрованное сообщение m по формуле $m = C2 \cdot K^{-1} \pmod{P}$.

Рисунок 5 иллюстрирует шаги описанного выше алгоритма.

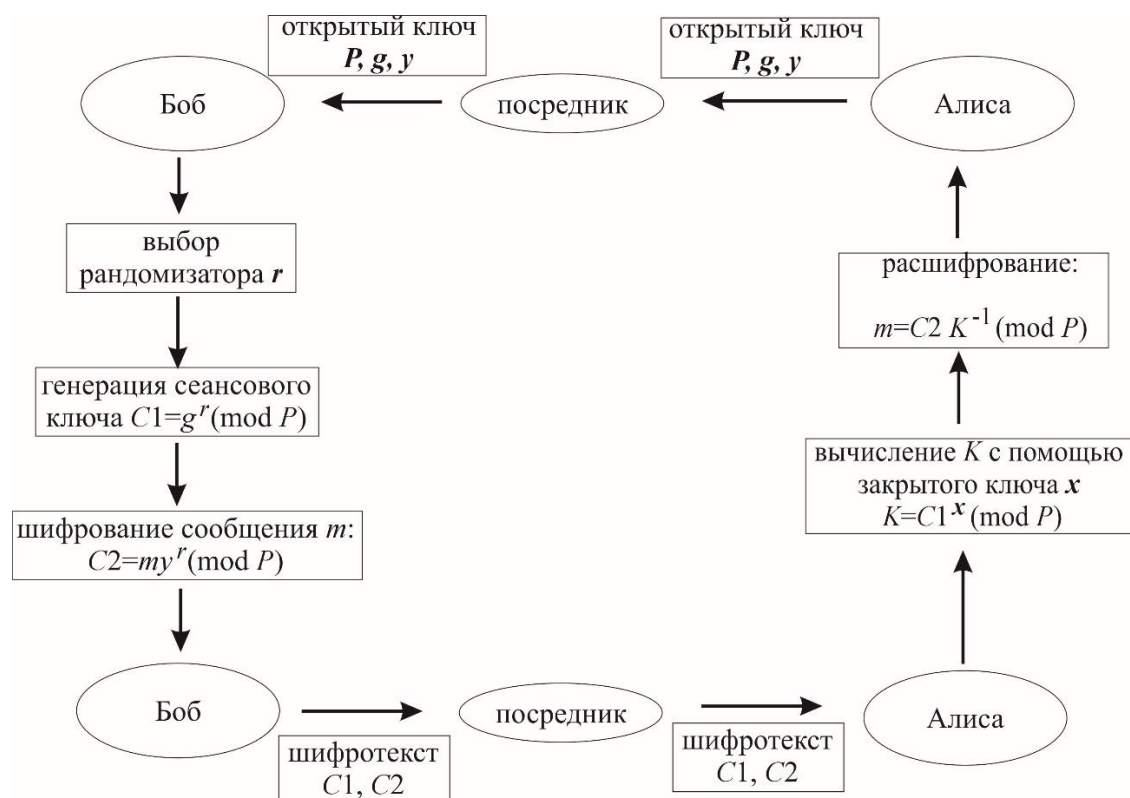


Рис. 5. Схема передачи сообщения с помощью криптосистемы Эль-Гамала

Обоснование криптосистемы Эль-Гамала

Покажем, что указанная процедура шифрования задает корректную и однозначную передачу данных и их расшифрование.

Докажем, что $C2 \cdot K^{-1} \pmod{P} = m$.

Действительно, так как $C1 = g^r \pmod{P}$, то $K = C1^x = g^{rx} \pmod{P}$ и $K^{-1} = (g^{rx})^{-1} \pmod{P}$. Также подробно преобразуем $C2$: $C2 \equiv my^r \pmod{P} = m(g^x)^r \pmod{P} = mg^{xr} \pmod{P}$. Тогда $C2 \cdot K^{-1} \pmod{P} = mg^{xr} \cdot (g^{rx})^{-1} \pmod{P} = m$.

Пример 3.11. Зашифровать букву «и» с использованием криптосистемы Эль-Гамала.

Вначале поставим в соответствие букве «и» ее порядковый номер в алфавите. Далее создадим ключ и зашифруем по указанному выше алгоритму Эль-Гамала. Шаги создания ключей и процесса шифрования занесем в таблицу 10.

Шифрование при использовании криптосистемы Эль-Гамала

№ шага	Действия	Примечание
1	Произвольно выбираем простое число $P = 587$	Создание ключей
2	Простым перебором находим число $g = 5$ – генератор мультипликативной группы классов вычетов $(\mathbb{Z}/P\mathbb{Z})^*$	
3	Выбираем случайным образом число $x = 269$ закрытый ключ	
4	Находим $y = g^x \pmod{P} = 5^{269} \pmod{587} = 556$	
5	$(P, g, y) = (587, 5, 556)$	
1	Выбираем случайное число $r = 83$	Шифрование
2	Генерируем открытый сеансовый ключ $C1 = g^r \pmod{P} = 5^{83} \pmod{587} = 388$	
3	Вычисляем $y^r \pmod{P} = 556^{83} \pmod{587} = 288$	
4	Шифротекстом сообщения $m = 10$ будет: $C2 \equiv my^r \pmod{P} = 10 \cdot 288 \pmod{587} = 532$	

Таким образом, адресат получит набор их открытого сеансового ключа и самого шифра $(C1, C2) = (388, 532)$.

Несмотря на то, что в рассмотренном примере намеренно использовались небольшие числа, уже на этапе создания открытых ключей потребовалось использовать алгоритмы быстрого возведения в степень.

Подробные примеры алгоритма дешифровки можно изучить в типовых заданиях для лабораторных работ с образцами их решения.

5. Характеристики криптосистемы Эль-Гамала

Пункт 1 алгоритма шифрования – введение случайного числа (**рандомизатора**) r делает шифр Эль-Гамала *шифром многозначной замены*, в котором одному символу исходного алфавита соответствует не единственная замена, и поэтому для него открытые текст и ключ не определяют шифротекст однозначно. При условии, что для разных сообщений m и m' используются разные рандомизаторы r и r' , даже если взломщику известны m , $C1$, $C2$, он не сможет без знания секретного ключа отыскать m' по $C1'$ и $C2'$, поэтому криптосистема Эль-Гамала относится к *схемам вероятностного шифрования*.

Стойкость криптосистемы Эль-Гамала основана на сложности задачи дискретного логарифмирования: решения уравнения $y = g^x \pmod{P}$ в мультипликативной группе $(\mathbb{Z}/P\mathbb{Z})^*$ относительно x , где g – генератор мультипликативной группы $(\mathbb{Z}/P\mathbb{Z})^*$. Наиболее очевидный способ – способ простого перебора x до

тех пор, пока не получим значения x , удовлетворяющего уравнению. Для больших n этот способ не эффективен и применяется редко. Существуют другие, более быстрые алгоритмы решения этого уравнения (алгоритм «малый шаг – большой шаг», p -алгоритм Полларда, алгоритм Полига – Хеллмана, см. [1]), однако есть предположение, что не существует полиномиального алгоритма решения проблемы дискретного логарифма. Считается, что задача дискретного логарифма практически не решается, если P содержит не менее 150 десятичных знаков. Рекомендуется также, чтобы $P - 1$ содержало большой простой делитель.

Криптосистема Эль-Гамала может быть обобщена для применения в любой конечной циклической группе G . Пример еще одной циклической группы, в которой используется криптосистема Эль-Гамала, будет приведен в модуле 5 «Конечные поля».

Недостатком схемы шифрования Эль-Гамала является удвоение длины зашифрованного текста по сравнению с начальным текстом. Кроме того, криптосистема Эль-Гамала не является стойкой к атакам на основе подобранного шифротекста. Тем не менее эта криптосистема входит в гибридные криптосистемы, где используется для шифрования ключа, с помощью которого само сообщение шифруется в симметричной криптосистеме.

ТИПОВЫЕ ЗАДАНИЯ ПО ТЕМЕ «ИСТОРИЧЕСКИЕ И СОВРЕМЕННЫЕ КРИПТОСИСТЕМЫ» С ОБРАЗАЦАМИ РЕШЕНИЙ¹

Задание 1. Дешифровать криптотекст RSA (n, e, c) , где n – модуль, e – открытая экспонента, c – шифр: а) $(n = 253, e = 13, c = 179)$; б) $(n = 4116037, e = 451737, c = 833207)$. При переводе натурального числа в текст полагать, что каждая буква задается своим двузначным номером в русском алфавите: «а» – 01, «б» – 02 и т. д. (см. приложение 1).

Решение

а) Для дешифрования криптотекста $(n = 253, e = 13, c = 179)$ необходимо возвести шифр c в степень секретной экспоненты d по модулю n . Поскольку в данной задаче не указана скрытая экспонента, то алгоритм дешифрования включает дополнительные шаги по ее нахождению.

Реализация алгоритма дешифрования.

1. Найдем каноническое разложение числа n (модуля): $n = 253 = 11 \cdot 23$. **Замечание:** схема шифрования RSA требует, чтобы каноническое разложение числа n содержало только два простых множителя.

2. Вычисляем функцию Эйлера от модуля n : $\varphi(n) = \varphi(253) = \varphi(11 \cdot 23) = (11-1) \cdot (23-1) = 220$.

3. Найдем скрытую экспоненту d как число, обратное к открытой экспоненте $e=13$ в ее числовом сравнении по модулю $\varphi(n) = 220$:

$$d = e^{-1}(\bmod \varphi(n)) \Leftrightarrow \bar{d} = \bar{e}^{-1} \text{ в кольце классов вычетов } \mathbb{Z}/\varphi(n)\mathbb{Z}.$$

Для отыскания обратного класса воспользуемся соотношением Безу для взаимно простых чисел $e = 13$ и $\varphi(n) = 220$:

$$\text{НОД}(220, 13) = 1 = 221 - 220 = 220 \cdot (-1) + 13 \cdot 17.$$

В данном случае коэффициенты соотношения Безу легко подбираются, но в общем случае можно воспользоваться расширенным алгоритмом Евклида. Тогда классом, обратным к классу $\bar{13}$ в кольце классов вычетов $\mathbb{Z}/220\mathbb{Z}$, является класс $\bar{17}$ (см. модуль 1), а скрытая экспонента $d = 17$.

4. Возведем шифр $c = 179$ в степень скрытой экспоненты $d = 17$ по модулю $n = 253$, чтобы получить зашифрованное число m :

$$m = 179^{17}(\bmod 253).$$

Возведение в семнадцатую степень проведем с помощью бинарного метода справа налево, раскладывая 17 по степеням двойки:

$$179^2 = 32041 \equiv 163(\bmod 253),$$

$$179^4 \equiv 163^2 = 26569 \equiv 4(\bmod 253),$$

¹ В данном разделе приводится подробное решение заданий по криптосистемам RSA и Эль-Гамала (задачи 5 и 6 в индивидуальном варианте лабораторной работы). Принципы шифрования и расшифровки шифротекста историческими криптосистемами (задачи 1–4 в индивидуальном варианте лабораторной работы) подробно проиллюстрированы в разделе «Теоретические сведения» этого модуля.

$$179^8 \equiv 16 \pmod{253},$$

$$179^{16} \equiv 16^2 = 256 \equiv 3 \pmod{253},$$

$$179^{17} = 179^{16+1} = 179^{16} \cdot 179 \equiv 3 \cdot 179 = 537 \equiv 31 \pmod{253}.$$

Таким образом, зашифрованное число $m = 31$, что соответствует букве «э» русского алфавита. ▲

б) Для дешифрования сообщения ($n = 4116037$, $e = 451737$, $c = 833207$), созданного алгоритмом RSA, действуем аналогично пункту «а».

1. Найдем каноническое разложение модуля n : $n = 4116037 = 1367 \cdot 3011$.

2. Вычислим функцию Эйлера от модуля n :

$$\varphi(n) = \varphi(4116037) = \varphi(1367 \cdot 3011) = (1367 - 1) \cdot (3011 - 1) = 4111660.$$

3. Найдем скрытую экспоненту d – число, обратное по модулю $\varphi(n) = 4111660$ к открытой экспоненте e , используя расширенный алгоритм Евклида (подробные вычисления алгоритма опускаем): $d = 3870733$.

4. Возведем шифр $c = 833207$ в степень скрытой экспоненты $d = 3870733$ по модулю $n = 4116037$, чтобы получить зашифрованное число m :

$$m = 833207^{3870733} \pmod{4116037}.$$

Возведение большого основания в большую степень способом, указанным в пункте «а», становится неэффективным. Поэтому применим китайскую теорему об остатках и CRT-представление чисел c и m по модулю n .

Опишем поэтапно последующие действия:

4.1. Найдем CRT-разложение основания $c = 833207$. Для этого вычислим остатки от деления $c = 833207$ на числа $p = 1367$ и $q = 3011$ – делители модуля $n = 4116037$, найденные на первом шаге алгоритма:

$$833207 \equiv 704 \pmod{1367}, 833207 \equiv 2171 \pmod{3011}.$$

Тогда CRT-разложение $833207 \leftrightarrow (704, 2171)$.

4.2 Найдем CRT-представление зашифрованного числа m . По свойствам CRT-представления

$$833207^{3870733} \pmod{4116037} \leftrightarrow (704^{3870733}, 2171^{3870733}).$$

Задача упрощается не только благодаря тому, что необходимо возводить в степень меньшие основания, но и за счет того, что возведение в степень каждой координаты CRT-представления проводится по простому модулю, меньшему степени (первая координата по модулю $p = 1367$, вторая по модулю $q = 3011$). Следовательно, можно использовать малую теорему Ферма $a^{p-1} \equiv 1 \pmod{p}$ и учесть, что

$$704^{1366} \equiv 1 \pmod{1367}, \text{ и } 2171^{3010} \equiv 1 \pmod{3011}.$$

Вычислим остатки от деления степени 3870733 на 1366 и 3010:

$$3870733 = 855 \pmod{1366}, 3870733 = 2883 \pmod{3010}.$$

Тогда

$$704^{3870733} = 704^{1366 \cdot m_1 + 855} = (704^{1366})^{m_1} \cdot 704^{855} \equiv 1 \cdot 704^{855} \pmod{1367};$$

$$2171^{3870733} = 2171^{3010 \cdot m_2 + 2883} = (2171^{3010})^{m_2} \cdot 2171^{2883} \equiv 1 \cdot 2171^{2883} \pmod{3011}.$$

Теперь приступим к возведению в степень, используя алгоритм быстрого возведения в степень (бинарный метод справа налево), для чего вычислим сравнения для показателей степеней вида 2^k : $704^{2^k} \equiv a \pmod{1367}$, $2171^{2^k} \equiv b \pmod{3011}$. Результаты вычислений представим в таблицах:

Степень числа 704	Результат сравнения по модулю 1367
2	762
4	1036
8	201
16	758
32	424
64	699
128	582
256	1075
512	510

Степень числа 2171	Результат сравнения по модулю 3011
2	1026
4	1837
8	2249
16	2532
32	605
64	1694
128	153
256	2332
512	358
1024	1702
2048	222

Такие таблицы легко рассчитать, например, в Excel, так как на каждом шаге заполнения строки второго столбца достаточно вычислить остаток от деления квадрата предыдущей ячейки этого же столбца на нужный модуль, например для вычисления $704^{16} \pmod{1367}$ учитываем, что $704^8 \equiv 201 \pmod{1367}$, тогда $704^{16} = (704^8)^2 \equiv 201^2 \pmod{1367}$. Теперь, используя свойства сравнений и представляя каждый показатель степени как сумму степеней двойки, легко выполним возведение:

$$704^{855} = 704^{512+256+64+16+4+2+1} = 704^{512} \cdot 704^{256} \cdot 704^{64} \cdot 704^{16} \cdot 704^4 \cdot 704^2 \cdot 704 \equiv \\ \equiv 510 \cdot 1075 \cdot 699 \cdot 758 \cdot 1036 \cdot 762 \cdot 704 \pmod{1367}.$$

В этом выражении каждую степень числа 704 заменили на сравнимое с ней число из первой таблицы. Таким образом, вычислив остаток от деления последнего произведения на 1367, получим

$$704^{855} \equiv 1229 \pmod{1367}.$$

Аналогичным способом используя вторую таблицу, вычислим $2171^{2883} \pmod{3011}$:

$$2171^{2883} = 2171^{2048+512+256+64+2+1} = 2171^{2048} \cdot 2171^{512} \cdot 2171^{256} \cdot 2171^{64} \cdot 2171^2 \cdot 2171 \equiv \\ \equiv 222 \cdot 358 \cdot 2332 \cdot 1694 \cdot 1026 \cdot 2171 \pmod{3011} \equiv 2238 \pmod{3011}.$$

Теперь имеем CRT-представление зашифрованного числа m :

$$833207^{3870733} \pmod{4116037} \leftrightarrow (1229, 2238).$$

4.3. Восстановим число m по его CRT-представлению. Для этого необходимо решить систему из двух сравнений:

$$\begin{cases} m \equiv 1229 \pmod{1367}, \\ m \equiv 2238 \pmod{3011}. \end{cases}$$

Ее можно решать общим методом Гаусса, но для частного случая системы из двух сравнений со взаимно простыми модулями целесообразно использовать

формулы Гарнера: если m – решение системы $\begin{cases} m \equiv a \pmod{p}, \\ m \equiv b \pmod{q}, \end{cases}$

то $m = ((b - a)(p^{-1} \pmod{q}) \pmod{q})p + a$ или $m = ((a - b)(q^{-1} \pmod{p}) \pmod{p})q + b$.

Воспользуемся первой из этих формул при $a = 1229$, $b = 2238$, $p = 1367$, $q = 3011$. Предварительно вычислив с помощью расширенного алгоритма Евклида $p^{-1} \pmod{q} = 1367^{-1} \pmod{3011} = 2174$, получим:

$$m = ((2238 - 1229) \cdot 2174) \pmod{3011} \cdot 1367 + 1229 = 1558 \cdot 1367 + 1229 = 2131015$$

Переведем число в текст, учитывая, что каждой букве ставится в соответствие ее двузначный номер в русском алфавите. Так как число m содержит нечетное число знаков, то припишем в его начале 0:

02 13 10 15 → «блин».

Таким образом, после дешифрования мы получили сообщение «блин». ▲

Задание 2. Дешифровать криптотекст Эль-Гамала $(P, g, y, C1, C2)$, где P – простое число, g – генератор мультипликативной группы $(\mathbb{Z}/P\mathbb{Z})^*$, $y = g^x$ – открытый ключ, $C1$ – открытый сеансовый ключ, $C2$ – шифр:

а) $(P = 29, g = 2, y = 18, C1 = 14, C2 = 12)$;

б) $(P = 521, g = 3, y = 165, C1 = 358, C2 = 502)$.

При переводе натурального числа в текст полагать, что каждая буква задается своим двузначным номером в русском алфавите: «а» – 01, «б» – 02 и т. д. (см. приложение 1).

Решение

Заметим, что в обоих случаях неизвестен скрытый ключ x , поэтому в алгоритм дешифрования включим этапы его нахождения.

а) Пусть дан криптотекст Эль-Гамала $(P = 29, g = 2, y = 18, C1 = 14, C2 = 12)$.

Опишем поэтапно последующие действия его дешифрования:

1. Для того чтобы определить скрытый ключ, решим сравнение $g^x \equiv y \pmod{P}$: $2^x \equiv 18 \pmod{29}$.

В данном примере несложно перебрать все степени двойки по модулю 29, до тех пор, пока не получим верное сравнение при $x = 11$.

2. Вычислим $C1^x \pmod{P} = g^{rx} \pmod{P}$:

$$14^{11} = 14^8 \cdot 14^2 \cdot 14 \equiv 22 \cdot 23 \cdot 14 \pmod{29} \equiv 8 \pmod{29}.$$

Здесь, как и в задании 1, был использован алгоритм быстрого возведения в степень.

3. Вычислим $(C1^x)^{-1} \pmod{P}$, используя расширенный алгоритм Евклида:

$$8^{-1} \pmod{29} = 11.$$

4. Найдем зашифрованное число $m = C2 \cdot (C1^x)^{-1} \pmod{P}$:

$$m = 12 \cdot 11 \pmod{29} \Rightarrow m = 16.$$

Таким образом, зашифрованным сообщением является число 16, соответствующее букве «о». ▲

Δ б) Пусть дан криптотекст Эль-Гамала ($P = 521$, $g = 3$, $y = 165$, $C1 = 358$, $C2 = 502$).

Опишем поэтапно последующие действия его дешифрования:

1. Для отыскания скрытого ключа x решаем сравнение $3^x \equiv 165 \pmod{521}$.

Решать его простым перебором можно с помощью простого алгоритма, реализованного, например, в системе компьютерной алгебры Wolfram Mathematica или на любом языке программирования. Алгоритм заключается в следующем.

ВХОД. Ввод данных. Основание – натуральное число g , простой модуль p , натуральное число a .

Тело алгоритма.

1. $i = 1$; $b = g$.

2. Пока $b \neq a$ выполнять следующее:

2.1 $b = b \cdot g \pmod{p}$;

2.2 $i = i + 1$;

3. Вернуть i .

ВЫХОД. Вывод данных. Степень i такая, что $g^i \equiv a \pmod{p}$.

Этот алгоритм основан на использовании свойства сравнений: если $b^k \equiv l \pmod{p}$, то $b^k \cdot b \equiv l \cdot b \pmod{p}$.

Применив этот алгоритм, находим $x = 351$. Остальные шаги дешифрования проводим аналогично пункту «а».

2. Вычислим $C1^x \pmod{P} = g^{rx} \pmod{P}$:

$$358^{351} = 358^{256} \cdot 358^{64} \cdot 358^{16} \cdot 358^8 \cdot 358^4 \cdot 358^2 \cdot 358 \equiv 33 \pmod{521}.$$

3. Вычислим $(C1^x)^{-1} \pmod{P}$, используя расширенный алгоритм Евклида:

$$33^{-1} \pmod{521} = 300.$$

4. Найдем зашифрованное число $m = C2 \cdot (C1^x)^{-1} \pmod{P}$:

$$m = 502 \cdot 300 \pmod{521} \Rightarrow m = 31.$$

Таким образом, зашифрованным сообщением является число 31, соответствующее букве «э». ▲

ТЕСТ ДЛЯ САМОПРОВЕРКИ ПО ТЕМЕ «ИСТОРИЧЕСКИЕ И СОВРЕМЕННЫЕ КРИПТОСИСТЕМЫ»

Вопрос 1. Установить соответствие между названием способа шифрования и его характеристиками. Ответ записать в виде сочетания букв и цифр, соблюдая алфавитную последовательность букв. Некоторые данные правого столбца могут использоваться несколько раз или не использоваться вообще.

Способ шифрования	Характеристика
А. Шифр Цезаря	1) При дешифровке используется возведение шифра в степень закрытого ключа по модулю n .
В. Криптосистема Кардано	2) В качестве ключа используется фраза-девиз, буквы которой подписываются под буквами сообщения.
С. Постолбцовая транспозиция	3) Используется линейное преобразование n -грамм по формуле $\bar{y}_j = T\bar{x}_j \pmod{N}$, где T - матрица, имеющая обратную, N – число букв в алфавите.
Д. Шифр Тригеммы	4) Используется прямоугольный трафарет с вырезами, поворачивая его и выписывая буквы в вырезах, читают зашифрованное сообщение.
Е. Криптосистема Хилла	5) Стойкость криптосистемы основана на сложности проблемы дискретного логарифма.
Ф. Криптосистема RSA	6) Сообщение записывается построчно, при записи шифротекста буквы считывают по столбцам.
Г. Криптосистема Эль-Гамала	7) Замена каждой буквы сообщения на отстоящую от нее по алфавиту на определенное число позиций по циклу

Вопрос 2. Зашифровать с помощью шифра Цезаря первые две строчки белорусского государственного гимна, используя белорусский алфавит (с диграфами «дз», «дж»). Сдвиг подобрать таким образом, чтобы букве исходного сообщения «м» соответствовала буква шифра «з» (знаки препинания опустить).

- А) зф ьажыломф здліфш жчягд
Мцлтыз ыяяытфш лйяіые гшзжд
- В) зф ьвжыломф здзліфш жчядждз
Мцлтыз ыяяыіфш лйяіые джшзждз
- С) зф ьвжыломф здзліфш жчбдз
Мцлтыз ыяяыіфш лйяіые джшзждз

Вопрос 3. Используя криптосистему Тригеммы, расшифровать сообщение «рѐеттцѐм оемфѝысыв» с девизом «земля».

Вопрос 4. Используя постолбцовую транспозицию, расшифровать четверостишие известного белорусского поэта «пгііўяаун юнгчжніа мпаеогіат асло-
кюдеі жцхчодем знўславкп яагътгън анаакаліс кзянііряй шжщтімяо
ўмільычмл іекмсасле». Порядок считывания букв в ряде может меняться от
столбца к столбцу.

Вопрос 5. Зная исходное сообщение «каждая мелочь важна» и зашифрованное с помощью криптосистемы Кардано «олье амба ячнл жюва», выбрать решетку, которую использовали при шифровании.

A)

О	О	Х	О
О	Х	О	О
О	О	О	О
Х	О	Х	О

B)

О	О	О	О
Х	О	О	Х
О	Х	О	О
О	О	О	Х

C)

О	Х	О	О
Х	О	О	Х
О	Х	О	О
О	О	О	Х

D)

Х	О	О	О
О	О	Х	О
О	О	О	Х
О	О	О	Х

Вопрос 6. Расшифровать методом Хилла сообщение «ау», если линейное преобразование задается матрицей $T = \begin{pmatrix} 9 & 2 \\ 7 & 3 \end{pmatrix}$.

A) ьм;

B) рг;

C) щп;

D) гр;

E) мь.

Вопрос 7. Установить верный порядок действий при создании ключей и шифрования в криптосистеме RSA. Ответ привести в виде последовательности букв, например AFCDBE.

- A) Выбрать случайное число e – открытую экспоненту.
- B) Найти модуль $n = pq$.
- C) Найти секретную экспоненту.
- D) Вычислить функцию Эйлера $\varphi(n)$.
- E) Шифрование сообщения m : $c = m^e \pmod{n}$.
- F) Выбрать произвольные простые числа p и q .

Вопрос 8. CRT-представлением числа 1151^{443} по модулю 2047 является:

- A) (1, 83);
- B) (11, 51);
- C) (1, 51);
- D) (83, 51).

Вопрос 9. Установить верный порядок действий при создании ключей и шифрования в криптосистеме Эль-Гамала. Ответ приведите в виде последовательности букв, например AFCDBE.

- A) Выбрать случайным закрытый ключ.
- B) Сгенерировать открытый сеансовый ключ $C1$ и найти число $y^r \pmod{P}$.
- C) Выбрать произвольное достаточно большое простое число P .
- D) Найти число $y = g^x \pmod{P}$.
- E) Выбрать случайное число r .
- F) Зашифровать сообщение m по формуле $C2 \equiv my^r \pmod{P}$.
- G) Найти генератор мультипликативной группы классов вычетов $(\mathbb{Z}/P\mathbb{Z})^*$.

Вопрос 10. Характеристикой криптосистемы Эль-Гамала НЕ является:

- A) Шифр Эль-Гамала – шифр многозначной замены.
- B) Стойкость криптосистемы основана на проблеме дискретного логарифма.
- C) Криптосистема может быть адаптирована для любой конечной циклической группы.
- D) Для шифрования и дешифровки сообщений нет необходимости в алгоритмах быстрого возведения в степень.

Ключ к тесту:

<i>Номер вопроса</i>	<i>Ответ</i>
1	<i>A7B4C6D2E3F1G5</i>
2	<i>C</i>
3	<i>зачётная ведомость</i>
4	<i>М. Багдановіч «Паміж няскоў Егіпецкай зямлі...»</i>
5	<i>C</i>
6	<i>A</i>
7	<i>FBDACE</i>
8	<i>B</i>
9	<i>CGADEBF</i>
10	<i>D</i>

ИНДИВИДУАЛЬНЫЕ ЗАДАНИЯ ДЛЯ ЛАБОРАТОРНОЙ РАБОТЫ № 3 «ИСТОРИЧЕСКИЕ И СОВРЕМЕННЫЕ КРИПТОСИСТЕМЫ»

1. Расшифровать сообщение на белорусском, русском или английском языке, зашифрованное указанным шифром маршрутизации.

2. Расшифровать сообщение с девизом: расшифровать криптотекст на белорусском, русском или английском языке, используя криптосистему Тритемиуса.

3. Дешифровать криптотекст на белорусском, русском или английском языке, используя криптосистему Кардано и симметричные отражения решетки относительно средних линий.

4. Расшифровать сообщение, зашифрованное методом Хилла, при условии, что линейное преобразование задается матрицей T :

Варианты 1–7: матрица $T = \begin{pmatrix} 18 & 16 \\ 9 & 1 \end{pmatrix}$, нумерация букв русского алфавита

начинается с единицы, тридцать четвертый символ – это пробел, тридцать пятый – восклицательный знак, тридцать шестой – вопросительный знак, а тридцать седьмой – точка (т. е. вычисления проводить по $\text{mod } 37$);

Варианты 8–15: ключевая матрица $T = \begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix}$, нумерация букв белорусского алфавита начинается с 1, тридцать третий символ – апостроф, тридцать четвертый – гэта пробел, тридцать пятый – клічнік, тридцать шестой – пыталнік, а тридцать седьмой – кропка (гэта значыць вылічэнні праводзіць па $\text{mod } 37$).

5. Дешифровать криптотекст RSA (n, e, c), где n – модуль, e – открытая экспонента, c – шифр. В отчете привести результаты каждого шага алгоритма расшифровки по образцу решений типовых задач. В пункте «б» подробно описать применение китайской теоремы об остатках: CRT-представление чисел, алгоритм быстрого возведения в степень.

6. Дешифровать криптотекст Эль-Гамала ($P, g, y, C1, C2$), где P – простое число, g – генератор мультипликативной группы $(\mathbb{Z}/P\mathbb{Z})^*$, $y = g^x$ – открытый ключ, $C1$ – открытый сеансовый ключ, $C2$ – шифр. В отчете привести результаты каждого шага алгоритма расшифровки по образцу решений типовых задач. В пункте «б» указать использованный способ нахождения ключа.

В заданиях № 5 и № 6 при использовании онлайн-ресурсов для расчетов указать использованный ресурс; при реализации алгоритмов быстрого возведения в степень и (или) использовании китайской теоремы об остатках на каком-либо языке программирования или в системах компьютерной алгебры к отчету приложить листинг программы.

Вариант 1

1. ОТКСЯ СДЎТЗ РДІ ЫДЫГ Е ДЗЛМС ЖІСМГПАСЯ ХЁТЎ М ЖБХЯ ХЁТЎ РТЁД (шифр Цезаря, белорусский алфавит, сдвиг на + 4 буквы).

2. Девиз: ANNE BRONTE

PPSFWLXTOQBWRKWDACZLSOQJ (английский язык).

3. Решетка Кардано

X			
X		X	
			X
		X	
	X		

ЛИЫАЮА ЕОНПД ИШСОПР ИБЫПАН (русский язык).

4. Бхесу.фцц (последний символ - пробел).

5. Расшифровать криптотекст RSA (n , e , c):

а) $n = 91$; $e = 5$; $c = 5$;

б) $n = 1269083$; $e = 19$; $c = 505509$.

6. Расшифровать криптотекст Эль-Гамала (P , g , y , $C1$, $C2$):

а) $P = 41$; $g = 7$; $y = 38$; $C1 = 20$; $C2 = 16$;

б) $P = 547$; $g = 5$; $y = 24$; $C1 = 34$; $C2 = 202$.

Вариант 2

1. БХТ СІ УДЁДКДІ ЎТЗСЦЬ РТЁЦ СІ УДЁДКДІ ЎТЗСЯ СДЎТЗ
(шифр Цезаря, белорусский алфавит, сдвиг на + 4 буквы).

2. Девиз: АГОНЬ

ШЯБРЛЮАВОЮБОПДМЁЭКРМГЎ (белорусский язык).

3. Решетка Кардано (симметричные отражения)

		X	X
X		X	

ННДЕ АОТУ МТАТ НННС (английский язык).

4. Лэкащпгф амжмлёсьлсея!ёхё

5. Расшифровать криптотекст RSA (n , e , c):

а) $n = 85$; $e = 7$; $c = 5$;

б) $n = 366257$; $e = 1331$; $c = 346552$.

6. Расшифровать криптотекст Эль-Гамала (P , g , y , $C1$, $C2$):

а) $P = 137$; $g = 5$; $y = 77$; $C1 = 92$; $C2 = 108$;

б) $P = 599$; $g = 7$; $y = 262$; $C1 = 182$; $C2 = 332$.

Вариант 3

1. ИКЙПЮ ЯФР ОЕПРДЖПКЖ (шифр Цезаря, русский алфавит, сдвиг на +2 буквы).

2. Девиз: БУСЕЛ

ЫПДЗЫПЎСЙЎАФТЯЗТХВУЗБЕСЧЗ (белорусский язык).

3. Решетка Кардано (симметричные отражения)

		X	
	X		X
X			

ЕОУС HNAR AIBT MESN (английский язык)

4. Еайъкашнжтфуеё

5. Расшифровать криптотекст RSA (n, e, c)

а) $n = 221; e = 11; c = 70$;

б) $n = 573449; e = 19687; c = 61303$.

6. Расшифровать криптотекст Эль-Гамала ($P, g, y, C1, C2$)

а) $P = 149; g = 3; y = 101; C1 = 137; C2 = 83$;

б) $P = 541; g = 2; y = 33; C1 = 308; C2 = 441$.

Вариант 4

1. LURRUC ZNK HRGIQ IRUGQ (шифр Цезаря, английский алфавит, сдвиг на +6 букв).

2. Девиз: БУРАК

ЙХХСГФЭРМСППШОЎЙІКЪЭДДАЬ (белорусский язык).

3. Решетка Кардано

X			
	X		X
		X	

WHGD TEET RENA UACT (английский язык).

4. Еб.уёу к?лоф

5. Расшифровать криптотекст RSA (n, e, c):

а) $n = 33; e = 17; c = 19$;

б) $n = 16074587; e = 17; c = 814279$.

6. Расшифровать криптотекст Эль-Гамала ($P, g, y, C1, C2$):

а) $P = 23; g = 5; y = 10; C1 = 16; C2 = 7$;

б) $P = 577; g = 7; y = 381; C1 = 343; C2 = 431$.

Вариант 5

1. ОТ ZNK ZUCKX ОТ ZNK KGYZ UL ZNK LUXKYZ (шифр Цезаря, английский алфавит, сдвиг на + 6 букв).

2. Девиз: ЗИМНЕЕ УТРО

ХШЮЭНОЁВЭЭЯОСУУВЛЖХФЪЧИШ (русский язык).

3. Решетка Кардано

X			
	X		X
		X	

SOIE TOWG LMNA RVEE (английский язык).

4. рфнъызфщч(первый символ – пробел).

5. Расшифровать криптотекст RSA (n, e, c):

а) $n = 77; e = 53; c = 4$;

б) $n = 10419203; e = 29581; c = 8966261$.

6. Расшифровать криптотекст Эль-Гамала ($P, g, y, C1, C2$):

а) $P = 79; g = 3; y = 6; C1 = 8; C2 = 6$;

б) $P = 563; g = 5; y = 95; C1 = 25; C2 = 158$.

Вариант 6

1. FHYDER KV DSHYDER (аффинная система подстановок Цезаря, английский алфавит, $a = 3, b = 5, m = 26$).

2. Девиз: ПАРУС

ТУЕБТЮЁЮГГПДААЁСПЮ (русский язык).

3. Решетка Кардано

	X		X
X	X		

EUIA FRRE SRTT AECS (английский язык).

4. Жжы.ъычьфму

5. Расшифровать криптотекст RSA (n, e, c):

а) $n = 65; e = 43; c = 62$;

б) $n = 2462491; e = 1361; c = 1699797$.

6. Расшифровать криптотекст Эль-Гамала ($P, g, y, C1, C2$):

а) $P = 97; g = 5; y = 8; C1 = 29; C2 = 74$;

б) $P = 631; g = 3; y = 536; C1 = 98; C2 = 353$.

Вариант 7

1. MDQR TDKA SV ERXERKH (аффинная система подстановок Цезаря, английский алфавит, $a = 3, b = 5, m = 26$).

2. Девиз: ПОСЛУШАЙТЕ

ТФИЩКМУЫЗЦЧЗЫЩЗУЦЁОВ (русский язык).

3. Решетка Кардано

X		X	
		X	X

ГООМ ПДХЯ ОМДО РИАТ (русский язык).

4. Июхинюслв!с?у.

5. Расшифровать криптотекст RSA (n, e, c):

а) $n = 91; e = 67; c = 50$;

б) $n = 747749; e = 4229; c = 653148$.

6. Расшифровать криптотекст Эль-Гамала ($P, g, y, C1, C2$):

а) $P = 103; g = 11; y = 15; C1 = 83; C2 = 64$;

б) $P = 523; g = 2; y = 298; C1 = 128; C2 = 175$.

Вариант 8

1. БИ КЫЃЁЩХ ОЭКЕЪЧ ЛНЯЪ ЖЗНИЫНЧ (аффинная система подстановок Цезаря, русский алфавит $a = 2, b = 4, m = 33$).

2. Девиз: РОЗА

ЯПМРСАСЗЦЬЦЁТЮЪЙЯФН (русский язык).

3. Решетка Кардано

	X		
X		X	
			X

ЗТЛИ ЧЕНТ НОИС УЖЪМ (русский язык).

4. Юлкпйяюхдюїчжха

5. Расшифровать криптотекст RSA (n, e, c):

а) $n = 51; e = 7; c = 4$;

б) $n = 10262017; e = 1523; c = 8071402$.

6. Расшифровать криптотекст Эль-Гамала ($P, g, y, C1, C2$):

а) $P = 127; g = 7; y = 89; C1 = 119; C2 = 19$;

б) $P = 661; g = 2; y = 358; C1 = 512; C2 = 395$.

Вариант 9

1. ILUWDWJ GUWO TU DQOQT QR TLW KUJRPQG CMTO IQOWFS (аффинная система подстановок Цезаря, английский алфавит, $a = 5, b = 3, m = 26$).

2. Девиз: ОСЕНЬ

ВЫЫЭЯЖТЯУЙЮЦМУЯФЮЕ (русский язык).

3. Решетка Кардано

X		X			
X					
	X	X			
	X				

АНІВ АСАА ЯЛЦА РЕАШ СЛІВЕ ЫЦАЧ (белорусский язык).

4. ‘я.зхр’еудзк?эір

5. Расшифровать криптотекст RSA (n, e, c):

а) $n = 33; e = 13; c = 29$;

б) $n = 39367961; e = 1231; c = 31039931$.

6. Расшифровать криптотекст Эль-Гамала ($P, g, y, C1, C2$):

а) $P = 139; g = 2; y = 128; C1 = 65; C2 = 63$;

б) $P = 587; g = 5; y = 375; C1 = 568; C2 = 56$.

Вариант 10

1. В ЯДФПЫ ЫАЁБЗЬ ЯБ ГБИНЕВЫ З ЯНП ЗНЕК (аффинная система подстановок Цезаря, русский алфавит $a = 2, b = 4, m = 33$).

2. Девиз: WILDE

XWAQSFKGWFZAAWXQQQFWFMSI (английский язык).

3. Решетка Кардано

		X	X
	X		
X		X	
			X

МНЧПЎЎ АСЫКРН ЛСААОА ЕЫПОДЎ (белорусский язык).

4. Пбябс?’лкйфр’бо фрюх

5. Расшифровать криптотекст RSA (n , e , c):

а) $n = 65$; $e = 29$; $c = 10$;

б) $n = 11258129$; $e = 29411$; $c = 11158209$.

6. Расшифровать криптотекст Эль-Гамала (P , g , y , $C1$, $C2$):

а) $P = 29$; $g = 2$; $y = 3$; $C1 = 6$; $C2 = 9$;

б) $P = 521$; $g = 7$; $y = 414$; $C1 = 217$; $C2 = 501$.

Вариант 11

1. ВРЕЛ СОДЮ ЕГУД ДИТЯ ОВКМ (постолбцовая транспозиция).

2. Девиз: SHAKESPEARE

ТТМWTЛІІTSWXZFДУННJESSWAPCWHMХFFІ (английский язык).

3. Решетка Кардано

	X		X
X	X		

ДКУА ГІШН ЗОЕМ ЛКВЬ (белорусский язык).

4. Эфбъаооелктьдлх (апошні сімвал – прабел).

5. Расшифровать криптотекст RSA (n , e , c):

а) $n = 143$; $e = 23$; $c = 109$;

б) $n = 29246011$; $e = 105623$; $c = 7507944$.

6. Расшифровать криптотекст Эль-Гамала (P , g , y , $C1$, $C2$):

а) $P = 53$; $g = 5$; $y = 43$; $C1 = 25$; $C2 = 2$;

б) $P = 673$; $g = 11$; $y = 219$; $C1 = 204$; $C2 = 631$.

Вариант 12

1. ТИЯЯ ЫВИБ ЭТНЕ ТСЕТ ОЙТО ТЕДГ ВДРО ОИУГ (постолбцовая транспозиция).

2. Девиз: BYRON

VGWLWURVVOTLSZR (английский язык).

3. Решетка Кардано

	X		
X		X	
			X

ЬМНЛ ЗВНЕ АОУЯ СОАГ (белорусский язык).

4. Йшп!мцовзккп?тдддэёуь.

5. Расшифровать криптотекст RSA (n , e , c):

а) $n = 55$; $e = 37$; $c = 9$;

б) $n = 11086213$; $e = 65537$; $c = 7264383$.

6. Расшифровать криптотекст Эль-Гамала (P , g , y , $C1$, $C2$):

а) $P = 61$; $g = 7$; $y = 22$; $C1 = 38$; $C2 = 54$;

б) $P = 659$; $g = 7$; $y = 542$; $C1 = 528$; $C2 = 376$.

Вариант 13

1. ДОТ ЕВВ ЛЕО АРЕ ЙНЙ ТОД ОДУ ЧЛШ ТЯИ (постолбцовая транспозиция).

2. Девиз: KIPLING

ZWUYJBRYJTXIZLWTEXZVXXDEJMZ (английский язык).

3. Решетка Кардано

X	X		
	X		X

ААНІ ТЯЕК НААЦ АНСР (белорусский язык).

4. Ршыш'я'шхмхажу

5. Расшифровать криптотекст RSA (n , e , c):

а) $n = 77$; $e = 53$; $c = 64$;

б) $n = 2041951$; $e = 1423$; $c = 37170$.

6. Расшифровать криптотекст Эль-Гамала (P , g , y , $C1$, $C2$):

- а) $P = 59$; $g = 11$; $y = 2$; $C1 = 44$; $C2 = 58$;
 б) $P = 691$; $g = 3$; $y = 220$; $C1 = 114$; $C2 = 186$.

Вариант 14

1. PTAR! ETEHU WENHG AEEBO LRGVL LIDIB (построковая транспозиция).
2. Девиз: БРОСЬТЕ
МАЭЧФБФЯДЮАВЕТЖВВО (русский язык).
3. Решетка Кардано

		X	
			X
			X
	X		
	X		
			X

ЫБЕОДЗ ЕЯБВАН ССХБЕЬ АЛАОЛТ (русский язык).

4. Еэь.тэш?нж
5. Расшифровать криптотекст RSA (n , e , c):
 а) $n = 55$; $e = 13$; $c = 13$;
 б) $n = 16305587$; $e = 17863$; $c = 11410057$.
6. Расшифровать криптотекст Эль-Гамала (P , g , y , $C1$, $C2$):
 а) $P = 73$; $g = 5$; $y = 52$; $C1 = 20$; $C2 = 40$;
 б) $P = 569$; $g = 3$; $y = 88$; $C1 = 188$; $C2 = 491$.

Вариант 15

1. #TSUO YNEAE LNNAT SVODV OTHER ITEHN NEBOF (построковая транспозиция).
2. Девиз: СВАЮ КРЫЎДУ
ТЭУНКАХДДЖЖЫЭМЛППШАЛГОАЦЛІ (белорусский язык).

3. Решетка Кардано

X			
X		X	
			X
		X	
	X		

БУЕННМ ЮВИСОМ ЕДИМЁТ ЫМЕДЧЬ (русский язык).

4. Овцебъ гцхеубъйдуд

5. Расшифровать криптотекст RSA (n, e, c):

а) $n = 91; e = 7; c = 67$;

б) $n = 6999737; e = 1283; c = 5900867$.

6. Расшифровать криптотекст Эль-Гамала ($P, g, y, C1, C2$):

а) $P = 89; g = 3; y = 65; C1 = 42; C2 = 63$;

б) $P = 683; g = 5; y = 32; C1 = 599; C2 = 517$.

МОДУЛЬ № 4. КОЛЬЦА. ИДЕАЛЫ КОЛЕЦ

ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ ПО ТЕМЕ «КОЛЬЦА. ИДЕАЛЫ КОЛЕЦ»¹

§ 1. Кольца и идеалы колец

К основным алгебраическим структурам относятся группы, кольца и поля. В модуле 2 рассмотрены основные понятия теории групп. В данном модуле мы изучим кольца, идеалы колец и дадим определение поля.

1. Основные определения

Определение 4.1. *Кольцом* называется непустое множество K , на котором заданы две бинарные алгебраические операции, называемые сложением (+) и умножением ($\cdot$) и удовлетворяющие следующим аксиомам:

1) ассоциативность сложения:

$$\forall a, b, c \in K \text{ верно } (a + b) + c = a + (b + c);$$

2) существование нейтрального элемента относительно сложения:

$\exists e \in K$ такой, что $\forall a \in K$ имеют место равенства $a + e = e + a = a$;

3) существование противоположного элемента:

$$\forall a \in K \exists -a \in K \text{ такой, что } a + (-a) = (-a) + a = e;$$

4) коммутативность сложения:

$$\forall a, b \in K \text{ верно } a + b = b + a;$$

5) дистрибутивность умножения относительно сложения:

$$\forall a, b, c \in K \text{ верно } (a + b) \cdot c = a \cdot c + b \cdot c \text{ и } a \cdot (b + c) = a \cdot b + a \cdot c.$$

Из аксиом 1–4 следует, что всякое кольцо K является абелевой группой относительно сложения. Эта группа называется *аддитивной группой кольца K* , нейтральный элемент которой обозначают 0. Для кольца относительно сложения справедливы все следствия аксиом аддитивной группы, а также к ним добавляются следствия, связанные с операцией умножения:

1. $\forall a \in K$ верно $a \cdot 0 = 0 \cdot a = 0$;

2. $\forall a, b \in K$ верно $a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$;

3. $\forall a, b, c \in K$ верно $(a - b) \cdot c = a \cdot c - b \cdot c$ и $a \cdot (b - c) = a \cdot b - a \cdot c$.

В зависимости от того, какие дополнительные аксиомы выполняются для операции умножения, среди колец выделяются следующие типы:

- **коммутативное кольцо:** $\forall a, b \in K$ верно $a \cdot b = b \cdot a$ – коммутативность умножения;

- **ассоциативное кольцо:** $\forall a, b, c \in K$ верно $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ – ассоциативность умножения;

¹ При подготовке данного раздела использовались следующие источники: [1, 5, 6, 16, 20, 21].

- **кольцо с единицей:** ассоциативное кольцо, в котором существует нейтральный элемент относительно умножения, обозначаемый 1 , такой, что $\forall a \in K$ верно $a \cdot 1 = 1 \cdot a = a$.

В кольце с единицей можно ввести понятие элемента a^{-1} , **обратного к элементу a** .

Определение 4.2. Элемент a^{-1} кольца с единицей называется **обратным к элементу a** , если $a \cdot a^{-1} = a^{-1} \cdot a = 1$. Элемент a является **обратимым**, если существует обратный к нему элемент, и **необратимым** в противном случае.

Пример 4.1. Множества $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ с операциями сложения и умножения являются коммутативными кольцами с единицей. В кольце $\mathbb{Z}$ обратимыми являются только числа 1 и -1 , а в кольцах $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ – все ненулевые элементы.

Пример 4.2. Как было показано в модуле № 1, множество $\mathbb{Z}/m\mathbb{Z}$ классов вычетов по модулю m является коммутативным кольцом с единицей относительно операций сложения и умножения классов вычетов. Обратимыми элементами являются классы вычетов, взаимно простых с модулем.

Пример 4.3. Рассмотрим множество полиномов с действительными коэффициентами:

$\mathbb{R}[x] = \{f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \mid a_i \in \mathbb{R}, i = 0, \dots, n, a_n \neq 0\}$, где n , степень многочлена $f(x)$, будем далее обозначать $n = \deg f(x)$. Это множество образует коммутативное кольцо с единицей относительно стандартных операций сложения и умножения многочленов.

Пример 4.4. Множество квадратных матриц порядка n с элементами из множества действительных чисел $M_n(\mathbb{R})$ образует некоммутативное кольцо с единицей относительно операций сложения и матричного умножения. Обратимыми элементами являются все невырожденные матрицы.

Пример 4.5. Множество свободных векторов пространства $\mathbb{R}^3$ с операциями сложения $\vec{a} + \vec{b}$ и векторного умножения $\vec{a} \times \vec{b}$ образует некоммутативное и неассоциативное кольцо.

Определение 4.3. **Подкольцом L кольца K** называется подгруппа аддитивной группы кольца K , замкнутая относительно операции умножения: $\forall a, b \in L$ имеет место $a \cdot b = c \in L$.

Иными словами, подкольцо L кольца K – это подмножество кольца K , которое само является кольцом относительно операций, заданных в K .

Пример 4.6. Матричное кольцо квадратных матриц второго порядка содержит подкольцо матриц вида $C = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, где $a, b \in \mathbb{R}$. Несложно проверить замкнутость множества матриц такого вида относительно операций сложения и умножения.

Определение 4.4. **Левый идеал J кольца K** – это подкольцо кольца K , такое, что для любого элемента a кольца K его произведение на любой элемент j подкольца J в порядке $a \cdot j$ принадлежит подкольцу J : $\forall a \in K, \forall j \in J \quad a \cdot j \in J$. Иными

словами, подкольцо J является **левым идеалом** кольца K , если для любого элемента a кольца K множество $aJ = \{a \cdot j \mid j \in J\}$ содержится в J : $aJ \subseteq J$. Аналогичным образом определяется **правый идеал** J кольца K : для любого элемента a кольца K множество $Ja = \{j \cdot a \mid j \in J\}$ содержится в J : $Ja \subseteq J$. Если идеал является одновременно левым и правым идеалом, то он называется **двусторонним идеалом** или просто **идеалом**.

Пример 4.7. Исследовать, является ли множество матриц $J = \begin{pmatrix} a & a \\ a & a \end{pmatrix}$ идеалом в кольце матриц $M = \begin{pmatrix} a & b \\ b & a \end{pmatrix}$, где $a, b \in \mathbb{R}$.

Вначале проверим, является ли заданное множество J подгруппой аддитивной группы кольца M . Согласно критерию подгруппы, для этого необходимо и достаточно, чтобы множество J было замкнуто относительно операции сложения и для любого элемента множества J противоположный ему элемент также принадлежал J . Рассмотрим произвольные элементы множества J :

$$A = \begin{pmatrix} a & a \\ a & a \end{pmatrix}; \quad B = \begin{pmatrix} b & b \\ b & b \end{pmatrix}.$$

Их сумма:

$$A + B = \begin{pmatrix} a+b & a+b \\ a+b & a+b \end{pmatrix} \in J.$$

Противоположный A элемент: $-A = \begin{pmatrix} -a & -a \\ -a & -a \end{pmatrix} \in J.$

Таким образом, J является подгруппой аддитивной группы M . Проверим замкнутость множества J относительно операции умножения.

$$AB = \begin{pmatrix} a & a \\ a & a \end{pmatrix} \begin{pmatrix} b & b \\ b & b \end{pmatrix} = \begin{pmatrix} 2ab & 2ab \\ 2ab & 2ab \end{pmatrix} \in J.$$

Так как для любых двух элементов J их произведение также принадлежит J , то J является подкольцом кольца M .

Возьмем произвольный элемент кольца M :

$$C = \begin{pmatrix} c & d \\ d & c \end{pmatrix}$$

и построим множество $CJ = \{CA \mid A \in J\}$. Для произвольного элемента $A \in J$ в результате умножения получим:

$$CA = \begin{pmatrix} c & d \\ d & c \end{pmatrix} \begin{pmatrix} a & a \\ a & a \end{pmatrix} = \begin{pmatrix} a(c+d) & a(c+d) \\ a(d+c) & a(d+c) \end{pmatrix} \in J.$$

Поскольку матрица A была выбрана произвольно, то $\forall A \in J \quad CA \in J$, следовательно, $CJ \subseteq J$. Но так как и матрица C также выбрана произвольно, то

$\forall C \in M \quad CJ \subseteq J$. Тогда согласно определению, множество J является левым идеалом кольца M .

В силу того что при умножении элементов A и C в обратном порядке имеет место

$$AC = \begin{pmatrix} a & a \\ a & a \end{pmatrix} \begin{pmatrix} c & d \\ d & c \end{pmatrix} = \begin{pmatrix} a(c+d) & a(d+c) \\ a(c+d) & a(d+c) \end{pmatrix} \in J,$$

то, рассуждая аналогично, делаем вывод, что множество J является также и правым идеалом, а следовательно, и двусторонним идеалом кольца M .

Несложно показать, что для любого кольца K множества $\{K\}$ и $\{0\}$ являются идеалами. Эти идеалы называются **несобственными или тривиальными**, все остальные – **собственными**.

Теорема 4.1. Для любого элемента a кольца K множество $aK = \{ak | k \in K\}$, состоящее из всевозможных произведений элемента a на элементы кольца K , является правым идеалом кольца K . Для любого элемента a кольца K множество $Ka = \{ka | k \in K\}$ является левым идеалом.

Определение 4.5. Идеалы $aK = \{ak | k \in K\}$ и $Ka = \{ka | k \in K\}$, где $\forall a \in K$, называются соответственно правым и левым **главными идеалами**, или идеалами, **порожденными элементом a** .

Замечание. В коммутативных кольцах всякий идеал, в том числе и главный, является двусторонним.

Главный идеал, порожденный элементом a , будем обозначать также $\langle a \rangle$.

Пример 4.8. В кольце классов вычетов $\mathbb{Z}/4\mathbb{Z}$ построить главные идеалы, порожденные элементами $\bar{2}$ и $\bar{3}$.

Согласно определению, главный идеал $\langle \bar{2} \rangle$ состоит из элементов:

$\bar{2} \cdot \bar{0}; \bar{2} \cdot \bar{1}; \bar{2} \cdot \bar{2}; \bar{2} \cdot \bar{3}$. Выполнив умножение классов вычетов, получим:
 $\langle \bar{2} \rangle = \{\bar{0}, \bar{2}\}$.

Аналогичным образом составим главный идеал $\langle \bar{3} \rangle$:

$\langle \bar{3} \rangle = \{\bar{3} \cdot \bar{0}; \bar{3} \cdot \bar{1}; \bar{3} \cdot \bar{2}; \bar{3} \cdot \bar{3}\} = \{\bar{0}; \bar{3}; \bar{2}; \bar{1}\} = \mathbb{Z}/4\mathbb{Z}$.

Отметим, что главный идеал $\langle \bar{2} \rangle$ является собственным, а главный идеал $\langle \bar{3} \rangle$ – несобственным.

Этот пример иллюстрирует следующее свойство кольца классов вычетов.

Теорема 4.2. В кольце классов вычетов $\mathbb{Z}/n\mathbb{Z}$ главный идеал $\langle \bar{a} \rangle$ совпадает с циклической аддитивной подгруппой, порожденной классом $\bar{a}$.

Обратим также внимание на то, что в рассмотренном примере элемент, породивший несобственный идеал $\langle \bar{3} \rangle$, являлся обратимым, а породивший собственный идеал $\langle \bar{2} \rangle$ – необратимым. Это является следствием более общего утверждения.

Теорема 4.3. Если идеал J ассоциативного кольца с единицей K содержит обратимый элемент кольца K , то $J = K$.

Следствие. Главный идеал $\langle a \rangle$, порожденный ненулевым элементом a , является собственным тогда и только тогда, когда a необратим.

Определение 4.6. Собственный идеал M называется **максимальным идеалом** кольца K , если он не содержится ни в одном большем собственном идеале этого кольца.

Теорема 4.4. В коммутативном кольце K для необратимых элементов a, b , c , таких, что $ab = c$, имеют место включения $\langle c \rangle \subset \langle a \rangle$ и $\langle c \rangle \subset \langle b \rangle$.

Как следует из определения максимального идеала, идеал $\langle c \rangle$ из теоремы 4.4 максимальным не является.

2. Мультипликативная группа кольца. Определение поля

Теорема 4.5. В ассоциативном кольце с единицей K множество всех обратимых элементов образует группу относительно операции умножения.

Эта группа называется **мультипликативной группой** кольца K и обозначается K^* .

Пример 4.9. В кольце классов вычетов $\mathbb{Z}/m\mathbb{Z}$ мультипликативную группу $\mathbb{Z}/m\mathbb{Z}^*$ составляют обратимые классы, т. е. такие $\bar{a}_i$, что $\text{НОД}(a_i, m) = 1$.

Пример 4.10. В кольце целых чисел $\mathbb{Z}$ мультипликативную группу $\mathbb{Z}^*$ составляют только два числа: 1 и -1 .

Определение 4.7. **Делителями нуля** называются такие ненулевые элементы кольца K , произведение которых равно нулю: $a, b \in K, a \neq 0, b \neq 0, ab = 0$.

Пример 4.11. В кольце $\mathbb{Z}/6\mathbb{Z}$ делителями нуля являются классы $\bar{2}$, $\bar{3}$ и $\bar{4}$: $\bar{2} \cdot \bar{3} = \bar{6} = \bar{0}$; $\bar{3} \cdot \bar{4} = \bar{12} = \bar{0}$. Отметим, что все они являются необратимыми.

Теорема 4.6. В ассоциативном кольце с единицей K все делители нуля необратимы.

Обратное утверждение, вообще говоря, неверно: не всегда необратимый элемент кольца K является делителем нуля. Примером может служить кольцо целых чисел, в котором нет делителей нуля, но все элементы, кроме 1 и -1 , необратимы.

Определение 4.8. **Поле** называется коммутативное ассоциативное кольцо с единицей, в котором каждый ненулевой элемент обратим.

Иными словами, поле – это коммутативное ассоциативное кольцо P с единицей, мультипликативная группа которого содержит все элементы за исключением 0: $P^* = P \setminus \{0\}$.

Пример 4.12. Множества $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ с введенными на них стандартными операциями сложения и умножения являются полями.

Пример 4.13. Кольцо целых чисел $\mathbb{Z}$ полем не является, так как среди ненулевых элементов обратимыми являются только 1 и -1 .

Пример 4.14. Кольцо классов вычетов $\mathbb{Z}/m\mathbb{Z}$ будет полем тогда и только тогда, когда модуль m – простое число.

Характерными свойствами любых полей являются:

- отсутствие делителей нуля;

- отсутствие собственных идеалов (следует из теоремы 4.3 и отсутствия в поле ненулевых необратимых элементов).

3. Кольца главных идеалов

Определение 4.9. *Кольцо главных идеалов* – коммутативное кольцо, в котором всякий идеал главный.

Теорема 4.7. *Кольцо целых чисел – кольцо главных идеалов.*

Доказательство этой теоремы приводит к тому, что всякий собственный идеал J кольца целых чисел можно представить как главный идеал, порожденный целым числом t : $J = \langle t \rangle = \{tq | q \in \mathbb{Z}\}$ ($t \neq 1$). На основании этого, а также утверждения теоремы 4.4 можно доказать следующую теорему.

Теорема 4.8. *Главный идеал J кольца целых чисел является максимальным тогда и только тогда, когда он порожден простым числом p : $J = \langle p \rangle$.*

Множество полиномов с коэффициентами из поля P образует кольцо относительно стандартных операций сложения и умножения. Такое кольцо обозначают $P[x]$ и называют кольцом полиномов над полем P .

Теорема 4.9. *Кольцо полиномов $P[x]$ с коэффициентами из поля P – кольцо главных идеалов.*

Доказательства теорем 4.7 и 4.9 схожи и основаны на том, что и в кольце целых чисел, и в кольце полиномов над полем P можно ввести правило деления с остатком. Кольца, в которых введено такое правило, называются **евклидовыми кольцами**, и они всегда являются кольцами главных идеалов.

Для кольца полиномов также можно сформулировать аналог теоремы 4.8, если определить полином в кольце $P[x]$, являющийся аналогом простого числа. Рассмотрим кольцо $P[x]$ и этот вопрос подробнее ниже.

§ 2. Кольцо полиномов

К характерным свойствам кольца полиномов с коэффициентами из поля P относятся следующие:

1. Кольцо полиномов $P[x]$ – коммутативное, ассоциативное кольцо с единицей;
2. В кольце $P[x]$ отсутствуют делители нуля;
3. Обратимыми элементами в кольце $P[x]$ являются только полиномы нулевой степени, т. е. ненулевые элементы поля P . Иными словами, мультипликативную группу кольца $P[x]$ составляют ненулевые элементы поля P ;
4. Кольцо полиномов $P[x]$ – кольцо главных идеалов, т. е. для любого идеала J в кольце $P[x]$ найдется такой многочлен $m(x)$, что $J = \langle m(x) \rangle = \{m(x)q(x) | q(x) \in P[x]\}$.

Кольцо многочленов обладает еще одним свойством по отношению к идеалам, однако для его формулировки необходимо ввести ряд определений.

Теорема 4.10 (о делении многочленов с остатком). Для любых двух многочленов $f(x), g(x) \in P[x]$, $g(x) \neq 0$ существуют определенные единственным образом многочлены $q(x), r(x) \in P[x]$, такие, что

$$f(x) = g(x)q(x) + r(x),$$

причем $\deg r(x) < \deg g(x)$ либо $r(x) = 0$.

Определение 4.10. В теореме о делении с остатком многочлен $q(x)$ называется **частным (неполным частным)** от деления $f(x)$ на $g(x)$, а многочлен $r(x)$ – **остатком** от этого деления.

Пример 4.15. Рассмотрим многочлены $f(x) = x^3 + 3x^2 - x + 1$, $g(x) = x + 1$, $h(x) = x^4 + 5x + 1$ из кольца $\mathbb{R}[x]$ действительных многочленов. Выполнив деление многочлена $f(x)$ на $g(x)$ в столбик, получим:

$$x^3 + 3x^2 - x + 1 = (x + 1)(x^2 + 2x - 3) + 4.$$

В данном случае неполным частным является многочлен $q(x) = x^2 + 2x - 3$, остатком – многочлен нулевой степени $r(x) = 4$.

Можно выполнить деление многочлена $f(x)$ и на многочлен $h(x)$. В этом случае, поскольку степень многочлена $h(x)$ больше степени многочлена $f(x)$, то неполным частным является нулевой многочлен $q(x) = 0$, а остаток $r(x)$ равен самому многочлену $f(x)$:

$$x^3 + 3x^2 - x + 1 = 0(x^4 + 5x + 1) + x^3 + 3x^2 - x + 1.$$

Определение 4.11. Если многочлен $g(x) \neq 0$ и при делении многочлена $f(x)$ на $g(x)$ остаток $r(x) = 0$, то многочлен $g(x)$ называется **делителем многочлена $f(x)$** (говорят, что $f(x)$ делится на $g(x)$).

Определение 4.12. Многочлен ненулевой степени $f(x)$ кольца $P[x]$ называется **неприводимым**, если он не имеет никаких других делителей, кроме многочленов нулевой степени и многочленов вида $\alpha f(x)$, где $\alpha \in P, \alpha \neq 0$.

Пример 4.16. Неприводимыми многочленами в кольце многочленов с действительными коэффициентами $\mathbb{R}[x]$ являются многочлены первой степени и многочлены второй степени с отрицательным дискриминантом. Любой многочлен степени выше второй является приводимым!

Пример 4.17. Неприводимыми многочленами в кольце многочленов с комплексными коэффициентами $\mathbb{C}[x]$ являются многочлены только первой степени.

Обратите внимание на схожесть определения простого числа в кольце $\mathbb{Z}$ и определения неприводимого многочлена в кольце $P[x]$. Сформулируем теперь заявленное выше свойство по отношению к идеалам кольца $P[x]$ – теорему, аналогичную теореме 4.8 о максимальных идеалах кольца $\mathbb{Z}$.

Теорема 4.11. В кольце полиномов $P[x]$ идеал $J = \langle m(x) \rangle$ максимален тогда и только тогда, когда порождающий его полином $m(x)$ является неприводимым над полем P .

Является ли конкретный полином $f(x)$ неприводимым над полем P существенно зависит от рассматриваемого поля P . Тем не менее можно сформулировать общее для всех полей необходимое условие неприводимости полинома. Для его формулировки дадим определение корня многочлена.

Определение 4.13. *Корень многочлена $f(x)$ из кольца $P[x]$ – элемент α поля $F \supseteq P$, такой, что $f(\alpha)=0$.*

Под полем F здесь понимают любое поле относительно тех же операций, что и поле P , включающее в себя поле P либо совпадающее с ним. Например, мнимая единица i является корнем многочлена $x^2 + 1$ с действительными коэффициентами, хотя сама она принадлежит полю комплексных чисел, включающему в себя поле действительных чисел. Под 0 в выражении $f(\alpha)=0$ понимают нейтральный элемент поля F относительно сложения.

Теорема 4.12. (Безу) *Элемент α поля $F \supseteq P$ является корнем многочлена $f(x)$ из кольца $P[x]$ тогда и только тогда, когда $f(x)$ делится без остатка на $x - \alpha$:*

$$f(x) = (x - \alpha)g(x), g(x) \in F[x].$$

Следствие *(необходимое условие неприводимости многочлена над заданным полем). Неприводимый над полем P многочлен не имеет корней из этого поля.*

Пример 4.18. Многочлен $x^2 + 1$ является неприводимым над полем $\mathbb{R}$, но приводим над полем $\mathbb{C}$.

Для колец полиномов над полями $\mathbb{R}$ и $\mathbb{C}$ выше были перечислены все возможные случаи неприводимых полиномов: над полем $\mathbb{R}$ не существует неприводимых полиномов степени выше второй, над полем $\mathbb{C}$ – выше первой. Рассмотрим кольцо полиномов над конечным (т. е. содержащим конечное число элементов) полем классов вычетов $\mathbb{Z}/p\mathbb{Z}$, где p – простое число. Это кольцо полиномов обозначим $(\mathbb{Z}/p\mathbb{Z})[x]$:

$$(\mathbb{Z}/p\mathbb{Z})[x] = \{a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \mid n \in \mathbb{N} \cup \{0\}, a_i \in \mathbb{Z}/p\mathbb{Z}, i = 0, \dots, n\}.$$

В кольце $(\mathbb{Z}/p\mathbb{Z})[x]$ существуют неприводимые полиномы любой ненулевой степени. Поэтому вопрос о неприводимости полинома степени n в кольце $(\mathbb{Z}/p\mathbb{Z})[x]$ часто решается непосредственной проверкой необходимого условия, а затем – проверкой делимости на всевозможные неприводимые многочлены кольца $(\mathbb{Z}/p\mathbb{Z})[x]$ степени не выше $\lfloor n/2 \rfloor$. Этот алгоритм схож по смыслу с просеиванием возможных простых делителей некоторого целого числа с помощью «решета Эратосфена».

Для справки укажем здесь нормированные (т. е. со старшим коэффициентом, равным 1) неприводимые многочлены второй и третьей степени над полями $\mathbb{Z}/2\mathbb{Z}$ и $\mathbb{Z}/3\mathbb{Z}$.

Над полем $\mathbb{Z}/2\mathbb{Z}$:

$$x^2 + x + 1;$$

$$x^3 + x + 1;$$

$$x^3 + x^2 + 1.$$

Над полем $\mathbb{Z}/3\mathbb{Z}$:

$$x^2 + 1;$$

$$x^2 + x + 2;$$

$$x^2 + 2x + 2.$$

$$x^3 + 2x + 1;$$

$$x^3 + 2x + 2;$$

$$x^3 + x^2 + 2;$$

$$x^3 + x^2 + x + 2;$$

$$x^3 + x^2 + 2x + 1;$$

$$x^3 + 2x^2 + 1;$$

$$x^3 + 2x^2 + x + 1;$$

$$x^3 + 2x^2 + 2x + 2.$$

Отметим, что над полем $\mathbb{Z}/3\mathbb{Z}$ можно получить еще столько же ненормированных неприводимых многочленов, умножив перечисленные на два.

Замечание. При проверке многочлена на неприводимость имеет смысл определять делимость только на нормированные неприводимые многочлены.

ТИПОВЫЕ ЗАДАНИЯ ПО ТЕМЕ «КОЛЬЦА. ИДЕАЛЫ КОЛЕЦ» С ОБРАЗЦАМИ РЕШЕНИЙ

Задание 1. Является ли идеалом в кольце целых чисел множество всех чисел, кратных заданному числу k ? Если является, будет ли этот идеал главным и в каком случае идеал будет максимален?

Решение

Рассмотрим элементы множества A чисел, кратных k : $A = \{kq | q \in \mathbb{Z}\}$. Проверим для них выполнение всех требований из определения идеала.

1. Множество A является подгруппой аддитивной группы целых чисел, так как выполняются оба условия критерия подгруппы:

1.1. Сумма двух чисел, кратных k , также кратна k : $\forall kq_1, kq_2 \in A$ имеет место $kq_1 + kq_2 = k(q_1 + q_2) = kq_3, q_3 \in \mathbb{Z} \Rightarrow (kq_1 + kq_2) \in A$.

1.2. Число, противоположное кратному k , также делится на k нацело:

$\forall kq \in A$ имеет место $-kq = kq', q' \in \mathbb{Z} \Rightarrow -kq \in A$.

Подгруппа A является замкнутой относительно операции умножения: произведение чисел, кратных k , делится на k без остатка: $\forall kq_1, kq_2 \in A$ имеет место $kq_1 \cdot kq_2 = k^2 q_1 q_2 = kq_3, q_3 \in \mathbb{Z} \Rightarrow kq_1 \cdot kq_2 \in A$. Следовательно, A является подкольцом кольца целых чисел.

2. Выберем произвольный элемент подкольца A – элемент $a = kq_1, q_1 \in \mathbb{Z}$ и произвольный элемент m кольца целых чисел. Их произведение $am = kq_1 m, (q_1 m) \in \mathbb{Z}$ принадлежит подкольцу A , поскольку кратно k . Так как a и m были выбраны произвольно, то имеем $mA = Am \subseteq A \forall m \in \mathbb{Z} (mA = \{ma | a \in A\})$.

Согласно определению, подкольцо A является двусторонним идеалом кольца целых чисел. Так как по теореме 4.7 кольцо целых чисел – кольцо главных идеалов, то любой идеал, в том числе и идеал A , является главным.

Так как кольцо целых чисел является коммутативным, то для главного идеала $A = \langle k \rangle$ справедливо утверждение теоремы 4.4: если a, b, c – необратимые элементы кольца и $a = bc$, тогда выполняются включения главных идеалов $\langle a \rangle \subseteq \langle b \rangle, \langle a \rangle \subseteq \langle c \rangle$. Поэтому если число k не является простым, то порожденный им идеал $\langle k \rangle$ будет включен в идеалы, порожденные делителями k . Если k простое, то содержащих $\langle k \rangle$ несобственных идеалов не существует, и $\langle k \rangle$ является максимальным идеалом. ▲

Задание 2. Выяснить, являются ли идеалами данные множества:

а) множество A целых чисел, сравнимых с 3 по модулю 7: $A = \{a \in \mathbb{Z} | a \equiv 3 \pmod{7}\}$ в кольце целых чисел $\mathbb{Z}$;

б) множество целых чисел $\mathbb{Z}$ в кольце полиномов с целыми коэффициентами $\mathbb{Z}[x]$;

в) множество многочленов со старшими четными коэффициентами в кольце многочленов с целыми коэффициентами $\mathbb{Z}[x]$;

г) множество необратимых элементов в кольце классов вычетов $\mathbb{Z}/9\mathbb{Z}$.

Решение

а) Проверим, является ли множество целых чисел, сравнимых с 3 по модулю 7, аддитивной подгруппой группы целых чисел: если $a \equiv 3(mod 7)$ и $b \equiv 3(mod 7)$, то $a + b \equiv 3 + 3 = 6(mod 7)$. Сумма элементов не принадлежит исходному множеству, следовательно, множество не замкнуто относительно операции сложения. Оно не является подгруппой и тем более подкольцом, а тогда и не является идеалом кольца целых чисел.

б) Множество целых чисел является кольцом относительно стандартных операций сложения и умножения, следовательно, оно является подкольцом кольца многочленов с целыми коэффициентами $\mathbb{Z}[x]$. Возьмем какой-либо многочлен из кольца $\mathbb{Z}[x]$, например x , и произвольное целое число a из подкольца $\mathbb{Z}$. Результат произведения этих элементов ax не принадлежит подкольцу $\mathbb{Z}$, а следовательно, это множество не является идеалом.

в) Рассмотрим два произвольных элемента множества J многочленов со старшими четными коэффициентами в кольце $\mathbb{Z}[x]$:

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \text{ и } g(x) = b_m x^m + b_{m-1} x^{m-1} + \dots + b_1 x + b_0,$$

где $a_i \in \mathbb{Z}, i = \overline{1, n}, b_i \in \mathbb{Z}, i = \overline{1, m}$, а числа a_n и b_m – четные. Старшим коэффициентом суммы многочленов $f(x)$ и $g(x)$ будет либо a_n , либо b_m , либо $a_n + b_m$ – число в любом случае четное. Следовательно, сумма многочленов $f(x)$ и $g(x)$ – также многочлен из множества J . Этому же множеству, очевидно, принадлежит многочлен, противоположный $f(x)$: $h(x) = -f(x) = -a_n x^n - a_{n-1} x^{n-1} - \dots - a_0$, так как его старший коэффициент $-a_n$, как и a_n , является четным. На основании этого делаем вывод, что множество J является подгруппой аддитивной группы многочленов с целыми коэффициентами. При умножении двух многочленов $f(x)$ и $g(x)$ старший коэффициент произведения $f(x)g(x)$ равен произведению $a_n b_m$, а так как оно является четным числом, то $f(x)g(x)$ также принадлежит исходному множеству J . Таким образом, множество J замкнуто относительно умножения и является подкольцом кольца $\mathbb{Z}[x]$.

Рассмотрим произвольный элемент $p(x)$ кольца $\mathbb{Z}[x]$:

$$p(x) = p_l x^l + p_{l-1} x^{l-1} + \dots + p_1 x + p_0.$$

В результате его умножения на произвольный многочлен $f(x)$ подкольца J получим многочлен со старшим коэффициентом $p_l a_n$, который также является четным в силу четности сомножителя a_n . Имеем: $\forall p(x) \in \mathbb{Z}[x]$ и $\forall f(x) \in J$ произведение $p(x)f(x) \in J$, или, иными словами, $pJ = Jp \subseteq J \forall p(x) \in \mathbb{Z}[x]$, где $pJ = \{p(x)f(x) | f(x) \in J\}$. Согласно определению, множество J является идеалом кольца $\mathbb{Z}[x]$.

г) Множество необратимых элементов кольца классов вычетов $\mathbb{Z}/9\mathbb{Z}$ состоит из трех элементов: $A = \{\bar{0}, \bar{3}, \bar{6}\}$. Легко проверить, что все возможные суммы этих элементов, обратные к ним, и все возможные произведения также принадлежат

множеству A , следовательно, оно является подкольцом кольца $\mathbb{Z}/9\mathbb{Z}$. В результате произведения элементов кольца $\mathbb{Z}/9\mathbb{Z}$, отличных от $\bar{0}, \bar{3}, \bar{6}$, на элементы множества A получим лишь $\bar{0}, \bar{3}, \bar{6}$:

$$\bar{1} \cdot \bar{3} = \bar{3}; \bar{2} \cdot \bar{3} = \bar{6}; \bar{4} \cdot \bar{3} = \bar{12} = \bar{3}; \bar{5} \cdot \bar{3} = \bar{15} = \bar{6}; \bar{7} \cdot \bar{3} = \bar{21} = \bar{3}; \bar{8} \cdot \bar{3} = \bar{24} = \bar{6};$$

$$\bar{1} \cdot \bar{6} = \bar{6}; \bar{2} \cdot \bar{6} = \bar{12} = \bar{3}; \bar{4} \cdot \bar{6} = \bar{24} = \bar{6}; \bar{5} \cdot \bar{6} = \bar{30} = \bar{3}; \bar{7} \cdot \bar{6} = \bar{42} = \bar{6}; \bar{8} \cdot \bar{6} = \bar{48} = \bar{3}.$$

Имеем: $\forall n \in \mathbb{Z}/9\mathbb{Z}$ и $\forall a \in A$ произведение $an \in A$, или, иными словами, $nA = An \subseteq A \forall n \in \mathbb{Z}/9\mathbb{Z}$, где $nA = \{na \mid a \in A\}$. Согласно определению, множество A является идеалом кольца $\mathbb{Z}/9\mathbb{Z}$. ▲

Задание 3. Найти все идеалы кольца $\mathbb{Z}/18\mathbb{Z}$. Расположить их в порядке возрастания. Указать максимальные в этом кольце.

Решение

На основании теорем 4.2 и 4.3 будем строить только собственные идеалы кольца $\mathbb{Z}/18\mathbb{Z}$ как циклические аддитивные подгруппы, порожденные необратимыми классами $\bar{2}, \bar{3}, \bar{4}, \bar{6}, \bar{8}, \bar{9}, \bar{10}, \bar{12}, \bar{14}, \bar{15}, \bar{16}$. Построим циклические подгруппы, порожденные необратимыми элементами $\bar{2}, \bar{3}, \bar{6}, \bar{9}$ (обратите внимание, что их наименьшие положительные представители делят 18 нацело).

$$J_2 = \langle \bar{2} \rangle = \{\bar{0}, \bar{2}, \bar{2} + \bar{2} = \bar{4}, \bar{4} + \bar{2} = \bar{6}, \bar{8}, \bar{10}, \bar{12}, \bar{14}, \bar{16}\};$$

$$J_3 = \langle \bar{3} \rangle = \{\bar{0}, \bar{3}, \bar{3} + \bar{3} = \bar{6}, \bar{6} + \bar{3} = \bar{9}, \bar{12}, \bar{15}\};$$

$$J_6 = \langle \bar{6} \rangle = \{\bar{0}, \bar{6}, \bar{6} + \bar{6} = \bar{12}\};$$

$$J_9 = \langle \bar{9} \rangle = \{\bar{0}, \bar{9}\}.$$

Читатель может самостоятельно убедиться, что, взяв в качестве порождающих элементов оставшиеся необратимые классы $\bar{4}, \bar{8}, \bar{10}, \bar{12}, \bar{14}, \bar{15}, \bar{16}$, можно построить лишь такие идеалы, которые совпадают с одним из уже полученных.

Расположим полученные идеалы в порядке включения (идеал является включенным в другой идеал, если все элементы первого содержатся во втором идеале):

$$J_9 \subset J_3; J_6 \subset J_2.$$

Не включенными ни в один другой идеал являются J_2 и J_3 , следовательно, они максимальные. ▲

Задание 4. Исследовать, при каких действительных значениях параметров α, β и γ идеал $\langle \alpha x^4 + \beta x^2 + \gamma x + 4 \rangle$ является максимальным в кольце многочленов с действительными коэффициентами.

Решение

Согласно теореме 4.11, в кольце $P[x]$ многочленов над полем P идеал, порожденный многочленом $g(x)$, является максимальным тогда и только тогда, когда $g(x)$ – неприводимый над заданным полем. В условии задачи дано кольцо

многочленов над полем действительных чисел, и в таком случае неприводимыми многочленами являются *многочлены первой степени и второй степени с отрицательным дискриминантом (следствие из основной теоремы алгебры)*. Тогда многочлен $g(x) = \alpha x^4 + \beta x^2 + \gamma x + 4$ неприводим в двух случаях. В обоих из них необходимо, чтобы α равнялось нулю. В первом случае также потребуем равенство нулю параметра β , тогда $g(x)$ является многочленом первой степени и удовлетворяет определению неприводимости при любом ненулевом значении γ . Во втором случае положим $\beta \neq 0$ и потребуем отрицательного значения дискриминанта:

$$D = \gamma^2 - 16\beta < 0 \Leftrightarrow \beta > \frac{\gamma^2}{16}.$$

Окончательно имеем, что идеал $\langle \alpha x^4 + \beta x^2 + \gamma x + 4 \rangle$ является максимальным в кольце многочленов с действительными коэффициентами, если $\alpha = 0$, $\beta = 0$, $\gamma \in \mathbb{R} \setminus \{0\}$ или если $\alpha = 0$, $\beta > \frac{\gamma^2}{16}$, $\gamma \in \mathbb{R}$. ▲

Задание 5. Выяснить, максимален ли идеал в кольце полиномов с коэффициентами из $\mathbb{Z}/2\mathbb{Z}$, порожденный полиномом $f(x) = x^7 + x^5 + x^4 + x^2 + 1$.

Решение

Для того чтобы выяснить, является ли идеал $\langle x^7 + x^5 + x^4 + x^2 + 1 \rangle$ максимальным, необходимо установить, является ли порождающий его многочлен неприводимым. Многочлен n -й степени с коэффициентами из $\mathbb{Z}/2\mathbb{Z}$ будет приводимым в любом из следующих случаев: или многочлен имеет корни в $\mathbb{Z}/2\mathbb{Z}$ (тогда он делится на x или $x - 1$); или многочлен делится на какой-либо неприводимый многочлен степени 2, 3, ..., $n - 1$. Если же не выполняется ни одно из условий, то исследуемый многочлен неприводимый. Последовательно выполняя проверку этих условий, можно установить приводимость (или неприводимость) многочлена. Отметим, что нет необходимости проверять делимость на неприводимые многочлены выше $\lfloor n/2 \rfloor$, так как делимость на многочлен степени $m > \lfloor n/2 \rfloor$ равносильна делимости на многочлен степени $n - m \leq \lfloor n/2 \rfloor$.

Так как степень многочлена $f(x)$, порождающего заданный идеал, равна семи, то необходимо проверить, имеет ли этот многочлен корни в $\mathbb{Z}/2\mathbb{Z}$, и в случае отрицательного ответа – делится ли он на неприводимый многочлен второй или третьей степени. Далее все действия выполняются по модулю 2. Проверим наличие корней:

$$f(0) = 1 \neq 0;$$

$$f(1) = 1 + 1 + 1 + 1 + 1 = 5 = 1 \neq 0$$

Таким образом, $f(x)$ не имеет корней в $\mathbb{Z}/2\mathbb{Z}$ – выполнено необходимое условие неприводимого многочлена.

Следующим шагом необходимо проверить делимость на неприводимые многочлены второй степени. Среди многочленов второй степени с коэффициен-

тами из $\mathbb{Z}/2\mathbb{Z}$ существует всего один неприводимый: $x^2 + x + 1$. Проверку осуществляем непосредственным делением в столбик, учитывая, что в $\mathbb{Z}/2\mathbb{Z}$ $-1 = 1$, $2 = 0$:

$$\begin{array}{r}
 \underline{x^7 + 0x^6 + x^5 + x^4 + 0x^3 + x^2 + 1} \quad | \quad \underline{x^2 + x + 1} \\
 \underline{x^7 + x^6 + x^5} \qquad \qquad \qquad | \quad \underline{x^5 + x^4 + x^3 + x^2} \\
 \hline
 \underline{x^6 + 0x^5 + x^4} \qquad \qquad \qquad \\
 \underline{x^6 + x^5 + x^4} \qquad \qquad \qquad \\
 \hline
 \underline{x^5 + 0x^4 + 0x^3} \qquad \qquad \qquad \\
 \underline{x^5 + x^4 + x^3} \qquad \qquad \qquad \\
 \hline
 \underline{x^4 + x^3 + x^2} \qquad \qquad \qquad \\
 \underline{x^4 + x^3 + x^2} \qquad \qquad \qquad \\
 \hline
 \qquad \qquad \qquad \qquad \qquad \qquad +1
 \end{array}$$

Получили ненулевой остаток (единицу), следовательно, $f(x)$ на $x^2 + x + 1$ не делится.

Далее аналогичным образом проверим делимость на неприводимые многочлены третьей степени: $x^3 + x + 1$ и $x^3 + x^2 + 1$. Получим, что $f(x)$ делится на $x^3 + x^2 + 1$, частное – многочлен $x^4 + x^3 + 1$. Следовательно, $f(x)$ является приводимым многочленом, а порожденный им идеал не является максимальным. ▲

Задание 6. Выяснить, максимален ли идеал в кольце полиномов с коэффициентами из $\mathbb{Z}/3\mathbb{Z}$, порожденный полиномом $g(x) = x^5 + x^3 + x^2 + 2x + 2$.

Решение

Для выполнения данного задания справедливы те же рассуждения, что и для задания 5: необходимо исследовать многочлен $g(x)$ на приводимость, последовательно проверяя наличие корней и делимость на неприводимые многочлены степени не выше $\lfloor 5/2 \rfloor = 2$. Отличие заключается лишь в поле, над которым задан многочлен: $\mathbb{Z}/3\mathbb{Z}$. Проверим, есть ли среди элементов этого поля корни многочлена $g(x)$ (все действия проводим по модулю 3):

$$g(0) = 2 \neq 0$$

$$g(1) = 1 + 1 + 1 + 2 + 2 = 7 = 1 \neq 0$$

$$g(2) = 32 + 8 + 4 + 4 + 2 = 50 = 2 \neq 0.$$

Корней из $\mathbb{Z}/3\mathbb{Z}$ нет. Далее необходимо проверить делимость на неприводимые многочлены второй степени (нормированные). Укажем их:

$$x^2 + 1;$$

$$x^2 + x + 2;$$

$$x^2 + 2x + 2.$$

Деление выполняется, как и ранее, в столбик, однако теперь, учитывая поле, над которым заданы многочлены, выполняются равенства коэффициентов по модулю 3: $-1=2$, $-2=1$, $3=0$; $4=1$. Приведем в качестве примера деление $g(x)$ на $x^2 + 2x + 2$:

$$\begin{array}{r}
\underline{-x^5 + 0x^4 + x^3 + x^2 + 2x + 2} \quad \left| \begin{array}{l} x^2 + 2x + 2 \\ x^3 + x^2 + 2 \end{array} \right. \\
\underline{x^5 + 2x^4 + 2x^3} \qquad \qquad \qquad \left| \begin{array}{l} x^3 + x^2 + 2 \\ x^4 + 2x^3 + x^2 \end{array} \right. \\
\qquad \underline{-x^4 + 2x^3 + x^2} \\
\qquad \qquad \underline{x^4 + 2x^3 + 2x^2} \\
\qquad \qquad \qquad \underline{-2x^2 + 2x + 2} \\
\qquad \qquad \qquad \qquad \underline{2x^2 + x + 1} \\
\qquad \qquad \qquad \qquad \qquad \underline{x + 1}
\end{array}$$

Как следует из наличия ненулевого остатка $x + 1$, многочлен $g(x)$ не делится на $x^2 + 2x + 2$. Выполнив проверку делимости на остальные два многочлена $x^2 + 1$ и $x^2 + x + 2$, убедимся, что $g(x)$ не делится ни на один из них. Следовательно, $g(x)$ является неприводимым над полем $\mathbb{Z}/3\mathbb{Z}$, а порожденный им идеал – максимальный в кольце многочленов с коэффициентами из $\mathbb{Z}/3\mathbb{Z}$. ▲

Напомним, что для многочленов шестой и седьмой степени в случае, если они не имеют корней в $\mathbb{Z}/3\mathbb{Z}$ и не делятся ни на один из неприводимых многочленов второй степени, необходимо выполнить проверку на делимость на неприводимые многочлены третьей степени.

ТЕСТ ДЛЯ САМОПРОВЕРКИ ПО ТЕМЕ «КОЛЬЦА. ИДЕАЛЫ КОЛЕЦ»

Вопрос 1. Какие множества являются идеалами в кольце $\mathbb{Z}$ целых чисел?

- A) $\{1\}$;
- B) $\{30k \mid k \in \mathbb{Z}\}$ – множество целых чисел, кратных 30;
- C) $\{5k + 2 \mid k \in \mathbb{Z}\}$ – множество целых чисел, дающих остаток 2 при делении на 5;
- D) $\{13k + 12 \mid k \in \mathbb{Z}\}$ – множество целых чисел, дающих остаток 12 при делении на 13;
- E) $\{0\}$.

Вопрос 2. Выбрать множества, которые являются полями относительно стандартных операций сложения и умножения:

- A) $\mathbb{Z}/21\mathbb{Z}$ – множество классов вычетов по модулю 21;
- B) $\mathbb{Q}$ – множество рациональных чисел;
- C) $\mathbb{Z}$ – множество целых чисел;
- D) $\mathbb{Z}/23\mathbb{Z}$ – множество классов вычетов по модулю 23;
- E) $\mathbb{C}$ – множество комплексных чисел.

Вопрос 3. Какие из перечисленных идеалов в кольце $\mathbb{Z}/16\mathbb{Z}$ являются максимальными?

- A) $\langle \overline{8} \rangle$;
- B) $\langle \overline{4} \rangle$;
- C) $\langle \overline{12} \rangle$;
- D) $\langle \overline{10} \rangle$;
- E) $\langle \overline{2} \rangle$.

Вопрос 4. Многочлен $f(x) = x^4 + \alpha x^3 + \beta x^2 + x + 16$ является неприводимым в кольце $\mathbb{R}[x]$ многочленов с действительными коэффициентами:

- A) только если $\alpha = 0$;
- B) только если $\alpha = \beta = 0$;
- C) при любых α и β ;
- D) ни при каких α и β не является неприводимым;
- E) только если α и β отрицательные.

Вопрос 5. Для начала каждого предложения А–Е подобрать его окончание так, чтобы получилось верное утверждение. Ответ запишите в виде сочетания букв и цифр, соблюдая алфавитную последовательность букв. Если началу предложения соответствует несколько верных окончаний, укажите их все. Некоторые данные правого столбца могут использоваться несколько раз или не использоваться вообще. Например, A14B1C27D3E3.

Начало предложения	Окончание предложения
А. В любом поле отсутствуют ... В. Все идеалы в кольце целых чисел – это... С. В любом поле ненулевой элемент – ... D. Если p – простое число, то в кольце целых чисел множества вида $\{pk \mid k \in \mathbb{Z}\}$ – это... Е. Если в кольце многочленов над полем P идеал $J = \langle f(x) \rangle$ – максимальный, то $f(x)$ –	1) Простое число. 2) Максимальные идеалы. 3) Левые идеалы. 4) Собственные идеалы. 5) Главные идеалы. 6) Делители нуля. 7) Неприводимый. 8) Обратимый.

Вопрос 6. В кольце $M_2(\mathbb{R})$ действительных квадратных матриц 2-го порядка рассмотрим множество всех матриц вида $\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}$, где $a, b \in \mathbb{R}$. Является ли данное множество идеалом?

- А) является левым идеалом, но не является правым идеалом;
- В) является и левым, и правым идеалом;
- С) является правым идеалом, но не является левым идеалом;
- Д) не является идеалом;
- Е) является двусторонним идеалом, только если $b = -a$.

Вопрос 7. Дано кольцо полиномов с коэффициентами из $\mathbb{Z}/3\mathbb{Z}$. Какие из перечисленных ниже идеалов, порожденных соответствующими многочленами, являются максимальными?

- А) $x^2 + 2x$;
- В) $x^3 + 2x^2 + 2x + 1$;
- С) $x^3 + x^2 + 2$;
- Д) $2x^2 + 2x + 2$;
- Е) $2x^2 + x + 1$.

Вопрос 8. Указать НЕВЕРНЫЕ утверждения:

- А) в кольце $\mathbb{Z}$ целых чисел идеал $\langle 61 \rangle$ является максимальным;
- В) в кольце полиномов $\mathbb{R}[x]$ обратимыми элементами являются только ненулевые многочлены нулевой степени: $\mathbb{R}/\{0\}$;
- С) в кольце полиномов над конечным полем можно отыскать делители нуля;
- Д) многочлен $x^4 + 128$ является неприводимым над полем действительных чисел;
- Е) в кольце многочленов $(\mathbb{Z}/3\mathbb{Z})[x]$ не существует неприводимых многочленов степени выше третьей.

Вопрос 9. Указать ВЕРНЫЕ утверждения:

- A) всякое поле является кольцом;
- B) всякое кольцо является полем;
- C) множество свободных векторов с операциями сложения и векторного умножения образует поле;
- D) в кольце может быть несколько элементов, нейтральных относительно сложения;
- E) в поле для одного и того же ненулевого элемента можно отыскать несколько различных обратных элементов.

Вопрос 10. Какое минимальное количество элементов может содержать поле?

- A) 1;
- B) 2;
- C) 3;
- D) 5;
- E) 20.

Ключ к тесту:

<i>Номер вопроса</i>	<i>Ответ</i>
1	B, E
2	B, D, E
3	D, E
4	D
5	A46B5C8D25E7
6	A
7	C, E
8	C, D, E
9	A
10	B

ИНДИВИДУАЛЬНЫЕ ЗАДАНИЯ ДЛЯ ЛАБОРАТОРНОЙ РАБОТЫ № 4 «КОЛЬЦА. ИДЕАЛЫ КОЛЕЦ»

1. Исследовать, образуют ли указанные подмножества целых чисел идеалы в кольце целых чисел. В случае положительного ответа выяснить, максимален ли этот идеал.

2. Является ли идеалом данное множество?

3. Найти все собственные идеалы в кольце $\mathbb{Z}/m\mathbb{Z}$. Расположить их в порядке возрастания. Указать максимальные идеалы в этом кольце. Какие классы вычетов по модулю m необходимо выбирать в качестве порождающего элемента идеала, чтобы полученные идеалы не совпадали друг с другом? В каком случае при различных порождающих элементах будут получены одинаковые идеалы? Ответы на последние два вопроса обосновать в общем виде для произвольного m .

4. При каких значениях параметров α , β и γ главный идеал в кольце полиномов над полем действительных чисел, порожденный многочленом $h(x)$, является максимальным?

5. Максимален ли идеал в кольце полиномов с коэффициентами из $\mathbb{Z}/2\mathbb{Z}$, порожденный полиномом: а) $s(x)$? б) $t(x)$?

6. Максимален ли идеал $\langle s(x) \rangle$ в кольце полиномов с коэффициентами из $\mathbb{Z}/3\mathbb{Z}$?

Вариант 1

1. а) $\{179k \mid k \in \mathbb{Z}\}$; б) $\{9k^2 + 1 \mid k \in \mathbb{Z}\}$.

2. Симметрическая разность двух идеалов.

3. $\mathbb{Z}/20\mathbb{Z}$.

4. $\alpha x^4 + \beta x^3 + \gamma x + 144$.

5. а) $s(x) = x^6 + x^5 + x^4 + x^3 + x^2 + 1$; б) $t(x) = x^6 + x^3 + 1$.

6. $s(x) = x^6 + x^3 + 2x^2 + 2x + 2$.

Вариант 2

1. а) $\{183k \mid k \in \mathbb{Z}\}$; б) $\{3k + 2 \mid k \in \mathbb{Z}\}$.

2. Дополнение к идеалу в кольце.

3. $\mathbb{Z}/24\mathbb{Z}$.

4. $\alpha x^3 + 15\beta x - 16\gamma$.

5. а) $s(x) = x^6 + x^4 + x^3 + x^2 + x + 1$; б) $t(x) = x^6 + x + 1$.

6. $s(x) = x^6 + 2x^4 + 2x^3 + 2x^2 + 1$.

Вариант 3

1. а) $\{919k \mid k \in \mathbb{Z}\}$; б) $\{k^2 + k + 2 \mid k \in \mathbb{Z}\}$.
2. Объединение двух идеалов.
3. $\mathbb{Z}/28\mathbb{Z}$.
4. $\alpha x^4 + \beta x^2 + \gamma x + 81$.
5. а) $s(x) = x^6 + x^5 + x^3 + x^2 + x + 1$; б) $t(x) = x^6 + x^4 + x^3 + x + 1$.
6. $s(x) = x^6 + 2x^5 + x^4 + x^3 + 2$.

Вариант 4

1. а) $\{177k \mid k \in \mathbb{Z}\}$; б) $\{7k - 3 \mid k \in \mathbb{Z}\}$.
2. Пересечение двух идеалов.
3. $\mathbb{Z}/30\mathbb{Z}$.
4. $\alpha x^4 + \beta x^3 + \gamma x + 4$.
5. а) $s(x) = x^6 + x^3 + x^2 + 1$; б) $t(x) = x^7 + x^3 + 1$.
6. $s(x) = x^6 + x^5 + x^4 + 2x^2 + x + 2$.

Вариант 5

1. а) $\{631k \mid k \in \mathbb{Z}\}$; б) $\{3k^2 + 6k + 1 \mid k \in \mathbb{Z}\}$.
2. Произведение двух идеалов.
3. $\mathbb{Z}/32\mathbb{Z}$.
4. $\alpha x^4 + \beta x^2 + \gamma x + 1$.
5. а) $s(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$; б) $t(x) = x^7 + x^4 + 1$.
6. $s(x) = x^6 + x^5 + 2x^4 + 2x^2 + x + 1$.

Вариант 6

1. а) $\{209k \mid k \in \mathbb{Z}\}$; б) $\{-k^2 + 16 \mid k \in \mathbb{Z}\}$.
2. Множество всех четных чисел в кольце целых чисел.
3. $\mathbb{Z}/34\mathbb{Z}$.
4. $\alpha x^4 + \beta x^2 + \gamma x - 1$.
5. а) $s(x) = x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$; б) $t(x) = x^6 + x^5 + x^4 + x + 1$.
6. $s(x) = x^6 + 2x^4 + x^3 + 2x^2 + 1$.

Вариант 7

1. а) $\{611k \mid k \in \mathbb{Z}\}$; б) $\{2k + 1 \mid k \in \mathbb{Z}\}$.
2. Множество всех нечетных чисел в кольце целых чисел.
3. $\mathbb{Z}/35\mathbb{Z}$.
4. $\alpha x^3 + \beta x^2 + 8x - \gamma$.
5. а) $s(x) = x^7 + x^5 + x^4 + x^3 + x^2 + 1$; б) $t(x) = x^7 + x^6 + 1$.
6. $s(x) = x^6 + 2x^5 + x^4 + 2x^2 + 2x + 2$.

Вариант 8

1. а) $\{163k \mid k \in \mathbb{Z}\}$; б) $\{k^2 - 3k + 4 \mid k \in \mathbb{Z}\}$.
2. Множество 0, 1, 2, 3, 4, 5, 6, 7, 8 в кольце целых чисел.
3. $\mathbb{Z}/36\mathbb{Z}$.
4. $\alpha x^4 + \beta x^2 + 3\gamma x + 16$.
5. а) $s(x) = x^7 + x^6 + x^4 + x^3 + x^2 + 1$; б) $t(x) = x^7 + x^6 + x^3 + x + 1$.
6. $s(x) = x^6 + x^5 + 2x^3 + 2x + 2$.

Вариант 9

1. а) $\{703k \mid k \in \mathbb{Z}\}$; б) $\{k^2 - 4 \mid k \in \mathbb{Z}\}$.
2. В кольце полиномов множество всех многочленов степени не выше 10.
3. $\mathbb{Z}/22\mathbb{Z}$.
4. $\alpha x^4 + 12\beta x^2 + 37\gamma$.
5. а) $s(x) = x^7 + x^6 + x^5 + x^3 + x + 1$; б) $t(x) = x^6 + x^5 + x^2 + x + 1$.
6. $s(x) = x^6 + x^4 + x + 1$.

Вариант 10

1. а) $\{167k \mid k \in \mathbb{Z}\}$; б) $\{17k + 5 \mid k \in \mathbb{Z}\}$.
2. В кольце полиномов множество всех многочленов степени не ниже 10.
3. $\mathbb{Z}/38\mathbb{Z}$.
4. $\alpha x^4 + 8\beta x^2 + \gamma x + 49$.
5. а) $s(x) = x^7 + x^6 + x^5 + x^4 + x^2 + 1$; б) $t(x) = x^7 + x^6 + x^5 + x^4 + x^2 + x + 1$.
6. $s(x) = x^6 + x^5 + x^3 + 2x + 2$.

Вариант 11

1. а) $\{559k \mid k \in \mathbb{Z}\}$; б) $\{5k^2 + k - 1 \mid k \in \mathbb{Z}\}$.
2. Симметрическая разность двух идеалов.
3. $\mathbb{Z}/21\mathbb{Z}$.
4. $3\alpha x^4 + \beta x^2 + 25\gamma$.
5. а) $s(x) = x^7 + x^5 + x^4 + x^3 + x + 1$; б) $t(x) = x^6 + x^5 + 1$.
6. $s(x) = x^6 + 2x^5 + 2x^4 + 2x^2 + 2x + 1$.

Вариант 12

1. а) $\{317k \mid k \in \mathbb{Z}\}$; б) $\{11k + 2 \mid k \in \mathbb{Z}\}$.
2. В кольце $M_2[\mathbb{R}]$ вещественных квадратных матриц порядка 2 множество всех матриц вида $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$; $a, b, c \in \mathbb{R}$.
3. $\mathbb{Z}/27\mathbb{Z}$.
4. $\alpha x^4 + \beta x^2 + 2\gamma x + 144$.
5. а) $s(x) = x^6 + x^5 + x^4 + x^3 + x^2 + 1$; б) $t(x) = x^6 + x^3 + 1$.
6. $s(x) = x^6 + 2x^5 + x^3 + x + 2$.

Вариант 13

1. а) $\{649k \mid k \in \mathbb{Z}\}$; б) $\{2k^2 - 2k + 1 \mid k \in \mathbb{Z}\}$.
2. В кольце вещественных квадратных матриц порядка 2 множество всех матриц вида $\begin{pmatrix} a & 0 \\ b & c \end{pmatrix}$.
3. $\mathbb{Z}/39\mathbb{Z}$.
4. $\alpha x^6 + \beta x^4 + \gamma x^2 + 1$.
5. а) $s(x) = x^7 + x^4 + x^3 + x^2 + x + 1$; б) $t(x) = x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + 1$.
6. $s(x) = x^6 + x^5 + x^4 + 2x^3 + 2$.

Вариант 14

1. а) $\{409k \mid k \in \mathbb{Z}\}$; б) $\{6k + 1 \mid k \in \mathbb{Z}\}$.
2. В кольце вещественных квадратных матриц порядка 2 множество всех матриц вида $\begin{pmatrix} 0 & a \\ b & c \end{pmatrix}$.
3. $\mathbb{Z}/33\mathbb{Z}$.
4. $\alpha x^5 + \gamma x^3 + \beta x + 1$.

5. а) $s(x) = x^7 + x^3 + x^2 + 1$; б) $t(x) = x^7 + x^6 + x^4 + x + 1$.

6. $s(x) = x^6 + 2x^5 + 2x^3 + x + 2$.

Вариант 15

1. а) $\{623k \mid k \in \mathbb{Z}\}$; б) $\{6k^2 - 5k + 1 \mid k \in \mathbb{Z}\}$.

2. В кольце вещественных квадратных матриц порядка 2 множество всех матриц вида $\begin{pmatrix} 0 & a \\ b & 0 \end{pmatrix}$.

3. $\mathbb{Z}/42\mathbb{Z}$.

4. $\alpha x^4 + 3\beta x^3 + 3\gamma x^2 + 4$.

5. а) $s(x) = x^6 + x^4 + x^3 + 1$; б) $t(x) = x^7 + x + 1$.

6. $s(x) = x^6 + 2x^3 + 2x^2 + x + 2$.

МОДУЛЬ № 5. КОНЕЧНЫЕ ПОЛЯ

ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ ПО ТЕМЕ «КОНЕЧНЫЕ ПОЛЯ»¹

§ 1. Фактор-кольца

Рассмотрим кольцо K с собственным двусторонним идеалом J . По определению всякое кольцо является аддитивной абелевой группой (см. модуль 4, определение 4.1), а идеал J является подгруппой этой группы, причем в силу ее коммутативности идеал J – нормальная подгруппа (см. модуль 2, определение 2.19). Рассмотрим множество смежных классов (или классов смежности) по подгруппе J , обозначаемое K/J .

Напомним, что смежный класс по аддитивной подгруппе J представляет собой множество всевозможных сумм $a + j$, где $j \in J$, a – фиксированный элемент кольца K . Этот смежный класс обозначается $a + J$, $a \in K$:

$$a + J = \{a + j \mid j \in J\}.$$

Говорят, что элементы одного и того же смежного класса *сравнимы между собой по модулю J* .

Множество K/J смежных классов является фактор-группой относительно индуцированной операции сложения (см. модуль 2, теорему 2.13). Это означает, что смежные классы по подгруппе J можно складывать друг с другом. Правило сложения классов $(a + J)$ и $(b + J)$ задается следующим образом:

$$(a + J) + (b + J) = (a + b) + J,$$

т. е. сумма двух классов $(a + J)$ и $(b + J)$ является классом, содержащим элемент $a + b$.

Так как в кольце K задана также операция умножения элементов a и b , то можно определить и операцию умножения смежных классов. Зададим ее формулой

$$(a + J) \cdot (b + J) = ab + J,$$

т. е. произведением двух классов $(a + J)$ и $(b + J)$ является классом, содержащим элемент $a \cdot b$.

Корректность такого определения операции умножения следует из того, что смежный класс $ab + J$, получаемый в результате произведения, не зависит от выбора представителей перемножаемых классов (доказательство этого утверждения изложено в [20]).

Теорема 5.1. *Если J – двусторонний идеал кольца K , то множество K/J смежных классов с введенными на нем операциями сложения и умножения по правилам*

$$(a + J) + (b + J) = (a + b) + J, \quad (a + J) \cdot (b + J) = ab + J$$

¹ При подготовке данного раздела использовались следующие источники: [5, 6, 16, 20, 21].

является кольцом. Если кольцо K коммутативно, то и кольцо K/J также коммутативно.

Определение 5.1. Фактор-кольцо K/J кольца K по идеалу J – это множество K/J смежных классов с введенными на нем операциями сложения и умножения согласно правилам теоремы 5.1.

Пример 5.1. Кольцо классов вычетов $\mathbb{Z}/m\mathbb{Z}$ является фактор-кольцом кольца целых чисел $\mathbb{Z}$ по идеалу, порожденному числом m : $\langle m \rangle = \{mq | q \in \mathbb{Z}\}$.

Пример 5.2. В кольце полиномов $P[x]$ с действительными коэффициентами можно построить фактор-кольцо смежных классов по идеалу $\langle f(x) \rangle$, порожденному полиномом $f(x)$. Смежные классы этого фактор-кольца представляют собой множества вида $\bar{r} = \{r(x) + f(x)q(x) | q(x) \in P[x]\}$, где $r(x)$ – полином степени ниже степени $f(x)$. Подробно случай построения такого фактор-кольца разобран в решении типовых задач лабораторной работы «Конечные поля».

Понятие фактор-кольца позволяет строить на основании известных колец другие алгебраические структуры, в частности поля с конечным числом элементов.

Теорема 5.2. Фактор-кольцо K/J коммутативного ассоциативного кольца K с единицей по идеалу J является полем тогда и только тогда, когда идеал J – максимальный.

Пример 5.3. Кольцо классов вычетов $\mathbb{Z}/p\mathbb{Z}$ по простому модулю p – это фактор-кольцо кольца целых чисел по идеалу $\langle p \rangle = \{pq | q \in \mathbb{Z}\}$. Как было показано в модуле 4 «Кольца. Идеалы колец», этот идеал максимален. Согласно теореме 5.2, кольцо классов вычетов должно быть полем. Это действительно так, поскольку каждый ненулевой класс вычетов по простому модулю обратим, что было показано в модуле 2.

§ 2. Вычисления в конечных полях

Определение 5.2. Конечное поле – это поле, число элементов которого конечно. Такие поля также называются **полями Галуа** и обозначаются $GF(q)$, где q – количество элементов поля Галуа.

Пример 5.4. Любое кольцо классов вычетов по простому модулю $\mathbb{Z}/p\mathbb{Z}$ – конечное поле.

Определение 5.3. Характеристика поля – наименьшее натуральное число n , такое, что в поле P сумма n единиц равна нулю. Если такого n не существует, то говорят, что поле имеет характеристику ноль. В противном случае P называют полем положительной характеристики.

Характеристика поля P обозначается $\text{char } P$.

Пример 5.5. Поле $\mathbb{Z}/2\mathbb{Z}$ – поле характеристики 2. Действительно, в нем $\bar{1} + \bar{1} = \bar{0}$, т. е. сумма двух единиц равна нулю.

Теорема 5.3 Если поле P – поле положительной характеристики p , то p может быть только простым числом.

Теорема 5.4 Для любого простого p и для любого натурального числа n существует единственное с точностью до изоморфизма конечное поле, содержащее p^n элементов.

Свойства конечного поля $GF(p^n)$:

1. Имеет характеристику p .
2. Является линейным пространством над полем $\mathbb{Z}/p\mathbb{Z}$, размерность этого пространства равна n .
3. Поле $\mathbb{Z}/p\mathbb{Z}$ является подполем поля $GF(p^n)$.
4. С точностью до изоморфизма поле $GF(p^n)$ совпадает с фактор-кольцом $(\mathbb{Z}/p\mathbb{Z})[x]/\langle f(x) \rangle$ кольца полиномов $(\mathbb{Z}/p\mathbb{Z})[x]$ по идеалу $\langle f(x) \rangle$, порожденному неприводимым многочленом $f(x)$ степени n .
5. Мультипликативная группа конечного поля $GF(p^n)$ является циклической.

Определение 5.4. Примитивный элемент – всякая образующая мультипликативной группы конечного поля $GF(p^n)$.

Свойства 4 и 5 позволяют задать элементы конечного поля. Согласно свойству 4, для любого числа p^n можно построить конечное поле $GF(p^n)$, состоящее из смежных классов кольца $(\mathbb{Z}/p\mathbb{Z})[x]$ по идеалу $\langle f(x) \rangle$. Эти классы задаются формулой

$$\bar{r} = \{r(x) + f(x)q(x) | q(x) \in (\mathbb{Z}/p\mathbb{Z})[x]\},$$

где $r(x) \in (\mathbb{Z}/p\mathbb{Z})[x]$.

Каждый класс полностью определяется полиномом $r(x)$ степени ниже степени неприводимого над $\mathbb{Z}/p\mathbb{Z}$ полинома $f(x)$, поэтому, для того чтобы задать все элементы конечного поля, достаточно перечислить все такие полиномы $r(x)$. Операции сложения и умножения элементов поля задаются правилами сложения и умножения смежных классов $\bar{r}$.

С другой стороны, исходя из свойства 5, все ненулевые элементы поля $GF(p^n)$ можно представить в виде α^k , где α – примитивный элемент, $1 \leq k \leq p^n - 1$. В данном случае конкретная природа примитивного элемента α не существенна, а важно установить правила, по которым выполняется операция сложения различных степеней α . Эти правила следуют из общих свойств элементов конечных полей. Укажем основные из этих свойств.

Свойства элементов конечного поля $GF(p^n)$:

1. Все элементы конечного поля $GF(p^n)$ являются корнями уравнения $x^{p^n} - x = 0$ (обобщенная теорема Ферма).

2. Примитивный элемент α поля Галуа $GF(p^n)$ всегда является корнем неприводимого над $\mathbb{Z}/p\mathbb{Z}$ полинома степени n из кольца полиномов $(\mathbb{Z}/p\mathbb{Z})[x]$, причем все остальные корни этого полинома также являются примитивными элементами. Такой полином называется **примитивным**.

3. Если примитивный элемент α является корнем неприводимого многочлена $f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_0$, то для любой степени k такой, что $n \leq k \leq p^n - 1$, можно представить α^k в виде линейной комбинации степеней примитивного элемента α : $\alpha^0 = 1, \alpha, \alpha^2, \dots, \alpha^{k-1}$ с коэффициентами из поля $\mathbb{Z}/p\mathbb{Z}$. Это следует из цепочки равенств:

$$\begin{aligned} \alpha^n + a_{n-1}\alpha^{n-1} + \dots + a_0 &= 0 \Rightarrow \\ \Rightarrow \alpha^n &= -a_{n-1}\alpha^{n-1} - \dots - a_0 \Rightarrow \\ \Rightarrow \alpha^{n+1} &= \alpha(-a_{n-1}\alpha^{n-1} - \dots - a_0) = -a_{n-1}\alpha^n - \dots - a_0\alpha = \\ &= -a_{n-1}(-a_{n-1}\alpha^{n-1} - \dots - a_0) - \dots - a_0\alpha \Rightarrow \dots \end{aligned}$$

4. Из свойства 3 следует, что любой элемент конечного поля $GF(p^n)$ может быть представлен как n -мерный вектор линейного пространства $GF(p^n)$ в базисе $1, \alpha, \alpha^2, \dots, \alpha^{k-1}$ с коэффициентами из поля $\mathbb{Z}/p\mathbb{Z}$. Такое задание элементов поля называется аддитивным.

Пользуясь свойством 3 элементов поля Галуа, можно составить таблицу соответствия степеней примитивного элемента и n -мерных векторов в базисе $1, \alpha, \alpha^2, \dots, \alpha^{k-1}$. Эта таблица устанавливает взаимно однозначную связь между мультипликативным и аддитивным способами задания поля. При решении практических задач для выполнения операции умножения рационально использовать мультипликативное задание элементов, а для выполнения операции сложения – аддитивное.

Таким образом, приходим к выводу о том, что если ненулевые элементы конечного поля заданы как степени примитивного элемента, то для выполнения операции сложения необходимо знать конкретный вид примитивного полинома, имеющий среди корней используемый примитивный элемент. Примитивный полином – всегда неприводимый над полем $\mathbb{Z}/p\mathbb{Z}$. Число неприводимых полиномов над полем $\mathbb{Z}/p\mathbb{Z}$ конечно, однако только в случае, если $p^n - 1$ является простым числом, можно гарантировать, что любой неприводимый полином является примитивным. В остальных случаях среди неприводимых полиномов могут встретиться непримитивные, и тогда требуется непосредственная проверка того, является ли корень выбранного полинома примитивным элементом. В процессе проверки вычисляются степени корня полинома по схеме, приведенной в свойстве 3 элементов поля Галуа, и если $\alpha^k = 1$ при $k < p^n$, то полином примитивным не является.

ТИПОВЫЕ ЗАДАНИЯ ПО ТЕМЕ «КОНЕЧНЫЕ ПОЛЯ» С ОБРАЗЦАМИ РЕШЕНИЙ

Задание 1. Задан многочлен $f(x)$ с коэффициентами из поля $\mathbb{Z}/2\mathbb{Z}$.

а) $f(x) = x^2 + 1$; б) $f(x) = x^3 + x^2 + 1$.

Для обоих пунктов выполнить следующие задания:

- 1) Выяснить, является ли многочлен $f(x)$ неприводимым.
- 2) Перечислить все элементы фактор-кольца K/J , где K – кольцо многочленов $K = (\mathbb{Z}/2\mathbb{Z})[x]$, а J – идеал этого кольца, порожденный многочленом $f(x)$: $J = \langle f(x) \rangle$.
- 3) Составить таблицы сложения и умножения элементов указанного фактор-кольца.
- 4) Пользуясь составленными таблицами, выписать пары взаимно обратных элементов.
- 5) Определить порядок мультипликативной группы фактор-кольца K/J .
- 6) Выяснить, является ли мультипликативная группа фактор-кольца циклической. Если является, указать ее образующий элемент.
- 7) Выяснить, является ли фактор-кольцо K/J полем.

Решение

Пункт «а» $f(x) = x^2 + 1$:

1. Так как $f(1) = 1^2 + 1 = 0$ в поле $\mathbb{Z}/2\mathbb{Z}$, т. е. 1 является корнем многочлена $f(x)$, то по теореме Безу $f(x)$ делится на $x - 1$ (над полем $\mathbb{Z}/2\mathbb{Z}$ $x - 1 = x + 1$), а следовательно, является приводимым: $x^2 + 1 = (x + 1)^2$ (обратите внимание, что при возведении в квадрат слагаемое $2x$ обращается в 0, так как в поле $\mathbb{Z}/2\mathbb{Z}$ $2 = 0$).

2. Элементами фактор-кольца K/J , где J – идеал кольца K , являются смежные классы по подгруппе J аддитивной группы кольца K . Согласно определению (см. модуль 2), смежный класс по аддитивной подгруппе J можно построить, выбрав элемент a кольца K и найдя для этого элемента все возможные суммы вида $a + j$, где $j \in J$. Из такого построения следует, что разность любых двух элементов $b_1 = a + j_1, j_1 \in J$ и $b_2 = a + j_2, j_2 \in J$ одного смежного класса по идеалу J принадлежит этому идеалу: $b_2 - b_1 = a + j_2 - (a + j_1) = j_2 - j_1 = j_3 \in J$ ($j_2 - j_1 \in J$ по критерию подгруппы J).

Рассмотрим в качестве кольца K кольцо многочленов $P[x]$ с коэффициентами из поля P , а в качестве идеала J этого кольца – идеал, порожденный многочленом $f(x)$: $J = \langle f(x) \rangle$, т. е. состоящий из всевозможных произведений многочленов $f(x)q(x), q(x) \in P[x]$. Тогда, согласно выводу, сделанному в предыдущем абзаце, разность любых двух многочленов $g_1(x)$ и $g_2(x)$ одного смежного класса по J принадлежит идеалу J , что равносильно выражению

$$g_2(x) - g_1(x) = f(x)q(x), q(x) \in P[x].$$

Это равенство возможно тогда и только тогда, когда многочлены $g_1(x)$ и $g_2(x)$ имеют равные остатки от деления на многочлен $f(x)$. Следовательно, все элементы смежного класса по $J = \langle f(x) \rangle$, и только они, при делении на $f(x)$ имеют один и тот же остаток $r(x)$. Таким образом, смежный класс по J полностью определяется остатком $r(x)$, а элементами этого класса являются многочлены вида $r(x) + f(x)q(x), q(x) \in P[x]$. Далее будем обозначать такой смежный класс $\overline{r(x)}$:

$$\overline{r(x)} = \{r(x) + f(x)q(x) \mid q(x) \in P[x]\}.$$

Таким образом, для указания всех элементов фактор-кольца $P[x]/\langle f(x) \rangle$ (всех смежных классов) достаточно перечислить всевозможные остатки от деления на многочлен $f(x)$. Эти остатки представляют множество всех многочленов из кольца $P[x]$, степень которых ниже степени $f(x)$. Если поле P , над которым задано кольцо многочленов $P[x]$, конечно, то и число таких многочленов также конечно.

Перечислим все элементы фактор-кольца $(\mathbb{Z}/2\mathbb{Z})[x]/\langle f(x) \rangle$, где $f(x) = x^2 + 1$. Ими являются все смежные классы по $\langle f(x) \rangle$, задаваемые многочленами меньше второй, т. е. нулевой и первой степени с коэффициентами из $\mathbb{Z}/2\mathbb{Z}$:

$$(\mathbb{Z}/2\mathbb{Z})[x]/\langle x^2 + 1 \rangle = \{\bar{0}, \bar{1}, \bar{x}, \overline{x+1}\}.$$

Отметим, что над полем $\mathbb{Z}/2\mathbb{Z}$ количество многочленов степени меньшей, чем n , равно 2^n . Конкретно в данном случае $n = 2$, откуда количество многочленов степени меньше второй равно четырем.

3. В фактор-кольце K/J определены операции сложения и умножения смежных классов. Сформулируем правила этих операций для случая фактор-кольца $P[x]/\langle f(x) \rangle$.

Суммой классов $\overline{r_1(x)}$ и $\overline{r_2(x)}$ называется такой класс $\overline{r_3(x)}$, который содержит многочлен $r_1(x) + r_2(x)$. Например, суммой классов $\bar{x}$ и $\overline{x+1}$ будет являться класс, содержащий $x + x + 1 = 2x + 1 = 1$ (здесь учитываем, что в $\mathbb{Z}/2\mathbb{Z}$ $2 = 0$). Очевидно, этим классом является $\bar{1}$. Таким образом, $\bar{x} + \overline{x+1} = \bar{1}$.

Согласно приведенному правилу найдем все возможные суммы элементов фактор-кольца $(\mathbb{Z}/2\mathbb{Z})[x]/\langle f(x) \rangle$, записывая их в таблицу 11 (в ячейке содержится сумма классов, указанных в соответствующих строке и столбце).

Таблица сложения элементов фактор-кольца $(\mathbb{Z}/2\mathbb{Z})[x]/\langle f(x) \rangle$

$\oplus$	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$	$\overline{x+1}$	$\bar{x}$
$\bar{x}$	$\bar{x}$	$\overline{x+1}$	$\bar{0}$	$\bar{1}$
$\overline{x+1}$	$\overline{x+1}$	$\bar{x}$	$\bar{1}$	$\bar{0}$

Произведением классов $\overline{r_1(x)}$ и $\overline{r_2(x)}$ называется такой класс $\overline{r_3(x)}$, который содержит многочлен $r_1(x)r_2(x)$. Если произведение многочленов $r_1(x)r_2(x)$ имеет степень равную или большую, чем степень полинома $f(x)$, породившего идеал J , то для того, чтобы установить класс, который содержит $r_1(x)r_2(x)$, необходимо найти остаток от деления многочлена $r_1(x)r_2(x)$ на $f(x)$.

Например, произведением классов $\bar{1}$ и $\overline{x+1}$ будет являться класс, содержащий $1(x+1) = x+1$. Очевидно, что $\bar{1} \cdot \overline{x+1} = \overline{x+1}$.

Произведением классов $\bar{x}$ и $\overline{x+1}$ будет являться класс, содержащий $x(x+1) = x^2 + x$. Его степень равна степени многочлена $f(x) = x^2 + 1$, породившего идеал J . Найдем остаток от деления $x^2 + x$ на $f(x)$. Для этого можно выполнить деление многочлена на многочлен в столбик (см. модуль 4), но можно записать тождество: $x^2 + x = (x^2 + 1) + x + 1$. Здесь, как и везде выше, учитывается, что в $\mathbb{Z}/2\mathbb{Z}$ $2 = 0$. Из этого тождества видно, что остатком от деления $x^2 + x$ на $f(x) = x^2 + 1$ является $x + 1$. Таким образом, $\bar{x} \cdot \overline{x+1} = \overline{x+1}$.

Согласно приведенному правилу, найдем все возможные произведения элементов фактор-кольца $(\mathbb{Z}/2\mathbb{Z})[x]/\langle f(x) \rangle$ и запишем их в таблицу 12 (в ячейке содержится произведение классов, указанных в соответствующих строке и столбце).

Таблица 12

Таблица сложения элементов фактор-кольца $(\mathbb{Z}/2\mathbb{Z})[x]/\langle f(x) \rangle$

$\otimes$	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$
$\bar{x}$	$\bar{0}$	$\bar{x}$	$\bar{1}$	$\overline{x+1}$
$\overline{x+1}$	$\bar{0}$	$\overline{x+1}$	$\overline{x+1}$	$\bar{0}$

Симметрия заполнения обеих таблиц отражает свойство коммутативности сложения и умножения классов.

4. Взаимно обратными элементами будут являться такие элементы фактор-кольца, произведение которых равно классу $\bar{1}$. Каждый из взаимно обратных элементов обратим. Используя таблицу умножения, выпишем обратимые элементы: класс $\bar{1}$ и класс $\bar{x}$ (взаимно обратные самим себе).

5. Мультипликативную группу $(K/J)^*$ фактор-кольца K/J образуют все обратимые элементы. В данном случае только два элемента обратимы – это $\bar{1}$ и $\bar{x}$. Следовательно, $((\mathbb{Z}/2\mathbb{Z})[x]/\langle f(x) \rangle)^* = \{\bar{1}, \bar{x}\}$. Таким образом, порядок мультипликативной группы фактор-кольца $(\mathbb{Z}/2\mathbb{Z})[x]/\langle f(x) \rangle$ равен двум.

6. Любая мультипликативная группа из двух элементов является циклической, следовательно, $((\mathbb{Z}/2\mathbb{Z})[x]/\langle f(x) \rangle)^*$ – это циклическая группа с образующим элементом $\bar{x}$.

7. Поскольку среди ненулевых элементов фактор-кольца $(\mathbb{Z}/2\mathbb{Z})[x]/\langle f(x) \rangle$ есть необратимые, то данное фактор-кольцо не является полем.

Пункт «б» $f(x) = x^3 + x^2 + 1$.

1. Как было отмечено в модуле 4, для того чтобы убедиться в неприводимости многочлена третьей степени над полем $\mathbb{Z}/p\mathbb{Z}$, достаточно убедиться, что он не имеет корней, принадлежащих этому полю. Выполним проверку наличия корней многочлена среди элементов поля $\mathbb{Z}/2\mathbb{Z}$:

$$f(0) = 1 \neq 0$$

$$f(1) = 1 + 1 + 1 = 3 = 1 \neq 0$$

Таким образом, $f(x)$ не имеет корней в поле $\mathbb{Z}/2\mathbb{Z}$, следовательно, он является неприводимым.

2. Как было показано в пункте «а», элементами фактор-кольца $(\mathbb{Z}/2\mathbb{Z})[x]/\langle f(x) \rangle$ являются смежные классы по идеалу $\langle f(x) \rangle$, каждый класс полностью определяется многочленом из $(\mathbb{Z}/2\mathbb{Z})[x]$, степень которого ниже степени $f(x)$. В случае, когда $f(x) = x^3 + x^2 + 1$, имеем:

$$(\mathbb{Z}/2\mathbb{Z})[x]/\langle x^3 + x^2 + 1 \rangle = \{\bar{0}, \bar{1}, \bar{x}, \overline{x+1}, \overline{x^2}, \overline{x^2+1}, \overline{x^2+x}, \overline{x^2+x+1}\}.$$

3. Таблицы сложения (таблица 13) и умножения (таблица 14) смежных классов по $\langle f(x) \rangle$ в фактор-кольце $(\mathbb{Z}/2\mathbb{Z})[x]/\langle f(x) \rangle$ составляются по тем же правилам, что и в пункте «а» – эти правила являются общими для сложения и умножения в любых фактор-кольцах вида $(\mathbb{Z}/p\mathbb{Z})[x]/\langle f(x) \rangle$. Для примера здесь

приведем подробные вычисления произведения классов $\overline{x^2 + x + 1}$ и $\overline{x^2 + 1}$.

$$(x^2 + x + 1)(x^2 + 1) = x^4 + x^3 + x^2 + x^2 + x + 1 = x^4 + x^3 + x + 1.$$

Здесь учтено, что $x^2 + x^2 = 2x^2 = 0$.

Найдем остаток от деления многочлена $x^4 + x^3 + x + 1$ на многочлен $f(x) = x^3 + x^2 + 1$:

$$\begin{array}{r} \overline{x^4 + x^3 + 0x^2 + x + 1} \overline{x^3 + x^2 + 1} \\ \underline{\overline{x^4 + x^3 + 0x^2 + x} \quad | x} \\ +1 \end{array}$$

Следовательно, $\overline{x^2 + x + 1} \cdot \overline{x^2 + 1} = \bar{1}$.

4. Пользуясь составленной таблицей умножения, выпишем пары взаимно обратных элементов, в произведении дающих класс $\bar{1}$:

$(\bar{x}, \overline{x^2 + x}), (\overline{x + 1}, \overline{x^2}), (\overline{x^2 + 1}, \overline{x^2 + x + 1})$. Элемент $\bar{1}$ является взаимно обратным самому себе.

5. Как следует из предыдущего пункта решения, мультипликативную группу $((\mathbb{Z}/2\mathbb{Z})[x]/\langle f(x) \rangle)^*$ составляют все ненулевые элементы фактор-кольца:

$$((\mathbb{Z}/2\mathbb{Z})[x]/\langle x^3 + x^2 + 1 \rangle)^* = \{\bar{1}, \bar{x}, \overline{x + 1}, \overline{x^2}, \overline{x^2 + 1}, \overline{x^2 + x}, \overline{x^2 + x + 1}\}.$$

Порядок этой группы равен семи (числу ее обратимых членов).

Таблица 13

Таблица сложения элементов фактор-кольца $(\mathbb{Z}/2\mathbb{Z})[x]/\langle f(x) \rangle$

$\oplus$	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$	$\overline{x^2}$	$\overline{x^2+1}$	$\overline{x^2+x}$	$\overline{x^2+x+1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$	$\overline{x^2}$	$\overline{x^2+1}$	$\overline{x^2+x}$	$\overline{x^2+x+1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$	$\overline{x+1}$	$\bar{x}$	$\overline{x^2+1}$	$\overline{x^2}$	$\overline{x^2+x+1}$	$\overline{x^2+x}$
$\bar{x}$	$\bar{x}$	$\overline{x+1}$	$\bar{0}$	$\bar{1}$	$\overline{x^2+x}$	$\overline{x^2+x+1}$	$\overline{x^2}$	$\overline{x^2+1}$
$\overline{x+1}$	$\overline{x+1}$	$\bar{x}$	$\bar{1}$	$\bar{0}$	$\overline{x^2+x+1}$	$\overline{x^2+x}$	$\overline{x^2+1}$	$\overline{x^2}$
$\overline{x^2}$	$\overline{x^2}$	$\overline{x^2+1}$	$\overline{x^2+x}$	$\overline{x^2+x+1}$	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$
$\overline{x^2+1}$	$\overline{x^2+1}$	$\overline{x^2}$	$\overline{x^2+x+1}$	$\overline{x^2+x}$	$\bar{1}$	$\bar{0}$	$\overline{x+1}$	$\bar{x}$
$\overline{x^2+x}$	$\overline{x^2+x}$	$\overline{x^2+x+1}$	$\overline{x^2}$	$\overline{x^2+1}$	$\bar{x}$	$\overline{x+1}$	$\bar{0}$	$\bar{1}$
$\overline{x^2+x+1}$	$\overline{x^2+x+1}$	$\overline{x^2+x}$	$\overline{x^2+1}$	$\overline{x^2}$	$\overline{x+1}$	$\bar{x}$	$\bar{1}$	$\bar{0}$

Таблица 14

Таблица умножения элементов фактор-кольца $(\mathbb{Z}/2\mathbb{Z})[x]/\langle f(x) \rangle$

$\otimes$	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$	$\overline{x^2}$	$\overline{x^2+1}$	$\overline{x^2+x}$	$\overline{x^2+x+1}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$	$\overline{x^2}$	$\overline{x^2+1}$	$\overline{x^2+x}$	$\overline{x^2+x+1}$
$\bar{x}$	$\bar{0}$	$\bar{x}$	$\overline{x^2}$	$\overline{x^2+x}$	$\overline{x^2+1}$	$\overline{x^2+x+1}$	$\bar{1}$	$\overline{x+1}$
$\overline{x+1}$	$\bar{0}$	$\overline{x+1}$	$\overline{x^2+x}$	$\overline{x^2+1}$	$\bar{1}$	$\bar{x}$	$\overline{x^2+x+1}$	$\overline{x^2}$
$\overline{x^2}$	$\bar{0}$	$\overline{x^2}$	$\overline{x^2+1}$	$\bar{1}$	$\overline{x^2+x+1}$	$\overline{x+1}$	$\bar{x}$	$\overline{x^2+x}$
$\overline{x^2+1}$	$\bar{0}$	$\overline{x^2+1}$	$\overline{x^2+x+1}$	$\bar{x}$	$\overline{x+1}$	$\overline{x^2+x}$	$\overline{x^2}$	$\bar{1}$
$\overline{x^2+x}$	$\bar{0}$	$\overline{x^2+x}$	$\bar{1}$	$\overline{x^2+x+1}$	$\bar{x}$	$\overline{x^2}$	$\overline{x+1}$	$\overline{x^2+1}$
$\overline{x^2+x+1}$	$\bar{0}$	$\overline{x^2+x+1}$	$\overline{x+1}$	$\overline{x^2}$	$\overline{x^2+x}$	$\bar{1}$	$\overline{x^2+1}$	$\bar{x}$

6. Получена мультипликативная группа $((\mathbb{Z}/2\mathbb{Z})[x]/\langle f(x) \rangle)^*$ простого порядка, тогда, согласно следствию из теоремы Лагранжа, она является циклической. Циклическая группа порядка g имеет $\varphi(g)$ образующих, поэтому если g – простое число, то эта группа будет иметь $g - 1$ образующих. Это означает, что любой элемент, кроме $\bar{1}$, является образующей циклической мультипликативной группы $((\mathbb{Z}/2\mathbb{Z})[x]/\langle f(x) \rangle)^*$. Если бы порядок циклической группы был составным числом, то искать образующую пришлось бы непосредственным перебором.

7. Так как все ненулевые элементы фактор-кольца $(\mathbb{Z}/2\mathbb{Z})[x]/\langle f(x) \rangle$ являются обратимыми, то исследуемое фактор-кольцо является полем. Этот вывод можно было сделать и без составления таблицы умножения, так как, в соответствии с теоремой 5.2, фактор-кольцо K/J является полем тогда и только тогда, когда идеал J максимальный. Поскольку в первом пункте решения было показано, что многочлен $f(x)$ неприводимый, то порождаемый им идеал $J = \langle f(x) \rangle$ является максимальным, следовательно, $(\mathbb{Z}/2\mathbb{Z})[x]/\langle f(x) \rangle$ – поле. Обратим также внимание на то, что как только установлено, что фактор-кольцо является полем, на основании свойства 5 полей можно сразу сделать вывод о том, что его мультипликативная группа является циклической. Тот факт, что любой элемент, кроме $\bar{1}$, является ее образующей, следует из более общего утверждения для любых групп простого порядка. ▲

Задание 2. Построить поле Галуа из шестнадцати элементов $GF(16) = GF(2^4)$.

Решение

Согласно свойствам конечных полей, одним из способов решения этой задачи является построение фактор-кольца $(\mathbb{Z}/2\mathbb{Z})[x]/\langle f(x) \rangle$, где $f(x)$ – неприводимый полином четвертой степени над полем $\mathbb{Z}/2\mathbb{Z}$. Элементами такого поля являются полиномы степени не выше третьей, и, хотя перечислить их несложно, но операции сложения, а особенно, умножения, являются громоздкими и требуют составления соответствующих таблиц. Уже в случае поля с восемью элементами эти таблицы содержат 64 ячейки и не очень удобны в пользовании. Чтобы построить искомое поле и сделать операции над его элементами более простыми с точки зрения вычислений, воспользуемся тем фактом, что все конечные поля из шестнадцати элементов изоморфны между собой, следовательно, можно не конкретизировать природу элементов этого поля, а опираться на следующие свойства конечных полей:

- любое конечное поле можно представить как его мультипликативную группу, дополненную нулевым элементом: $GF(m) = \{0\} \cup (GF(m))^*$;
- мультипликативная группа любого конечного поля является циклической, поэтому для ее построения достаточно указать ее образующую α – примитивный элемент;

- примитивный элемент поля Галуа $GF(p^n)$ является корнем неприводимого над $\mathbb{Z}/p\mathbb{Z}$ полинома степени n из кольца многочленов $\mathbb{Z}/p\mathbb{Z}$, где p – простое число. Благодаря этому факту можно представить любую степень α , большую n , в виде линейной комбинации степеней $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$ с коэффициентами из поля $\mathbb{Z}/p\mathbb{Z}$.

Тогда построение конечного поля сводится к тому, чтобы указать примитивный полином – неприводимый полином степени n такой, чтобы его корень был образующей мультипликативной группы $GF(p^n)$. В случае если $p^n - 1$ является простым числом, то любой неприводимый полином степени n будет примитивным. Если же $p^n - 1$ является составным, то для выбранного полинома необходимо выполнить непосредственную проверку, являются ли его корни примитивными, и в случае отрицательного ответа перейти к проверке следующего неприводимого полинома. После того, как установлен необходимый примитивный полином, следует с его помощью составить таблицу соответствия степеней примитивного элемента линейным комбинациям степеней $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$ с коэффициентами из поля $\mathbb{Z}/p\mathbb{Z}$.

В данном случае необходимо построить поле $GF(16) = GF(2^4)$. Число $2^4 - 1 = 15$ не является простым, поэтому необходимо проверкой подобрать примитивный полином.

Над полем $\mathbb{Z}/2\mathbb{Z}$ есть три неприводимых полинома четвертой степени: $x^4 + x^3 + x^2 + x + 1$, $x^4 + x^3 + 1$ и $x^4 + x + 1$.

Проверим полином $x^4 + x^3 + x^2 + x + 1$. Если α – его корень в поле $GF(2^4)$, тогда $\alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1 = 0$. Выразим из этого равенства α^4 , учитывая, что $-1 = 1$ в поле $\mathbb{Z}/2\mathbb{Z}$: $\alpha^4 = -\alpha^3 - \alpha^2 - \alpha - 1 = \alpha^3 + \alpha^2 + \alpha + 1$. Найдем α^5 , умножив обе части полученного выражения на α :

$$\alpha^5 = \alpha(\alpha^3 + \alpha^2 + \alpha + 1) = \alpha^4 + \alpha^3 + \alpha^2 + \alpha.$$

В последнее выражение подставим равенство $\alpha^4 = \alpha^3 + \alpha^2 + \alpha + 1$ и помня, что $2 = 0$ в $\mathbb{Z}/2\mathbb{Z}$, получим

$$\alpha^5 = \alpha^3 + \alpha^2 + \alpha + 1 + \alpha^3 + \alpha^2 + \alpha = 1.$$

Поскольку $\alpha^5 = 1$, то порядок этого элемента равен 5 и не совпадает с порядком мультипликативной группы, равным 15. Следовательно, α не является образующей этой циклической группы.

Перейдем к проверке следующего полинома $x^4 + x^3 + 1$. Пусть α – его корень в поле $GF(2^4)$, тогда $\alpha^4 = \alpha^3 + 1$. Найдем выражения для более высоких степеней α , всякий раз заменяя в вычислениях $\alpha^4 = \alpha^3 + 1$ и учитывая, что $2 = 0$ в $\mathbb{Z}/2\mathbb{Z}$:

$$\alpha^5 : \alpha^5 = \alpha(\alpha^3 + 1) = \alpha^4 + \alpha = \alpha^3 + 1 + \alpha = \alpha^3 + \alpha + 1;$$

$$\alpha^6 : \alpha^6 = \alpha(\alpha^3 + \alpha + 1) = \alpha^4 + \alpha^2 + \alpha = \alpha^3 + 1 + \alpha^2 + \alpha = \alpha^3 + \alpha^2 + \alpha + 1;$$

$$\alpha^7 : \alpha^7 = \alpha(\alpha^3 + \alpha^2 + \alpha + 1) = \alpha^4 + \alpha^3 + \alpha^2 + \alpha = \alpha^3 + 1 + \alpha^3 + \alpha^2 + \alpha = \alpha^2 + \alpha + 1;$$

$$\alpha^8 : \alpha^8 = \alpha(\alpha^2 + \alpha + 1) = \alpha^3 + \alpha^2 + \alpha;$$

$$\alpha^9 : \alpha^9 = \alpha(\alpha^3 + \alpha^2 + \alpha) = \alpha^4 + \alpha^3 + \alpha^2 = \alpha^3 + 1 + \alpha^3 + \alpha^2 = \alpha^2 + 1;$$

$$\alpha^{10} : \alpha^{10} = \alpha(\alpha^2 + 1) = \alpha^3 + \alpha;$$

$$\alpha^{11} : \alpha^{11} = \alpha(\alpha^3 + \alpha) = \alpha^4 + \alpha^2 = \alpha^3 + 1 + \alpha^2 = \alpha^3 + \alpha^2 + 1;$$

$$\alpha^{12} : \alpha^{12} = \alpha(\alpha^3 + \alpha^2 + 1) = \alpha^4 + \alpha^3 + \alpha = \alpha^3 + 1 + \alpha^3 + \alpha = \alpha + 1;$$

$$\alpha^{13} : \alpha^{13} = \alpha(\alpha + 1) = \alpha^2 + \alpha;$$

$$\alpha^{14} : \alpha^{13} = \alpha(\alpha^2 + \alpha) = \alpha^3 + \alpha^2;$$

$$\alpha^{15} : \alpha^{15} = \alpha(\alpha^3 + \alpha^2) = \alpha^4 + \alpha^3 = \alpha^3 + 1 + \alpha^3 = 1.$$

Таким образом, получили, что $\alpha^{15} = 1$, следовательно, порядок элемента α совпадает с порядком циклической группы. Это означает, что корень многочлена $x^4 + x^3 + 1$ является образующей мультипликативной группы $(GF(2^4))^*$, т. е. примитивным элементом, а многочлен $x^4 + x^3 + 1$ является примитивным многочленом.

Итак, поле $GF(2^4)$ состоит из всех степеней α от первой до пятнадцатой, дополненных нулевым элементом. Обратите внимание на то, что мы не указываем конкретно, чем является α – полиномом, числом, классом вычетов, матрицей или элементом другой природы, для построения поля нам достаточно знать лишь свойство о том, что при подстановке элемента α в $x^4 + x^3 + 1$ он обращается в нуль. Благодаря этому свойству каждый другой ненулевой элемент поля $GF(2^4)$ может быть задан либо как степень α , что представляет собой мультипликативное задание поля, либо как линейная комбинация его степеней не выше третьей с коэффициентами из $\mathbb{Z}/2\mathbb{Z}$, что соответствует аддитивному заданию поля. Этих представлений вполне достаточно, чтобы проводить все необходимые действия над элементами поля Галуа $GF(2^4)$.

Элементы поля запишем в таблицу 15, указывая для степени примитивного элемента α соответствующую ей линейную комбинацию степеней α не выше третьей.

Таблица 15

Таблица соответствия мультипликативной и аддитивной форм задания элементов поля Галуа $GF(2^4)$

Степень примитивного элемента	Линейная комбинация $1, \alpha, \alpha^2, \alpha^3$
α	α
α^2	α^2
α^3	α^3
α^4	$\alpha^3 + 1$
α^5	$\alpha^3 + \alpha + 1$
α^6	$\alpha^3 + \alpha^2 + \alpha + 1$
α^7	$\alpha^2 + \alpha + 1$
α^8	$\alpha^3 + \alpha^2 + \alpha$
α^9	$\alpha^2 + 1$
α^{10}	$\alpha^3 + \alpha$
α^{11}	$\alpha^3 + \alpha^2 + 1$
α^{12}	$\alpha + 1$
α^{13}	$\alpha^2 + \alpha$
α^{14}	$\alpha^3 + \alpha^2$
α^{15}	1

Задание 3. Решить над полем Галуа $GF(16)$ с корнем α полинома $x^4 + x^3 + 1$ следующую систему уравнений:
$$\begin{cases} (\alpha^3 + \alpha^2 + \alpha + 1)x + (\alpha^3 + 1)y = \alpha + 1 \\ (\alpha^4 + \alpha + 1)x + (\alpha^2 + \alpha + 1)y = \alpha^3 + \alpha \end{cases}$$

Решение

Поскольку любой ненулевой элемент поля обратим, в поле можно задать операцию деления следующим образом: определим деление на элемент a как умножение на обратный к нему элемент a^{-1} :

$$b : a = b \cdot a^{-1}, a, b \in GF(16).$$

Поэтому при решении систем можно воспользоваться правилом Крамера. Для удобства вычислений определителей перепишем уравнения системы, заменяя выражения для коэффициентов при неизвестных степенями примитивного элемента. Для этого будем использовать таблицу из задания 2, так как поле $GF(16)$ построено с корнем α того же полинома, что и в этом задании:

$$\begin{cases} \alpha^6 x + \alpha^4 y = \alpha^{12} \\ \alpha^{10} x + \alpha^7 y = \alpha^{10} \end{cases}$$

Обратим внимание, что коэффициент при x во втором уравнении следует предварительно преобразовать: $\alpha^4 + \alpha + 1 = \alpha^3 + 1 + \alpha + 1 = \alpha^3 + \alpha$. Такая запись системы упрощает операции умножения при вычислении определителя матрицы системы:

$$\Delta = \begin{vmatrix} \alpha^6 & \alpha^4 \\ \alpha^{10} & \alpha^7 \end{vmatrix} = \alpha^{13} - \alpha^{14} = \alpha^{13} + \alpha^{14} = \alpha^2 + \alpha + \alpha^3 + \alpha^2 = \alpha^3 + \alpha = \alpha^{10}.$$

При выполнении операции сложения от мультипликативного задания поля переходили к аддитивному, используя таблицу задания 2.

Вычислим определители Δ_x и Δ_y , полученные из определителя матрицы системы заменой первого и второго столбца соответственно на столбец свободных членов:

$$\Delta_x = \begin{vmatrix} \alpha^{12} & \alpha^4 \\ \alpha^{10} & \alpha^7 \end{vmatrix} = \alpha^{19} - \alpha^{14} = \alpha^4 + \alpha^3 + \alpha^2 = \alpha^3 + 1 + \alpha^3 + \alpha^2 = \alpha^2 + 1 = \alpha^9;$$

$$\Delta_y = \begin{vmatrix} \alpha^6 & \alpha^{12} \\ \alpha^{10} & \alpha^{10} \end{vmatrix} = \alpha^{16} - \alpha^{22} = \alpha + \alpha^7 = \alpha + \alpha^2 + \alpha + 1 = \alpha^2 + 1 = \alpha^9.$$

При вычислении данных определителей использовался тот факт, что элемент α имеет порядок 15: $\alpha^{19} = \alpha^{15}\alpha^4 = 1\alpha^4 = \alpha^4$, $\alpha^{16} = \alpha^{15}\alpha = 1\alpha = \alpha$, $\alpha^{22} = \alpha^{15}\alpha^7 = \alpha^7$.

Найдем элемент, обратный к Δ :

$$\alpha^{15} = 1 \Leftrightarrow \alpha^{10}\alpha^5 = 1 \Leftrightarrow \Delta\alpha^5 = 1 \Leftrightarrow \Delta^{-1} = \alpha^5.$$

Вычислим неизвестные x и y , умножив Δ_x и Δ_y на Δ^{-1} (операция деления на Δ):

$$x = \Delta_x\Delta^{-1} = \alpha^9\alpha^5 = \alpha^{14} = \alpha^3 + \alpha^2;$$

$$y = \Delta_y\Delta^{-1} = \alpha^9\alpha^5 = \alpha^3 + \alpha^2. \blacktriangle$$

ТЕСТ ДЛЯ САМОПРОВЕРКИ ПО ТЕМЕ «КОНЕЧНЫЕ ПОЛЯ»

Вопрос 1. Пусть $K = (\mathbb{Z}/3\mathbb{Z})[x]$ – кольцо полиномов с коэффициентами из $\mathbb{Z}/3\mathbb{Z}$ и $J = \langle x^2 + x + 2 \rangle$ – идеал, порожденный многочленом $x^2 + x + 2$. Указать количество элементов фактор-кольца K/J .

- A) 9;
- B) 15;
- C) 27;
- D) 8;
- E) 16.

Вопрос 2. В кольце $(\mathbb{Z}/2\mathbb{Z})[x]/\langle x^3 + x^2 + x + 1 \rangle$ найти элемент, обратный к элементу $\bar{x}$.

- A) элемент $\bar{x}$ необратим;
- B) $\overline{x^2}$;
- C) $\overline{x^2 + x}$;
- D) $\overline{x^2 + 1}$;
- E) $\overline{x^2 + x + 1}$.

Вопрос 3. В кольце $(\mathbb{Z}/3\mathbb{Z})[x]/\langle x^3 + 2x + 2 \rangle$ вычислить произведение элементов $\overline{x + 2}$ и $\overline{2x^2 + 2}$.

- A) $\overline{x^2 + x}$;
- B) $\overline{x^2 + 2x + 2}$;
- C) $\overline{x + 2}$;
- D) $\overline{x^2 + x + 1}$;
- E) $\overline{2x^2 + 2x}$.

Вопрос 4. Чему равна характеристика поля Галуа, содержащего 125 элементов?

- A) 125;
- B) 124;
- C) 5;
- D) 3;
- E) 2.

Вопрос 5. Размерность линейного пространства, являющегося полем Галуа, содержащего 64 элемента, равна:

- A) 5;
- B) 64;
- C) 2;

- D) 6;
- E) 4.

Вопрос 6. Характеристика поля Галуа, в котором для любого элемента a выполняется равенство $12a = 2a$, равна:

- A) 10;
- B) 0;
- C) 6;
- D) 3;
- E) 5.

Вопрос 7. Какие из приведенных чисел могут быть характеристикой поля?

- A) 2;
- B) -1 ;
- C) 0;
- D) 6;
- E) 157.

Вопрос 8. Поле Галуа, состоящее из 625 элементов, с точностью до изоморфизма совпадает с фактор-кольцом кольца $K = (\mathbb{Z}/5\mathbb{Z})[x]$ по идеалу J , порожденному полиномом $f(x)$, если степень полинома равна:

- A) 25;
- B) 5;
- C) 4;
- D) 2;
- E) 125.

Вопрос 9. Порядок примитивного элемента поля Галуа, состоящего из 32 элементов, равен:

- A) 32;
- B) 8;
- C) 4;
- D) 16;
- E) 31.

Вопрос 10. Порядок примитивного элемента поля Галуа равен 15. Чему равна степень примитивного полинома?

- A) 15;
- B) 4;
- C) 3;
- D) 5;
- E) 16.

Ключ к тесту:

<i>Номер вопроса</i>	<i>Ответ</i>
1	<i>A</i>
2	<i>E</i>
3	<i>A</i>
4	<i>C</i>
5	<i>D</i>
6	<i>E</i>
7	<i>A, C, E</i>
8	<i>B</i>
9	<i>E</i>
10	<i>B</i>

ИНДИВИДУАЛЬНЫЕ ЗАДАНИЯ ДЛЯ ЛАБОРАТОРНОЙ РАБОТЫ № 5 «КОНЕЧНЫЕ ПОЛЯ»

Задание 1. Задан многочлен $f(x)$ с коэффициентами из поля $\mathbb{Z}/2\mathbb{Z}$.

а) $p(x)$; б) $q(x)$.

Для обоих пунктов выполнить следующие задания:

1) Выяснить, является ли многочлен неприводимым.

2) Перечислить все элементы фактор-кольца K/J , где K – кольцо многочленов $K = (\mathbb{Z}/2\mathbb{Z})[x]$, а J – идеал этого кольца, порожденный многочленом $f(x)$: $J = \langle f(x) \rangle$.

3) Составить таблицы сложения и умножения элементов указанного фактор-кольца.

4) Пользуясь составленными таблицами, выписать пары взаимно обратных элементов.

5) Определить порядок мультипликативной группы фактор-кольца K/J .

6) Выяснить, является ли мультипликативная группа фактор-кольца циклической. Если является, указать ее образующий элемент.

7) Выяснить, является ли фактор-кольцо K/J полем.

Задание 2. Сформировать поле Галуа с 32 элементами (варианты 1–12) и с 16 элементами (варианты 13 – 15), а также с примитивным полиномом $p(x)$.

Задание 3. Решить в этом поле систему уравнений: $\begin{cases} ax + by = c, \\ dx + ey = f. \end{cases}$ Проверить правильность найденных решений.

Вариант 1

1. а) $p(x) = x^4 + x + 1$;

б) $q(x) = x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + 1$.

2. $p(x) = x^5 + x^4 + x^3 + x^2 + 1$. 3.
$$\begin{cases} (\alpha^3 + \alpha + 1)x + \alpha y = \alpha^4 + \alpha^3 + 1, \\ (\alpha^2 + \alpha + 1)x + (\alpha + 1)y = \alpha^3 + \alpha. \end{cases}$$

Вариант 2

1. а) $p(x) = x^4 + x^3 + 1$;

б) $q(x) = x^6 + x^5 + x^3 + x^2 + 1$.

2. $p(x) = x^5 + x^4 + x^3 + x + 1$. 3.
$$\begin{cases} (\alpha^3 + \alpha + 1)x + \alpha y = \alpha^4 + \alpha^3 + 1, \\ (\alpha^2 + \alpha + 1)x + (\alpha + 1)y = \alpha^3 + \alpha. \end{cases}$$

Вариант 3

1. а) $p(x) = x^4 + x^3 + x^2 + x + 1$; б) $q(x) = x^6 + x^3 + 1$.

2. $p(x) = x^5 + x^4 + x^2 + x + 1$. 3.
$$\begin{cases} (\alpha^3 + \alpha + 1)x + \alpha y = \alpha^4 + \alpha^3 + 1, \\ (\alpha^2 + \alpha + 1)x + (\alpha + 1)y = \alpha^3 + \alpha. \end{cases}$$

Вариант 4

1. а) $p(x) = x^3 + x + 1;$

б) $q(x) = x^6 + x^5 + x^4 + x + 1.$

2. $p(x) = x^5 + x^3 + 1.$

3.
$$\begin{cases} (\alpha^3 + \alpha + 1)x + \alpha y = \alpha^4 + \alpha^3 + 1, \\ (\alpha^2 + \alpha + 1)x + (\alpha + 1)y = \alpha^3 + \alpha. \end{cases}$$

Вариант 5

1. а) $p(x) = x^3 + x^2 + 1;$

б) $q(x) = x^6 + x^4 + x^3 + x + 1.$

2. $p(x) = x^5 + x^3 + 1.$

3.
$$\begin{cases} (\alpha^3 + \alpha + 1)x + \alpha y = \alpha^4 + \alpha^3 + 1, \\ (\alpha^2 + \alpha + 1)x + (\alpha + 1)y = \alpha^3 + \alpha. \end{cases}$$

Вариант 6

1. а) $p(x) = x^4 + x + 1;$

б) $q(x) = x^6 + x^5 + x^2 + x + 1.$

2. $p(x) = x^5 + x^3 + x^2 + x + 1.$

3.
$$\begin{cases} (\alpha^3 + \alpha + 1)x + \alpha y = \alpha^4 + \alpha^3 + 1, \\ (\alpha^2 + \alpha + 1)x + (\alpha + 1)y = \alpha^3 + \alpha. \end{cases}$$

Вариант 7

1. а) $p(x) = x^4 + x^3 + 1;$

б) $q(x) = x^6 + x + 1.$

2. $p(x) = x^5 + x^4 + x^3 + x + 1.$

3.
$$\begin{cases} (\alpha^3 + \alpha^2 + \alpha + 1)x + (\alpha^3 + 1)y = \alpha + 1, \\ (\alpha^4 + \alpha + 1)x + (\alpha^2 + \alpha + 1)y = \alpha^3 + \alpha. \end{cases}$$

Вариант 8

1. а) $p(x) = x^4 + x^3 + x^2 + x + 1;$

б) $q(x) = x^5 + x^4 + x^3 + x + 1.$

2. $p(x) = x^5 + x^4 + x^3 + x^2 + 1.$

3.
$$\begin{cases} (\alpha^3 + \alpha^2 + \alpha + 1)x + (\alpha^3 + 1)y = \alpha + 1, \\ (\alpha^4 + \alpha + 1)x + (\alpha^2 + \alpha + 1)y = \alpha^3 + \alpha. \end{cases}$$

Вариант 9

1. а) $p(x) = x^3 + x + 1;$

б) $q(x) = x^5 + x^4 + x^3 + x^2 + 1.$

2. $p(x) = x^5 + x^4 + x^2 + x + 1.$

3.
$$\begin{cases} (\alpha^3 + \alpha^2 + \alpha + 1)x + (\alpha^3 + 1)y = \alpha + 1, \\ (\alpha^4 + \alpha + 1)x + (\alpha^2 + \alpha + 1)y = \alpha^3 + \alpha. \end{cases}$$

Вариант 10

1. а) $p(x) = x^3 + x^2 + 1$;

б) $q(x) = x^5 + x^4 + x^2 + 1$.

2. $p(x) = x^5 + x^3 + x^2 + x + 1$.

3.
$$\begin{cases} (\alpha^3 + \alpha^2 + \alpha + 1)x + (\alpha^3 + 1)y = \alpha + 1, \\ (\alpha^4 + \alpha + 1)x + (\alpha^2 + \alpha + 1)y = \alpha^3 + \alpha. \end{cases}$$

Вариант 11

1. а) $p(x) = x^4 + x + 1$;

б) $q(x) = x^5 + x^3 + x^2 + x + 1$.

2. $p(x) = x^5 + x^3 + 1$.

3.
$$\begin{cases} (\alpha^3 + \alpha^2 + \alpha + 1)x + (\alpha^3 + 1)y = \alpha + 1, \\ (\alpha^4 + \alpha + 1)x + (\alpha^2 + \alpha + 1)y = \alpha^3 + \alpha. \end{cases}$$

Вариант 12

1. а) $p(x) = x^4 + x^3 + 1$;

б) $q(x) = x^5 + x^3 + 1$.

2. $p(x) = x^5 + x^2 + 1$.

3.
$$\begin{cases} (\alpha^3 + \alpha^2 + \alpha + 1)x + (\alpha^3 + 1)y = \alpha + 1, \\ (\alpha^4 + \alpha + 1)x + (\alpha^2 + \alpha + 1)y = \alpha^3 + \alpha. \end{cases}$$

Вариант 13

1. а) $p(x) = x^4 + x^3 + x^2 + x + 1$;

б) $q(x) = x^5 + x^2 + 1$.

2. $p(x) = x^4 + x^3 + 1$.

3.
$$\begin{cases} (\alpha^3 + \alpha^2 + \alpha + 1)x + (\alpha^3 + 1)y = \alpha + 1, \\ (\alpha^4 + \alpha + 1)x + (\alpha^2 + \alpha + 1)y = \alpha^3 + \alpha. \end{cases}$$

Вариант 14

1. а) $p(x) = x^3 + x^2 + 1$;

б) $q(x) = x^6 + x^4 + x^2 + x + 1$.

2. $p(x) = x^4 + x + 1$.

3.
$$\begin{cases} (\alpha^3 + \alpha^2 + \alpha + 1)x + (\alpha^3 + 1)y = \alpha + 1, \\ (\alpha^4 + \alpha + 1)x + (\alpha^2 + \alpha + 1)y = \alpha^3 + \alpha. \end{cases}$$

Вариант 15

1. а) $p(x) = x^4 + x + 1$;

б) $q(x) = x^6 + x^3 + 1$.

2. $p(x) = x^4 + x^3 + 1$.

3.
$$\begin{cases} (\alpha^3 + \alpha + 1)x + (\alpha^3 + 1)y = \alpha^2 + 1, \\ (\alpha^3 + \alpha^2 + 1)x + (\alpha^2 + \alpha + 1)y = \alpha^3 + \alpha + 1. \end{cases}$$

Таблицы порядковых номеров букв белорусского, русского и английского алфавитов

Таблица порядковых номеров букв белорусского алфавита

А	Б	В	Г	Д	Е	Ё	Ж	З	І	Й	К	Л	М	Н	О
01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16

П	Р	С	Т	У	Ў	Ф	Х	Ц	Ч	Ш	Ы	Ь	Э	Ю	Я
17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32

Таблица порядковых номеров букв русского алфавита

А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О
01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16

П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33

Таблица порядковых номеров букв английского алфавита

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

Q	R	S	T	U	V	W	X	Y	Z
17	18	19	20	21	22	23	24	25	26

**Функции математического пакета Wolfram Mathematica,
рекомендуемые для использования при выполнении лабораторных работ**

№ п/п	Наименование функции	Результат функции
1	Divisors[n]	Возвращает список целочисленных делителей числа n
2	GCD[n1,n2,...,nk]	Находит наибольший делитель целых чисел $n1, n2, \dots, nk$
3	LCM[n1,n2,...,nk]	Находит наименьшее общее кратное целых чисел $n1, n2, \dots, nk$
4	Prime[n]	Возвращает n -е простое число
5	NextPrime[n]	Находит наименьшее простое число, превосходящее n
6	Mod[m,n]	Находит остаток от деления числа m на число n
7	PrimeQ[n]	Проверяет число n на простоту
8	FactorInteger[n]	Возвращает факторизацию целого числа n в виде список простых делителей с соответствующими степенями
9	EulerPhi[n]	Возвращает значение функции Эйлера от числа n
10	PowerMod[a,b,m]	Возводит число a в степень b по модулю m
11	ModularInverse[k,n]	Возвращает обратное к числу k по модулю m
12	ChineseRemainder [{r1,r2,...}, {m1,m2,...}]	Возвращает наименьшее неотрицательное решение системы сравнений $x \equiv r_i \pmod{m_i}$
13	PermutationProduct[a,b,c]	Возвращает произведение подстановок в порядке cba
14	PermutationCycles[perm]	Раскладывает подстановку $perm$ в произведение циклов
15	PrimitivePolynomialQ[poly,p]	Проверяет, является ли полином $poly$ примитивным над полем $\mathbb{Z}/p\mathbb{Z}$

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Авдошин, С.М. Дискретная математика. Модулярная алгебра, криптография, кодирование / С. М. Авдошин, А. А. Набебин. – Москва : ДМК Пресс, 2017. – 352 с.
2. Айерлэнд, К. Классическое введение в современную теорию чисел / К. Айерлэнд, М. Роузен. – М. : Мир, 1987. – 416 с.
3. Аршинов, Н. Н. Коды и математика / Н. Н. Аршинов, Л. Е. Садовский. – М. : Наука, 1983. – 124 с.
4. Бейкер, А. Введение в теорию чисел / А. Бейкер; пер. с англ. – Мн. : Вышэйшая школа, 1995.
5. Беньаш-Кривец, В. В. Лекции и семинары по алгебре: группы, кольца, поля: пособие для студентов фак. прикл. математики и информатики и мех.-мат. фак. / В. В. Беньаш-Кривец, Г. Е. Пунинский. – Минск: БГУ, 2015. – 152 с.
6. Беньаш-Кривец, В. В. Лекции по алгебре: группы, кольца, поля: пособие для студентов фак. прикл. математики и информатики и мех.-мат. фак. / В. В. Беньаш-Кривец, О. В. Мельников. – Минск: БГУ, 2009. – 116 с.
7. Биркгоф, Г. Современная прикладная алгебра / Г. Биркгоф, Т. Барти. – М. : Мир, 1976. – 400 с.
8. Борович, З. И. Теория чисел / З. И. Борович, И. Р. Шафаревич. – 3-е изд., доп. – М.: Наука, 1985. – 504 с.
9. Василенко, О. Н. Теоретико-числовые алгоритмы в криптографии / О. Н. Василенко. – М. : Изд-во МЦМНО, 2003. – 326 с.
10. Введение в криптографию: новые математические дисциплины: учеб.; под ред. В. В. Яценко. – СПб. : Питер, 2001. – 288 с.
11. Вейль, А. Основы теории чисел / А. Вейль; пер. с англ. А. Н. Вассерштейна, А. Н. Паршина; под ред. И. И. Пятецкого-Шапиро. – М. : Мир, 1972. – 410 с.
12. Вернер, М. Основы кодирования: учеб. для вузов / М. Вернер. – М. : Техносфера, 2006. – 288 с.
13. Виноградов, И. М. Основы теории чисел: учеб. пособие. / И. М. Виноградов. – 11-е изд., стер. – СПб. : Лань, 2006. – 176 с.
14. Зензин, О. С. Стандарт криптографической защиты AES. Конечные поля / О. С. Зензин, М. А. Иванов. – М.: Кудиц-Образ, 2002. – 168 с.
15. Каргополов, М. И. Основы теории групп / М. И. Каргополов, Ю. И. Мерзляков. – 3-е изд., перераб. и доп. – М. : Наука, 1982. – 288 с.
16. Прикладная математика: метод. пособие для студентов специальностей 1-45 01 05 «Сети телекоммуникаций», 1-45 01 03 «Системы распределения мультимедийной информации», 1-98 01 02 «Защита информации в телекоммуникациях» днев. формы обуч. / В. А. Липницкий [и др.]. – Минск: БГУИР, 2010. – 87 с.
17. Прикладная теория кодирования: в 2 т. / В.К. Конопелько [и др.] – Минск: БГУИР, 2004. – 688 с.

18. Коутинхо, С. Введение в теорию чисел. Алгоритм RSA / С. Коутинхо. – М. : Постмаркет, 2001. – 324 с.
19. Куликов, Л. Я. Сборник задач по алгебре и теории чисел / Л. Я. Куликов, А. И. Москаленко, А. А. Фомин. – М. : Просвещение, 1993. – 288 с.
20. Лидл, Р. Конечные поля: в 2 т. / Р. Лидл, Г. Нидеррайтер. – М. : Мир, 1988. – 882 с.
21. Липницкий, В. А. Современная прикладная алгебра. Математические основы защиты информации от помех и несанкционированного доступа: учеб.-метод. пособие по курсу «Высшая математика» для студентов специальностей «Сети телекоммуникаций» и «Информатика» всех форм обучения / В. А. Липницкий. – 2-е изд., испр. – Мн : БГУИР, 2006. – 88 с.
22. Логачев, О. А. Булевы функции в теории кодирования и криптологии / О. А. Логачев, А. А. Сальников, В. В. Ященко. – М. : Изд-во МЦМНО, 2004. – 470 с.
23. Мао, В. Современная криптография: теория и практика / В. Мао; пер. с англ. – М. : Вильямс, 2005.
24. Математика. Применение пакета Mathematica: в 2 ч. Ч. 1 : Линейная алгебра. Аналитическая геометрия. Введение в математический анализ: пособие / О. А. Вагнер, Л. А. Фомичёва. – Минск : БГУИР, 2019. – 180 с. : ил.
25. Монахов, В. С. Введение в теорию конечных групп и их классов / В. С. Монахов. – Минск: Вышэйш. шк., 2006.
26. Нестеренко, Ю. В. Введение в теорию чисел: учебное пособие для вузов по спец. «Математика» / Ю. В. Нестеренко, А. Б. Шидловский, А. И. Галочкин, под ред. А. Б. Шидловского. – М.: МГУ, 1984.
27. Нидеррайтер, Г. Конечные поля: в 2 т. Т. 1 / Г. Нидеррайтер, Р. Лидл; пер. с англ. А. Е. Жукова, В. И. Петрова; под ред. В. И. Нечаева. – М. : Мир, 1988.
28. Основы криптографии: учеб. пособие для студентов вузов / А. П. Алферов [и др.]. – 2-е изд., испр. и доп. – М. : Изд-во Гелиос АРВ, 2002.
29. Прасолов, В. В. Многочлены / В.В. Прасолов – М. : Изд-во МЦМНО, 2000. – 336 с.
30. Радьков, А. М. Алгебра и теория чисел / А. М. Радьков, Б. Д. Чеботаревский. – Минск: Вышэйш. шк., 1992.
31. Стрейникова, Е. Д. Основы прикладной алгебры: учеб.-метод. пособие для студентов вузов / Е. Д. Стрейникова. – Мн. : БГУИР, 2010.
32. Харин, Ю. С. Компьютерный практикум по математическим методам защиты информации / Ю. С. Харин, С. В. Агиевич. – Минск : БГУ, 2001. – 190 с.
33. Ширяев, В. М. Прикладная алгебра. Теория чисел : сб. задач для студентов фак. прикл. математики и информатики / В. М. Ширяев – Минск : БГУ, 2009.
34. Шнеперман, Л. Б. Сборник задач по алгебре и теории чисел / Л. Б. Шнеперман. – Минск : Вышэйш. шк., 1982.
35. Иллюстрированный самоучитель по «MatLab», «Mathematica». – Режим доступа: <http://samoucka.ru>.
36. Wolfram Mathematica. – URL: <https://reference.wolfram.com>.

37. Нестерова, Л. Ю. Китайская теорема об остатках в области главных идеалов / Л. Ю. Нестерова // Молодой ученый. – 2014. – № 21 (80). – С. Т.1. 240-243. – URL: <https://moluch.ru/archive/80/13832/> (дата обращения: 29.04.2025).

38. Липницкий, В. А. Линейные коды и кодовые последовательности: учеб.-метод. пособие для студентов мех.-мат. фак. БГУ / В. А. Липницкий, Н. В. Чесалин. – Минск : БГУ, 2008. – 41 с.

Учебное издание

Глецевич Марина Александровна
Каянович Сергей Сергеевич
Малышева Ольга Николаевна
Семеняко Андрей Николаевич

ПРИКЛАДНАЯ МАТЕМАТИКА

ПОСОБИЕ

Редактор *Л. И. Артёмова*
Корректор *Ж. А. Чернецкая*
Компьютерная правка, оригинал-макет *Е. Г. Бабичева*

Подписано в печать 14.09.2026. Формат 60×84 1/16. Бумага офсетная. Гарнитура «Таймс».
Отпечатано на ризографе. Усл. печ. л. 10,11. Уч.-изд. л. 9,4. Тираж 100 экз. Заказ 4.

Издатель и полиграфическое исполнение: учреждение образования
«Белорусский государственный университет информатики и радиоэлектроники».
Свидетельство о государственной регистрации издателя, изготовителя,
распространителя печатных изданий №1/238 от 24.03.2014,
№2/113 от 07.04.2014, №3/615 от 07.04.2014.
Ул. П. Бровки, 6, 220013 г. Минск