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

Кафедра высшей математики

ПРИКЛАДНАЯ МАТЕМАТИКА

Методическое 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»
дневной формы обучения

Минск БГУИР 2010

УДК 512(076)
ББК 22.144я73
П75

А в т о р ы:
В. А. Липницкий, Н. В. Спичекова, С. Ф. Данцевич, Д. Н. Олешкевич

Р е ц е н з е н т:
заведующий кафедрой информатики учреждения образования
«Белорусский государственный университет информатики
и радиоэлектроники, доктор физико-математических наук,
профессор Л. И. Минченко

П75 **Прикладная** математика : метод. пособие для студ. спец. 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. : ил.
ISBN 978-985-488-526-1.

Методическое пособие служит цели практического освоения студентами материала специального курса «Прикладная математика». Приведен материал для практических, лабораторных и самостоятельных занятий по теории чисел, теории групп, теории колец и полей. Пособие практически знакомит с основными криптографическими системами, с применением современной алгебры в теории и практике помехоустойчивого кодирования.

УДК 512(076)
ББК 22.144я73

ISBN 978-985-488-526-1

Введение

Студенты БГУИР изучают весь спектр вопросов, связанных с обработкой, хранением, передачей и защитой информации от помех и несанкционированного доступа. Соответствующие лекционные курсы являются относительно новыми, многие из них находятся в динамике становления или развития в соответствии с технологической революцией и потребностями времени, требуют изучения новых разделов математики, не вошедших в классический курс «Высшая математика» – необходимую базу высшего технического образования. Такие курсы, как «Цифровая обработка сигналов», «Прикладная теория кодирования», «Криптографические методы защиты информации» и ряд других предполагают основательное знание структур современной алгебры.

Поэтому на кафедре высшей математики разработан курс «Прикладная математика», где излагаются основы современной прикладной алгебры, закладываются математические основы защиты информации от помех и несанкционированного доступа. На протяжении ряда лет этот курс успешно читается студентам БГУИР специальностей «Информатика», «Сети телекоммуникаций», «Системы распределения мультимедийной информации», «Защита информации в телекоммуникациях». Дважды издавалось соответствующее учебно-методическое пособие «Современная прикладная алгебра. Математические основы защиты информации от помех и несанкционированного доступа», где изложен необходимый теоретический материал.

Опыт показывает, что глубокое и надежное усвоение нового материала невозможно без его основательной проработки на практических и лабораторных занятиях. Данное издание является необходимым пособием для проведения практических и лабораторных занятий по названному выше курсу. Предлагается рабочая модель девяти практических и лабораторных занятий по основным темам курса. При этом в зависимости от сложившейся традиции лабораторные задания можно рассматривать и как домашние – для самостоятельного индивидуального изучения и освоения.

Данное издание по названной тематике и широте охвата материала является первым в Республике Беларусь. Оно будет полезно не только студентам указанных специальностей, но и всем, кто изучает проблематику помехоустойчивого кодирования информации, формирования и обработки дискретных сигналов, защиты информации от помех и несанкционированного доступа.

1. ТЕОРИЯ ЧИСЕЛ

Теоретические сведения

Ниже рассматриваются N – множество натуральных чисел, Z – множество целых чисел. Множество целых чисел Z – счетное, состоит из элементов $0; \pm 1; \pm 2; ..., \pm n; ....$ На нем определены две алгебраические операции – сложение и умножение. Эти операции обладают следующими свойствами (для любых $a, b, c \in Z$):

1) ассоциативность: $a + (b + c) = (a + b) + c$; $a \cdot (b \cdot c) = a \cdot (b \cdot c)$;
коммутативность: $b + a = a + b$; $a \cdot b = b \cdot a$;

2) существует нейтральный элемент – 0 или 1 соответственно:
$a + 0 = 0 + a = a$; $a \cdot 1 = 1 \cdot a = a$;

3) $(a + b) \cdot c = a \cdot c + b \cdot c$ – закон дистрибутивности;

4) для каждого целого $a \in Z$ существует единственное противоположное целое b, такое, что $a + b = b + a = 0$.

Теорема 1.1 (о делении с остатком). *Для любых целых чисел* a *и* b, $b \neq 0$, *существуют единственные целые числа* q *и* r, $0 \le r < |b|$, *такие, что* $a = b \cdot q + r$.

В этом равенстве r называют остатком, а q – частным (неполным частным – при $r \neq 0$) от деления a на b. При $r = 0$ величины b и q называют делителями или множителями числа a. Читатель со школьной скамьи умеет находить частное и остаток методом деления уголком.

Следствие. Пусть b – натуральное число, $b > 1$. Для всякого целого числа a и максимального целого $m \ge 0$ с условием $a > b^m$ существуют единственные целые a_i, $0 \le a_i < b$, $0 \le i \le m$, такие, что

$$a = \pm (a_m b^m + a_{m-1} b^{m-1} + ... + a_0).$$

Такое равенство записывают сокращенно $a = \pm (a_m a_{m-1} ... a_0)_b$ или $a = \pm a_m a_{m-1} ... a_0$ (если b известно по контексту) и называют записью числа a в b-ичной позиционной системе счисления или системе счисления по основанию b. Кажется естественной привычная десятичная позиционная система записи целых чисел $(b = 10)$. В различных ситуациях более удобными оказываются другие основания. Например, во всех компьютерах на микроуровне вычисления проводятся в двоичной системе счисления. Для перехода к ней с десятичной применяют промежуточную 16-ричную систему счисления.

Лемма 1.1. Если в равенстве $a_1 + a_2 + ... + a_n = b_1 + b_2 + ... + b_m$ все слагаемые – целые числа и все, кроме, может быть, одного, делятся на целое d, то и это исключенное слагаемое также делится на d.

Определение 1.1. Если целые числа $a_1, a_2, ..., a_n$ делятся на целое d, то d называют их общим делителем.

В дальнейшем речь идет только о положительных целых делителях.

Определение 1.2. Максимальный из общих делителей целых чисел $a_1, a_2, \ldots, a_n$ называется их наибольшим общим делителем и обозначается через НОД $(a_1, a_2, \ldots, a_n)$.

Теорема 1.2. *Если* $a = b \cdot q + c$, *то* НОД $(a, b) =$ НОД (b, c).

Теорема 1.2 позволила Евклиду (примерно 2300 лет тому назад) обосновать следующий факт.

Теорема 1.3. *Наибольший общий делитель целых чисел a и b* $(a > b)$ *равен последнему отличному от нуля остатку цепочки равенств*:

$$a = b \cdot q_1 + r_1;$$
$$b = r_1 \cdot q_2 + r_2;$$
$$\ldots\ldots\ldots\ldots\ldots$$
$$r_{n-2} = r_{n-1} \cdot q_n + r_n;\ \text{т. е. } r_n = \text{НОД}\,(a,b).$$
$$r_{n-1} = r_n \cdot q_{n+1}.$$

Теорема 1.3 формулирует алгоритм Евклида для нахождения наибольшего общего делителя целых чисел. Его вариантом является следующий (второй способ вычисления наибольшего общего делителя по алгоритму Евклида): вычисляем последовательно разности $a - b = c;\ b - c = d; \ldots$ до получения последней ненулевой разности, которая и совпадает с НОД (a,b).

Пример 1.1. С помощью алгоритма Евклида найти НОД (72, 26).

Решение. В соответствии с теоремой 1.2 $72 = 26 \cdot 2 + 20;\ 26 = 20 \cdot 1 + 6;$ $20 = 6 \cdot 3 + 2;\ 6 = 2 \cdot 3$. Следовательно, НОД (72, 26) = 2.

Теорема 1.4. *Если* $d =$ НОД (a,b), *то существуют такие целые u и v, что выполняется следующее соотношение* (*соотношение Безу*)*:* $d = au + bv$.

Пример 1.2. Из примера 1.1 следует, что

$$2 = 20 + 6 \cdot (-3) = 20 + (26 + 20 \cdot (-1)) \cdot (-3) = 20 \cdot 4 + 26 \cdot (-3) =$$
$$= (72 + 26 \cdot (-2)) \cdot (4 + 26 \cdot (-3)) = 72 \cdot 4 + 26 \cdot (-11).$$

Такой способ получения соотношения Безу для конкретных целых чисел называется расширенным алгоритмом Евклида. Он состоит из двух этапов: собственно алгоритма Евклида – прогонки вниз и прогонки вверх – и последовательного выражения остатков в каждом из шагов предыдущего этапа (с соответствующим приведением подобных на каждом шаге).

Определение 1.3. Натуральное число $p > 1$ называется простым, если оно делится только на 1 и на себя.

Теорема 1.5. *Всякое натуральное число* $n > 1$ *либо является простым числом*, *либо имеет простой делитель.*

Заметим, что из соотношения $n = p \cdot q$ натуральных чисел, больших единицы, следует, что либо p, либо q принадлежит отрезку $[2; \sqrt{n}]$. Легко видеть, что наименьший натуральный делитель $p > 1$ натурального числа $n > 1$ является простым числом. Исторически первый метод проверки натурального числа $n > 1$ на простоту, заключающийся в делении его на простые числа, не превосходящие $\sqrt{n}$, носит название «решето Эратосфена». К настоящему времени разработан достаточно большой цикл алгоритмов проверки числа на простоту.

Теорема 1.6 (теорема Евклида). *Простых чисел бесконечно много.*

Значение простых чисел в том, что они по теореме 1.5 являются составными кирпичиками всех натуральных чисел.

Определение 1.4. Целые числа a и b называются взаимно простыми, если НОД $(a,b)=1$.

Теорема 1.7 (критерий взаимной простоты целых чисел). *Целые числа a и b взаимно просты тогда и только тогда, когда существуют такие целые u и v, что выполняется равенство $a\cdot u+b\cdot v=1$.*

Следствие. НОД$(ac,b)=1$ тогда и только тогда, когда НОД$(a,b)=1$, НОД$(c,b)=1$.

Важным в теории чисел и ее приложениях является следующее свойство взаимно простых целых чисел.

Лемма 1.2. Пусть произведение целых чисел ab делится на целое число c и НОД$(a,c)=1$. Тогда b делится на c.

Теорема 1.8 (основная теорема арифметики). *Всякое целое число $n>1$ однозначно раскладывается в произведение простых множителей*:

$$n=\pm p_1\cdot p_2\cdot\ldots\cdot p_s.$$

Если в этом равенстве собрать одинаковые множители, то получим каноническое разложение целого числа $n=p_1^{r_1}\cdot p_2^{r_2}\cdot\ldots p_t^{r_t}$.

Пример 1.3. Приведем примеры канонических разложений целых чисел: а) $196=2\cdot98=2\cdot2\cdot49=2^2\cdot7^2$; б) $2^{12}-1=4095=3^2\cdot5\cdot7\cdot13$.

Теорема 1.9. *Пусть m – натуральное число, $m>1$. Для любых целых чисел a и b следующие условия равносильны*:

1) *a и b имеют одинаковые остатки от деления на m*;

2) *$a-b$ делится на m, т. е. $a-b=mq$ для подходящего целого q*;

3) *$a=b+mq$ для некоторого целого q*.

Определение 1.5. Целые числа a и b называются сравнимыми по модулю m, если они удовлетворяют одному из условий теоремы 1.9. Этот факт обозначают формулой $a\equiv b(\mathrm{mod}\,m)$ или $a\equiv b(m)$ и называют данную формулу сравнением.

Пример 1.4. $-5\equiv7(\mathrm{mod}\,4)\equiv11(\mathrm{mod}\,4)\equiv23(\mathrm{mod}\,4)\equiv3(\mathrm{mod}\,4)$.

Пример 1.5. Если $a=mq+r$, то $a\equiv r(\mathrm{mod}\,m)$ – всякое целое число сравнимо по модулю m со своим остатком от деления на m. Это следует из определения 1.5 и второго условия теоремы 1.9. Ведь $a-r$ делится на m.

Основные свойства сравнений

1. Пусть $a\equiv b(\mathrm{mod}\,m)$. Тогда $(a\pm c)\equiv(b\pm c)(\mathrm{mod}\,m)$ для всякого целого числа c, то есть к обеим частям сравнения можно добавить (или вычесть из обеих частей) одно и то же число.

2. Сравнения можно почленно складывать и вычитать: если $a\equiv b(\mathrm{mod}m)$, $c\equiv d(\mathrm{mod}\,m)$, то $(a+c)\equiv(b+d)(\mathrm{mod}\,m)$; $(a-c)\equiv(b-d)(\mathrm{mod}m)$.

3. Сравнения можно почленно перемножать: если $a \equiv b(\mathrm{mod}\ m)$, $c \equiv d(\mathrm{mod}\, m)$, то $ac \equiv bd(\mathrm{mod}\, m)$.

4. Сравнения можно почленно возводить в любую натуральную степень: если $a \equiv b(\mathrm{mod}\, m)$, то $a^n \equiv b^n(\mathrm{mod}\, m)$.

5. Если в сравнении $a \equiv b(\mathrm{mod}\, m)$ числа a, b, m имеют общий множитель d, то на него сравнение можно сократить $\frac{a}{d} \equiv \frac{b}{d}\left(\mathrm{mod}\left(\frac{m}{d}\right)\right)$.

6. Сравнение можно сократить на общий множитель, взаимно простой с модулем: если $a = da_1, b = db_1$, НОД $(d, m) = 1$, то из сравнения $da_1 \equiv db_1(\mathrm{mod}\, m)$ следует сравнимость a_1 и b_1 по модулю m : $a_1 \equiv b_1(\mathrm{mod}\, m)$.

7. Сравнение можно умножить на любой целый множитель: если $a \equiv b(\mathrm{mod}\, m)$, то $at \equiv bt(\mathrm{mod}\, m)$ для всякого целого числа t.

8. Рефлексивность: $a \equiv a\ (\mathrm{mod}\, m)$ для любого целого a и всякого натурального $m > 1$.

9. Симметричность: если $a \equiv b\ (\mathrm{mod}\, m)$, то $b \equiv a\ (\mathrm{mod}\, m)$.

10. Транзитивность: если $a \equiv b\ (\mathrm{mod}\, m)$ и $b \equiv c\ (\mathrm{mod}\, m)$, то $a \equiv c\ (\mathrm{mod}\, m)$.

Теорема 1.10 (малая теорема Ферма). *Пусть p – простое число и целое число a не делится на p. Тогда $a^{p-1} \equiv 1(\mathrm{mod}\, p)$.*

Теория сравнений и малая теорема Ферма позволяют быстро находить остаток от деления большого числа на простое число.

Пример 1.6. Найдем остаток от деления 39^{149} на 31.

Решение. 39 не делится на простое число 31. Поэтому $39^{30} \equiv 1(\mathrm{mod}\, 31)$. Следовательно, $39^{149} = 39^{30 \cdot 3 + 29} \equiv 39^{29}(\mathrm{mod}\, 31)$. Далее $39 \equiv 8(\mathrm{mod}\, 31)$. Поэтому в силу свойства 4 сравнений $39^2 \equiv 8^2 \equiv 2(\mathrm{mod}\, 31)$. Двоичная запись 29 = 11101. Следовательно, для любого натурального a величина $a^{29} = a^{2^4} \cdot a^{2^3} \cdot a^{2^2} \cdot a$. Далее $39^4 \equiv 8^4 \equiv 2^2(\mathrm{mod}\, 31)$. Поэтому $39^8 = (39^4)^2 \equiv 4^2(\mathrm{mod}\, 31)$. Тогда $39^{16} = (39^8)^2 \equiv 16^2(\mathrm{mod}\, 31) \equiv 8(\mathrm{mod}\, 31)$. Следовательно,

$$39^{29} \equiv 8 \cdot 16 \cdot 4 \cdot 8(\mathrm{mod}\, 31) \equiv 4 \cdot 4 \cdot 8(\mathrm{mod}\, 31) \equiv 4(\mathrm{mod}\, 31).$$

Таким образом, остаток от деления 39^{149} на 31 равен 4.

Задания для аудиторной работы

Задание 1.1. Найти канонические разложения чисел $a = 627, b = 399$.

Решение.

627	3	399	3
209	11	133	7
19	19	19	19
1			

Следовательно, $627 = 3 \cdot 11 \cdot 19$, $399 = 3 \cdot 7 \cdot 19$.

Задание 1.2. Найти НОД (627, 399), воспользовавшись: а) алгоритмом Евклида; б) разложением чисел на простые множители.

Решение. Применим алгоритм Евклида:

$627 = 399 \cdot 1 + 228$;

$399 = 228 \cdot 1 + 171$;

$228 = 171 \cdot 1 + 57$;

$171 = 57 \cdot 3$. Следовательно, НОД (627; 399) = 57.

Найдем НОД (a, b), воспользовавшись разложением на простые множители чисел a и b, полученным в решении задания 1.1:

$$627 = 3 \cdot 11 \cdot 19; \quad 399 = 3 \cdot 7 \cdot 19.$$

Следовательно, наибольшим общим делителем будет произведение одинаковых множителей, входящих как в одно, так и в другое разложения чисел НОД (627; 399) = $3 \cdot 19 = 57$.

Найдем НОД (a, b) методом вычитаний:

$627 - 399 = 228$; $399 - 228 = 171$; $228 - 171 = 57$; $171 - 57 = 114$;

$114 - 57 = 57$; $57 - 57 = 0$. Следовательно, НОД (627; 399) = 57.

Задание 1.3. С помощью расширенного алгоритма Евклида найти целые числа u, υ, удовлетворяющие соотношению Безу: $au + b\upsilon = \text{НОД}(a, b)$ для целых чисел $a = 110$; $b = 48$.

Решение. Сначала найдем по алгоритму Евклида НОД (110, 48):

$110 = 48 \cdot 2 + 14$;

$48 = 14 \cdot 3 + 6$;

$14 = 6 \cdot 2 + 2$;

$6 = 3 \cdot 2$. Следовательно, НОД (110, 48) = 2.

Теперь построим соотношение Безу для данных a и b:

$110 = 48 \cdot 2 + 14$; поэтому $14 = 110 + 48 \cdot (-2)$;

$48 = 14 \cdot 3 + 6$; поэтому $6 = 48 + 14 \cdot (-3)$;

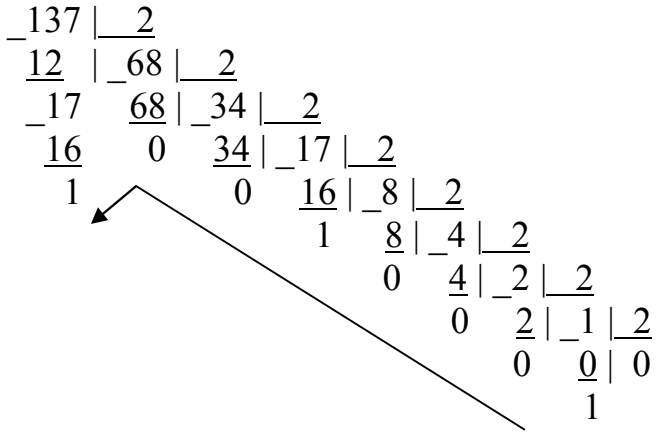
$14 = 6 \cdot 2 + 2$; поэтому $2 = 14 + 6 \cdot (-2)$. В это равенство подставим полученное выше выражение для 6 и приведем подобные относительно чисел 48 и 14. Итак, $2 = 14 + 6 \cdot (-2) = 14 + (48 + 14 \cdot (-3))(-2) = 14 \cdot 7 + 48 \cdot (-2)$.

В полученное выражение для НОД (110, 48) = 2 подставим вышеприведенное выражение числа 14. Получим окончательно

$2 = 14 \cdot 7 + 48 \cdot (-2) = (110 + 48 \cdot (-2))\, 7 + 48 \cdot (-2) = 110 \cdot 7 + 48 \cdot (-16) = 2$.

Задание 1.4: а) записать в двоичной системе счисления число 137.

Решение. Проведем последовательные деления на 2:



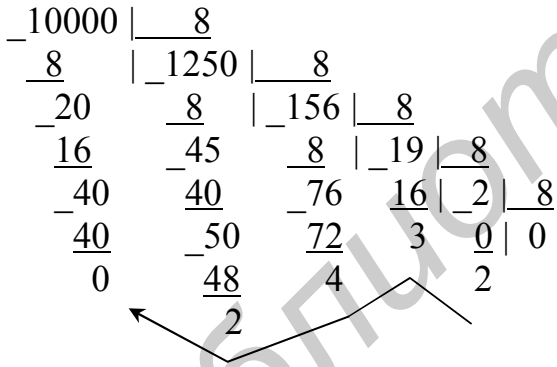
Число записываем по остаткам деления на 2, но в обратном порядке:
$137 = 10001001_2$;

б) перевести число 10001001_2 в десятичную систему:

$1\ 0\ 0\ 0\ 1\ 0\ 0\ 1_2 = (1 \cdot 2^7 + 0 \cdot 2^6 + 0 \cdot 2^5 \cdot 0 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0) =$
$= 7\ \ 6\ \ 5\ 4\ 3\ \ 2\ 1\ 0.$

$(2^7 + 2^3 + 1)_{10} = 128 + 8 + 1 = 137_{10}$;

в) перевести число 10000 в восьмеричную систему счисления:



$10000_{10} = 23420_8$.

Задание 1.5. Умножение и сложение в 16-ричной системе счисления.

В 16-ричной системе счисления используются цифры и латинские буквы 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F. Здесь буква A – это число 10, буква B – 11, C – 12, D – 13, E – 14, F – 15.

Для выполнения арифметических операций в 16-ричной системе построим табл. 1.1 и табл. 1.2.

Таблица 1.1

Сложение чисел в 16-ричной системе счисления

+	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
1	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	10
2	2	3	4	5	6	7	8	9	A	B	C	D	E	F	10	11
3	3	4	5	6	7	8	9	A	B	C	D	E	F	10	11	12
4	4	5	6	7	8	9	A	B	C	D	E	F	10	11	12	13
5	5	6	7	8	9	A	B	C	D	E	F	10	11	12	13	14
6	6	7	8	9	A	B	C	D	E	F	10	11	12	13	14	15
7	7	8	9	A	B	C	D	E	F	10	11	12	13	14	15	16
8	8	9	A	B	C	D	E	F	10	11	12	13	14	15	16	17
9	9	A	B	C	D	E	F	10	11	12	13	14	15	16	17	18
A	A	B	C	D	E	F	10	11	12	13	14	15	16	17	18	19
B	B	C	D	E	F	10	11	12	13	14	15	16	17	18	19	1A
C	C	D	E	F	10	11	12	13	14	15	16	17	18	19	1A	1B
D	D	E	F	10	11	12	13	14	15	16	17	18	19	1A	1B	1C
E	E	F	10	11	12	13	14	15	16	17	18	19	1A	1B	1C	1D
F	F	10	11	12	13	14	15	16	17	18	19	1A	1B	1C	1D	1E

Таблица 1.2

Умножение чисел в 16-ричной системе счисления

×	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
2	0	2	4	6	8	A	C	E	10	12	14	16	18	1A	1C	1E
3	0	3	6	9	C	F	12	15	18	1B	1E	21	24	27	2A	2D
4	0	4	8	C	10	14	18	1C	20	24	28	2C	30	34	38	3C
5	0	5	A	F	14	19	1E	23	28	2D	32	37	3C	41	46	4B
6	0	6	C	12	18	1E	24	2F	30	36	3C	42	48	4E	54	5A
7	0	7	E	15	1C	23	2A	31	38	3F	46	4D	54	5B	62	69
8	0	8	10	18	20	28	30	38	40	48	50	58	60	68	70	78
9	0	9	12	1B	24	2D	36	3F	48	51	5A	63	6C	75	7E	87
A	0	A	14	1E	28	32	3C	46	50	5A	64	6E	78	82	8C	96
B	0	B	16	21	2C	37	42	4D	58	63	6E	79	84	8F	9A	A5
C	0	C	18	24	30	3C	48	54	60	6C	78	84	90	9C	A8	B4
D	0	D	1A	27	34	41	4E	5B	68	75	82	8F	9C	A9	B6	C3
E	0	E	1C	2A	38	46	54	62	70	7E	8C	9A	A8	B6	C4	D2
F	0	F	1E	2D	3C	4B	5A	69	78	87	96	A5	B4	C3	D2	E1

Разберем пример сложения чисел непосредственно и с применением табл. 1.1.

$$\begin{array}{r} 8A97F \\ +\ 29873 \\ \hline B41F2 \end{array}$$

$F + 3 = 12$ (2 пишем, 1 переносим в старший разряд);

$7 + 7 = E + 1 = F$ (F пишем в сумме);

$9 + 8 = 11$ (1 пишем, 1 переносим в старший разряд);

$A + 9 + 1 = 13 + 1 = 14$ (4 пишем, 1 переносим в старший разряд);

$8 + 2 + 1 = A + 1 = B$ (B пишем).

Табл. 1.1 используется так: первое слагаемое (в данном примере $F, 7, 9, A$ или 8) отыскивается в строке таблицы сверху; второе слагаемое (в примере соответственно 3, 7, 8, 9 или 2) – в крайнем левом столбце, а сумма чисел находится внутри таблицы на пересечении столбца и строки:

$$\begin{array}{r} 7\ A\ C\ 9\ 3\ .\ F\ 9\ 4 \\ +\ 9\ C\ 7\ 8\ F\ .\ F\ 8\ 9 \\ \hline 11\ 7\ 4\ 2\ 3\ .\ F\ 1\ D \end{array}$$

Таблицу сложения (см. табл. 1.1) можно использовать и как таблицу для вычитания чисел:

$$\begin{array}{r} 13086 \\ -\ 8988 \\ \hline A6FE \end{array}$$

6 – 8 (для вычитания берем единицу второго разряда и превращаем в 10 единиц первого, во втором разряде осталось 7 единиц);

10 + 6 – 8 = 16 – 8 = E;

7 – 8 (для вычитания берем единицу третьего разряда, но так как записан 0, берем единицу четвертого разряда, превращаем ее в 10 единиц третьего разряда и единицу третьего – в 10 единиц второго; в четвертом разряде остались 2 единицы, в третьем – F единиц);

10 + 7 – 8 = 17 – 8 = F;

F – 9 – 6;

2 – 8 (для вычитания единицу пятого разряда превращаем в 10 единиц четвертого);

10 + 2 – 8 = 12 – 8 = A.

Для нахождения разности двух чисел по табл. 1.1 вычитаемое отыскивается в верхней строке, уменьшаемое – внутри таблицы в столбце, соответствующем вычитаемому, разность берется в крайнем левом столбце в соответствии с уменьшаемым.

Здесь умножение выполнялось следующим образом: $8 \cdot 4 = 20$ (0 пишем, 2 переносим в старший разряд).

$8 \cdot 9 = 4\underbrace{8 + 2}_{10 = A} = 4A$ (А пишем, 4 – в старший разряд);

$8 \cdot 7 = 3\overbrace{8+4}^{12=C} = 3C$ (3 пишем, С – пишем);

$7 \cdot 4 = 1C$ (С пишем, 1 – в старший разряд);

$7 \cdot 9 - 1 = 3\widehat{F} + 1 = 40$ (0 пишем, 4 – в старший разряд);

$7 \cdot 7 + 4 = 31 + 4 = 35$ (3 пишем, 5 – пишем);

$3 \cdot 4 = C$ (C пишем);

$3 \cdot 9 = 1B$ (B пишем, 1 – в старший разряд);

$3 \cdot 7^{+1} = 15 + 1 = 16$ (1 пишем, 6 – пишем).

Отобразим схему решения (используем табл. 1.2):

×	…	8
…		↓
4	→	20
…		↓
7	→	38
…		↓
9	→	48

×	…	7
…		↓
4	→	1C
…		↓
7	→	35
…		↓
9	→	3F

×	…	3
…		↓
4	→	C
…		↓
7	→	15
…		↓
9	→	1B

Задание 1.6: а) найти остаток от деления 2^{100} на 3.

Решение. 1-й способ: 2 делится на 3 с остатком 2, 2^2 делится на 3 с остатком 1. При дальнейшем возведении двойки в степень остатки от деления будут чередоваться: 2, 1, 2, 1, 2 … . Значит, в силу четности степени 100 остаток от деления требуемого числа на 3 будет равен 1. 2-й способ – методом сравнений по аналогии с примером 1.6: $2^{100} = 4^{50} = (3+1)^{50} \equiv 1^{50} = 1$;

б) найти остаток от деления $1989 \cdot 1990 \cdot 1991 + 1992^3$ на 7.

Решение. Заменим каждое число на его остаток от деления на 7:

```
_1989 |_7          _1990 |_7          1991 = 7 · 284 + 3;
 14   | 284         14   | 284
 _58                _59               1992 = 7 · 284 + 4.
  56                 56
  _29                _30
   28                 28
    1                  2
```

$1 \cdot 2 \cdot 3 + 4^3 = 6 + 64 = 70$. $70 : 7 = 10$. Следовательно, остаток равен нулю;

в) найти остаток от деления 9^{100} на 8.

Решение. Заменим 9 на его остаток 1 от деления на 8. Имеем $1^{100} = 1$. Значит, остаток от деления 9^{100} на 8 равен 1;

г) найти остаток от деления 3^{1989} на 7.

Решение. 3 делится на 7 с остатком 3. 3^2 делится на 7 с остатком 2. Далее достаточно на 3 умножить только остаток и сделать выводы. 3^3 делится на 7 с

остатком 6, 3^4 делится на 7 с остатком 4, 3^5 делится на 7 с остатком 5, 3^6 делится на 7 с остатком 1, 3^7 делится на 7 с остатком 3. Получили один из предыдущих остатков, значит «зациклились». Число 3^7 дает тот же остаток деления на 7, что и 3^1. Значит, длина цикла равна 6. $1989 = 331 \cdot 6 + 3$. Число 3^{1989} дает тот же остаток от деления на 7, что и 3^3, то есть 6.

Индивидуальные задания для лабораторной работы №1

1. Найти канонические разложения чисел a и b.

2. Найти НОД (a,b), воспользовавшись: а) алгоритмом Евклида; б) разложением чисел на простые множители.

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

4. Записать в q-ичной, 16-ричной и двоичной системах счисления десятичное число c.

5. Вычислить … в 16-ричной системе счисления.

6. Найти остаток от деления данного числа на простое число.

Вариант 1

1–3. $a = 101398751$, $b = 326147777$. 4. $q = 7$, $c = 972405821$.

5. Определитель $\begin{vmatrix} A2 & -D & BC \\ -3B & 1F & 5C \\ -EA & 18 & 98 \end{vmatrix}$

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

Вариант 2

1–3. $a = 5999801$, $b = 48685811$. 4. $q = 5$, $c = 5999801$.

5. Решить систему уравнений $\begin{cases} DAx - Fy = 8, \\ 20x + 8y = 90. \end{cases}$

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

Вариант 3

1–3. $a = 660422941$, $b = 36481301$. 4. $q = 8$, $c = 5999801$.

5. Решить систему уравнений $\begin{cases} Dx - F1y = -6F, \\ Bx + 61y = CF. \end{cases}$

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

Вариант 4

1–3. $a = 9002242397$, $b = 433817903$. 4. $q = 7$, $c = 5090801$.

5. Вычислить произведение двух матриц:

$$\begin{pmatrix} BF & -3A & CD \\ 10 & 3E & -F2 \\ -90 & AE & FA \end{pmatrix}\begin{pmatrix} A1 & BB & -17 \\ -AD & CF & 9E \\ 2A & -BA & FB \end{pmatrix}.$$

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

Вариант 5

1–3. $a = 9118515943$, $b = 3386496689$. 4. $q = 7$, $c = 75928301$.

5. Вычислить произведение двух матриц

$$\begin{pmatrix} B3 & -3B & FD \\ A0 & 7E & -FA \\ -9C & BE & DA \end{pmatrix}\begin{pmatrix} CA & BF & -E7 \\ -AC & DF & B0 \\ 7A & -BC & 3B \end{pmatrix}.$$

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

Вариант 6

1–3. $a = 5336161097$, $b = 196210799$. 4. $q = 9$, $c = 73425826$.

5. Вычислить определитель $\begin{vmatrix} AB & -2D & FC \\ -3C & AF & BC \\ -EF & 1A & A8 \end{vmatrix}$.

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

Вариант 7

1–3. $a = 7049964661$, $b = 168687989$. 4. $q = 7$, $c = 93475825$.

5. Вычислить определитель $\begin{vmatrix} 2B & -AD & BC \\ -9C & A8 & B6 \\ -EE & 4C & AF \end{vmatrix}$.

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

Вариант 8

1–3. $a = 83748733$, $b = 73435591$. 4. $q = 7$, $c = 86425836$.

5. Вычислить определитель $\begin{vmatrix} 7B & -2D & FC \\ -3C & AF & BE \\ -E3 & 10 & A8 \end{vmatrix}$.

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

Вариант 9

1–3. $a =$ 16254559, $b =$ 1029073. 4. $q = 7$, $c =$ 86425836.

5. Вычислить произведение $(Fx^2 + 1Ax - 3F)(Cx^2 - ABx + E3)$.

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

Вариант 10

1–3. $a =$ 6099377, $b =$ 9568217. 4. $q = 8$, $c =$ 87625859.

5. Вычислить произведение $(F1x^2 + BAx - 35)(CAx^2 - A3x + ED)$.

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

Вариант 11

1–3. $a =$ 7957549, $b =$ 23118553. 4. $q = 7$, $c =$ 89605809.

5. Вычислить произведение $(B5x^2 + CAx - 3A)(CDx^2 - ABx + E9)$.

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

Вариант 12

1–3. $a =$ 16088437, $b =$ 18216949. 4. $q = 7$, $c =$ 38615802.

5. Вычислить произведение $(5Ax^2 + CBx - 2A)(CEx^2 - A8x + EF)$.

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

Вариант 13

1–3. $a =$ 244604911, $b =$ 61875907. 4. $q = 8$, $c =$ 79605819.

5. Вычислить произведение $(F5x^2 + CBx - BA)(C5x^2 - A0x + F9)$.

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

Вариант 14

1–3. $a =$ 356216713, $b =$ 31238065. 4. $q = 7$, $c =$ 85678539.

5. Вычислить произведение $(45x^2 + C2x - 3B)(C5x^2 - FBx + E0)$.

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

Вариант 15

1–3. $a =$ 7409621, $b =$ 6793883. 4. $q = 7$. $c =$ 9605801.

5. Вычислить произведение $(A5x^2 + CCx - 5A)(CFx^2 - 5Bx + EF)$.

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

2. КЛАССЫ ВЫЧЕТОВ

Теоретические сведения

При делении целых чисел на натуральное целое $m>1$ существует m различных остатков: $0, 1, 2, ..., m-1$. Соответственно этим остаткам множество Z разбивается на m непересекающихся классов сравнимых друг с другом чисел, т. е. имеющих один и тот же остаток от деления на m. В соответствии с остатками от деления на m эти классы будем обозначать через $\overline{0}, \overline{1}, ..., \overline{m-1}$. Таким образом, класс $\bar{i} = (mq + i \mid q \in Z)$ для каждого целого $i = 0, 1, 2, ..., m-1$. Любой представитель класса однозначно определяет свой класс: для каждого натурального числа $mq+i$ класс $\overline{mq+i} = \bar{i}$. Поскольку остаток – по-латински residu – переводится на русский язык как вычет, то множество всех классов, сравнимых друг с другом по данному модулю m чисел, называют множеством классов вычетов по модулю m и обозначают через Z/mZ. В силу сказанного $Z/mZ = \{\overline{0}, \overline{1}, ..., \overline{m-1}\}$ – множество из m элементов.

Заметим, что для любых классов $\bar{k}, \bar{l} \in Z/mZ$ и для произвольных $k_1, k_2 \in k, l_1, l_2 \in l$ суммы $k_1 + l_1$ и $k_2 + l_2$ принадлежат одному классу из Z/mZ, так как эти суммы сравнимы друг с другом по модулю m согласно свойству 2 сравнений (см. теоретический материал к разд. 1). Аналогично произведения $k_1 \cdot l_1$ и $k_2 \cdot l_2$ лежат в одном классе из Z/mZ. Определим операции сложения и умножения на Z/mZ. Полагаем суммой $\bar{k} \oplus \bar{l}$ тот единственный класс $\bar{z}$ из Z/mZ, в который попадают все суммы $k_1 + l_1$ и $k_2 + l_2$ для $k_1, k_2 \in \bar{k}$, $l_1, l_2 \in \bar{l}$, а произведением $\bar{k}\,\bar{l}$ – тот класс из Z/mZ, в который попадают произведения $\tilde{k} \cdot \tilde{l}$ для произвольных $\tilde{k} \in \bar{k}$, $\tilde{l} \in \bar{l}$.

Поскольку сложение и умножение в Z/mZ однозначно определяются умножением представителей классов, то свойства 1 – 5 операций сложения и умножения целых чисел (см. разд. 1) справедливы и в Z/mZ:

1) $\bar{k} \oplus \bar{i} = \bar{i} \oplus \bar{k}$; $\bar{l}\bar{k} = \bar{k}\bar{l}$ – коммутативность;

2) $\bar{k} \oplus (\bar{l} \oplus r) = (\bar{k} \oplus \bar{l}) \oplus r$; $\bar{k}(\bar{l}r) = (\bar{k}\bar{l})\, r$ – ассоциативность;

3) существует нейтральный элемент: $\bar{k} \oplus \overline{0} = \bar{k}$; $\bar{k}\,\overline{1} = \bar{k}$;

4) для всякого $\bar{k} \in Z/mZ$ существует единственный класс $\bar{l}$, такой, что $\bar{k} \oplus \bar{l} = \overline{0}$, очевидно, им является класс $\bar{l} = \overline{m-k}$;

5) $(\bar{k} \oplus \bar{l})\, r = (\bar{k}\bar{r}) \oplus (\bar{l}\bar{r})$ – дистрибутивность.

Благодаря отмеченным свойствам операций сложения и умножения множество Z/mZ в алгебре относят к классу коммутативных колец с единицей и называют кольцом классов вычетов по модулю m.

Определение 2.1. Элемент $\bar{k} \in Z/mZ$ называется обратимым, если найдется такой класс $\bar{l} \in Z/mZ$, что $\bar{k}\bar{l} = \bar{1}$. Тогда класс $\bar{l}$ называют обратным к классу $\bar{k}$.

Из ассоциативности умножения в кольце Z/mZ вытекает, что если $\bar{k}$ обратимый класс, то обратный класс определен однозначно.

Лемма 2.1. Пусть $\bar{k} \in Z/mZ$ такой класс, что $\text{НОД}(k, m) = 1$. Тогда:

1) для каждого $\bar{l} \neq \bar{0}$ произведение $\bar{k}\,\bar{l} \neq \bar{0}$;

2) $\bar{k} \cdot \bar{l}_1 \neq \bar{k} \cdot \bar{l}_2$, если $\bar{l}_1 \neq \bar{l}_2$;

3) отображение $f : \bar{x} \to \bar{k} \cdot \bar{x}$ инъективно и, следовательно, биективно на множестве Z/mZ (на множестве ненулевых элементов из Z/mZ);

4) $\bar{k}$ – обратимый класс в кольце Z/mZ.

Замечание. В условиях леммы 2.1 $\text{НОД}(d, m) = 1$, поэтому согласно критерию взаимной простоты целых чисел существуют такие целые $u, v \in Z$, что $ku + mv = 1$. Тогда $\bar{1} = \bar{k}\bar{u} + \bar{m}\bar{v} = \bar{k}\bar{u}$. Следовательно, $\bar{u}$ – обратный к $\bar{k}$ класс.

Лемма 2.2. Пусть $\bar{k} \in Z/mZ -$ такой, что $\text{НОД}(k, m) = d > 1$. Тогда:

1) существует класс $\bar{l} \neq \bar{0}$, что $\bar{k}\,\bar{l} = \bar{0}$;

2) существуют классы $\bar{l}_1 \neq \bar{l}_2$, такие, что $\bar{k} \cdot \bar{l}_1 = \bar{k} \cdot \bar{l}_2$;

3) для всех $\bar{l} \neq \bar{0}$ произведение $\bar{k} \cdot \bar{l} \neq 1$, то есть класс $\bar{l}$ не обратим в кольце Z/mZ.

Теорема 2.1. *Класс $\bar{k}$ из кольца Z/mZ обратим тогда и только тогда, когда* $\text{НОД}(k, m) = 1$. *Если $m = p$ – простое число, то в кольце Z/pZ каждый ненулевой класс обратим. Обратный класс также обратим. Произведение обратимых классов есть обратимый класс.*

Поскольку Z/mZ состоит из конечного множества элементов, то сложение и умножение можно задавать поэлементно в виде таблиц.

Пример 2.1. Напишем таблицы сложения и умножения в кольце $Z/3Z$:

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

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

Из таблицы умножения непосредственно видно, что классы $\bar{1}$ и $\bar{2}$ обратны самим себе, то есть обратимы все ненулевые классы $Z/3Z$ в полном соответствии с теоремой 2.1.

Определение 2.2. Функция Эйлера – функция натурального аргумента $\varphi(m)$, которая каждому натуральному числу $m>1$ ставит в соответствие количество натуральных чисел, меньших m и взаимно простых с m.

Перечислим основные мультипликативные свойства функции Эйлера.

Свойство 1. $\varphi(p)=p-1$ для каждого простого числа p.

Свойство 2. $\varphi(p^n)=p^n-p^{n-1}$ для каждого простого числа p и для произвольного натурального $n\geq 1$.

Свойство 3. Если $\text{НОД}(n,m)=1$, то $\varphi(n\cdot m)=\varphi(n)\cdot\varphi(m)$.

Свойство 4. Если $n=p_1^{S1}p_2^{S2}\ldots p_t^{S_t}$ – каноническое разложение числа n, то

$$\varphi(n)=n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdot\ldots\cdot\left(1-\frac{1}{p_t}\right).$$

Пример 2.2. Вычислим $\varphi(48)$. Поскольку $48=3\cdot 2^4$, то согласно свойству 4 значение $\varphi(48)=48\cdot(1-1/3)\cdot(1-1/2)=16$.

Пример 2.3. Из теоремы 2.1 следует, что в кольце Z/mZ имеется в точности $\varphi(m)$ обратимых классов. Например, $\varphi(12)=4$. Значит, в кольце $Z/12Z$ имеется именно 4 обратимых элемента. Непосредственная проверка показывает, что этими классами являются $\overline{1},\overline{5},\overline{7},\overline{11}$.

Теорема 2.2 (теорема Эйлера). *Если для целого числа a и натурального m* $\text{НОД}(a,m)=1$, *то* $a^{\varphi(m)}\equiv 1(\text{mod}\,m)$.

Алгебраическим сравнением n-й степени с одной неизвестной называется сравнение вида

$$a_nx^n+a^{n-1}+\ldots+a_1x+a_0x^0\equiv 0\ (\text{mod}\,m),$$

где $a_n,a_{n-1},\ldots,a_0\in Z,\ n\in N,\ a_n\not\equiv 0\ (\text{mod}\,m)$.

Если при подстановке в уравнение сравнения вместо x числа x_0 получается верное числовое сравнение, то x_0 называется решением данного сравнения. При этом и любое целое число вида x_0+mt также будет решением данного сравнения. Поэтому решением алгебраического сравнения можно считать класс вычетов $\overline{x}_0$. Универсальным способом решения алгебраических сравнений является испытание полной системы вычетов по модулю m, то есть целых чисел $0,1,2,\ldots,m-1$. Сравнение будет иметь столько решений, сколько вычетов полной системы ему удовлетворяют.

Пример 2.4. Решить сравнение $x^5+x+1\equiv 0\ (\text{mod}\,7)$.

Решение. Среди чисел 0, 1, 2, 3, 4, 5, 6 полной системы вычетов по модулю 7 удовлетворяют данному сравнению только два числа: $x=2,\ x=4$. Поэтому указанное сравнение имеет два решения: $x\equiv 2(\text{mod}\,7),\ x\equiv 4(\text{mod}\,7)$.

При решении сравнений часто используют преобразования, приводящие к равносильным сравнениям.

Задания для аудиторной работы

Задание 2.1. Вычислить $\varphi(n)$ для всех натуральных n от 2 до 12.

Задание 2.2. Вычислить $\varphi(60)$, $\varphi(81)$, $\varphi(89)$, $\varphi(2017)$, $\varphi(2018)$.

Решение. $60 = 2^2 \cdot 3 \cdot 5$. Согласно свойству 4 функции Эйлера

$$\varphi(60) = 60\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right) = 60 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} = 2 \cdot 2 \cdot 4 = 16.$$

$81 = 3^4$. Поэтому согласно свойству 2 функции Эйлера

$$\varphi(81) = 3^4 - 3^{3-1} = 3^4 - 3^3 = 81 - 27 = 54.$$

$\sqrt{89} < 10$; 89 не делится на все простые 2, 3, 5, 7, меньшие 10. Следовательно, 89 – число простое. Поэтому $\varphi(89) = 88$.

Задание 2.3. В кольцах $Z/5Z$ и $Z/6Z$ составить таблицы сложения и умножения. Найти в этих кольцах пары взаимно обратных по умножению элементов. Указать количество таких пар и сравнить это количество с $\varphi(5)$ и $\varphi(6)$ соответственно.

Решение аналогично решению примера 2.1.

Задание 2.4. В кольце классов вычетов по модулю 15 к каждому обратимому элементу найти обратный элемент.

Решение можно получить, составив таблицу умножения в кольце $Z/15Z$. Рассмотрим ниже другой путь решения этой задачи.

Согласно теореме 2.1 в кольце $Z/15Z$ имеется $\varphi(15) = 8$ классов вычетов, взаимно простых с модулем $m = 15$. Прямая проверка показывает, что эти классы составляют множество $G = \{\bar{1}, \bar{2}, \bar{4}, \bar{7}, \bar{8}, \overline{11}, \overline{13}, \overline{14}\}$.

На языке сравнений равенство $\bar{a} \cdot \bar{x} = \bar{1}$ для $\bar{a} \in G$ выглядит как $ax \equiv 1 \pmod{15}$, а из теоремы Эйлера следует, что $a^8 \equiv 1 \pmod{15}$. Умножив сравнение $ax \equiv 1 \pmod{15}$ на a^7, получим $x \equiv a^7 \pmod{15}$ согласно свойствам сравнений. Последовательно вычисляем:

$2^7 = 2^3 \cdot 2^4 = 8 \cdot 16 \equiv 8 \pmod{15}$, следовательно, $(\bar{2})^{-1} = \bar{8}$;

$4^7 = 4^6 \cdot 4 = 16^3 \cdot 4 \equiv 4 \pmod{15}$, следовательно, $(\bar{4})^{-1} = \bar{4}$;

$7^7 = 49^3 \cdot 7 \equiv 4^3 \cdot 7 \equiv 13$, $(\bar{7})^{-1} \equiv 1\bar{3}$;

$11^7 = 121^3 \cdot 11 = 1^3 \cdot 11 \equiv 11 \pmod{15}$, $(1\bar{1})^{-1} = 11$;

$14^7 = 2^7 \cdot 7^7 \equiv 8 \cdot 13 \pmod{15} \equiv (-7) \cdot (-2) \pmod{15} = 14 \pmod{15}$; $(1\bar{4})^{-1} = 1\bar{4}$.

Задание 2.5. Найти обратные к классам $\bar{5}, \bar{6}, \bar{7}$ в кольце: а) $Z/2016Z$; б) $Z/2017Z$.

Решение. НОД $(2016, 5) = 1$. Этот наибольший общий делитель найдем по алгоритму Евклида: $2016 = 5 \cdot 403 + 1$. Отсюда легко получается соотноше-

ние Безу для $\text{НОД}(2016, 5) = 1.\ 1 = 2016 \cdot 1 + 5 \cdot (-403)$. Согласно замечанию к лемме 2.1 $5^{-1} = \overline{-403} = 2016 - 403 = 1613$. Проверка:

$$5 \cdot 1613 = 8065 = 2016 \cdot 4 + 1 \equiv 1 \pmod{2016}.$$

$\text{НОД}(2016, 6) = 6 > 1$. Поэтому в кольце $Z / 2016Z$ не существует 6^{-1}.

Индивидуальные задания для лабораторной работы №2

1. Построить таблицы сложения и умножения в кольце: а) Z / kZ; б) Z / nZ.

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

3. В кольцах Z / kZ и Z / nZ из первого задания найти пары взаимно обратных относительно умножения элементов.

4. В кольце Z / mZ найти обратные к элементам $\overline{5}, \overline{6}, \overline{7}$.

5. Решить кубическое сравнение согласно варианту.

6. В кольце Z / nZ решить систему уравнений: $\begin{cases} \overline{13}x + \overline{5}y = \overline{11}; \\ \overline{7}x + \overline{11}y = \overline{13}. \end{cases}$

7. В кольце Z / kZ решить уравнение $x^2 + \overline{5}x + \overline{7} = 0$.

Вариант 1

1–3. $k = 11;\ n = 24$. 4. $m = 2001$. 5. $132x^3 + 143x^2 + 23x - 19 \equiv 5 \pmod{11}$.

Вариант 2

1–3. $k = 13;\ n = 18$. 4. $m = 2002$ 5. $169x^3 + 143x^2 + 23x - 19 \equiv 5 \pmod{13}$.

Вариант 3

1–3. $k = 23;\ n = 12$. 4. $m = 2000$. 5. $253x^3 + 46x^2 + 29x - 49 \equiv 5 \pmod{23}$.

Вариант 4

1–3. $k = 17;\ n = 21$. 4. $m = 2003$. 5. $187x^3 + 34x^2 + 23x - 19 \equiv 5 \pmod{17}$.

Вариант 5

1–3. $k = 19;\ n = 26$. 4. $m = 2004$. 5. $132x^3 + 143x^2 + 23x - 19 \equiv 5 \pmod{11}$.

Вариант 6

1–3. $k = 13;\ n = 27$. 4. $m = 2005$. 5. $117x^3 + 143x^2 + 3x - 19 \equiv 5 \pmod{13}$.

Вариант 7

1–3. $k = 7;\ n = 28$. 4. $m = 2006$. 5. $63x^3 + 154x^2 + 23x - 19 \equiv 5 \pmod 7$.

Вариант 8

1–3. $k = 29;\ n = 12$. 4. $m = 2007$. 5. $319x^3 + 145x^2 + 23x - 19 \equiv 5 \pmod{29}$.

Вариант 9

1–3. $k = 23;\ n = 14$. 4. $m = 2008$. 5. $253x^3 + 115x^2 + 12x - 9 \equiv 5 \pmod{23}$.

Вариант 10

1–3. $k = 31;\ n = 12$. 4. $m = 2009$. 5. $341x^3 + 155x^2 + 23x - 19 \equiv 5 \pmod{31}$.

Вариант 11

1–3. $k = 17;\ n = 30$. 4. $m = 2010$. 5. $85x^3 + 204x^2 + 13x - 19 \equiv 5 \pmod{17}$.

Вариант 12

1–3. $k = 29;\ n = 9$. 4. $m = 2011$. 5. $145x^3 + 348x^2 + 23x - 17 \equiv 5 \pmod{29}$.

Вариант 13

1–3. $k = 17;\ n = 22$. 4. $m = 2012$. 5. $153x^3 + 187x^2 + 11x - 9 \equiv 5 \pmod{17}$.

Вариант 14

1–3. $k = 19;\ n = 14$. 4. $m = 2013$. 5. $361x^3 + 209x^2 + 23x - 11 \equiv 5 \pmod{19}$.

Вариант 15

1–3. $k = 16;\ n = 23$. 4. $m = 2014$. 5. $95x^3 + 228x^2 + 23x - 9 \equiv 5 \pmod{19}$.

3. ТЕОРИЯ ГРУПП

Теоретические сведения

Определение 3.1. Группой называется непустое множество G с одной определенной на нем бинарной алгебраической операцией, относительно которой выполняются следующие свойства:

1) ассоциативность: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ для любых $a, b, c \in G$;

2) существует нейтральный элемент (единица), то есть такой элемент $e \in G$, что $g \cdot e = e \cdot g = g$ для каждого $g \in G$;

3) каждый элемент $g \in G$ имеет обратный, то есть такой элемент $h \in G$, что $g \cdot h = h \cdot g = e$ (в этом случае пишут $h = g^{-1}$).

Группы делятся на конечные и бесконечные по числу элементов, на коммутативные и некоммутативные в соответствии со следующим определением.

Определение 3.2. Группа G называется коммутативной, или абелевой, если определенная в ней операция (в дополнение к свойствам 1 – 3) обладает свойством 4: $b \cdot a = a \cdot b$ для всех $a, b \in G$.

Определение 3.3. Порядком конечной группы G называется количество элементов этой группы и обозначается $|G|$.

По исторической традиции все аддитивные группы (с операцией сложения) относятся к классу коммутативных групп. Для каждого натурального n найдется коммутативная конечная группа порядка n. Например $(Z/nZ, +)$.

Теорема 3.1. *Пусть a – фиксированный элемент произвольной группы G. Пусть* $< a > = \{a^0 = e, a, a^2, ..., a^{-1}, a^{-2}, ...\}$ – *множество всевозможных степеней элемента a. Тогда* $< a >$ – *группа, причем абелева.*

Определение 3.4. Группа $< a >$ из теоремы 3.1 называется циклической группой, порожденной элементом a.

Теорема 3.2. *Пусть элемент* $a \in G$ *обладает свойством*: $a^n = e$ *для некоторого целого* n *и* $a^k \neq e$ *для всех целых* k, $1 \le k < n$. *Тогда циклическая группа* $< a >$ *имеет порядок* n *и* $< a > = \{a, a^2, ..., a^n = e\}$.

Определение 3.5. Величина n из теоремы 3.2 называется порядком элемента $a \in G$. Если же для элемента $a \in G$ такого n не существует, то говорят, что элемент $a \in G$ имеет бесконечный порядок.

Из определения циклической группы следует, что она абелева, содержит счетное или конечное множество элементов и во втором случае имеет четкую структуру, выражаемую теоремой 3.2.

Теорема 3.3. *Для каждого простого числа* p *множество всех ненулевых классов из кольца классов вычетов* Z/nZ *образует группу* Z/pZ^* *относительно операции умножения, причем эта группа является циклической.*

Пусть Ω – конечное множество из n элементов. Поскольку природа его элементов несущественна, удобно считать, что $\Omega = \{1, 2, ..., n\}$.

Определение 3.6. Всякая биекция, то есть взаимно однозначное отображение Ω в себя называется подстановкой на Ω.

Подстановку $f: i \to f(i),\ i = 1, 2, ..., n$, удобно изображать в наглядной развернутой форме в виде двустрочной таблицы: $f = \begin{pmatrix} 1 & 2 & \dots & n \\ f(1) & f(2) & \dots & f(n) \end{pmatrix}$. В этой таблице каждый i-й столбец четко указывает, в какой элемент $f(i)$ преобразуется элемент i, $1 \le i \le n$. Подстановки перемножаются в соответствии с общим правилом композиции отображений: $(gf)(i) = g(f(i))$. Чаще всего $gf \neq fg$, то есть композиция подстановок не обладает свойством коммутативности. Очевидно, тождественная подстановка $e = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}$ играет роль единицы относительно композиции подстановок. Как известно, композиция отображений является ассоциативной операцией, поэтому и композиция подстановок ассоциативна. Каждая подстановка – обратимая операция. Чтобы найти для подстановки f обратную подстановку f^{-1}, достаточно в таблице $\begin{pmatrix} 1 & 2 & \dots & n \\ f(1) & f(2) & \dots & f(n) \end{pmatrix}$ переставить строки местами, а затем столбцы упорядочить по возрастанию элементов первой строки.

Таким образом, подстановки на Ω образуют группу относительно операции композиции отображений – умножения подстановок. Ее называют симметрической группой на n элементах и обозначают через S_n.

Теорема 3.4. *Порядок группы S_n равен $n!$.*

Пусть f – произвольная подстановка из S_n. Из двустрочной таблицы, задающей f, выбросим столбцы с одинаковыми элементами.

Определение 3.7. Циклом длиной k называется подстановка вида

$$f_k = (i, f(i), ..., f^{t_k - 1}(i)) = \begin{pmatrix} i & f(i) & \dots & f^{t_k - 1}(i) \\ f(i) & f^2(i) & \dots & i \end{pmatrix}.$$

Цикл длиной 2 называется транспозицией. Циклы без общих элементов называются *независимыми*, или *непересекающимися*.

Теорема 3.5. *Каждая подстановка $f \in S_n$, $f \neq l$, является произведением независимых циклов длиной $l \ge 2$. Это разложение в произведение определено однозначно с точностью до порядка следования циклов.*

Теорема 3.6. *Каждая подстановка $f \in S_n$ раскладывается в произведение транспозиций. Любые два разложения данной подстановки в произведения транспозиций содержат либо четное число сомножителей, либо нечетное.*

Пример 3.1. Разложить в произведение циклов и транспозиций подстановку

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

Решение.

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

Разложение подстановки в произведение транспозиций неоднозначно. Например, вышеприведенную подстановку можно представить в виде иного, следующего произведения транспозиций:

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

Определение 3.8. Подстановка f называется четной (нечетной), если ее разложение в произведение транспозиций содержит четное (нечетное) количество сомножителей.

Задания для аудиторной работы

Задание 3.1. Привести десять примеров групп. Почему вы считаете, что это действительно группа? Это абелева группа? Ваша группа конечна?

Задание 3.2. Определить, является ли группой относительно операции умножения множество $\widetilde{C}$ всех комплексных чисел, имеющих единичный модуль.

Решение. 1) $z_1 \cdot (z_2 \cdot z_3) = (z_1 \cdot z_2) \cdot z_3$ для любых комплексных чисел;

2) нейтральный элемент $e = 1$: $z \cdot 1 = 1 \cdot z = z$ для любого комплексного числа;

3) для каждого $z = x + iy \in \widetilde{C}$ по условию $|z| = \sqrt{x^2 + y^2} = 1$, то есть $x^2 + y^2 = 1$; поэтому обратным элементом для $z = x + iy \in \widetilde{C}$ будет число $\bar{z} = x - iy$:

$$z \cdot \bar{z} = (x + iy) \cdot (x - iy) = z \cdot \bar{z} = (x - iy) \cdot (x + iy) = x^2 + y^2 = 1.$$

Следовательно, $\widetilde{C}$ – действительно является группой.

Задание 3.3. Выяснить, является ли группой множество всех положительных вещественных чисел с бинарной алгебраической операцией возведения в степень?

Решение. Нет, потому что данная операция не ассоциативна. Например, $(2^3)^4 = 2^{12}$, а $2^{(3^4)} = 2^{81}$.

Задание 3.4. Разложить в произведение циклов и транспозиций подстановку $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 4 & 3 & 1 & 6 & 5 & 2 \end{pmatrix}$. Определить четность f.

Решение. Подстановка f перемещает 1 в 7, 7 в 2, 2 в 4, 4 в 1. В соответствии с определением 3.8 подстановка, действующая на элементы 1, 7, 2, 4 по данному правилу, а на все остальные – тождественно, называется циклом длиной 4. В соответствии с определением 3.8 данный цикл кратко записывают так: (1724). Также f перемещает 3 в 3, 5 в 6 и 6 в 5. Так что запись $f = (1724)(3)(56)$ указывает на то, как f перемещает элементы множества $\{1, 2, 3, 4, 5, 6, 7\}$. Поскольку цикл, состоящий из одного элемента, совпадает с тождественной подстановкой, то его при записи обычно опускают, т. е.

$f = (1\ 7\ 2\ 4)(5\ 6)$ – произведение циклов. Отсюда получаем разложение подстановки f – произведение транспозиций: $f = (1\ 4)(1\ 2)(1\ 7)(5\ 6)$. Как видим, f – четная подстановка.

Задание 3.5. Вычислить произведение $f \cdot g^{-1}$ для $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 6 & 5 & 2 & 1 & 7 & 4 \end{pmatrix}$ и $g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 3 & 2 & 6 & 4 & 1 & 5 \end{pmatrix}$.

Решение. $g^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 3 & 2 & 5 & 7 & 4 & 1 \end{pmatrix}$. Тогда $f \cdot g^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 5 & 6 & 1 & 4 & 2 & 3 \end{pmatrix}$.

Задание 3.6. Вычислить произведение циклов и транспозиций

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

Решение.

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

Задание 3.7. Выписать циклическую группу, порожденную подстановкой

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

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

$f^4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 5 & 4 & 1 & 6 & 7 \end{pmatrix}$; $f^5 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 6 & 1 & 2 & 3 & 7 & 4 \end{pmatrix}$;

$f^6 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 7 & 3 & 6 & 5 & 4 & 2 \end{pmatrix}$; $f^7 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 4 & 5 & 7 & 1 & 2 & 6 \end{pmatrix}$;

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

$f^{10} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 7 & 5 & 6 & 1 & 4 & 2 \end{pmatrix}$; $f^{11} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 4 & 1 & 7 & 3 & 2 & 6 \end{pmatrix}$;

$f^{12} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{pmatrix} = e$.

Согласно теореме 3.2 группа $< f >$ – порядка 12.

Задание 3.8. Выяснить, обратима ли матрица $A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$ с элементами из кольца классов вычетов $Z / 2Z$.

Решение. Найдем определитель матрицы A. $\det A = 1 \neq 0$. Следовательно, матрица A обратима.

Задание 3.9. Выписать циклическую группу, порожденную матрицей из предыдущего задания, и указать ее порядок.

Решение. $A^2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = E$. Следовательно, $< A >= \{A,\ A^2 = E\}$ – группа порядка 2.

Задание 3.10. Является ли циклической аддитивная группа:

а) вещественных чисел?

б) рациональных чисел?

Задания для самостоятельной работы

1. Выяснить, является ли группой множество с заданной операцией?

2. а) разложить в произведение циклов и транспозиций подстановку f. Определить ее четность;

б) вычислить коммутатор $h = g^{-1}f^{-1}gf$ для данных подстановок f и g;

в) вычислить произведение циклов и транспозиций.

3. Выписать циклическую группу $< f >$. Указать ее порядок.

4. Выяснить, обратима ли матрица B с элементами из $Z/2Z$.

5. Выписать циклическую группу $< B >$. Указать ее порядок.

6. Найти f^{1000} и B^{1000} для подстановки f из второго задания и матрицы B из четвертого задания.

Вариант 1

1. Множество целых чисел с операцией вычитания.

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

в) $(7\ \ 1\ \ 8\ \ 5)(4\ \ 6\ \ 3)(8\ \ 2)(9\ \ 1\ \ 3\ \ 5)$. 4. $B = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix}$.

Вариант 2

1. Множество всех положительных вещественных чисел с операцией деления.

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

в) $(3\ \ 1\ \ 9\ \ 5)(4\ \ 2\ \ 3)(8\ \ 9)(7\ \ 1\ \ 6\ \ 5)$. 4. $B = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}$.

Вариант 3

1. Множество целых чисел с операцией $m \cdot n = mn + m$.

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

в) $(4\ \ 2\ \ 6\ \ 9)(5\ \ 2\ \ 7)(7\ \ 9)(7\ \ 3\ \ 8\ \ 1)$. 4. $B = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \end{pmatrix}$.

Вариант 4

1. Множество целых чисел с операцией $m \cdot n = m + 2n$.

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

в) $(2\ \ 4\ \ 9\ \ 5)(1\ \ 3\ \ 7)(5\ \ 8)(7\ \ 1\ \ 3\ \ 6)$. 4. $B = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix}$.

Вариант 5

1. Множество целых чисел с операцией умножения.

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

в) $(9\ \ 1\ \ 3\ \ 5)(6\ \ 2\ \ 8)(2\ \ 9)(7\ \ 1\ \ 4\ \ 8)$. 4. $B = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$.

Вариант 6

1. Множество вещественных чисел с операцией деления.

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

в) $(7\ \ 3\ \ 9\ \ 5)(4\ \ 1\ \ 3)(8\ \ 6)(9\ \ 1\ \ 2\ \ 5)$. 4. $B = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$.

Вариант 7

1. Множество комплексных чисел с операцией $z_1 \otimes z_2 = \sqrt{z_1 z_2}$.

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

в) $(9\ \ 1\ \ 4\ \ 5)(3\ \ 2\ \ 7)(3\ \ 6)(7\ \ 2\ \ 6\ \ 8)$. 4. $B = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix}$.

Вариант 8

1. Множество комплексных чисел с операцией деления.

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

в) $(4\ \ 2\ \ 9\ \ 5)(7\ \ 9\ \ 3)(6\ \ 1)(8\ \ 6\ \ 5\ \ 1)$. 4. $B = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix}$.

Вариант 9

1. Выяснить, является ли подгруппой симметрическая разность двух подгрупп.

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

в) $(9\ \ 1\ \ 3\ \ 5)(4\ \ 2\ \ 3)(5\ \ 7)(9\ \ 1\ \ 6\ \ 8)$. 4. $B = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$.

Вариант 10

1. Выяснить, является ли подгруппой дополнение к подгруппе.

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

в) $(8\ \ 1\ \ 9\ \ 5)(1\ \ 2\ \ 3)(7\ \ 9)(4\ \ 1\ \ 6\ \ 5)$. 4. $B = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$.

Вариант 11

1. Выяснить, является ли подгруппой объединение двух подгрупп.

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

в) $(4\ \ 1\ \ 9\ \ 5)(7\ \ 2\ \ 3)(2\ \ 6)(3\ \ 1\ \ 6\ \ 8)$. 4. $B = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \end{pmatrix}$.

Вариант 12

1. Выяснить, является ли подгруппой пересечение двух подгрупп.

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

в) $(8\ \ 1\ \ 9\ \ 5)(9\ \ 2\ \ 3)(6\ \ 7)(7\ \ 2\ \ 4\ \ 5)$. 4. $B = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix}$.

Вариант 13

1. Все комплексные числа верхней полуплоскости относительно умножения.

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

в) $(1\ \ 6\ \ 9\ \ 5)(2\ \ 4\ \ 7)(3\ \ 9)(6\ \ 1\ \ 7\ \ 8)$. 4. $B = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 1 \end{pmatrix}$.

Вариант 14

1. Комплексные чисел правой полуплоскости относительно умножения.

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

в) $(2\ \ 1\ \ 7\ \ 3)(4\ \ 9\ \ 3)(4\ \ 7)(5\ \ 2\ \ 6\ \ 9)$. 4. $B = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$.

Вариант 15

1. Комплексные чисел нижней полуплоскости относительно умножения.

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

в) $(8\ \ 3\ \ 9\ \ 5)(4\ \ 1\ \ 3)(7\ \ 9)(6\ \ 1\ \ 2\ \ 5)$. 4. $B = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$.

4. ПОДГРУППЫ

Теоретические сведения

Определение 4.1. Подгруппой в группе $(G,\cdot)$ называется всякое непустое подмножество H элементов множества G, которое в свою очередь является группой относительно той же операции. Подгруппа H группы G называется собственной, если $H \neq G$ и $H \neq \{e\}$.

Выяснить, какое из подмножеств группы является подгруппой помогает

Теорема 4.1 (критерий подгруппы). *Непустое подмножество H группы $(G,\cdot)$ является подгруппой тогда и только тогда, когда для произвольных элементов $a, b \in H$ имеет место включение $a, b^{-1} \in H$.*

Как правило, в каждой группе имеется много различных подгрупп. Например, всевозможные степени конкретного элемента группы образуют циклическую подгруппу. Отметим, что имеет место

Теорема 4.2. *Всякая подгруппа циклической группы является циклической.*

Во всякой некоммутативной группе G представляет интерес максимальная подгруппа элементов, коммутирующих со всеми элементами группы. Ее называют центром группы и обычно обозначают через $Z(G)$, а подгруппы $Z(G)$ называют центральными подгруппами группы G.

Определение 4.2. Пусть H – собственная подгруппа группы $(G,\cdot)$. Пусть $a \in G$. Через aH обозначим множество элементов $\{ah | h \in H\}$ и назовем его левым смежным классом группы G по подгруппе H.

Если существует $b \in G$, $b \notin H \cup aH$, можно построить новый левый смежный класс bH и т. д.

Аналогично строят правые смежные классы. Если каждый левый смежный класс совпадает с правым: $aH = Ha$, то тогда смежные классы называют двусторонними. Такими являются смежные классы в любой абелевой группе G. Смежные классы обладают радом важных свойств.

Теорема 4.3. *Пусть H – собственная подгруппа группы G. Тогда*:

1) *каждый элемент $g \in G$ принадлежит какому-нибудь левому смежному классу по подгруппе H;*

2) *два элемента $a, b \in G$ принадлежат одному левому смежному классу тогда и только тогда, когда $a^{-1} \cdot b \in H$;*

3) *любые два левых смежных класса либо не пересекаются, либо совпадают*;

4) *для всякого $a \in G$ мощности множеств aH и H совпадают*;

5) *G есть объединение попарно непересекающихся левых (правых) смежных классов по подгруппе H;*

6) *мощности множеств всех левых и соответственно правых смежных классов группы G. по подгруппе H равны*.

Определение 4.3. Индексом подгруппы H в группе G называется мощность множества всех смежных классов группы G по данной подгруппе и обозначается через $|G : H|$.

С помощью свойств смежных доказывается важнейшая в теории конечных групп.

Теорема 4.4 (теорема Лагранжа). *Порядок конечной группы делится на порядок любой ее подгруппы.*

Следствие 1. В конечной группе индекс подгруппы равен частному от деления порядка группы на порядок подгруппы.

Следствие 2. Любая группа простого порядка является циклической и не содержит собственных подгрупп.

Следствие 3. Если G – конечная группа из n элементов, то для каждого $a \in G \quad a^n = e$. Другими словами, в конечной группе порядок любого ее элемента делит порядок самой группы.

Определение 4.4. Подгруппа H группы G называется нормальной, если для каждого $a \in G \quad aH = Ha$.

Очевидно, всякая подгруппа индекса 2 является нормальной подгруппой.

Задания для аудиторной работы

Задание 4.1. Привести примеры подгрупп в группе $(Z,+)$. Образуют ли подгруппу:

а) все отрицательные числа; все положительные числа;

б) все четные числа; все нечетные числа;

в) множество целых чисел от 0 до 10; от –5 до 5;

г) все целые числа, делящиеся на 2009;

д) все целые числа с остатком 1999 при делении на 2009?

Задание 4.2. Привести примеры подгрупп: а) в группе $(C,+)$ всех комплексных чисел с операцией сложения; б) в группе C^*.

Задание 4.3. Привести примеры подгрупп в группе $GL_n(R)$ всех невырожденных вещественных квадратных матриц данного порядка $n \geq 2$. Найти центр этой группы.

Задание 4.4. Много ли подгрупп у произвольной группы? Какова минимальная подгруппа, содержащая данный элемент группы? Какие еще элементы группы она должна содержать?

Задание 4.5. Выяснить, является ли подгруппой: а) объединение подгрупп; б) дополнение к подгруппе; в) симметрическая разность двух подгрупп; г) пересечение подгрупп; д) множество всех k-х степеней всех элементов абелевой группы.

Задание 4.6. В любой группе имеются циклические подгруппы (иногда совпадающие с самой группой). При каких условиях в группе имеются нециклические подгруппы? Привести примеры.

Задание 4.7. Показать, что мультипликативная группа $Z/8Z^*$ абелева, но не циклична, а $Z/9Z^*$ – циклична.

Задание 4.8. Пусть $G = M_{1\times 4}(Z/2Z)$ – множество всевозможных строк-матриц с четырьмя координатами из $Z/2Z$ – группа относительно операции покоординатного сложения по модулю два. Сколько в этой группе элементов?

Пусть H – следующее подмножество элементов группы G:

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

здесь $\bar{0}=0,\ \bar{1}=1$. Убедиться, что H – подгруппа, выписать таблицу смежных классов группы G по H.

Решение. Поскольку каждая из координат может независимо от других принимать лишь два значения, то мощность группы G равна 16.

Уже неоднократно обсуждалось, что операция покоординатного сложения по модулю два ассоциативна. Составив таблицу сложения элементов множества H, можно убедиться, что сложение этих элементов не выводит за пределы H, то есть H замкнута относительно сложения. H содержит нейтральный элемент – нулевой вектор. Каждый вектор из H обратен самому себе. Таким образом, H удовлетворяет всем аксиомам из определения группы. Следовательно, H – подгруппа группы G.

Выпишем таблицу всех смежных классов группы G по подгруппе H.

№ п/п	Класс $a+H$	$\bar{a}+\bar{0}$	$\bar{a}+\bar{e}_1$	$\bar{a}+\bar{e}_2$	$\bar{a}+(\bar{e}_1+\bar{e}_2)$
1	$\bar{0}+H=H$	(0000)	(1011)	(0101)	(1110)
2	$(1000)+H$	(1000)	(0011)	(1101)	(0110)
3	$(0100)+H$	(0100)	(1111)	(0001)	(1010)
4	$(0010)+H$	(0010)	(1001)	(0111)	(1100)

Задание 4.9. Выписать все элементы мультипликативной группы $(Z/36Z)^*$, сравнить количество элементов этой группы с $\varphi(36)$. Выяснить, является ли эта группа циклической. Выписать таблицу смежных классов $(Z/36Z)^*/<25>$ группы $(Z/36Z)^*$ по циклической подгруппе $<25>$.

Решение. $G=(Z/36Z)^*=\{1,5,7,11,13,17,19,23,25,29,31,35\}$. $|G|=12$. $\varphi(36)=\varphi(2^2\cdot 3^2)=12$. Следовательно, $|G|=\varphi(36)$. Группа G циклична, если в ней найдется элемент порядка $|G|$, то есть циклическая группа, порожденная некоторым элементом, совпадает со всей группой G. Попытаемся найти такой элемент. Наудачу выпишем циклическую подгруппу <5>.

$<5>=\{5,\ 25,\ 5^3=17,\ 5^4=17\cdot 5=13,\ 5^5=13\cdot 5=29,\ 5^6=29\cdot 5=1\}$ – подгруппа порядка 6. По теореме Лагранжа все остальные элементы этой подгруппы имеют порядки, являющиеся делителями 6.

$<7>=\{7,7^2=13,7^3=13\cdot 7=19,7^4=19\cdot 7=25,7^5=25\cdot 7=31,7^6=31\cdot 7=1\}$ – подгруппа порядка 6. Следовательно, ее элементы 7, 19, 31, не принадлежащие $<5>$, также имеют порядок, не превышающий 6.

$<11> = \{11, 11^2 = 13, 11^3 = 13 \cdot 11 = 35, 11^4 = 11 \cdot 35 = 25, 11^5 = 25 \cdot 11 = 23, 11^6 = 23 \cdot 11 = 1\}$ – подгруппа порядка 6. Следовательно, ее элементы 11, 23, 35, не принадлежащие подгруппам $< 7 >$ и $< 5 >$, также имеют порядок, не превышающий 6. Таким образом, все 12 элементов группы G имеют порядок, не превосходящий 6. Поэтому группа G не может быть циклической.

$H = < 25 > = \{25, 13, 1\}$ – подгруппа из трех элементов. Поэтому таблица смежных классов $(Z/36Z)^* / < 25 >$ должна состоять из $12 : 3 = 4$ смежных классов. Одним из них всегда является подгруппа H. Вот оставшиеся три смежных класса: $5H = \{5 \cdot 25 = 17, 5 \cdot 13 = 29, 5\}$;

$7H = \{7 \cdot 25 = 31, 7 \cdot 13 = 19, 7\}$; $11H = \{11 \cdot 25 = 23, 11 \cdot 13 = 35, 11\}$.

Задание 4.10. Содержит ли группа $(Z/36Z)^*$ нециклическую подгруппу?

Решение. Да, содержит. В этой группе имеются три элемента второго порядка: 17, 19, 35. Эти элементы обратны сами себе, так как из условия $a^2 = e$ следует, что $a^{-1} = a$. Вместе с 1 они образуют замкнутую систему относительно умножения по модулю 36, и, следовательно, подгруппу – нециклическую подгруппу из четырех элементов.

Задания для самостоятельной работы

Вариант 1

1. Убедиться, что векторы $\overline{0}(00000)$, $\overline{a}(10101)$, $\overline{b}(10011)$, $\overline{c}(00110)$ образуют подгруппу относительно сложения в группе V_5 всех векторов с координатами из $Z/2Z$.

2. Выписать таблицу смежных классов группы V_5 по данной подгруппе.

3. Выписать все элементы мультипликативной группы кольца: а) $Z/17Z$; б) $Z/32Z$. Сравнить количество этих элементов с $\varphi(17)$ и $\varphi(32)$ соответственно. Является ли эта группа относительно умножения циклической?

4. Выписать таблицу смежных классов:

а) $(Z/17Z)^* / < 4 >$; б) $(Z/32Z)^* / < 17 >$.

5. Содержит ли группа $Z/32Z$ нециклическую подгруппу?

6. Является ли нормальной подгруппа $< f >$ в группе S_9 для подстановки f из задания 2 лабораторной работы №3.

Вариант 2

1. Убедиться, что векторы $\overline{0}(00000)$, $\overline{a}(10110)$, $\overline{b}(11001)$, $\overline{c}(01111)$ образуют подгруппу относительно сложения в группе V_5 всех пятимерных векторов с координатами из $Z/2Z$.

2. Выписать таблицу смежных классов группы V_5 по данной подгруппе.

3. Выписать все элементы мультипликативной группы кольца: а) $Z/19Z$; б) $Z/30Z$. Сравнить количество этих элементов с $\varphi(19)$ и $\varphi(30)$ соответственно. Является ли эта группа относительно умножения циклической?

4. Выписать таблицу смежных классов:

а) $(Z/19Z)^*/<7>$; б) $(Z/30Z)^*/<17>$.

5. Содержит ли группа $(Z/30Z)^*$ нециклическую подгруппу?

6. Является ли нормальной подгруппа $<f>$ в группе S_9 для подстановки f из задания 2 лабораторной работы №3.

Вариант 3

1. Убедиться, что векторы $\bar{0}(00000), \bar{a}(10110), b(10101), \bar{c}(00011)$ образуют подгруппу относительно сложения в группе V_5 всех векторов с координатами из $Z/2Z$.

2. Выписать таблицу смежных классов группы V_5 по данной подгруппе.

3. Выписать все элементы мультипликативной группы кольца: а) $Z/13Z$; б) $Z/34Z$. Сравнить количество этих элементов с $\varphi(13)$ и $\varphi(34)$ соответственно. Является ли эта группа относительно умножения циклической?

4. Выписать таблицу смежных классов:

а) $(Z/13Z)^*/<3>$; б) $(Z/34Z)^*/<19>$.

5.Содержит ли группа $(Z/34Z)^*$ нециклическую подгруппу?

6. Является ли нормальной подгруппа $<f>$ в группе S_9 для подстановки f из задания 2 лабораторной работы №3.

Вариант 4

1. Убедиться, что векторы $\bar{0}(00000), \bar{a}(11000), b(10110), \bar{c}(01110)$ образуют подгруппу относительно сложения в группе V_5 всех пятимерных векторов с координатами из $Z/2Z$.

2. Выписать таблицу смежных классов группы V_5 по данной подгруппе.

3. Выписать все элементы мультипликативной группы кольца: а) $Z/11Z$; б) $Z/28Z$. Сравнить количество этих элементов с $\varphi(11)$ и $\varphi(28)$ соответственно. Является ли эта группа относительно умножения циклической?

4. Выписать таблицу смежных классов:

а) $(Z/11Z)^*/<10>$; б) $(Z/28Z)^*/<17>$.

5. Содержит ли группа $(Z/28Z)^*$ нециклическую подгруппу?

6. Является ли нормальной подгруппа $<f>$ в группе S_9 для подстановки f из задания 2 лабораторной работы №3.

Вариант 5

1. Выписать все элементы подгруппы, порожденной векторами $\bar{a}(11011), b(11100), \bar{c}(00111)$ в аддитивной группе V_5 5-мерных векторов с координатами из $Z/2Z$.

2. Выписать таблицу смежных классов группы V_5 по данной подгруппе.

3. Выписать все элементы мультипликативной группы кольца: а) $Z/18Z$; б) $Z/31Z$. Сравнить количество этих элементов с $\varphi(18)$ и $\varphi(31)$ соответственно. Является ли эта группа относительно умножения циклической?

4. Выписать таблицу смежных классов:

а) $(Z/31Z)^* / <26>$; б) $(Z/18Z)^* / <17>$.

5. Содержит ли группа $(Z/18Z)*$ нециклическую подгруппу?

6. Является ли нормальной подгруппа $<f>$ в группе S_9 для подстановки f из задания 2 лабораторной работы №3.

Вариант 6

1. Выписать все элементы подгруппы, порожденной векторами $\bar{a}(11001), b(10110), \bar{c}(01111)$ в аддитивной группе V_5 5-мерных векторов с координатами из $Z/2Z$.

2. Выписать таблицу смежных классов группы V_5 по данной подгруппе.

3. Выписать все элементы мультипликативной группы кольца: а) $Z/29Z$; б) $Z/16Z$. Сравнить количество этих элементов с $\varphi(29)$ и $\varphi(16)$ соответственно. Является ли эта группа относительно умножения циклической?

4. Выписать таблицу смежных классов:

а) $(Z/29Z)^* / <12>$; б) $(Z/16Z)^* / <7>$.

5. Содержит ли группа $(Z/16Z)*$ нециклическую подгруппу?

6. Является ли нормальной подгруппа $<f>$ в группе S_9 для подстановки f из задания 2 лабораторной работы №3.

Вариант 7

1. Выписать все элементы подгруппы, порожденной векторами $\bar{a}(11001), b(10110), \bar{c}(01111)$ в аддитивной группе V_5 5-мерных векторов с координатами из $Z/2Z$.

2. Выписать таблицу смежных классов группы V_5 по данной подгруппе.

3. Выписать все элементы мультипликативной группы кольца: а) $Z/17Z$; б) $Z/26Z$. Сравнить количество этих элементов с $\varphi(17)$ и $\varphi(26)$ соответственно. Является ли эта группа относительно умножения циклической?

4. Выписать таблицу смежных классов:

а) $(Z/17Z)^* / <2>$; б) $(Z/26Z)^* / <7>$.

5. Содержит ли группа $(Z/26Z)*$ нециклическую подгруппу?

6. Является ли нормальной подгруппа $< f >$ в группе S_9 для подстановки f из задания 2 лабораторной работы №3.

Вариант 8

1. Выписать все элементы подгруппы, порожденной векторами $\bar{a}(11000), b(10110), \bar{c}(01110)$ в аддитивной группе V_5 5-мерных векторов с координатами из $Z/2Z$.

2. Выписать таблицу смежных классов группы V_5 по данной подгруппе.

3. Выписать все элементы мультипликативной группы кольца: а) $Z/23Z$; б) $Z/24Z$. Сравнить количество этих элементов с $\varphi(23)$ и $\varphi(24)$ соответственно. Является ли эта группа относительно умножения циклической?

4. Выписать таблицу смежных классов:

а) $(Z/23Z)^*/<2>$; б) $(Z/24Z)^*/<17>$.

5.Содержит ли группа $(Z/24Z)^*$ нециклическую подгруппу?

6. Является ли нормальной подгруппа $< f >$ в группе S_9 для подстановки f из задания 2 лабораторной работы №3.

Вариант 9

1. Выписать все элементы подгруппы, порожденной векторами $\bar{a}(11001), b(10110), \bar{c}(01111)$ в аддитивной группе V_5 5-мерных векторов с координатами из $Z/2Z$.

2. Выписать таблицу смежных классов группы V_5 по данной подгруппе.

3. Выписать все элементы мультипликативной группы кольца: а) $Z/23Z$; б) $Z/21Z$. Сравнить количество этих элементов с $\varphi(23)$ и $\varphi(21)$ соответственно. Является ли эта группа относительно умножения циклической?

4. Выписать таблицу смежных классов:

а) $(Z/23Z)^*/<3>$; б) $(Z/21Z)^*/<11>$.

5. Содержит ли группа $(Z/21Z)^*$ нециклическую подгруппу?

6. Является ли нормальной подгруппа $< f >$ в группе S_9 для подстановки f из задания 2 лабораторной работы №3.

Вариант 10

1. Выписать все элементы подгруппы, порожденной векторами $b(10110), \bar{c}(01111)$ в аддитивной группе V_5 5-мерных векторов с координатами из $Z/2Z$.

2. Выписать таблицу смежных классов группы V_5 по данной подгруппе.

3. Выписать все элементы мультипликативной группы кольца: а) $Z/31Z$; б) $Z/20Z$. Сравнить количество этих элементов с $\varphi(31)$ и $\varphi(20)$ соответственно. Является ли эта группа относительно умножения циклической?

4. Выписать таблицу смежных классов:

а) $(Z/31Z)^*/<2>$; б) $(Z/20Z)^*/<17>$.

5. Содержит ли группа $(Z/20Z)*$ нециклическую подгруппу?

6. Является ли нормальной подгруппа $<f>$ в группе S_9 для подстановки f из задания 2 лабораторной работы №3.

Вариант 11

1. Выписать все элементы подгруппы, порожденной векторами $\bar{a}(11001), \bar{b}(10110)$ в аддитивной группе V_5 5-мерных векторов с координатами из $Z/2Z$.

2. Выписать таблицу смежных классов группы V_5 по данной подгруппе.

3. Выписать все элементы мультипликативной группы кольца: а) $Z/14Z$; б) $Z/37Z$. Сравнить количество этих элементов с $\varphi(14)$ и $\varphi(37)$ соответственно. Является ли эта группа относительно умножения циклической?

4. Выписать таблицу смежных классов:

а) $(Z/14Z)^*/<11>$; б) $(Z/37Z)^*/<3>$.

5. Содержит ли группа $(Z/14Z)*$ нециклическую подгруппу?

6. Является ли нормальной подгруппа $<f>$ в группе S_9 для подстановки f из задания 2 лабораторной работы №3.

Вариант 12

1. Выписать все элементы подгруппы, порожденной векторами $\bar{a}(11001), \bar{c}(01111)$ в аддитивной группе V_5 5-мерных векторов с координатами из $Z/2Z$.

2. Выписать таблицу смежных классов группы V_5 по данной подгруппе.

3. Выписать все элементы мультипликативной группы кольца: а) $Z/17Z$; б) $Z/25Z$. Сравнить количество этих элементов с $\varphi(17)$ и $\varphi(25)$ соответственно. Является ли эта группа относительно умножения циклической?

4. Выписать таблицу смежных классов:

а) $(Z/17Z)^*/<10>$; б) $(Z/25Z)^*/<7>$.

5.Содержит ли группа $(Z/25Z)*$ нециклическую подгруппу?

6. Является ли нормальной подгруппа $<f>$ в группе S_9 для подстановки f из задания 2 лабораторной работы №3.

Вариант 13

1. Убедиться, что векторы $\bar{0}(00000), \bar{a}(00110), b(01001), \bar{c}(01111)$ образуют подгруппу относительно сложения в группе V_5 всех 5-мерных векторов с координатами из $Z/2Z$.

2. Выписать таблицу смежных классов группы V_5 по данной подгруппе.

3. Выписать все элементы мультипликативной группы кольца: а) $(Z/17Z)^*$; б) $(Z/27Z)^*$. Сравнить количество этих элементов с $\varphi(17)$ и $\varphi(27)$ соответственно. Является ли эта группа относительно умножения циклической?

4. Выписать таблицу смежных классов:

а) $(Z/17Z)^* / <10>$; б) $(Z/27Z)^* / <10>$.

5.Содержит ли группа $(Z/27Z)^*$ нециклическую подгруппу?

6. Является ли нормальной подгруппа $< f >$ в группе S_9 для подстановки f из задания 2 лабораторной работы №3.

Вариант 14

1. Убедиться, что векторы $\bar{0}(00000), \bar{a}(11100), \bar{b}(00111), \bar{c}(11011)$ образуют подгруппу относительно сложения в группе V_5 всех 5-мерных векторов с координатами из $Z/2Z$.

2. Выписать таблицу смежных классов группы V_5 по данной подгруппе.

3. Выписать все элементы мультипликативной группы кольца: а) $(Z/13Z)^*$; б) $(Z/22Z)^*$. Сравнить количество этих элементов с $\varphi(13)$ и $\varphi(22)$ соответственно. Является ли эта группа относительно умножения циклической?

4. Выписать таблицу смежных классов:

а) $(Z/13Z)^* / <10>$; б) $(Z/22Z)^* / <7>$.

5. Содержит ли группа $(Z/22Z)^*$ нециклическую подгруппу?

6. Является ли нормальной подгруппа $< f >$ в группе S_9 для подстановки f из задания 2 лабораторной работы №3.

Вариант 15

1. Убедиться, что векторы $\bar{0}(00000), \bar{a}(00111), \bar{b}(01001), \bar{c}(01110)$ образуют подгруппу относительно сложения в группе V_5 всех 5-мерных векторов с координатами из $Z/2Z$.

2. Выписать таблицу смежных классов группы V_5 по данной подгруппе.

3. Выписать все элементы мультипликативной группы кольца: а) $(Z/15Z)^*$; б) $(Z/29Z)^*$. Сравнить количество этих элементов с $\varphi(15)$ и $\varphi(29)$ соответственно. Является ли эта группа относительно умножения циклической?

4. Выписать таблицу смежных классов:

а) $(Z/15Z)^* / <7>$; б) $(Z/29Z)^* / <10>$.

5. Содержит ли группа $(Z/15Z)^*$ нециклическую подгруппу?

6. Является ли нормальной подгруппа $< f >$ в группе S_9 для подстановки f из задания 2 лабораторной работы №3.

5. ИСТОРИЧЕСКАЯ КРИПТОГРАФИЯ

Теоретические сведения

История цивилизации показывает, что практически сразу с появлением письменности появлялись и разного рода системы защиты информации от несанкционированного доступа. Рассмотрим наиболее популярные из них.

1. Шифр Цезаря. Суть его в том, что в тексте каждая буква заменяется отстоящей от нее по алфавиту на фиксированное число позиций по циклу. Так Юлий Цезарь в I веке новой эры в деловой переписке заменял в сообщении первую букву латинского алфавита (A) на четвертую (D), вторую (B) – на пятую (E), наконец, последнюю – на третью. Иными словами, замена производилась в соответствии с таблицей, которая в русском варианте имеет следующий вид (рис. 5.1).

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

Рис. 5.1

Пример 5.1. Знаменитое донесение римскому сенату об очередной победе выглядело (в русском переводе) следующим образом:

ТУЛЫИО ЦЕЛЖЗО ТСДЗЖЛО

Приложив достаточно серьезные усилия по расшифровке, можно убедиться, что истинный текст гласит: «Пришел, увидел, победил».

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.

2. Тарабарская грамота. Известна в России с XIII в. На уровне разговорного языка ею владели и Стенька Разин и Емельян Пугачев. Гиляровский В. А. еще в 30-е гг. XX в. встречал на московских рынках странных лиц, переговаривавшихся между собой на «тарабарском». Тарабарская грамота проста. В ней согласные буквы заменяются по схеме, представленной на рис. 5.2.

Б	В	Г	Д	Ж	З	К	Л	М	Н
Щ	Ш	Ч	Ц	Х	Ф	Т	С	Р	П

Рис. 5.2

При шифровании буквы, расположенные на одной вертикали, переходят одна в другую. Остальные буквы остаются без изменения.

Пример 5.2. Попробуйте прочитать следующее исключительно секретное сообщение:

РАРА РЫСА МАРУ

3. Криптосистема Тритемиуса. Данная система шифрования впервые была опубликована в 1518 г. в трактате, принадлежащем перу религиозного деятеля аббата Тритемиуса (1462 – 1516). Система Тритемиуса представляет собой дальнейшее усовершенствование системы шифрования Цезаря и базируется на идее применения девизов. Под текстом подписывался девиз (в дальнейшем его стали называть «ключом») с повторением, затем происходило постолбцовое суммирование букв текста и девиза («ключа» по новой терминологии), в результате получался шифротекст.

Пример 5.3. Зашифруем текст «Над Парижем небо синее» с помощью девиза «Роза». Как сказано выше, для этого выпишем две строки – строку текста и строку ключа с повторением. Сверху и снизу добавим по строке номеров соотаетствующих букв в русском алфавите. Получим следующую таблицу (рис. 5.3).

15	1	5	17	1	18	10	8	6	14	15	6	2	16	19	10	15	6	6
Н	*А*	*Д*	*П*	*А*	*Р*	*И*	*Ж*	*Е*	*М*	*Н*	*Е*	*Б*	*О*	*С*	*И*	*Н*	*Е*	*Е*
Р	*О*	*З*	*А*	*Р*	*О*	*З*	*А*	*Р*	*О*	*З*	*А*	*Р*	*О*	*З*	*А*	*Р*	*О*	*З*
18	16	9	1	18	16	9	1	18	16	9	1	18	16	9	1	18	16	9

Рис. 5.3

Для получения шифротекста суммируем числа каждого столбца полученной таблицы. Если сумма оказывается больше 33, то вычитаем из этой суммы 33. После этих вычислений от числа переходим к букве. Так, в первом столбце получаем число $15+18=33$, то есть букву «Я». Продолжив процедуру, получим следующее шифрованное сообщение:

Я П М Р С А С З Ц Ь Ц Ё Т Ю Ъ И Я Ф Н

Французский посол в Риме Блез де Виженер (1523 – 1596), по роду службы связанный с проблемой секретности дипломатической почты, написал большой «Трактат о шифрах» (опубликован в 1585 г.). 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 (табл. 5.1). Первая ее строка заполнена последовательно буквами алфавита. Вторая – тем же алфавитом, но сдвинутым на одну букву влево – в нашем случае начинается с буквы Б и заканчивается буквой А. Третья строка начинается буквой В и заканчивается буквой Б. И так далее до 33 строки включительно. Возвращаемся к примеру 5.3. На пересечении столбца с первой буквой Н и строки с первой буквой Р находим букву Я – первую букву шифротекста. И так далее.

В таком виде криптосистема с девизом применялась на протяжении 400 лет как абсолютно надежная и недешифруемая, особенно в военном деле. О том, что криптосистема Тритемиуса успешно применялась и в начале XX в. свидетельствуют, в частности, отдельные страницы бессмертной книги Я. Гашека «Похождения бравого солдата Швейка».

Таблица 5.1

Таблица Виженера

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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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

Опыт долгого применения рассмотренной криптографической системы указал на проблему ключей. Слишком долгое применение одного и того же ключа может навести противника на какие-то закономерности и, как следствие, к взлому криптосистемы. Проблема эта преодолевалась двумя путями. Сначала пришли к мысли применения длинных ключей. В идеале – длина ключа совпадает с длиной шифруемого текста. Затем, естественно, быстро пришли к идее частой смены ключей. Частая смена ключей порождают проблемы выбора новых ключей и их передачи. Выход был найден неожиданный и гениально простой – книга. Участники переписки используют идентичные экземпляры одного и того же издания конкретной книги. Новый ключ сообщается, называя страницу и абзац книги. Два числа, переданные почтой или публикацией в рекламном отделе газеты, вряд ли дадут содержательную информацию противнику.

4. Постолбцовая транспозиция. К классу «перестановка» относится шифр «маршрутная транспозиция» и его вариант «постолбцовая транспозиция». В данный прямоугольник $[n \times m]$ вписывается сообщение по строкам. Шифрованный текст найдем, если будем выписывать буквы в порядке следования столбцов.

Следующий пример демонстрирует шифрование методом «постолбцовой транспозиции».

Пример 5.4. Текст, состоящий из 30 букв, записан построчно змейкой в таблицу или матрицу размером 5×6 (рис. 5.4).

М	*И*	*Н*	*С*	*К*	*С*
А	*Ц*	*И*	*Л*	*О*	*Т*
Р	*Е*	*С*	*П*	*У*	*Б*
Е	*Б*	*И*	*К*	*И*	*Л*
Л	*А*	*Р*	*У*	*С*	*Ь*

Рис. 5.4

Шифрованный текст получается последовательной записью столбцов этой таблицы в строку, также змейкой, начиная с последнего:

МАРЕЛ АБЕЦИ НИСИР УКПЛС КОУИС ЬЛБТС

Конечно, возможны и другие способы-маршруты записи текста в таблицу и выписки столбцов. Например, такой, более естественный (рис. 5.5).

М	*И*	*Н*	*С*	*К*	*С*
Т	*О*	*Л*	*И*	*Ц*	*А*
Р	*Е*	*С*	*П*	*У*	*Б*
Л	*И*	*К*	*И*	*Б*	*Е*
Л	*А*	*Р*	*У*	*С*	*Ь*

→ *МТРЛЛ ИОЕИА НЛСКР СИПИУ КЦУБС САБЕЬ*

Рис. 5.5

Попробуйте прочитать еще одно сообщение, шифрованное методом «постолбцовой транспозиции».

Пример 5.5. МАСТ АЕРР ЕШРН ОЕРМ ИУПВ КЙТР ПНОИ

Усложнением этих двух вариантов шифрования является применение девизов. Суть их в том, что после записывания текста в таблицу столбцы таблицы переставляются каким-то образом, прежде чем выписывать шифротекст. В человеческой природе свойственно всякому действию придавать какой-нибудь, пусть и призрачный, смысл. Вот и пришла кому-то мысль не просто переставлять столбцы, а в порядке следования букв в девизе.

Пример 5.6. Усложним шифровку по первой таблице примера 5.4, 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 5.4:

СТБЛЬ РИСИН КОУИС УКПЛС ИЦЕБА ЛЕРАМ

5. Криптосистема Кардано. Пожалуй, наиболее сложный вариант «маршрутной перестановки» предоставляет *поворотная решетка*, или *решетка Кардано.* Джероламо Кардано (1501 – 1576) – знаменитый итальянский математик, механик, врач, философ. Как математик, он знаменит тем, что нашел формулы решения кубических уравнений. А как механик – прежде всего тем, что на его идеях реализовано в каждом автомобиле устройство под названием «карданный вал». Наконец, Кардано оставил глубокий след и в криптографии.

Авторству Джероламо Кардано принадлежит следующий метод шифрования. Для тайной передачи сообщения, содержащего $4mk$ букв, изготавливается трафарет из прямоугольного листа клетчатой бумаги размером $2m \times 2k$ клеток. В трафарете вырезают mk клеток так, чтобы при наложении его на такой же чистый лист бумаги четырьмя возможными способами его вырезы полностью покрывают всю площадь листа. Определяется заранее порядок этих четырех возможных 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 (рис. 5.6).

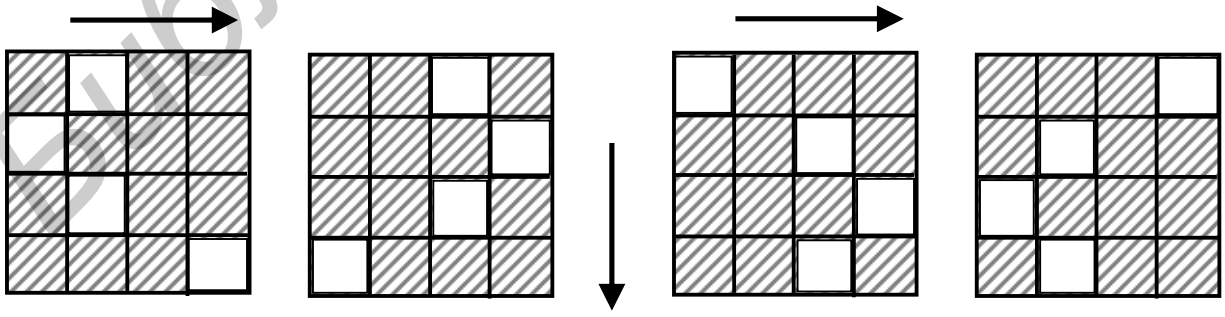


Рис. 5.6

Пример 5.7. Прочитайте записанное с помощью приведенного выше трафарета и в указанном выше порядке следующее краткое, но, несомненно важное сообщение:

ОТТВ РЧИЫ УЕТМ ЕЗЙВ

Задания для аудиторной работы

Задание 5.1. Прочитать текст, записанный с помощью шифра Цезаря:

а) еогфхя – ахс ефзёжг пгёв олщзжзмфхег;

б) тусхлерцб фхсусрц ргжс еюфоылегхя, нгн дю срг рз дюог тусхлерг.

Задание 5.2. Расшифровать «тарабарский» текст:

а) ш гухой ропалкымь ло лшоир улкашор пе жоцяк;

б) гко рохек лтафакь о передтой тсаллигелтой зисолозии рухгипа щеф нмонилти?

Задание 5.3. Расшифровать текст, созданный с помощью таблицы Виженера: а) ыодхчаюъбькящячгчгщщб; б) ксааофрем.

Задание 5.4. Расшифровать сообщения, зашифрованные методом постолбцовой транспозиции:

а) дбчргив ллуадны яёвваон онсдгчо снтартс коввуии огасбнм ропеаеа;

б) бниен еоету зепдю рболв аррир саота стжеж уадлд днаьу.

Задание 5.5. Расшифровать сообщения, зашифрованные по Кардано:

иснктг опорид азвоон туанят нквсчи ооутяс

x	x			x	
				x	
					x
		x			
		x	x		
		x			

Задания для самостоятельной работы

1. Расшифровать криптограмму Цезаря.
2. Перевести текст с «тарабарской» грамоты.
3. Расшифровать постолбцовый вариант маршрутной транспозиции.
4. Расшифровать сообщение с девизом «Я помню чудное мгновенье».
5. Расшифровать криптосистему Кардано.

Вариант 1

1. ефвнгв жлччзузрщлуцзпгв чцрнщлв рзтузуюерг.

2. хифпь нметмалпа цшуря шебари – ифугепиер ракеракити и её нменоца-шапиер.

3. тояаи овпдт лррлн ьеиеа кмнжм.
4. дбъх всеюъцн ихчвутйытнпгущн рё всн ч тстюутапйе.
5. сетсчт водблл еемчег кдуаер укаеив аьмаоо.

x				x	
			x		x
	x		x		
				x	
		x	x		

Вариант 2

1. рльхс рз езьрс тсж оцрсб.
2. паута лкапошикля ноцсиппой паутой ш кой лкенепи, ш татой носьфуекля ракеракигелтири рекоцари.
3. сттлёбео тььыпекс ыкешасни даченпиш икепыемь чпмотчос елбтентя саормен*.
4. мю ачьйуют пэрчг ыу муюин нэ рют очхсь р рсф яырчюеч.
5. нтипиа кдныпм аегари ояакии нзаткм аымоср.

	x			x	
x		x		x	
	x	x			
			x		x

Вариант 3

1. лфхсулв цьлх ьхс рлнгнгв еогфхэ рз дюегзх езьрсм.
2. паута щеф ракеракити – пе паута.
3. смауамр ычнчеуа пееттчд олпоаеу зооопме нвтноут аеозтос ёкмноня.
4. ряямпмобмш жпыойькпн нугфяуцр ёесьртзз вэтсбза.
5. еесрсв снеиив мтенто итоттн смжмоа мьйено.

	x				
x				x	
	x				x
			x		
			x		
x		x			

Вариант 4

1. лфхсульзфнл тзуеюз еюдсую тусыол е Лцжзз тул Тсрхлл Тлогхз.
2. тшапкошый торньюкем шфсораек сющую лошмереппую тминкочмазигелтую лилкеру.
3. сеяое лоддн утегн чклоы арате йыюоу нттвм ыиплы.
4. люхъь ёчгфьачы тьучеаш ж яьуэцик бд ыуцчсщкму щбч.
5. тулоеш рпжчет нлиины сжнорй ьзнмса аоррои.

		x			
x			x		
				x	
			x		x
	x				
x				x	

Вариант 5

1. нултхсёугчлв угкугдгхюегзх пзхсжю кгълхю лрчсупгщлл сх рзфгрнщлсрлуегррсёс.
2. аццикишпая чмунна л цоноспикесьпой онемадией урпохепия, лшяфаппой ло лсохепиер фатопари цилкмищукишполки, пафншаекля тосьдор.
3. сзветмт лаельае емлонял дыивазь оскеуан влоккна аягааия тмоесм∗ ьичсаа∗.
4. ю ввя фг шдтячрюв п ежтам пкфбчц ж яуётятаоян д фщью.
5. хнтпны сеторь астеоа якпарм воесвх оороин.

					x
		x			
x					
			x		
x		x		x	x
			x		

Вариант 6

1. хзсулв ьлфзо фзмьгф схрсфлхфв н угкувжц тулногжрюш ргцн.

2. гер пешехелкшеппей гесошет, кер щосее оп ушемеп, гко илкипа у нечо ш тамрапе.

3. ундити миетьт нклевб еаёреы икнязт монедь ейотен юойсзи щпцянг иребад йелыче.

4. оаэсшфаь фнртзш пумчьмуб эо ыяъ зуёый ссйсв ууоко.

5. ястоео аомаол зивзст икмило ыиисмв тиктсв.

x		x		x	
			x		
			x		
	x				x
x				x	

Вариант 7

1. нгйжюм еютцфнрлн дёцлу цезузррс еогжззх нсптэбхзусп.

2. пи оцип шекем пе щуцек нонукпыр цся томащся, токомый пе шывес иф чашапи.

3. клшуе тслтр ояяро нртув ааьда узтнт чмооь иымв∗.

4. оюсхоггп ст ачэгёьв зтмуэ яэчн яьычъачоцтб ойеое.

5. деуоля уртаеь тнаеом оеьртн юкетжо чбзссу.

		x			
	x		x		x
x					
		x			
			x		x
x					

Вариант 8

1. пухл – уцк хесзм пзьхю.

2. чмарр шоси шелик кяхесее, гер депкпем малллухцепия и ущехцепия.

3. уоори мтрдт гпеца ирчее боиит нтймс еисия твеп∗.

4. рыуон аищ цнщлс хмьхряы цсаоеыщб лфны ьсуыэл иниа.

5. елзэта еыьбзн надчтм сиюкыд вуанст ттеяёа.

			x		x
				x	
		x			x
				x	
x			x		
	x				

Вариант 9

1. носж ызррср веовзхфв сфрсестсосйрлнсп фсеузпзррсм кгълхю лрчсупгщлл.
2. рылсь ифмегеппая елкь сохь.
3. хняде оезур ррард оыщнр шлиыу иутхг ечамо мшоаг аатно.
4. оющм ъщ иёфьчс ьоньэ тн эшггзст ийв ць руьоьзвйа еъ.
5. ионквн йводаи гессир всуйсе терукт мныотс.

					x
	x	x			
x					x
x			x	x	
	x				

Вариант 10

1. тсжелж ц нсхсуёс ефз аозпзрхю сдугхлпю схрсфлхзоэрс стузжоиррсм е рзп гоёздугльзфнсм стзугщлл ргкюегзхфв ёуцттсм.
2. кьры пифтиж илкип пар цомохе Пал шофшываюбий ощрап
3. ссхгй рлолц еедаа дпнзр иыоыь
4. дбъх м ль ддяжнбубм ячь юаппхсыжь т ст юушцев йеебч.
5. иеируу буешсе ввррыи йлчсмн глаатт бусыйы.

	x			x	
	x				
x		x			x
				x	
			x		
					x

Вариант 11

1. фхсмнсфхэ нултхсфлфхзпю уфг сдцфосезрг фосйрсфхэб еюьзфозрлв чурнщлл Амозуг.

2. елси оцип маф нохасеевь, гко пе лтафас, ко лко маф нохасеевь, гко пе нморосгас.

3. жоьне еибег лдажо атвет юиела щсдащ еуёюи гдтщт.

4. рюъъдг ихиачч ьумыр ж рзеж эчдтбё еиоу лмун эётнжу.

5. рбкжнв мреешл ыокзот мионат ачнуаь омаьею.

	x	x			
		x		x	
	x				
			x		x
	x				x

Вариант 12

1. гулчпзхлнг нсозщ ногффсе еюьзхсе озйлх е сфрсез прсёлш фсе-узпзррюш нултхсёугчльзфнлш флфхзп.

2. елси кы панмашисля т деси и лкапевь цомочою вшымякь тарпяри шо шлятую саюбюю лощату, ко пе цойцёвь цо пеё.

3. удстщч тлтьеа еянтйс шныопт еехвоь нсианю ичмре∗ еаеис∗.

4. бкжсщ йьесцщ тм нюйнбдк фнуйенру еётхнщ еьцёшгкс.

5. ркжодт ворйьц иедачи аасбис нтитси веоыаи.

	x				
x			x		
x		x			x
	x				
				x	
x					

Вариант 13

1. жегжщгхлозхрлм тгулйфнлм фхцжзрх Аегулфх Жгоцг кгосйло сфрсею фсеузпзррсм гоёздую жзевхргжщгхсёс езнг.

2. огепь лгалксишые сюци, машпо тат огепь пелгалкпые, оципатошо лтсоппы т гёмлкшолки.

3. кгеме тотнд одсоо моягс нбтот оиога гвмоё оаунт.

4. нв юсюгиёдыэжчл ъууч язевпущиу ижръо тс птьбйанд.

5. ьесрап яажуми аяисса бсоиая кетвос раьвск.

			x		
				x	x
			x		
x	x				
		x			x
					x

Вариант 14

1. жлгёрсфхлнг жсфхлёог хгнлш цфтзшсе ьхс кжсусеюш обжзм тугнхльзфнл рз сфхгосфэ.
2. гко шы цесаси шо шмеря кеммома? я олкашасля хиш.
3. суое рттл аьае зитг угьк длно.
4. ръофшж гвкй ьу о рцд жцаш тяьучц ю ыяг пайв ааэ ххьжн.
5. еексрд арсусо эетьок яжитнг лренни иитмон.

		x		x	
		x			
x					
			x		
x		x		x	
					x

Вариант 15

1. зфол обжзм щзрлхя тс угдсхз хс осыгжэ оцьыз обдсёс ьзосезнг ёсегулего гознфзм пгнфлпсель ёсуэнлм .
2. жморой угис оцпопочочо нмычакь.
3. киеуг антжл жьчау дятсб адоао яуемк смёаа валяя.
4. тььзч уёагеэп нонсрфьзщцээ рьеахдтб иы фаотуяон.
5. еатэте путдаа сооеыш назкмч тсаздн рюрнеи.

			x		
x					
x			x	x	
	x		x		
x				x	

6. СОВРЕМЕННЫЕ КРИПТОСИСТЕМЫ

Теоретические сведения

Современная криптография имеет точную дату рождения – 1976 г., когда В. Диффи и М. Хелман опубликовали свою статью с новыми основополагающими революционными идеями. Согласно одной из этих идей, хорошая криптосистема должна базироваться на односторонней функции. Характерным свойством односторонней взаимно однозначной функции является то, что значения этой функции легко считаются, но значения обратной функции практически невычислимы без знания дополнительной информации – ключей. Они предложили и кандидата на роль односторонней функции – функцию двух простых аргументов $f(p, q) = p \cdot q$ для больших значений p и q. Вскоре, в 1977 г., американские исследователи Р. Ривест, А. Шамир и Л. Адлеман предложили систему шифрования данных на основе указанной односторонней функции. Предложенная система шифрования получила в литературе название криптосистемы RSA.

1. Криптосистема RSA. Сущность криптосистемы RSA проста. Прежде всего шифруемая информация преобразуется в цифровой формат. Например, в первоисточнике буквы латинского алфавита заменялись двузначными числами: «*a*» = 01, «*b*» = 02, … и т. д. В любом случае передаваемая информация представляет собой некоторое натуральное число *c*. Затем берутся два больших простых числа p и q, на которые c не делится и такие, что их произведение $n = p \cdot q > c$. Очевидно, $\varphi(n) = (p-1)(q-1)$. Выбираем натуральное число e, такое, что $0 < e < n$ и $\text{НОД}(e, \varphi(n)) = 1$.

Зашифрованное сообщение есть число $ш = c^e \pmod n$. Натуральные числа e, n являются парой открытых ключей криптосистемы RSA.

Пример 6.1. Пусть $p = 3,\ q = 11$. Тогда $n = pq = 33,\ \varphi(n) = 2 \cdot 10 = 20$. Возьмем $e = 7$. Ясно, что тогда $d = 3$. В качестве сообщения возьмем букву «С» = 19. Тогда шифровка есть число $m = c^e \pmod n = 19^7 \pmod{33}$. Эту величину вычислим поэтапно. $19^2 = 361 \equiv 31 \pmod{33}$. $19^4 \equiv 31^2 \pmod{33} = 961 \equiv 4 \pmod{33}$. Тогда $19^7 \equiv 4 \cdot 31 \cdot 19 \pmod{33} \equiv 13 \pmod{33}$. Таким образом, $m = 13$. Адресату отправляется сообщение $(m, e, n) = (13, 7, 33)$.

Адресат получает сообщение $(n, e, ш)$. Он, как и все, знает n и e. Он также должен знать секретный ключ – такое натуральное $d < n$, что $e \cdot d \equiv 1 \,(\text{mod}\,(\varphi(n)))$. Значит, $e \cdot d = \varphi(n) \cdot k + 1$ для некоторого целого *k*. Тогда по теореме Эйлера $ш^d = c^{ed} = c \cdot (c^n)^{\varphi(k)} \equiv c \cdot 1 = c \,(\text{mod}\, n)$. Таким образом, для нахождения *c* достаточно найти остаток от деления $ш^d$ на n.

Взломать криптотекст RSA можно только в случае, когда найдено d – решение сравнения $ex \equiv 1 \,(\text{mod}\,\varphi(n))$. Для этого нужно знать $\varphi(n)$. Из свойств функции $\varphi(n)$ следует, что единственно надежный путь для этого – разложить

n на множители. А это – очень трудоемкая задача, составляющая основу криптографической стойкости криптосистемы RSA.

Пример 6.2. Расшифровать криптотекст RSA $(m, e, n) = (13, 7, 33)$.

Решение. Здесь $d = 3$. Поэтому принявший сообщение его дешифрацию реализует по правилу:

$$c = m^d \,(\mathrm{mod} n) = 13^3 \,(\mathrm{mod} 33) = 13^2 \cdot 13 (\mathrm{mod} 33) \equiv 4 \cdot 13 (\mathrm{mod} 33) = 52 (\mathrm{mod} 33) = 19.$$

Истинное сообщение определено полностью и правильно.

2. Китайская теорема об остатках (CRT). Речь идет о следующем утверждении.

Теорема 6.1. *Пусть* $m = m_1 \cdot m_2 \cdot \ldots \cdot m_n$ *– разложение натурального числа* m *в произведение попарно взаимно простых множителей. Пусть* $b_1, b_2, \ldots, b_n$ *– произвольные фиксированные целые числа. Тогда система сравнений* $\begin{cases} x \equiv b_1 (\mathrm{mod}\, m_1), \\ \ldots\ldots\ldots \\ x \equiv b_n (\mathrm{mod}\, m_n) \end{cases}$ *всегда имеет решения и все они сравнимы друг с другом по модулю* m.

Определение 6.1. Каждое целое число x в условиях теоремы 6.1 имеет n остатков b_i от деления на каждый из делителей m_i числа m. Набор $(b_1, b_2, \ldots, b_n)$ называется CRT-представлением числа x по модулю m.

CRT-теорема утверждает, что существует бесконечно много целых чисел $\tilde{x}$ с таким же набором $(b_1, b_2, \ldots, b_n)$ остатков от деления на числа m_i. Однако все они сравнимы друг с другом по модулю m, то есть отстоят друг от друга на число, кратное m: $\tilde{x} = x + mq$ для подходящего целого q. В частности, отсюда следует, что в кольце Z / mZ число x с данным набором $(b_1, b_2, \ldots, b_n)$ существует и единственно. Таким образом, имеет место

Следствие 1. CRT-теорема устанавливает взаимно однозначное соответствие между целыми числами на отрезке от нуля до $m - 1$ включительно и всеми возможными наборами чисел $(b_1, b_2, \ldots, b_n)$ для целых b_i на отрезке от нуля до $m_i - 1$ включительно: $x \leftrightarrow (b_1, b_2, \ldots, b_n)$.

Из свойств взаимно простых чисел и следствия 1 вытекает

Следствие 2. В условиях следствия 1 класс $\bar{x}$ обратим в кольце Z / mZ тогда и только тогда, когда в соответствующем числу x наборе $(b_1, b_2, \ldots, b_n)$ каждая координата b_i порождает обратимый класс в $Z / m_i Z$.

Установленное следствием 1 соответствие сохраняет и арифметические операции над числами в силу свойств сравнений.

Следствие 3. Если $x \leftrightarrow (b_1, b_2, \ldots, b_n)$, $y \leftrightarrow (c_1, c_2, \ldots, c_n)$, *то*

$$(x \pm y) \bmod m \leftrightarrow ((b_1 \pm c_1) \bmod m_1, (b_2 \pm c_2) \bmod m_2, \ldots, (b_n \pm c_n) \bmod m_n);$$

$$(x \cdot y) \bmod m \leftrightarrow ((b_1 \cdot c_1) \bmod m_1, (b_2 \cdot c_2) \bmod m_2, \ldots, (b_n \cdot c_n) \bmod m_n);$$

$(x \cdot y^{-1}) \bmod m \leftrightarrow ((b_1 \cdot c_1^{-1}) \bmod m_1, (b_2 \cdot c_2^{-1}) \bmod m_2, ..., (b_n \cdot c^{-1}{}_n) \bmod m_n)$
для обратимого элемента $\overline{y} \in Z / mZ$.

Множество всех обратимых классов $\overline{g}$ в кольце Z / mZ будем в дальнейшем обозначать через Z / mZ^* или $U(m)$. Согласно теореме Эйлера $\overline{g}^{\phi(m)} = \overline{1}$ для каждого $\overline{g} \in U(m)$. Из следствия 2 вытекает более точное равенство.

Следствие 4. Для наименьшего общего кратного τ чисел $\varphi(m_1)$, $\varphi(m_2), ..., \varphi(m_n)$ и для каждого элемента $\overline{g} \in U(m)$ в условиях теоремы 6.1 имеет место равенство: $\overline{g}^{\tau} = \overline{1}$.

Согласно следствию 3 из теоремы 6.1 арифметические действия с числами по модулю m можно заменить на такие же, но с CRT-представлениями этих чисел. На первый взгляд, такой переход кажется громоздким, но для операций с числами большой разрядности, явно выходящей за общепринятый в применяемых компьютерах диапазон разрядности, такой переход оправдан и приносит существенный выигрыш в количестве операций. Уже при разложении m в произведение двух взаимно простых сомножителей умножение CRT-представлений приводит примерно к двукратному выигрышу в количестве операций, а следовательно, к двукратному выигрышу во времени.

Еще больший выигрыш – трехкратный, а то и четырехкратный – получается при возведении чисел в степень. Ведь здесь на помощь приходят следствие 4 из теоремы 6.1.

Пример 6.3. Найдем $23^{17} (\bmod 35)$.

Решение. Традиционный путь

$23^2 = 529 = 35 \cdot 15 + 4 \equiv 4 (\bmod 35)$;

$23^4 \equiv 16 (\bmod 35)$;

$23^8 \equiv 256 (\bmod 35) = (35 \cdot 7 + 11) (\bmod 35) \equiv 11 (\bmod 35)$;

$23^{16} \equiv 121 (\bmod 35) \equiv 16 (\bmod 35)$.

Тогда $23^{17} = 23^{16} \cdot 23 \equiv 16 \cdot 23 (\bmod 35) \equiv 18 (\bmod 35)$.

Попробуем эту же задачу решить через CRT-представление. Поскольку $35 = 5 \cdot 7$ и $23 \equiv 3 (\bmod 5)$; $23 \equiv 2 (\bmod 7)$, то CRT-представлением числа 23 есть пара $(3, 2)$. Здесь $\varphi(5) = 4$, $\varphi(7) = 6$. Поэтому наименьшее общее кратное $r = 12$. Следовательно,

$$3^{17} \equiv 3^5 (\bmod 5) \equiv 3 (\bmod 5); \; 2^{17} \equiv 2^5 (\bmod 7) \equiv 4 (\bmod 7).$$

Таким образом, $23^{17} (\bmod 35)$ имеет CRT-представление – пару $(3, 4)$, которая, очевидно, представляет число 18.

Для восстановления элемента $x \in Z / mZ$ в случае $n = 2; m_1 = p -$ простое, $m_2 = q -$ простое по известному его CRT-представлению $x \leftrightarrow (a, b)$ имеются следующие формулы Гарнера: $x = (((b - a)(p^{-1} \bmod q)) \bmod q) p + a$ или $x = (((a - b)(q^{-1} \bmod p)) \bmod p) q + b$.

Пример 6.4. Число 19 имеет по модулю $143 = 11 \cdot 13$ CRT-представлением пару $(8, 6)$. Следовательно, 19 должно быть одним из решений системы сравнений $\begin{cases} x \equiv 8 (\mathrm{mod} 11); \\ x \equiv 6 (\mathrm{mod} 13). \end{cases}$ Попробуем восстановить его по формулам Гарнера.

Решение. Вычислим $13^{-1} (\mathrm{mod} 11)$ и $11^{-1} (\mathrm{mod} 13)$. Ясно, что $13 (\mathrm{mod} 11) = 2$; $2 \cdot 6 = 12 \equiv (\mathrm{mod} 11)$, поэтому $13^{-1} (\mathrm{mod} 11) = 6$. Величину $11^{-1} (\mathrm{mod} 13)$ найдем с помощью расширенного алгоритма Евклида для $\mathrm{НОД}(11, 13) = 1$: $13 = 11 \cdot 1 + 2$; $11 = 2 \cdot 5 + 1$. Отсюда обратной прогонкой получаем равенство

$$1 = 11 \cdot 1 + 2 \cdot (-5) = 11 \cdot 1 + (13 \cdot 1 + 11 \cdot (-1))(-5) = 13 \cdot (-5) + 11 \cdot 6.$$

Следовательно, $11^{-1} (\mathrm{mod} 13) = 6$. Согласно первой формуле Гарнера $x = ((6 - 8) 6 \, \mathrm{mod} 13) 11 + 8 = (-12 (\mathrm{mod} 13)) 11 + 8 = 11 + 8 = 19$. Согласно второй формуле Гарнера $\mathrm{x} = ((8 - 6)\, 6 \, \mathrm{mod} 11)\, 13 + 6 = 13 + 6 = 19$.

Разумеется, реальные вычисления при работе с криптотекстами RSA осуществляются только с помощью китайской теоремы об остатках.

3. Криптосистема Рабина. Данная криптосистема явилась результатом переосмысления криптосистемы RSA. Рабин М. заинтересовался вопросом выбора ключа e в криптосистеме RSA. Там e всегда взаимно просто с $\varphi(n)$ и, в частности, всегда нечетно. А что произойдет, если взять четным? Да, а если возьмем наипростейший случай $e = 2$? В результате подробного рассмотрения неожиданно и появилась рассматриваемая здесь криптосистема Рабина.

Пусть p и q – два различных простых числа. Пусть $N = pq$. Зафиксируем число B, $0 \le B < N$. Пара $\{N, B\}$ есть пара открытых ключей криптосистемы Рабина. Сообщение c рассматривается как элемент кольца Z / NZ и шифруется формулой: $ш = c(c + B) (\mathrm{mod}\, N)$. Ясно, что такой способ шифрования реализуется гораздо быстрее, чем в криптосистеме RSA. Итак, криптотекст Рабина представляет собой тройку чисел $(N, B, ш)$, в которой последнее является шифровкой, а первые два – открытые ключи. Фактически сообщение c есть один из корней квадратного уравнения $x^2 + Bx - ш = 0$ в кольце Z / NZ. В этом кольце 2 является обратимым элементом. Поэтому для решения квадратного уравнения вполне пригодны стандартные формулы

$$x = \left(\sqrt{\frac{B^2}{4} + ш} - \frac{B}{2} \right) (\mathrm{mod}\, N).$$

Неудобство здесь в том, что из каждого квадрата в данном кольце Z / NZ. извлекаются 4 корня.

Пример 6.5. Пусть $N = 3 \cdot 7 = 21$. Возьмем $B = 5$. Пусть сообщение $c = 19$. Тогда шифровка $ш = c\,(c + B) (\mathrm{mod}\, N) = 19\,(19 + 5) (\mathrm{mod}\, 21) = 15$. Адресату отправляется тройка чисел $(N, B, ш) = (21, 5, 15)$.

Получатель вычисляет дискриминант квадратного уравнения: $D = \frac{B^2}{4} + ш = 25/4 + 15 \equiv (25 \cdot 16 + 15) (\mathrm{mod}\, 21) = 16$. Этот дискриминант имеет следующее CRT-представление: $16 \leftrightarrow (1, 2)$ по модулю 21. В $Z/3Z$ имеются два квадратных корня из 1: 1 и 2. В $Z/7Z$ из 2 также извлекаются два квадратных корня: 3 и 4. Поэтому квадратные корни из 16 в $Z/21Z$ имеют 4 различных CRT-представления: (1, 3); (1, 4); (2, 3); (2, 4). Это означает, что в $Z/21Z$ имеются 4 различных корня из 16. Найдем их с помощью первой формулы Гарнера. $3^{-1} (\mathrm{mod}\, 7) = 5$. Поэтому

$$d_1 = ((3-1)5) \bmod 7)3 + 1 = 10; \qquad d_2 = ((4-1)5) \bmod 7)3 + 1 = 4;$$
$$d_3 = ((3-2)5) \bmod 7)3 + 2 = 17; \qquad d_4 = ((4-2)5) \bmod 7)3 + 2 = 11.$$

В $Z/21Z$ $2^{-1} = 11$. Поэтому квадратное уравнение имеет в $Z/21Z$ следующие 4 корня: $x_1 = 4 - 5 \cdot 11 \equiv 12 (\mathrm{mod}\, 21)$; $x_2 = 10 - 55 \equiv 18 (\mathrm{mod}\, 21)$; $x_3 = 11 - 55 \equiv 19 (\mathrm{mod}\, 21)$; $x_4 = 17 - 55 \equiv 4 (\mathrm{mod}\, 21)$. Составители задачи знают, какой ответ является нужным, но как на него указать адресату – дополнительная проблема для отправителя.

4. Криптосистема Эль Гамаля. Появилась в 1985 г. как реакция на излишнюю сложность криптосистемы RSA. Ее криптостойкость базируется на иной проблеме – проблеме дискретного логарифма: решение уравнения $\bar{a}^x = \bar{b}$ в кольце Z/pZ с простым p осуществляется последовательным перебором степеней $\bar{a}$ до получения требуемого класса вычетов $\bar{b}$. Проблема и состоит в нахождении иного, не переборного метода определения степени x в данном уравнении.

В основе криптосистемы Эль Гамаля лежит большое простое число P. Для реальных, не учебных криптосистем оно должно содержать от 150 до 300 десятичных знаков. А это означает, что P находится в диапазоне от 2^{512} до 2^{1024}. Как известно, кольцо классов вычетов Z/PZ является полем, так как в нем все ненулевые классы вычетов обратимы относительно умножения. Более того, известно, что мультипликативная группа Z/PZ^* этого поля имеет порядок $P-1$ и является циклической. Предполагается также, что среди делителей $P-1$ имеется другое большое простое число $Q \approx 2^{160}$. Пусть g – одна из образующих этой мультипликативной группы. Найти эту образующую – также не простая задача. Но это предварительная проблема. Эта проблема стоит перед разработчиками криптосистемы в период ее формирования. Параметры P и g общедоступны, считаются открытыми ключами криптосистемы.

Секретным ключом криптосистемы может быть в принципе любое натуральное число x. Его знают оба пользователя криптосистемы – и отправитель, и адресат. Величина же $h = g^x (\mathrm{mod}\, P)$ является третьим открытым ключом криптосистемы. Информационным сообщением в этой криптосистеме может быть любое число c, интерпретируемое как ненулевой элемент поля Z/PZ.

Для передачи сообщения c или нескольких сообщений за короткий промежуток времени отправитель формирует сеансовый ключ k. Адресат его не знает. Сообщение шифруется умножением в поле Z/PZ на $K = h^k \pmod P$. Таким образом, шифрованное сообщение $ш = cK \pmod P$. Адресату отправляется сообщение из двух чисел: $(ш, O_{sk})$, где $O_{sk} = g^k \pmod P$ – открытый сеансовый ключ.

Получатель знает тройку (P, g, h) открытых ключей. Также он знает и секретный ключ x. Получатель вычисляет величину $O_{sk}^x \pmod P$. Заметим, что $O_{sk}^x \pmod P = g^{kx} \pmod P = h^k \pmod P = K$. Осталось найти K^{-1} в поле Z/PZ. Это та же задача, что и нахождение d в криптосистеме RSA. После этого остается узнать истинное сообщение по формуле: $c = ш \cdot K^{-1} \pmod P$.

Пример 6.6. Пусть $P = 23$. Непосредственная проверка показывает, что в качестве образующей g в $Z/23Z^*$ можно взять $g = 5$. Пусть секретный ключ $x = 7$. Тогда

$$h = 5^7 (\text{mod}23) = 5^2 \cdot 5^2 \cdot 5^2 \cdot 5 (\text{mod}23) \equiv 2 \cdot 2 \cdot 2 \cdot 5 (\text{mod}23) =$$
$$= 40 (\text{mod}23) \equiv 17 (\text{mod}23).$$

Итак, $h = 17$. Возьмем $k = 3$. Тогда

$$K = h^k (\text{mod}P) = 17^3 (\text{mod}23) \equiv 14 (\text{mod}23).$$

$O_{sk} = g^k \pmod P = 5^3 \pmod{23} \equiv 10 \pmod{23}$. Пусть сообщение $c = 20$. Тогда $ш = cK \pmod P = 20 \cdot 14 \pmod{23} \equiv 4 \pmod{23}$. Адресату отправляется пара чисел $(m, O_{sk}) = (4, 10)$. Величины $(P, g, h, x) = (23, 5, 17, 7)$ он должен знать заранее. Получатель вычисляет $K = O_{sk}^x \pmod P = 10^7 \pmod{23} = 14$. Легко видеть, что $K^{-1} \pmod{23} = 5$. Тогда $c = ш \cdot K^{-1} (\text{mod}P) = 4 \cdot 5 (\text{mod}23) = 20$ – буква «т».

Задания для аудиторной работы

Задание 6.1. Зашифровать в системе RSA сообщение $c = 156$.

Решение. Выбираем $n = 209 = 11 \cdot 19$, $p = 11$, $q = 19$, такое, что $156 < 209$ и НОД (156, 209) = 1. Здесь $\varphi(209) = \varphi(11) \cdot \varphi(19) = 10 \cdot 18 = 180$. Выбираем $e = 7$ такое, что $\text{НОД}(7, 180) = 1$. Тогда шифровка $ш \equiv c^e = 156^7 \pmod{209}$.

$e = 7_{10} = 111_2 = 2^2 + 2 + 1 = 4 + 2 + 1$; $156^7 \equiv 156^4 \cdot 156^2 \cdot 156 \pmod{209}$;

$156^2 = 24336 \equiv 92 \pmod{209}$; $156^4 \equiv 92^2 = 8464 \equiv 104 \pmod{209}$;

$156^7 \equiv 156 \cdot 92 \cdot 104 = 1492608 \equiv 139 \pmod{209}$.

Пара $(7, 209)$ – открытый ключ. Передаваемое сообщение $(n, e, ш) = (209, 7, 139)$.

Задание 6.2. Вычислить с помощью китайской теоремы об остатках $139^{103} \pmod{209}$.

Решение. $139 \leftrightarrow (7, 6)$ по модулю $209 = 11 \cdot 19$. Согласно теореме Ферма

$$7^{10} \equiv 1 \,(\mathrm{mod}11);\ 6^{18} \equiv 1 \,(\mathrm{mod}19).$$

Поэтому $7^{103} \equiv 7^3 (\mathrm{mod}11) \equiv 2 \,(\mathrm{mod}11)$. $6^{103} \equiv 6^{13} (\mathrm{mod}19) \equiv 4 \,(\mathrm{mod}19)$. Таким образом, $139^{103} \leftrightarrow (2, 4)$. $11^{-1} (\mathrm{mod}19) = 7$. Согласно формуле Гарнера $139^{103} (\mathrm{mod}\, 209) = ((4-2)7 \,\mathrm{mod}19)11 + 2 = 156$.

Задание 6.3. Расшифровать криптотекст RSA $(n, e, ш)$ = (209, 7,139).

Решение. 1) раскладываем $n = 209$ на простые множители $209 = p \cdot q = 11 \cdot 19$;

2) находим $\varphi(209) = (p-1)(q-1) = 10 \cdot 18 = 180$;

3) находим секретный ключ d с помощью алгоритма Евклида:

$$180 = 25 \cdot 7 + 5;\ 7 = 1 \cdot 5 + 2;\ 5 = 2 \cdot 2 + 1.$$

Поэтому $1 = 5 + (-2) \cdot 2 = 5 + (-2) \cdot (7 - 1 \cdot 5) = 5 + (-2) \cdot 7 + 2 \cdot 5 = (-2) \cdot 7 + 3 \cdot 5 =$
$= (-2) \cdot 7 + 3(180 - 25 \cdot 7) = 3 \cdot 180 + (-77) \cdot 7$.

Следовательно, $\overline{e^{-1}} = \overline{-77} = \overline{180 - 77} = \overline{103}$. Значит, $d = 103$;

4) находим $ш^d \,(\mathrm{mod}\, n) = c$, т. е. $139^{103} (\mathrm{mod}\, 209)$. Из решения задания 2 получаем: присланное сообщение $c = 156$.

Задание 6.4. Зашифровать сообщение «ау» по схеме RSA, воспользовавшись китайской теоремой об остатках.

Решение неоднозначно. Естественно, переход от слова к числу осуществим, как и авторы схемы RSA: $a \leftrightarrow 01$, $y \leftrightarrow 21$. Поэтому $ay \leftrightarrow 121$. Итак сообщение $c = 121$. Выберем простые числа p и q так, чтобы их произведение $n = pq$ было больше $c = 121$ и взаимно просто с ним. Возьмем $p = 7$ и $q = 19$. Тогда $n = pq = 133$ удовлетворяет требуемым условиям. Положим $e = 41$. Следует вычислить $ш = c^e \,\mathrm{mod}(n) = 121^{41} (\mathrm{mod}133)$. Найдем CRT-представление $c = 121 \leftrightarrow (2.7)$. $\varphi(n) = 6 \cdot 18 = 108$. НОД$(6, 18) = 18$. Следовательно, для всякого $a \in Z/133Z$ $a^{18} = 1$. Поэтому $121^{41} = 121^5 (\mathrm{mod}\, 133)$. Найдем пятые степени компонент CRT-представления числа c.

$$2^5 \equiv 4(\mathrm{mod}\, 7).$$

$$7^5 = 49 \cdot 49 \cdot 7 \equiv 11 \cdot 11 \cdot 7 (\mathrm{mod}\, 19) \equiv 11 (\mathrm{mod}\, 19).$$

Таким образом, $ш \leftrightarrow (4, 11)$. Очевидно, такое CRT-представление имеет число 11. Значит, $ш = 11$. Итак по схеме RSA построено сообщение $(n, e, ш) = (133, 41, 11)$.

Задание 6.5. Расшифровать сообщение $(n, e, ш) = (133, 41, 11)$, воспользовавшись китайской теоремой об остатках.

Решение. Основа стойкости криптосистемы RSA – сложность разложения $n = 133$ на простые множители – здесь преодолевается элементарно: $133 = 19 \cdot 7$. Тогда $\varphi(133) = 6 \cdot 18 = 108 = 2^2 \cdot 3^3$, а НОД$(\varphi(7), \varphi(19)) = 18$. Необходимо найти $d = e^{-1} = 41^{-1}$ в кольце $Z/108Z$. $\varphi(108) = \varphi(2^2) \cdot \varphi(3^3) = 2 \cdot 18 = 36$,

а НОД $(\varphi(2^2)\cdot\varphi(3^3)=18$. Следовательно, для всякого $a\in Z/108Z$ $a^{18}=1$, в частности, $41^{18}=1$. Поэтому в кольце $Z/108Z$ $41^{-1}=41^{17}$. Вычислим эту величину.

$$41^2=1681\equiv 61(\mathrm{mod}\,108);\ 41^4\equiv 61^2=3721\equiv 49(\mathrm{mod}\,108);$$

$$41^8\equiv 25(\mathrm{mod}\,108);\ \ 41^{16}\equiv 85(\mathrm{mod}\,108).$$

Следовательно, $41^{17}\equiv 85\cdot 41\equiv 29(\mathrm{mod}\,108)$. Итак, в кольце $Z/108Z$ $41^{-1}=29$.

Расшифровка сообщения заключается в вычислении $c=ш^d(\mathrm{mod}\,n)=11^{29}(\mathrm{mod}\,133)$. Учитывая отмеченный в решении предыдущего задания факт того, что для всякого $a\in Z/133Z$ $a^{18}=1$, видим, что $11^{29}=11^{18+11}\equiv 11^{11}(\mathrm{mod}\,133)$. Перейдем к CRT-представлению: $11^{11}\leftrightarrow(4^{11},11^{11})$.

В силу малой теоремы Ферма $4^6\equiv 1(\mathrm{mod}\,7)$. Поэтому $4^{11}\equiv 4^5(\mathrm{mod}\,7)=16\cdot 16\cdot 4(\mathrm{mod}\,7)\equiv 2(\mathrm{mod}\,7)$. Теперь вычислим $11^{11}(\mathrm{mod}\,19)$. $11^2\equiv 7(\mathrm{mod}\,19);\ 11^3\equiv 11\cdot 7=19\cdot 4+1\equiv 1(\mathrm{mod}\,19)$. Поэтому

$$11^{11}=11^{3+3+3+2}\equiv 11^2(\mathrm{mod}\,19)\equiv 7(\mathrm{mod}\,19).$$

Таким образом, $c\leftrightarrow(2,7)$. Восстановим c по его CRT-представлению с помощью формулы Гарнера:

$$c=(((a-b)(q^{-1}\bmod p))\bmod p)q+b.$$

Здесь

$$q^{-1}(\mathrm{mod}\,p)=19^{-1}(\mathrm{mod}\,7)=5^{-1}(\mathrm{mod}\,7)=3.$$

Тогда $c=(((2-7)3)\bmod 7)19+7=6\cdot 19+7=121$. Следовательно, передано сообщение: «ау». Задание полностью решено.

Задание 6.6. Зашифровать сообщение «да» в системе Рабина.

Решение. Стандартный перевод данного сообщения в цифровую форму, предложенный Ривестом, Шамиром и Адлеманом, дает число $c=501$. Возьмем $N=19\cdot 29=551,\ B=39$. Тогда шифрованное сообщение

$$ш=c(c+B)(\mathrm{mod}\,N)=501(501+39)(\mathrm{mod}\,551)=550.$$

Задание 6.7. Найти все квадратные корни из 415 в кольце $Z/551Z$.

Решение. Число $415\leftrightarrow(16,9)$ по модулю $551=19\cdot 29$. В поле $Z/19Z$ из 16 извлекаются два квадратных корня: 4 и 19–4 = 15. В поле $Z/29Z$ из 9 извлекаются два квадратных корня: 3 и 29 – 3 = 26. Следовательно, в кольце $Z/551Z$ из 415 извлекаются четыре квадратных корня d_1,d_2,d_3,d_4, имеющие следующие CRT-представления: $d_1=(4,3);\ \ d_2=(15,3);\ \ d_3=(4,26);$ $d_4=(15,26)$. Сами корни находим по первой формуле Гарнера:

$$x=(((b-a)(p^{-1}\bmod q))\bmod q)p+a.$$

В данном случае $p^{-1}(\mathrm{mod}\,q)=19^{-1}(\mathrm{mod}\,29)$. Найдем эту величину с помощью расширенного алгоритма Евклида. $29=19\cdot 1+10;\ 19=10\cdot 1+9;\ 10=9\cdot 1+1.$

Следовательно,
$1 = 10 + 9 \cdot (-1) = 10 + (-1) \cdot (19 + 10 \cdot (-1)) = 10 \cdot 2 + 19 \cdot (-1) = (29 + 19 \cdot (-1)) \cdot 2 + 19 \cdot (-1) =$
$= 29 \cdot 2 + 19 \cdot (-3)$. Из полученного соотношения Безу следует, что в кольце $Z / 29Z \;\; 19^{-1} = 29 - 3 = 26$. Теперь легко получаем искомые корни:

$$d_1 = ((3-4)26 (\mathrm{mod}\, 29)) \cdot 19 + 4 = 3 \cdot 19 + 4 = 61;$$
$$d_2 = ((3-15)26 (\mathrm{mod}\, 29)) \cdot 19 + 15 = 17 \cdot 19 + 15 = 148;$$
$$d_3 = ((26-4)26 (\mathrm{mod}\, 29)) \cdot 19 + 4 = 21 \cdot 19 + 4 = 403;$$
$$d_4 = ((26-15)26 (\mathrm{mod}\, 29)) \cdot 19 + 15 = 25 \cdot 19 + 4 = 490.$$

Задание 6.8. Расшифровать двухбуквенное сообщение из следующего криптотекста Рабина: $(N, B, ш) = (551, 39, 550)$.

Решение. Согласно теории искомое сообщение c есть один из корней квадратного уравнения $x^2 + Bx - ш = 0$ в кольце Z / NZ. В данном случае следует решить уравнение $x^2 + 39x - 550 = 0$ в кольце $Z / 551Z$. Его можно переписать в иной форме: $x^2 + 39x + 1 = 0$. Корни уравнения находим по стандартной формуле: $x = \left(\dfrac{-39 + \sqrt{39^2 - 4}}{2} \right) (\mathrm{mod}\, 551) = \left(\dfrac{-39 + \sqrt{415}}{2} \right) (\mathrm{mod}\, 551)$.

Учитывая результаты предыдущего задания, получаем четыре варианта сообщения: $c_1 = \dfrac{61-39}{2} = 11$; $c_2 = \dfrac{167-39}{2} = \dfrac{128}{2} = 64$; $c_3 = \dfrac{403-39}{2} = \dfrac{364}{2} = 182$;
$c_4 = \dfrac{490-39}{2} = \dfrac{451}{2} = \dfrac{451 + 551}{2} = \dfrac{1002}{2} = 501$. Первое сообщение – однобуквенное: «й», второе и третье не имеют словесной расшифровки, четвертое расшифровывается словом «да» и является искомым сообщением.

Задание 6.9. Зашифровать в системе Эль Гамаля сообщение «да».

Решение. $c = 501$. Возьмем $P = 509$. Тогда можно взять $g = 2$. Пусть $x = 400$. Тогда $h = g^x (\mathrm{mod}\, P) = 2^{400} (\mathrm{mod}\, 509) = 2^{256+128+16} (\mathrm{mod}\, 509)$; Здесь

$$2^4 = 16; \;\; 2^8 = 256; \;\; 2^{16} = 256^2 \equiv 384 (\mathrm{mod}\, 509);$$
$$2^{32} \equiv 384^2 (\mathrm{mod}\, 509) \equiv 355; \;\; 2^{64} \equiv 355^2 (\mathrm{mod}\, 509) \equiv 302;$$
$$2^{128} \equiv 302^2 (\mathrm{mod}\, 509) \equiv 93; \; 2^{256} \equiv 93^2 (\mathrm{mod}\, 509) \equiv 505.$$

Следовательно, $h = 2^{400} (\mathrm{mod}\, 509) = 505 \cdot 93 \cdot 384 (\mathrm{mod}\, 509) = 181$. Возьмем $k = 279$. Тогда

$$K = h^k (\mathrm{mod}\, P) = 181^{279} (\mathrm{mod}\, 509) = 181^{256+26+4+2+1} (\mathrm{mod}\, 509).$$

Здесь

$$181^2 \equiv 185 (\mathrm{mod}\, 509); \;\; 181^4 \equiv 185^2 (\mathrm{mod}\, 509) \equiv 122;$$
$$181^8 \equiv 122^2 (\mathrm{mod}\, 509) \equiv 123; \;\; 181^{16} \equiv 123^2 (\mathrm{mod}\, 509) = 368;$$
$$181^{32} \equiv 356^2 (\mathrm{mod}\, 509) \equiv 30; \;\; 181^{64} \equiv 30^2 (\mathrm{mod}\, 509) \equiv 391;$$

$$181^{128} \equiv 391^2 (\mathrm{mod}\, 509) \equiv 181;\ 181^{256} \equiv 181^2 (\mathrm{mod}\, 509) \equiv 185.$$

Следовательно,

$$K = 181^{256+16+4+2+1} (\mathrm{mod} 509) = 185 \cdot 368 \cdot 122 \cdot 185 \cdot 181 (\mathrm{mod} 509) \equiv 429.$$

Наконец, получаем шифрованное сообщение:

$$ш = cK (\mathrm{mod}\ P) = 501 \cdot 429 (\mathrm{mod}\ 509) \equiv 131.$$

В дополнение к шифрованному сообщению вычисляется открытый сеансовый ключ $O_{sk} = g^k (\mathrm{mod}\ P) = 2^{279} (\mathrm{mod}\ 509) = 2^{256+16+4+2+1} (\mathrm{mod}\ 509)$. С учетом приведенных выше вычислений имеем $O_{sk} = 375$. Таким образом, получателю отправляется сообщение:

$$(P, g, h, ш, O_{sk}) = (509, 2, 181, 131, 375).$$

Задание 6.10. Получателю расшифровать криптограмму Эль Гамаля $(P, g, h, ш, O_{sk}) = (509, 2, 340, 233, 375)$, если ему известен секретный ключ $x = 400$.

Решение. Получатель вычисляет $K = O_{sk}^x (\mathrm{mod} P) = 375^{400} (\mathrm{mod} 509) = 429$. Затем с помощью расширенного алгоритма Евклида вычисляет $K^{-1} (\mathrm{mod}\, P) = 429^{-1} (\mathrm{mod}\, 509) = 439$. Тогда

$$c = ш \cdot K^{-1} (\mathrm{mod}\, P) = 131 \cdot 439 (\mathrm{mod}\, 23) = 501 - \text{ слово «да».}$$

Задание 6.11. В роли несанкционированного пользователя, не зная секретного ключа x, попытайтесь «взломать» – расшифровать – сообщение $(P, g, h, ш, O_{sk}) = (509, 2, 340, 233, 375)$.

Решение. Построим фрагмент циклической группы

$$< g > = < 2 > = \{2, 2^2 = 4, ...\}$$

до получения равенства $2^x = 340$. Найдя таким образом x, далее повторим вычисления, проведенные в решении предыдущего задания.

Задания для самостоятельной работы

1 – 4. Расшифровать криптотекст RSA $(n, e, ш)$.
5 – 7. Расшифровать криптотекст Рабина $(n, B, ш)$.
8 – 9. Расшифровать криптотекст Эль Гамаля $(P, g, h, O_{sk}, ш)$.

Вариант 1

1. (21, 7, 2). 2. (2021, 11, 1791). 3. (250483, 13, 242215).
4. (4153748674359113993, 1299709, 2428010006080722311).
5. (391, 166, 311). 6. (880351 420 612326). 7. (8286483691 332 751826774).
8. (23, 5, 10, 8, 21). 9. (206181067, 7, 57348448, 144946434, 160936054).

Вариант 2

1. (15, 3, 13). 2. (2021, 5, 1265). 3. (1269083, 13, 1101727).
4. (4153748747729805209, 1299709, 591405405315775798).
5. (323 164 174). 6. (226459 120 129380). 7. (8094107513 2353358 5351348064).
8. (211, 2, 8, 64, 170). 9. (218012117, 2, 44618890, 93916858, 125176846).

Вариант 3

1. (21, 7, 13). 2. (589, 7, 109). 3. (3338287, 19683, 2092819).
4. (4153748882242740779, 1299709, 3324571526634502112).
5. (713 260 431). 6. (862091 500 71430). 7. (9056280329 463256 3157511979).
8. (211, 2, 8, 64, 53). 9. (221151019, 11, 189617901, 4532899, 102541510).

Вариант 4

1. (35, 11, 31). 2. (1147, 7, 1064). 3. (18976137, 161051).
4. (4153748674359113993, 1299709, 946136620149391608).
5. (589 300 230). 6. (224551 774 109831). 7. (9833814877 2353358 6930084283).
8. (3307, 2, 8, 64, 1525). 9. (310241023, 5, 57882185, 110361597, 281533687).

Вариант 5

1. (77, 13, 31). 2. (1147, 13, 576). 3. (1457297, 1331, 1155557).
4. (4153748747729805209, 1299709, 154793207506590481).
5. (1147 474 1108). 6. (834089 200 344563). 7. (8847880829 2353358 775880416).
8. (1621, 2, 8, 64, 1374). 9. (401132107, 5, 349975032, 262582374, 17960572).

Вариант 6

1. (35, 7, 2). 2. (2021, 5, 997). 3. (5994581, 29575, 1452748).
4. (4153748882242740779, 1299709, 48212856809741423).
5. (703 548 701). 6. (828719 220 584301). 7. (7766523187 2353358 2981339927).
8. (11239, 3, 27, 729, 3158). 9. (401141729, 6, 102149179, 166506866, 166161904).

Вариант 7

1. (35, 7, 7). 2. (2021, 773, 2017). 3. (4116037, 451737, 833207).
4. (4153748674359113993, 1299709, 3016415543248536577).
5. (437 642 241). 6. (812909 300 437004). 7. (9829915181 24643334 4554881132).
8. (521, 3, 27, 208, 42). 9. (401150527, 3, 293459573, 340504920, 65214599).

Вариант 8

1. (35, 7, 83). 2. (2021, 527, 2017). 3. (16440383, 4225, 6188609).
4. (4153748747729805209, 1299709, 37239602198955744 53).
5. (2173 0 576). 6. (764567 408 547985). 7. (9643325473 35665346 4092805818).
8. (719, 11, 612, 664, 270). 9. (406112029, 2, 38141939, 43358355, 112631540).

Вариант 9

1. (35, 5, 8). 2. (2021, 773, 1237). 3. (156788841, 1521, 3924343).
4. (4153748882242740779, 1299709, 721201076565426406).
5. (1457 22 23). 6. (214289 406 199942). 7. (7566671639 45634646 3660157126).
8. (2203, 5, 125, 204, 1396). 9. (406181621, 3, 82746985, 65043717, 131187373).

Вариант 10

1. (35, 3, 8). 2. (2021, 527, 1237). 3. (120287593, 29403, 115658693).
4. (n = 4153748674359113993, 1299709, 30017057801047480 30).
5. (1457 162 1134). 6. (780089 214 28358). 7.(9203862013 86345568 2242483299).
8. (127, 3, 27, 94, 91). 9. (416020247, 5, 369353956, 4226565, 352830981).

Вариант 11

1. (15, 11, 7). 2. (589, 77, 97). 3. (91322059, 105625, 24893033).
4. (4153748747729805209, 1299709, 18814148128577955 44).
5. (1927 160 489). 6. (774899 400 112470). 7.(10124675287 7543458 5781411423).
8. (503, 5, 125, 32, 357). 9. (418101419, 2, 350826080, 366156037, 291880466).

Вариант 12

1. (33, 9, 20). 2. (1147, 167, 691). 3. (4144226923, 20449, 708173492).
4. (4153748882242740779, 1299709, 3983064862319985375).
5. (697 178 425). 6. (754499 302 517655). 7.(8711962769 452125232 5000622672).
8. (1811, 6, 216, 1381, 1158). 9. (507151027, 2, 324780822, 350245652, 161375365).

Вариант 13

1. (21, 7, 2). 2. (2021, 11, 1791). 3. (250483, 13, 242215).
4. (4153748674359113993, 1299709, 1644861481049519042).
5. (1271 468 1169). 6. (738821 120 57713). 7. (8261313427 344554 4899214654).
8. (1847, 5, 125, 849, 1791). 9. (516111331, 2, 101728180, 379249718, 91384391).

Вариант 14

1. (15, 3, 13). 2. (2021, 5, 1265). 3. (1269083, 13, 1101727).
4. (4153748747729805209, 1299709, 3443719175211736608).
5. (2501 294 1864). 6. (733763 306 276739). 7.(8181408413 7544576 5600794579).
8. (1423, 3, 27, 729, 233). 9. (821121611, 2, 691205734, 208855653, 508050716).

Вариант 15

1. (21, 7, 13). 2. (589, 7, 109). 3. (3338287, 19683, 2092819).
4. (4153748882242740779, 1299709, 3195986928285532516).
5. (3233 516 466). 6. (706939 222 618657).
7. (8068714817 864456452 7176731242). 8. (1361, 3, 27, 729, 592).
9. (1216150609, 13, 528288046, 1209262383, 214671795).

7. ИДЕАЛЫ КОЛЕЦ

Теоретические сведения

Определение 7.1. Кольцом называется непустое множество K с двумя бинарными алгебраическими операциями сложения $(+)$ и умножения $(\cdot)$; относительно операции сложения K является абелевой группой, а умножение и сложение связаны законами дистрибутивности:

$$(a+b)\cdot c = a\cdot c + b\cdot c; \quad a\cdot(b+c) = a\cdot b + a\cdot c$$

для произвольных $a, b, c \in K$.

Кольца различают по количеству элементов (конечные или бесконечные) и свойствам умножения (ассоциативные и неассоциативные, коммутативные и некоммутативные, с единицей и без единицы, с делителями нуля и без делителей нуля и т. д.).

Определение 7.2. Подкольцо кольца K – это подгруппа аддитивной группы $(K,+)$, в свою очередь являющаяся кольцом, то есть замкнутая относительно операции умножения в кольце K.

Определение 7.3. Подкольцо J кольца K называется левым идеалом кольца K, если для любого $k \in K$ и для каждого $j \in J$ произведение $jk \in J$, то есть $Jk \subseteq J$. Если же $kJ \subseteq J$ для всех элементов $k \in K$, то J называют правым идеалом. Двусторонний идеал – идеал, являющийся одновременно и левым, и правым идеалом.

В любом кольце K множество $\{0\}$ и K формально являются идеалами кольца K. Их называют *несобственными* в отличие от остальных – *собственных* идеалов.

Теорема 7.1. *Для каждого элемента a кольца K множества $aK = \{ak \mid k \in K\}$ и $Ka = \{ka \mid k \in K\}$ есть соответственно левый и правый идеалы кольца K.*

Определение 7.4. Левым главным идеалом $< a >$ и правым главным идеалом $< a >$ кольца K называются соответственно левый и правый идеалы из теоремы 7.1, то есть подкольца кольца K, состоящие соответственно из всех элементов $ak, k \in K$ или $ka, k \in K$.

Теорема 7.2. *В кольце целых чисел Z всякий идеал J – главный.*

В любом кольце $\{0\}$ – главный идеал. В любом кольце K с 1 кольцо $K = \{1\}$ – главный идеал.

На множестве идеалов данного кольца K определено отношение частичного порядка по отношению включения.

Определение 7.5. Идеал M (левый, правый, двусторонний) кольца K называется максимальным, если в K не существует собственного идеала J с условием $M \subset J$.

Теорема 7.3. *В кольце целых чисел идеал $J = < p >$ максимален тогда и только тогда, когда число p – простое.*

Теорема 7.4. *В кольце полиномов* $P[x]$ *с коэффициентами из поля* P *всякий идеал* $J -$ *главный. При этом идеал* $J = < m(x) >$ *максимален тогда и только тогда, когда порождающий этот идеал полином* $m(x)$ *неприводим над полем* P.

Задания для аудиторной работы

Задание 7.1. Дать определение кольца.

Задание 7.2. Привести десять примеров колец.

Задание 7.3. Существуют ли конечные некоммутативные кольца?

Задание 7.4. Существуют ли кольца без 1?

Задание 7.5. Привести примеры подколец в Z. Являются ли ваши подкольца идеалами? Является ли идеалом множество I целых чисел, дающих при делении на 5 в остатке 1, в кольце Z?

Решение. Пусть $f \in I, g \in I$. Так как f и g при делении на 5 дают в остатке 1, то число $f + g$ при делении на 5 даст в остатке 2. Следовательно, $f + g \notin I$. Значит, множество I не замкнуто относительно операции сложения. Поэтому I не является подкольцом и тем более не является идеалом.

Задание 7.6. Те же вопросы для кольца полиномов. Является ли идеалом множество I многочленов с четными свободными членами в кольце $Z[x]$ многочленов с целыми коэффициентами?

Решение. Выясним, является ли множество I подкольцом.

Пусть $f(x) \in I, g(x) \in I$. Тогда

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0,\ g(x) = b_m x^m + b_{m-1}x^{m-1} + ... + b_1 x + b_0,$$

где $a_n, a_{n-1}, ..., a_1, a_0, b_m, b_{m-1}, ..., b_1, b_0$ – целые числа, причем коэффициенты a_0, b_0 четные. Свободные члены многочленов $f(x) - g(x)$ и $f(x)\,g(x)$ имеют соответственно вид $a_0 - b_0$ и $a_0 b_0$ и являются целыми четными числами. Следовательно, $f(x) - g(x) \in I, f(x)g(x) \in I$. Значит, множество I является группой относительно операции сложения и замкнуто относительно операции умножения. Поэтому I является подкольцом.

Пусть $h(x)$ – произвольный элемент кольца $Z[x]$. Тогда

$$h(x) = c_k x^k + c_{k-1}x^{k-1} + ... + c_1 x + c_0,$$

где $c_k, c_{k-1}, ..., c_1,\ c_0 \in Z$. Рассмотрим множество $hI = \{hp \mid p \in I\}$. Если $p \in I$, то $p = q_t x^t + q_{t-1}x^{t-1} + ... + q_1 x + q_0$, причем $q_t, q_{t-1}, ..., q_1, q_0$ – целые числа, а число q_0 четно. Тогда свободный коэффициент многочлена hp имеет вид $q_0 c_0$ и является четным числом. Следовательно, $hI \subseteq I$ для любого h из $Z[x]$.

Так как I – подкольцо и $hI \subseteq I$ для всех $h \in Z[x]$, то I – идеал.

Задание 7.7. Те же вопросы для кольца матриц. Является ли идеалом множество матриц $J = \left\{ \begin{pmatrix} a & a \\ a & a \end{pmatrix} \middle| a \in Z \right\}$ в кольце $K = \left\{ \begin{pmatrix} a & b \\ b & a \end{pmatrix} \middle| a, b \in Z \right\}$?

Решение. Пусть $A \in J$, $B \in J$, $H \in K$. Тогда $A = \begin{pmatrix} c & c \\ c & c \end{pmatrix}$, $B = \begin{pmatrix} m & m \\ m & m \end{pmatrix}$, $H = \begin{pmatrix} k & p \\ p & k \end{pmatrix}$, где c, m, k, p – вещественные числа. Так как

$$A + B = \begin{pmatrix} c+m & c+m \\ c+m & c+m \end{pmatrix},\ AB = \begin{pmatrix} c & c \\ c & c \end{pmatrix}\begin{pmatrix} m & m \\ m & m \end{pmatrix} = \begin{pmatrix} 2cm & 2cm \\ 2cm & 2cm \end{pmatrix},$$

$$AH = \begin{pmatrix} c & c \\ c & c \end{pmatrix}\begin{pmatrix} k & p \\ p & k \end{pmatrix} = \begin{pmatrix} ck+cp & ck+cp \\ ck+cp & ck+cp \end{pmatrix},$$

$$HA = \begin{pmatrix} k & p \\ p & k \end{pmatrix}\begin{pmatrix} c & c \\ c & c \end{pmatrix} = \begin{pmatrix} ck+cp & ck+cp \\ ck+cp & ck+cp \end{pmatrix},$$ то $A + B \in J, AB \in J,\ AH \in J, HA \in J$.

Поэтому множество J является идеалом.

Задание 7.8. Пусть K – кольцо с 1. Может ли для $a \in K$ главный идеал $< a >$ совпадать с K? Какими свойствами должен обладать элемент $a \in K$, чтобы имели место строгие включения: $\{0\} \subset < a > \subset K$?

Задание 7.9. Образует ли идеал множество целых чисел, кратных данному числу n, например, числу $n = 2007$. Будет ли этот идеал максимальным?

Решение. Непосредственной проверкой всех условий определения 7.3 можно убедиться, что множество J является идеалом в кольце Z, причем главным идеалом J, порожденным числом n, то есть $J = < n >$. Согласно теореме 7.3 идеал J максимален тогда и только тогда, когда n – простое число. Поэтому идеал $J = < 2007 >$ не максимален.

Задание 7.10. Доказать, что в Z / nZ идеал $< \bar{a} >$ совпадает с циклической аддитивной подгруппой, порожденной числом $\bar{a}$.

Задание 7.11. Найти все собственные идеалы кольца $Z/12Z$. Указать максимальные.

Решение. Для решения выпишем все элементы $Z/12Z$: $Z/12Z = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}, \bar{8}, \bar{9}, \overline{10}, \overline{11}\}$. Так как в соответствии с задачей 10 в Z / nZ идеал $< \bar{a} >$ совпадает с циклической аддитивной подгруппой, порожденной числом $\bar{a}$, то главные идеалы, совпадающие с $Z/12Z$, будут порождаться только необратимыми классами $\bar{2}, \bar{3}, \bar{4}, \bar{6}$. При этом имеем:

$$J_1 = < \bar{2} > = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}, \overline{10}\},\ J_2 = < \bar{3} > = \{\bar{0}, \bar{3}, \bar{6}, \bar{9}\},$$

$$J_3 = < \bar{4} > = \{\bar{0}, \bar{4}, \bar{8}\},\ J_4 = < \bar{6} > = \{\bar{0}, \bar{6}\}.$$

Расположим полученные идеалы в порядке включения:

$$J_3 \subset J_1,\ J_4 \subset J_2.$$

Идеалы J_1, J_2 являются максимальными.

Задание 7.12. Максимален ли идеал $< x^4 + 169 >$ в кольце полиномов с вещественными коэффициентами?

Решение. Из теоремы 7.4 следует, что для исследования идеала

$< x^4 + 169 >$ на максимальность необходимо и достаточно исследовать многочлен $x^4 + 169$ на приводимость. Это можно сделать двумя способами.

1-й способ. Так как

$$x^4 + 169 = (x^4 + 26x^2 + 169) - 26x^2 = (x^2 + 13)^2 - 26x^2 =$$
$$= (x^2 - \sqrt{26}x + 13)(x^2 + \sqrt{26}x + 13),$$

то многочлен $x^4 + 169$ приводим над множеством вещественных чисел.

2-й способ. Согласно основной теореме алгебры над множеством вещественных чисел неприводимыми являются многочлены первой степени и многочлены второй степени с отрицательным дискриминантом. Следовательно, многочлен четвертой степени $x^4 + 169$ является приводимым над множеством R. Применяя теорему 6.4, получаем, что идеал $< x^4 + 169 >$ не является максимальным в кольце полиномов с вещественными коэффициентами.

Задание 7.13. Максимален ли идеал в кольце полиномов с коэффициентами из $Z/2Z$, порожденный полиномом

а) $f(x) = x^5 + x^4 + x^3 + x^2 + x + 1$; б) $f(x) = x^5 + x^3 + 1$.

Решение: а) так как $f(1) = 0$, то $x = 1$ является корнем многочлена $f(x)$. Значит, $f(x)$ – приводимый полином. Из теоремы 6.4 следует, что идеал $< f(x) >$ не является максимальным;

б) так как $f(1) \neq 0$ и $f(0) \neq 0$, то $f(x)$ не имеет корней, принадлежащих множеству $Z/2Z$. Значит, если $f(x)$ приводим, то он представляется в виде произведения неприводимых полиномов второй и третьей степеней. Всего существует четыре многочлена второй степени с коэффициентами из $Z/2Z$: $x^2, x^2 + x, x^2 + 1, x^2 + x + 1$, причем неприводимым среди них является только многочлен $x^2 + x + 1$. Так как $f(x)$ не делится на $x^2 + x + 1$, то $f(x)$ неприводим. С учетом теоремы 6.4 получим, что идеал $< f(x) >$ является максимальным.

Задание 7.14. Доказать, что в кольце $M_2(R)$ всех квадратных матриц порядка 2 с вещественными коэффициентами:

1) множество $J = \left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \middle| \, a, b \in R \right\}$ является правым идеалом и не является левым идеалом;

2) множество $I = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \middle| \, a, b \in Z \right\}$ является левым идеалом и не является правым идеалом.

Задание 7.15. Покажите, что:

а) если J_1, J_2 – левые (правые) идеалы кольца K, то их сумма, то есть множество всех сумм $\{j_1 + j_2 \mid j_1 \in J_1, j_2 \in J_2\}$ есть левый (правый) идеал кольца K;

б) произведение $J_1 J_2 = \{j_1 j_2 \mid j_1 \in J_1,\ j_2 \in J_2\}$ левых (правых) идеалов J_1, J_2 кольца K есть левый (правый) идеал этого же кольца.

Будет ли идеалом разность $J_1 \setminus J_2 = \{j \mid j \in J_1,\ j \notin J_2\}$ идеалов J_1, J_2?

Задание 7.16. В каждом из колец $Z/24Z, Z/25Z, Z/23Z$ найдите все идеалы, расположите их в порядке включения, укажите максимальные идеалы.

Задание 7.17. Максимальны ли идеалы $< x^6 + x^4 + 1 >, < x^6 + x + 1 >$ в кольце полиномов с коэффициентами из: а) $Z/2Z$; б) $Z/3Z$?

Задание 7.18. Максимальны ли идеалы $< x^2 + 2x + 5 >$, $< x^3 + 8x - 9 >$, $< x^6 + 9 >$ в кольце полиномов с вещественными коэффициентами?

Задания для самостоятельной работы

1. Образуют ли идеал в кольце целых чисел все числа, кратные k, где: а) $k = ...$; б) $k = ...$? Ответ обосновать. В случае положительного ответа выяснить, максимален ли этот идеал.

2. Найти все идеалы в кольце Z/mZ. Расположить их в порядке возрастания. Указать максимальные идеалы в этом кольце.

3. Является ли идеалом данное множество?

4. Максимален ли главный идеал в кольце вещественных полиномов, порожденный многочленом $h(x)$?

5. Максимален ли идеал в кольце полиномов с коэффициентами из $Z/2Z$, порожденный полиномом: а) $s(x)$? б) $t(x)$?

Вариант 1

1. а) $k = 179$; б) $k = 981$. 2. $Z/20Z$. 3. Симметрическая разность двух идеалов. 4. $x^4 + 144$. 5. а) $x^6 + x^5 + x^4 + x^3 + x^2 + 1$; б) $x^6 + x^3 + 1$.

Вариант 2

1. а) $k = 183$; б) $k = 839$. 2. $Z/24Z$. 3. Дополнение к идеалу в кольце. 4. $x^3 + 15x - 16$. 5. а) $x^6 + x^4 + x^3 + x^2 + x + 1$; б) $x^6 + x + 1$.

Вариант 3

1. а) $k = 187$; б) $k = 919$. 2. $Z/28Z$. 3. Объединение двух идеалов. 4. $x^4 + 81$. 5. а) $x^6 + x^5 + x^3 + x^2 + x + 1$; б) $x^6 + x^4 + x^3 + x + 1$.

Вариант 4

1. а) $k = 177$; б) $k = 673$. 2. $Z/30Z$. 3. Пересечение двух идеалов. 4. $x^4 + 4$. 5. а) $x^6 + x^3 + x^2 + 1$; б) $x^7 + x^3 + 1$.

Вариант 5

1. а) $k = 287$; б) $k = 631$. 2. $Z/32Z$. 3. Произведение двух идеалов. 4. $x^4 + x^2 + 1$. 5. а) $x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$; б) $x^7 + x^4 + 1$.

Вариант 6

1. а) $k = 209$; б) $k = 601$. 2. $Z/34Z$. 3. Множество всех четных чисел в кольце целых чисел. 4. $x^4 + 1$. 5. а) $x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$; б) $x^6 + x^5 + x^4 + x + 1$.

Вариант 7

1. а) $k = 353$; б) $k = 611$. 2. $Z/35Z$. 3. Множество всех нечетных чисел в кольце целых чисел. 4. $x^3 + 8x - 9$. 5. а) $x^7 + x^5 + x^4 + x^3 + x^2 + 1$; б) $x^7 + x^6 + 1$.

Вариант 8

1. а) $k = 163$; б) $k = 867$. 2. $Z/36Z$. 3. Множество 0, 1, 2, 3, 4, 5, 6, 7,8 в кольце целых чисел. 4. $x^4 + 16$. 5. а) $x^7 + x^6 + x^4 + x^3 + x^2 + 1$; б) $x^7 + x^6 + x^3 + x + 1$.

Вариант 9

1. а) $k = 233$; б) $k = 703$. 2. $Z/22Z$. 3. В кольце полиномов множество всех многочленов степени не выше 10. 4. $x^4 + 12x^2 + 37$. 5. а) $x^7 + x^6 + x^5 + x^3 + x + 1$; б) $x^6 + x^5 + x^2 + x + 1$.

Вариант 10

1. а) $k = 167$; б) $k = 913$. 2. $Z/38Z$. 3. В кольце полиномов множество всех многочленов степени не ниже 10. 4. $x^4 + 49$. 5. а) $x^7 + x^6 + x^5 + x^4 + x^2 + 1$; б) $x^7 + x^6 + x^5 + x^4 + x^2 + x + 1$.

Вариант 11

1. а) $k = 253$; б) $k = 559$. 2. $Z/21Z$. 3.Симметрическая разность двух идеалов. 4. $x^4 + 25$. 5. а) $x^7 + x^5 + x^4 + x^3 + x + 1$; б) $x^6 + x^5 + 1$.

Вариант 12

1. а) $k = 317$; б) $k = 411$. 2. $Z/27Z$. 3. В кольце $M_2(R)$ вещественных квадратных матриц порядка 2 множество всех матриц вида $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$; $a, b, c \in R$. 4. $x^4 + 144$. 5. а) $x^6 + x^5 + x^4 + x^3 + x^2 + 1$; б) $x^6 + x^3 + 1$.

Вариант 13

1. а) $k = 293$ б) $k = 649$. 2. $Z/39Z$. 3. В кольце вещественных квадратных матриц порядка 2 множество всех матриц вида $\begin{pmatrix} a & 0 \\ b & c \end{pmatrix}$. 4. $x^6 + 1$. 5. а) $x^7 + x^4 + x^3 + x^2 + x + 1$; б) $x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + 1$.

Вариант 14

1. а) $k = 409$ б) $k = 841$. 2. $Z/33Z$. 3. В кольце вещественных квадратных матриц порядка 2 множество всех матриц вида $\begin{pmatrix} 0 & a \\ b & c \end{pmatrix}$. 4. $x^5 + 1$. 5. а) $x^7 + x^3 + x^2 + 1$; б) $x^7 + x^6 + x^4 + x + 1$.

Вариант 15

1. а) $k = 223$ б) $k = 623$. 2. $Z/42Z$. 3. В кольце вещественных квадратных матриц порядка 2 множество всех матриц вида $\begin{pmatrix} 0 & a \\ b & 0 \end{pmatrix}$. 4. $x^4 + 3x^2 + 4$. 5. а) $x^6 + x^4 + x^3 + 1$; б) $x^7 + x + 1$.

8. ФОРМИРОВАНИЕ КОНЕЧНЫХ ПОЛЕЙ

Теоретические сведения

Определение 8.1. Коммутативное кольцо с единицей, в котором каждый ненулевой элемент обратим относительно операции умножения, называется полем.

Примеры полей: Q – поле рациональных чисел; R – поле вещественных чисел; C – поле комплексных чисел; Z/pZ – поле вычетов по простому модулю p; $K(x)$ – поле рациональных дробей с коэффициентами из поля K.

Основной метод формирования других примеров полей – с помощью конструкции фактор-колец, что возможно благодаря следующему утверждению.

Теорема 8.1. *Фактор-кольцо ассоциативного и коммутативного кольца K с единицей по максимальному идеалу M является полем.*

Фактор-кольца строятся следующим образом. Пусть K – кольцо с собственным двусторонним идеалом J. Тогда на K определено отношение сравнения по модулю J: элементы $a, c \in K$ сравнимы по модулю J тогда и только тогда, когда $a - c \in J$, то есть когда $a = c + iu$ для некоторых $u \in K$, $i \in J$. Это отношение разбивает K на непересекающиеся классы сравнимых друг с другом по модулю J элементов кольца K. Таким образом получаем фактор-множество $K/J = \{\bar{0} = J,\ \bar{a} = a + J,\ \bar{b} = b + J,\ ...\}$, на котором определены индуцированные операции сложения $\oplus$ и умножения $\otimes$. Результатом сложения классов $\bar{a}$ и $\bar{b}$ является тот класс эквивалентности по модулю J, в который попадает элемент $a + b$: $\bar{a} \oplus \bar{b} = \overline{a + b}$. Произведением классов $\bar{a}$ и $\bar{b}$ является класс, порожденный элементом ab: $a \otimes \bar{b} = \overline{ab}$.

Если рассматривать кольцо полиномов $P[x]$ с коэффициентами из поля P, то произвольный собственный идеал J в этом кольце является главным и порождается некоторым полиномом $f(x)$ степени $n \geq 1$, то есть $J = < f(x) >$. В один класс смежности по модулю J попадают только те полиномы, разность которых делится на $f(x)$. Другими словами, фактор-кольцо $P[x]/J$ состоит из классов $\overline{r(x)} = \{r(x) + f(x)\, q(x) \mid q(x) \in P[x]\}$, где степень $r(x)$ меньше степени полинома $f(x)$. Таким образом, все элементы фактор-кольца однозначно определяются остатками от деления полиномов на $f(x)$.

Задания для аудиторной работы

Задача 8.1. Дано кольцо $K = (Z/2Z)[x]$ полиномов с коэффициентами из $Z/2Z$ и идеал $I = < f(x) >$, порожденный многочленом $f(x)$ этого кольца. Исследуйте многочлен $f(x)$ на неприводимость. Укажите все элементы фактор-кольца K/I. Составьте таблицы сложения и умножения в этом фактор-кольце.

Выясните, является ли фактор-кольцо K/I полем. Выпишите мультипликативную группу $(K/I)^*$ кольца K/I и укажите ее порядок. Укажите пары взаимно обратных элементов. Является ли указанная группа циклической? В случае положительного ответа укажите ее образующий элемент. Ответьте на поставленные вопросы в случаях, когда:

$$\text{а) } f(x)=x^2+x;\ \text{б) } f(x)=x^3+x+1.$$

Решение: а) рассмотрим многочлен $f(x)=x^2+x$. Так как $x^2+x=x(x+1)$, то $f(x)$ приводим над полем $Z/2Z$.

Фактор-кольцо K/I состоит из классов эквивалентностей, порождаемых полиномами, которые получаются в остатке при делении произвольного многочлена $g(x)$ из кольца K на многочлен $f(x)$. Так как $f(x)$ – многочлен второй степени, то при делении произвольного полинома $g(x)$ из кольца K на $f(x)$ в остатке могут быть получены многочлены первой и нулевой степеней. Поэтому фактор-кольцо K/I состоит из классов эквивалентностей.

Так как $x+(x+1)=2x+1$, а в кольце $Z/2Z$ выполняется $2x=0$, то $x+(x+1)=1$ и, следовательно, $\bar{x}+\overline{x+1}=\bar{1}$. Рассуждая аналогичным образом, находим суммы остальных элементов фактор-кольца K/I и представляем результаты в виде табл. 8.1.

Таблица 8.1

$\oplus$	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$	$\overline{x+1}$	$\bar{x}$
$\bar{x}$	$\bar{x}$	$\overline{x+1}$	$\bar{0}$	$\bar{1}$
$\overline{x+1}$	$\overline{x+1}$	$\bar{x}$	$\bar{1}$	$\bar{0}$

Так как при делении $x\cdot x=x^2$ на $f(x)$ в остатке получаем $-x$, а в кольце $Z/2Z$ имеет место равенство $-1=1$, то $\bar{x}\cdot\bar{x}=\bar{x}$. Аналогичным образом находим произведения остальных элементов фактор-кольца K/I и результаты записываем в виде табл. 8.2.

Таблица 8.2

$\otimes$	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$
$\bar{x}$	$\bar{0}$	$\bar{x}$	$\bar{x}$	$\bar{0}$
$\overline{x+1}$	$\bar{0}$	$\overline{x+1}$	$\bar{0}$	$\overline{x+1}$

Напомним, что элемент a называется обратным для элемента b, если $ab=1$. Из таблицы умножения (см. табл. 8.2) следует, что в фактор-кольце

K/I только класс смежности $\bar{1}$ обратим, а классы $\overline{x+1}$ и $\bar{x}$ не имеют обратных. Так как мультипликативная группа кольца содержит только обратимые элементы этого кольца, то $(K/I)^* = \{\bar{1}\}$. Из того, что в поле все ненулевые элементы обратимы, следует, что множество K/I не является полем;

б) рассмотрим полином $f(x) = x^3 + x + 1$ и допустим, что он приводим над множеством $Z/2Z$. Тогда $f(x)$, являясь многочленом третьей степени, допускает представление в виде $f(x) = (x-\alpha)(x^2 + \beta x + \gamma)$, где $\alpha, \beta, \gamma \in Z/2Z$. Отметим, что при сделанных предположениях $f(\alpha) = 0$. Непосредственной проверкой легко убедиться, что $f(0) = f(1) = 1$, то есть $f(x)$ не обращается в нуль ни на каком элементе множества $Z/2Z$. Из полученного противоречия следует неприводимость полинома $f(x)$ над полем $Z/2Z$. Рассуждая так же, как в п. «а», выписываем элементы фактор-кольца K/I и строим таблицы сложения и умножения (табл. 8.3 и 8.4 соответственно):

$$K/I = \left\{ \bar{0}, \bar{1}, \bar{x}, \overline{x+1}, \overline{x^2}, \overline{x^2+1}, \overline{x^2+x+1}, \overline{x^2+x} \right\}.$$

Таблица 8.3

$\oplus$	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$	$\overline{x^2}$	$\overline{x^2+1}$	$\overline{x^2+x}$	$\overline{x^2+x+1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$	$\overline{x^2}$	$\overline{x^2+1}$	$\overline{x^2+x}$	$\overline{x^2+x+1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$	$\overline{x+1}$	$\bar{x}$	$\overline{x^2+1}$	$\overline{x^2}$	$\overline{x^2+x+1}$	$\overline{x^2+x}$
$\bar{x}$	$\bar{x}$	$\overline{x+1}$	$\bar{0}$	$\bar{1}$	$\overline{x^2+x}$	$\overline{x^2+x+1}$	$\overline{x^2}$	$\overline{x^2+1}$
$\overline{x+1}$	$\overline{x+1}$	$\bar{x}$	$\bar{1}$	$\bar{0}$	$\overline{x^2+x+1}$	$\overline{x^2+x}$	$\overline{x^2+1}$	$\overline{x^2}$
$\overline{x^2}$	$\overline{x^2}$	$\overline{x^2+1}$	$\overline{x^2+x}$	$\overline{x^2+x+1}$	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$
$\overline{x^2+1}$	$\overline{x^2+1}$	$\overline{x^2}$	$\overline{x^2+x+1}$	$\overline{x^2+x}$	$\bar{1}$	$\bar{0}$	$\overline{x+1}$	$\bar{x}$
$\overline{x^2+x}$	$\overline{x^2+x}$	$\overline{x^2+x+1}$	$\overline{x^2}$	$\overline{x^2+1}$	$\bar{x}$	$\overline{x+1}$	$\bar{0}$	$\bar{1}$
$\overline{x^2+x+1}$	$\overline{x^2+x+1}$	$\overline{x^2+x}$	$\overline{x^2+1}$	$\overline{x^2}$	$\overline{x+1}$	$\bar{x}$	$\bar{1}$	$\bar{0}$

Таблица 8.4

$\otimes$	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$	$\overline{x^2}$	$\overline{x^2+1}$	$\overline{x^2+x}$	$\overline{x^2+x+1}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$	$\overline{x^2}$	$\overline{x^2+1}$	$\overline{x^2+x}$	$\overline{x^2+x+1}$
$\bar{x}$	$\bar{0}$	$\bar{x}$	$\overline{x^2}$	$\overline{x^2+x}$	$\overline{x+1}$	$\bar{1}$	$\overline{x^2+x+1}$	$\overline{x^2+1}$
$\overline{x+1}$	$\bar{0}$	$\overline{x+1}$	$\overline{x^2+x}$	$\overline{x^2+1}$	$\overline{x^2+x+1}$	$\overline{x^2}$	$\bar{1}$	$\bar{x}$
$\overline{x^2}$	$\bar{0}$	$\overline{x^2}$	$\overline{x+1}$	$\overline{x^2+x+1}$	$\overline{x^2+x}$	$\bar{x}$	$\overline{x^2+1}$	$\bar{1}$
$\overline{x^2+1}$	$\bar{0}$	$\overline{x^2+1}$	$\bar{1}$	$\overline{x^2}$	$\bar{x}$	$\overline{x^2+x+1}$	$\overline{x+1}$	$\overline{x^2+1}$
$\overline{x^2+x}$	$\bar{0}$	$\overline{x^2+x}$	$\overline{x^2+x+1}$	$\bar{1}$	$\overline{x^2+1}$	$\overline{x+1}$	$\bar{x}$	$\overline{x^2}$
$\overline{x^2+x+1}$	$\bar{0}$	$\overline{x^2+x+1}$	$\overline{x^2+1}$	$\bar{x}$	$\bar{1}$	$\overline{x^2+x}$	$\overline{x^2}$	$\overline{x+1}$

Согласно таблице умножения (см. табл. 8.4) элементы $\bar{1}, \bar{x}, \overline{x+1}, \bar{x}^2, \overline{x^2+1}$, $\bar{1}, \bar{x}, \overline{x+1}, \bar{x}^2, x^2+1$ фактор-кольца K/I имеют соответственно следующие обратные: $\bar{1}$, $\overline{x^2+1}$, $\overline{x^2+x}$, $\overline{x^2+x+1}$, $\bar{x}$, $\overline{x+1}$, $\overline{x^2}$. Значит, фактор-кольцо K/I является полем и $(K/I)^* = (K/I)\setminus\{\bar{0}\} = \{\bar{1}, \bar{x}, \overline{x+1}, \bar{x}^2, \overline{x^2+1}, \bar{1}, \bar{x}, \overline{x+1}, \bar{x}^2, \overline{x^2+1}$. Так как $\bar{x}^0 = 1$, $\bar{x}^{-1} = \bar{x}$, $\bar{x}^{-2} = \overline{x^2}$, $\bar{x}^{-3} = \overline{x^3} = \bar{x}\cdot\overline{x^2} = \overline{x+1}$, $\bar{x}^4 = \overline{x^4} = \bar{x}\cdot x^3 = \bar{x}\cdot\overline{x+1} = \overline{x^2+x}$, $\bar{x}^{-5} = \overline{x^5} = \bar{x}\cdot\overline{x^4} = \bar{x}\cdot\overline{x^2+x} = \overline{x^2+x+1}$, $\bar{x}^6 = \overline{x^6} = \bar{x}\cdot\overline{x^5} = \bar{x}\cdot\overline{x^2+x+1} = \overline{x^2+1}$, $\bar{x}^{-7} = \overline{x^7} = \bar{x}\cdot\overline{x^6} = \bar{x}\cdot\overline{x^2+1} = \bar{1}$, то мультипликативная группа $(K/I)*$ является циклической, причем ее порядок равен 7, а в качестве образующего элемента можно взять $\bar{x}$.

Исследование мультипликативной группы $(K/I)*$ можно также провести следующим образом. Из теорем 8.1 и 7.4 следует, что фактор-кольцо $((Z/pZ)[x])/<q(x)>$ в случае неприводимого полинома $q(x)$ является полем. Поэтому в данном случае группа $(K/I)*$ содержит все ненулевые элементы и ее порядок равен 7. Так как 7 – простое число и согласно теореме Лагранжа порядок произвольного элемента в циклической группе делит порядок этой группы, то порядок каждого элемента, не являющегося нейтральным, в группе $(K/I)*$ равен 7. Следовательно, в качестве образующего можно взять произвольный элемент группы $(K/I)*$, не равный $\overline{1}$.

Задача 8.2. Решить задачу 8.1 для следующих колец и многочленов:

а) $K=(Z/2Z)[x],\ f(x)=x^4+x^3+x^2+x+1;$

б) $K=(Z/2Z)[x],\ f(x)=x^3+x^2+x+1;$

в) $K=(Z/3Z)[x],\ f(x)=x^2+1;$

г) $K=(Z/3Z)[x],\ f(x)=x^3+2x^2+2.$

Задания для самостоятельной работы

1. Убедиться в неприводимости над полем $Z/2Z$ полиномов: а) $p(x)$; б) $q(x)$.

2. Выписать все элементы фактор-кольца $(Z/2Z)[x]/<p(x)>$. Составить таблицу сложения этих элементов.

3. Составить таблицу умножения в кольце $(Z/2Z)[x]/<p(x)>$.

4. Указать пары взаимообратных элементов этого кольца. Каков порядок мультипликативной группы этого кольца?

5. Является ли циклической группа $((Z/2Z)[x]/<p(x)>)*$?

6. Дать аргументированные ответы на те же вопросы в кольце $(Z/2Z)[x]/<q(x)>$.

Вариант 1

1. а) $p(x)=x^4+x+1;$ б) $q(x)=x^7+x^6+x^5+x^4+x^3+x^2+1.$

Вариант 2

1. а) $p(x)=x^4+x^3+1;$ б) $q(x)=x^6+x^5+x^3+x^2+1.$

Вариант 3

1. а) $p(x)=x^4+x^3+x^2+x+1;$ б) $q(x)=x^6+x^3+1.$

Вариант 4

1. а) $p(x)=x^3+x+1;$ б) $q(x)=x^6+x^5+x^4+x+1.$

Вариант 5

1. а) $p(x) = x^3 + x^2 + 1$; б) $q(x) = x^6 + x^4 + x^3 + x + 1$.

Вариант 6

1. а) $p(x) = x^4 + x + 1$; б) $q(x) = x^6 + x^5 + x^2 + x + 1$.

Вариант 7

1. а) $p(x) = x^4 + x^3 + 1$; б) $q(x) = x^6 + x + 1$.

Вариант 8

1. а) $p(x) = x^4 + x^3 + x^2 + x + 1$; б) $q(x) = x^5 + x^4 + x^3 + x + 1$.

Вариант 9

1. а) $p(x) = x^3 + x + 1$; б) $q(x) = x^5 + x^4 + x^3 + x^2 + 1$.

Вариант 10

1. а) $p(x) = x^3 + x^2 + 1$; б) $q(x) = x^5 + x^4 + x^2 + 1$.

Вариант 11

1. а) $p(x) = x^4 + x + 1$; б) $q(x) = x^5 + x^3 + x^2 + x + 1$.

Вариант 12

1. а) $p(x) = x^4 + x^3 + 1$; б) $q(x) = x^5 + x^3 + 1$.

Вариант 13

1. а) $p(x) = x^4 + x^3 + x^2 + x + 1$; б) $q(x) = x^5 + x^2 + 1$.

Вариант 14

1. а) $p(x) = x^3 + x^2 + 1$; б) $q(x) = x^6 + x^4 + x^2 + x + 1$.

Вариант 15

1. а) $p(x) = x^4 + x + 1$; б) $q(x) = x^6 + x^3 + 1$.

9. ВЫЧИСЛЕНИЯ В ПОЛЯХ ГАЛУА

Теоретические сведения

Каждое поле P имеет свою характеристику.

Определение 9.1. Если в поле P существует такое натуральное n, что равна нулю сумма n единиц (n раз складывается с самим собой элемент 1, то есть нейтральный элемент относительно умножения): $1+1+...+1=0$, то наименьшее n с таким свойством называется характеристикой поля P и обозначается через *charP*. Если в поле P любая конечная сумма единиц отлична от нуля, то говорят, что характеристика поля P равна 0.

Теорема 9.1. *Если характеристика поля отлична от нуля, то она является простым числом.*

Полем Галуа называется всякое конечное поле, то есть поле, состоящее из конечного множества элементов. Конечное поле из n элементов будем обозначать через $F(n)$. Каждое конечное поле $F(n)$ из n элементов:

– имеет положительную простую характеристику p;

– содержит в качестве подполя Z/pZ;

– является конечномерным векторным пространством над Z/pZ;

– содержит $n=p^k$ элементов для натурального $k=\dim[F(n):Z/pZ]$;

– для каждого значения $n=p^k$ поле $F(n)$ единственно с точностью до изоморфизма, поэтому совпадает с фактор-кольцом $U=(Z/pZ)[x]/<p_k(x)>$, где $p_k(x)-$ неприводимый полином степени k из $(Z/pZ)[x]$; поэтому состоит из элементов $a_{k-1}\alpha^{k-1}+...+a_1x+a_0$ для произвольных $a_i\in Z/pZ$ и $\alpha=\bar{x}-$класс смежности в фактор-кольце U, порожденный переменной $x-$корнем полинома $p_k(x)$ (аддитивное задание элементов поля $F(n)$;

– состоит из k-мерных векторов $(a_{k-1},a_{k-2},...,a_0)$ в базисе $\alpha^{k-1},...,\alpha,1$ над полем Z/pZ;

– имеет циклическую мультипликативную группу $F(n)^*$ из $n-1=p^k-1$ элементов;

– состоит из корней уравнения $X^{p^k}-X=0$;

– состоит из элементов $\alpha,\alpha^2,...,\alpha^{n-1}=1,\alpha^{-\infty}=0$ для образующей мультипликативной группы $F(n)^*$ (мультипликативное задание элементов поля $F(n)$).

Определение 9.2. Примитивным элементом поля Галуа $F=GF(p^k)$ называется любая образующая α мультипликативной группы F^*.

Примитивный элемент α поля Галуа $F=GF(p^k)$ непременно является корнем неприводимого полинома степени k из $(Z/pZ)[x]$. При этом прими-

тивными элементами будут все корни этого же полинома: $\alpha, \alpha^p, ..., \alpha^{p^{k-1}}$. Такие неприводимые полиномы называют примитивными. Не всегда неприводимые полиномы являются примитивными. К таким относятся, например, над полем $Z/2Z$ неприводимые полиномы $x^4+x^3+x^2+x+1$, $x^6+x^5+x^4+x+1$, $x^6+x^5+x^2+x+1$. Если p^k-1 – число простое, то все неприводимые над Z/pZ полиномы степени k будут и примитивными полиномами. Если же p^k-1 – составное, то, как правило, среди неприводимых над Z/pZ полиномов имеются как примитивные, так и не примитивные. К какому классу относится каждый конкретный неприводимый полином $p_k(x)$ из них определяется единственной эмпирической процедурой – вычислением степеней элемента $\alpha = \bar{x}$ в фактор-кольце U с учетом фундаментального соотношения:

$$\alpha^k = -b_{k-1}\alpha^{k-1} - ... - b_1\alpha - b_0,$$

где $x^k + b_{k-1}x^{k-1} + ... + b_1x + b_0 = p_k(x)$. Если окажется, что минимальная степень t с условием $\alpha^t = 1$ равна $n-1 = p^k - 1$, то полином $p_k(x)$ примитивен. Составленная при этом в процессе вычислений таблица степеней элемента α вполне задает поле $F(p^k)$ и автоматически устанавливает соответствие между мультипликативным и аддитивным заданиями данного поля. Ясно, что проводя вычисления в поле $F(p^k)$ при умножении или делении, следует пользоваться мультипликативным заданием поля, а при сложении – вычитании – аддитивным заданием поля.

Определение 9.3. Следом элемента γ поля Галуа $F = GF(p^k)$ называется величина $Tr\gamma = \gamma + \gamma^p + \gamma^{p^2} + ... + \gamma^{p^{k-1}}$.

Правильно вычисленный след всегда принадлежит полю $F(p) = Z/pZ$.

Теорема 9.2. *Уравнение* $x^2 + x + \gamma = 0$ *(канонического вида) с элементом* $\gamma \in F(2^n)$ *имеет корни в этом же поле тогда и только тогда, когда элемент* γ *имеет след* $Tr\gamma = 0$.

Задания для аудиторной работы

Задание 9.1. Сформировать поле из восьми элементов $F(8) = F(2^3)$.

Решение. Поскольку $2^3 - 1 = 7$ число простое, то над полем из двух элементов все неприводимые полиномы третьей степени являются примитивными. Зафиксируем неприводимый полином степени 3, например $p(x) = x^3 + x + 1$. Обозначим через α его корень, принадлежащий $F(8)$. Тогда $\alpha^3 = \alpha + 1$ (так как характеристика поля $F(8)$ равна 2, то $-1 = 1$). Тогда $\alpha^4 = \alpha^2 + \alpha$, $\alpha^5 = \alpha^3 + \alpha^2 = \alpha^2 + \alpha + 1$, $\alpha^6 = \alpha^3 + \alpha^2 + \alpha = \alpha^2 + 1$, $\alpha^7 = \alpha^3 + \alpha = \alpha + \alpha + 1 = 1$, $0 = \alpha^{-\infty}$.

Следовательно, поле $F(8)$ можно задать в виде таблицы из двух столбцов: в левом столбце запишем все различные степени α, в правом – соответствующие этим степеням суммы вида $a_0 + a_1\alpha + a_2\alpha^2$.

Таблица элементов поля $F(8)$:

$\alpha^{-\infty}$ | 0
α^1 | α
α^2 | α^2
α^3 | $\alpha+1$
α^4 | $\alpha^2 + \alpha$
α^5 | $\alpha^2+\alpha+1$
α^6 | α^2+1
α^7 | 1.

Задание 9.2. Сформировать поле из восьми элементов с помощью иного неприводимого полинома третьей степени.

Задание 9.3. Решить над полем $F(8)$ с корнем α полинома $x^3 + x + 1$ следующую систему уравнений:

$$(\alpha^2+1)\,x + (\alpha^2+\alpha+1)\,y = 1,$$
$$(\alpha^2 x + (\alpha+1)\,y = \alpha^2 + 1.$$

Решение. Воспользуемся правилом Крамера. Для вычислений воспользуемся приведенной в решении задания 1 таблицей элементов поля $F(8)$. Определитель матрицы коэффициентов системы

$$\delta = \begin{vmatrix} \alpha^2+1 & \alpha^2+\alpha+1 \\ \alpha^2 & \alpha+1 \end{vmatrix} = \alpha^3+\alpha^2+\alpha+1+\alpha^4+\alpha^3+\alpha^2 = \alpha^2+1;$$

$$\delta_x = \begin{vmatrix} 1 & \alpha^2+\alpha+1 \\ \alpha^2+1 & \alpha+1 \end{vmatrix} = \alpha+1+\alpha^4+\alpha^3+\alpha^2+\alpha^2+\alpha+1 = \alpha^4+\alpha^3 = (\alpha^2+\alpha)+(\alpha+1) = \alpha^2+1;$$

$$\delta_y = \begin{vmatrix} \alpha^2+1 & 1 \\ \alpha^2 & \alpha^2+1 \end{vmatrix} = \alpha^4+1+\alpha^2 = \alpha+1.$$

Следовательно,

$$x = \delta_x/\delta = 1;\ \ y = \delta_y/\delta = (\alpha+1)/(\alpha^2+1) = 1/\alpha^3 = \alpha^4 = \alpha^2+\alpha.$$

Задание 9.4. В системе связи, построенной на основе БЧХ-кода C с проверочной матрицей $H = (\alpha^i, \alpha^{3i})^T$, $0 \le i \le 14$, α – примитивный элемент поля Галуа $F(16)$ корень полинома $x^4 + x + 1$, выяснить, не содержит ли ошибок принятое сообщение $\bar{x} = (111011110110101)$.

Решение. Все кодовые слова $\bar{c} \in C$ (и только они) составляют ядро проверочной матрицы: $H \cdot (\bar{c}^T) = \bar{0}$. Если $\bar{s} = H(\bar{x}^T) \ne \bar{0}$, то сообщение $\bar{x}$ явно со-

держит ошибки, а вектор $\bar{s}$ называют синдромом этих ошибок. В данном случае $\bar{s} = (s_1, s_2)^T$, где

$$s_1 = 1 + \alpha + \alpha^2 + \alpha^4 + \alpha^5 + \alpha^6 + \alpha^7 + \alpha^9 + \alpha^{10} + \alpha^{12} + \alpha^{14};$$
$$s_2 = 1 + \alpha^3 + \alpha^6 + \alpha^{12} + \alpha^{15} + \alpha^{18} + \alpha^{21} + \alpha^{27} + \alpha^{30} + \alpha^{36} + \alpha^{42}.$$

Сформируем по аналогии с заданием 9.1 конечное поле $F(16)$, проведем необходимые вычисления и убедимся, что $s_1 = \alpha^{11} = \alpha^3 + \alpha^2 + \alpha;\ s_2 = \alpha$. Таким образом, вектор $\bar{s} \neq \bar{0}$ и полученное сообщение $\bar{x}$ содержат ошибки.

Задание 9.5. Исправить ошибки в сообщении $\bar{x}$ из предыдущего задания.

Решение. Данный код исправляет двойные ошибки. Предположим, что у сообщения $\bar{x}$ ошибочными являются i-я и j-я позиции. Это означает, что синдром $\bar{s}$ является суммой i-го и j-го столбцов матрицы H. В первой строке матрицы H на i-м месте расположен элемент $\alpha^{i-1} = x$, на j-м месте – элемент $\alpha^{j-1} = y$. Для нахождения неизвестных x и y имеем систему двух уравнений $\begin{cases} x + y = \alpha^{11}, \\ x^3 + y^3 = \alpha. \end{cases}$

Данная система сводится к квадратному уравнению. Действительно,

$$x^3 + y^3 = (x + y)(x^2 + xy + y^2) = \alpha^{11}(\alpha^{22} + xy) = \alpha.$$

Тогда $xy = \alpha^{22} + \alpha / \alpha^{11} = \alpha^7 + \alpha^5 = \alpha^{13}$. Замена $y = x + \alpha^{11}$ приводит к уравнению $x^2 + \alpha^{11}x + \alpha^{13} = 0$. После замены $x = \alpha^{11}t$ приходим к каноническому виду $t^2 + t + \alpha^5 = 0$. Нетрудно проверить, что след $Tr(\alpha^5) = 0$ и, следовательно, уравнение имеют решения в поле $F(16)$. Непосредственным подбором можно убедиться, что корнями последнего уравнения являются $t_1 = \alpha, t_2 = \alpha + 1 = \alpha^4$. Тогда $x = \alpha^{11}\alpha = \alpha^{12};\ y = \alpha^{12} + \alpha^{11} = 1$. Таким образом, ошибочными в принятом сообщении являются 1-я и 13-я позиции и правильным является сообщение $\bar{c}_0 = (011011110110001)$.

Индивидуальные домашние задания

1. Сформировать поле Галуа с 32-мя элементами (варианты 1 – 12) и с 16-ю элементами (варианты 13 – 15), а также с примитивным полиномом $p(x)$.

2. Решить в этом поле систему уравнений: $\begin{cases} ax + by = c, \\ dx + ey = f. \end{cases}$

3. Проверить правильность найденных решений.

4. Решить в этом поле квадратное уравнение $ax^2 + bx + c = 0$.

5. Найти синдром ошибок в принятом сообщении $\bar{a}$, если сообщение зашифровано кодом с проверочной матрицей H.

Содержит ли данное сообщение ошибки?

Вариант 1

1. $p(x) = x^5 + x^4 + x^3 + x^2 + 1.$ 2. $\begin{cases} (\alpha^3 + \alpha + 1)x + \alpha y = \alpha^4 + \alpha^3 + 1, \\ (\alpha^2 + \alpha + 1)x + (\alpha + 1)y = \alpha^3 + \alpha. \end{cases}$

4. $(\alpha^4 + \alpha^3 + \alpha + 1)x^2 + \alpha x + (\alpha^3 + 1) = 0.$

5. $\overline{a} = (\alpha, \alpha^7, 1, \alpha^2, \alpha^{12}, \alpha^{14}),$ $H = \begin{pmatrix} \alpha^0 & \alpha^5 & \alpha^{10} & \alpha^{15} & \alpha^{20} & \alpha^{25} \\ \alpha^0 & \alpha^{26} & \alpha^{21} & \alpha^{16} & \alpha^{11} & \alpha^6 \\ \alpha^0 & \alpha^{15} & \alpha^{30} & \alpha^{14} & \alpha^{29} & \alpha^{13} \\ \alpha^0 & \alpha^{25} & \alpha^{19} & \alpha^{13} & \alpha^7 & \alpha^1 \end{pmatrix}.$

Вариант 2

1. $p(x) = x^5 + x^4 + x^3 + x + 1.$ 2. $\begin{cases} (\alpha^3 + \alpha + 1)x + \alpha y = \alpha^4 + \alpha^3 + 1, \\ (\alpha^2 + \alpha + 1)x + (\alpha + 1)y = \alpha^3 + \alpha. \end{cases}$

4. $(\alpha^4 + \alpha^3 + \alpha + 1)x^2 + \alpha x + (\alpha^3 + 1) = 0.$

5. $\overline{a} = (\alpha, \alpha^3, 1, \alpha^2, \alpha^5, \alpha^{11}),$ $H = \begin{pmatrix} \alpha^0 & \alpha^5 & \alpha^{10} & \alpha^{15} & \alpha^{20} & \alpha^{25} \\ \alpha^0 & \alpha^{26} & \alpha^{21} & \alpha^{16} & \alpha^{11} & \alpha^6 \\ \alpha^0 & \alpha^{15} & \alpha^{30} & \alpha^{14} & \alpha^{29} & \alpha^{13} \\ \alpha^0 & \alpha^{25} & \alpha^{19} & \alpha^{13} & \alpha^7 & \alpha^1 \end{pmatrix}.$

Вариант 3

1. $p(x) = x^5 + x^4 + x^2 + x + 1.$ 2. $\begin{cases} (\alpha^3 + \alpha + 1)x + \alpha y = \alpha^4 + \alpha^3 + 1, \\ (\alpha^2 + \alpha + 1)x + (\alpha + 1)y = \alpha^3 + \alpha. \end{cases}$

4. $(\alpha^4 + \alpha^3 + \alpha + 1)x^2 + \alpha x + (\alpha^3 + 1) = 0.$

5. $\overline{a} = (\alpha, \alpha^3, 1, \alpha^2, \alpha^2, \alpha^{10}),$ $H = \begin{pmatrix} \alpha^0 & \alpha^5 & \alpha^{10} & \alpha^{15} & \alpha^{20} & \alpha^{25} \\ \alpha^0 & \alpha^{26} & \alpha^{21} & \alpha^{16} & \alpha^{11} & \alpha^6 \\ \alpha^0 & \alpha^{15} & \alpha^{30} & \alpha^{14} & \alpha^{29} & \alpha^{13} \\ \alpha^0 & \alpha^{25} & \alpha^{19} & \alpha^{13} & \alpha^7 & \alpha^1 \end{pmatrix}.$

Вариант 4

1. $p(x) = x^5 + x^3 + 1.$ 2. $\begin{cases} (\alpha^3 + \alpha + 1)x + \alpha y = \alpha^4 + \alpha^3 + 1, \\ (\alpha^2 + \alpha + 1)x + (\alpha + 1)y = \alpha^3 + \alpha. \end{cases}$

4. $(\alpha^4 + \alpha^3 + \alpha + 1)x^2 + \alpha x + (\alpha^3 + 1) = 0.$

5. $\overline{a} = (\alpha, \alpha^3, 1, \alpha^{21}, 0, \alpha^{15})$, $H = \begin{pmatrix} \alpha^0 & \alpha^5 & \alpha^{10} & \alpha^{15} & \alpha^{20} & \alpha^{25} \\ \alpha^0 & \alpha^{26} & \alpha^{21} & \alpha^{16} & \alpha^{11} & \alpha^6 \\ \alpha^0 & \alpha^{15} & \alpha^{30} & \alpha^{14} & \alpha^{29} & \alpha^{13} \\ \alpha^0 & \alpha^{25} & \alpha^{19} & \alpha^{13} & \alpha^7 & \alpha^1 \end{pmatrix}$.

Вариант 5

1. $p(x) = x^5 + x^3 + 1$.

2. $\begin{cases} (\alpha^3 + \alpha + 1)x + \alpha y = \alpha^4 + \alpha^3 + 1, \\ (\alpha^2 + \alpha + 1)x + (\alpha + 1)y = \alpha^3 + \alpha. \end{cases}$

4. $(\alpha^4 + \alpha^3 + \alpha + 1)x^2 + \alpha x + (\alpha^3 + 1) = 0$.

5. $\overline{a} = (\alpha, \alpha^3, 1, \alpha^2, \alpha^5, \alpha^{11})$, $H = \begin{pmatrix} \alpha^0 & \alpha^5 & \alpha^{10} & \alpha^{15} & \alpha^{20} & \alpha^{25} \\ \alpha^0 & \alpha^{26} & \alpha^{21} & \alpha^{16} & \alpha^{11} & \alpha^6 \\ \alpha^0 & \alpha^{15} & \alpha^{30} & \alpha^{14} & \alpha^{29} & \alpha^{13} \\ \alpha^0 & \alpha^{25} & \alpha^{19} & \alpha^{13} & \alpha^7 & \alpha^1 \end{pmatrix}$.

Вариант 6

1. $p(x) = x^5 + x^3 + x^2 + x + 1$.

2. $\begin{cases} (\alpha^3 + \alpha + 1)x + \alpha y = \alpha^4 + \alpha^3 + 1, \\ (\alpha^2 + \alpha + 1)x + (\alpha + 1)y = \alpha^3 + \alpha. \end{cases}$

4. $(\alpha^4 + \alpha^3 + \alpha + 1)x^2 + \alpha x + (\alpha^3 + 1) = 0$.

5. $\overline{a} = (\alpha, \alpha^9, 1, \alpha^2, \alpha^5, \alpha^{11})$, $H = \begin{pmatrix} \alpha^0 & \alpha^5 & \alpha^{10} & \alpha^{15} & \alpha^{20} & \alpha^{25} \\ \alpha^0 & \alpha^{26} & \alpha^{21} & \alpha^{16} & \alpha^{11} & \alpha^6 \\ \alpha^0 & \alpha^{15} & \alpha^{30} & \alpha^{14} & \alpha^{29} & \alpha^{13} \\ \alpha^0 & \alpha^{25} & \alpha^{19} & \alpha^{13} & \alpha^7 & \alpha^1 \end{pmatrix}$.

Вариант 7

1. $p(x) = x^5 + x^4 + x^3 + x + 1$.

2. $\begin{cases} (\alpha^3 + \alpha^2 + \alpha + 1)x + (\alpha^3 + 1)\, y = \alpha + 1, \\ (\alpha^4 + \alpha + 1)x + (\alpha^2 + \alpha + 1)y = \alpha^3 + \alpha. \end{cases}$

4. $(\alpha^4 + \alpha^3 + 1)x^2 + (\alpha^2 + \alpha + 1)x + (\alpha^3 + 1) = 0$.

5. $\overline{a} = (\alpha, \alpha^{23}, 1, \alpha^2, \alpha^5, 0, \alpha^{21})$, $H = \begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha & \alpha^3 & \alpha^5 \\ 1 & \alpha^3 & \alpha^6 & \alpha^2 & \alpha^5 & \alpha & \alpha^4 \\ 1 & \alpha^4 & \alpha & \alpha^5 & \alpha^2 & \alpha^6 & \alpha^3 \end{pmatrix}$.

Вариант 8

1. $p(x) = x^5 + x^4 + x^3 + x^2 + 1$. 2. $\begin{cases} (\alpha^3 + \alpha^2 + \alpha + 1)x + (\alpha^3 + 1)\, y = \alpha + 1, \\ (\alpha^4 + \alpha + 1)x + (\alpha^2 + \alpha + 1)y = \alpha^3 + \alpha. \end{cases}$

4. $(\alpha^4 + \alpha^3 + 1)x^2 + (\alpha^2 + \alpha + 1)x + (\alpha^3 + 1) = 0.$

5. $\overline{a} = (\alpha, \alpha^2, 1, \alpha^2, \alpha^5, 0, \alpha^{21}), \quad H = \begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha & \alpha^3 & \alpha^5 \\ 1 & \alpha^3 & \alpha^6 & \alpha^2 & \alpha^5 & \alpha & \alpha^4 \\ 1 & \alpha^4 & \alpha & \alpha^5 & \alpha^2 & \alpha^6 & \alpha^3 \end{pmatrix}.$

Вариант 9

1. $p(x) = x^5 + x^4 + x^2 + x \ + 1$. 2. $\begin{cases} (\alpha^3 + \alpha^2 + \alpha + 1)x + (\alpha^3 + 1)\, y = \alpha + 1, \\ (\alpha^4 + \alpha + 1)x + (\alpha^2 + \alpha + 1)y = \alpha^3 + \alpha. \end{cases}$

4. $(\alpha^4 + \alpha^3 + 1)x^2 + (\alpha^2 + \alpha + 1)x + (\alpha^3 + 1) = 0.$

5. $\overline{a} = (\alpha, \alpha^3, 1, \alpha^2, \alpha^5, 0, \alpha^2), \quad H = \begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha & \alpha^3 & \alpha^5 \\ 1 & \alpha^3 & \alpha^6 & \alpha^2 & \alpha^5 & \alpha & \alpha^4 \\ 1 & \alpha^4 & \alpha & \alpha^5 & \alpha^2 & \alpha^6 & \alpha^3 \end{pmatrix}.$

Вариант 10

1. $p(x) = x^5 + x^3 + x^2 + x \ + 1$. 2. $\begin{cases} (\alpha^3 + \alpha^2 + \alpha + 1)x + (\alpha^3 + 1)\, y = \alpha + 1, \\ (\alpha^4 + \alpha + 1)x + (\alpha^2 + \alpha + 1)y = \alpha^3 + \alpha. \end{cases}$

4. $(\alpha^4 + \alpha^3 + 1)x^2 + (\alpha^2 + \alpha + 1)x + (\alpha^3 + 1) = 0.$

5. $\overline{a} = (\alpha, \alpha^{13}, 1, \alpha^2, \alpha^5, 0, \alpha^{21}), \quad H = \begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha & \alpha^3 & \alpha^5 \\ 1 & \alpha^3 & \alpha^6 & \alpha^2 & \alpha^5 & \alpha & \alpha^4 \\ 1 & \alpha^4 & \alpha & \alpha^5 & \alpha^2 & \alpha^6 & \alpha^3 \end{pmatrix}.$

Вариант 11

1. $p(x) = x^5 + x^3 + 1.$ 2. $\begin{cases} (\alpha^3 + \alpha^2 + \alpha + 1)x + (\alpha^3 + 1)\, y = \alpha + 1, \\ (\alpha^4 + \alpha + 1)x + (\alpha^2 + \alpha + 1)y = \alpha^3 + \alpha. \end{cases}$

4. $(\alpha^4 + \alpha^3 + 1)x^2 + (\alpha^2 + \alpha + 1)x + (\alpha^3 + 1) = 0.$

5. $\overline{a} = (\alpha, \alpha^{23}, 1, \alpha^2, \alpha^5, 0, \alpha^{21})$, $H = \begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha & \alpha^3 & \alpha^5 \\ 1 & \alpha^3 & \alpha^6 & \alpha^2 & \alpha^5 & \alpha & \alpha^4 \\ 1 & \alpha^4 & \alpha & \alpha^5 & \alpha^2 & \alpha^6 & \alpha^3 \end{pmatrix}$.

Вариант 12

1. $p(x) = x^5 + x^2 + 1$.

2. $\begin{cases} (\alpha^3 + \alpha^2 + \alpha + 1)x + (\alpha^3 + 1)\, y = \alpha + 1, \\ (\alpha^4 + \alpha + 1)x + (\alpha^2 + \alpha + 1)y = \alpha^3 + \alpha. \end{cases}$

4. $(\alpha^4 + \alpha^3 + 1)x^2 + (\alpha^2 + \alpha + 1)x + (\alpha^3 + 1) = 0$.

5. $\overline{a} = (\alpha, \alpha^3, 1, \alpha^2, \alpha^5, 0, \alpha^{21})$, $H = \begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha & \alpha^3 & \alpha^5 \\ 1 & \alpha^3 & \alpha^6 & \alpha^2 & \alpha^5 & \alpha & \alpha^4 \\ 1 & \alpha^4 & \alpha & \alpha^5 & \alpha^2 & \alpha^6 & \alpha^3 \end{pmatrix}$.

Вариант 13

1. $p(x) = x^4 + x^3 + 1$.

2. $\begin{cases} (\alpha^3 + \alpha^2 + \alpha + 1)x + (\alpha^3 + 1)\, y = \alpha + 1, \\ (\alpha^4 + \alpha + 1)x + (\alpha^2 + \alpha + 1)y = \alpha^3 + \alpha. \end{cases}$

4. $(\alpha^3 + \alpha^2 + 1)x^2 + (\alpha^2 + \alpha + 1)x + (\alpha^3 + 1) = 0$.

5. $\overline{a} = (\alpha, \alpha^9, 1, \alpha^2, \alpha^3, 0, 1)$, $H = \begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha & \alpha^3 & \alpha^5 \\ 1 & \alpha^3 & \alpha^6 & \alpha^2 & \alpha^5 & \alpha & \alpha^4 \\ 1 & \alpha^4 & \alpha & \alpha^5 & \alpha^2 & \alpha^6 & \alpha^3 \end{pmatrix}$.

Вариант 14

1. $p(x) = x^4 + x \ \ + 1$.

2. $\begin{cases} (\alpha^3 + \alpha^2 + \alpha + 1)x + (\alpha^3 + 1)\, y = \alpha + 1, \\ (\alpha^4 + \alpha + 1)x + (\alpha^2 + \alpha + 1)y = \alpha^3 + \alpha. \end{cases}$

4. $(\alpha^3 + \alpha^2 + 1)x^2 + (\alpha^2 + \alpha + 1)x + (\alpha^3 + 1) = 0$.

5. $\overline{a} = (1, \alpha^2, 1, \alpha^2, \alpha^5, 0, 1)$, $H = \begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha & \alpha^3 & \alpha^5 \\ 1 & \alpha^3 & \alpha^6 & \alpha^2 & \alpha^5 & \alpha & \alpha^4 \\ 1 & \alpha^4 & \alpha & \alpha^5 & \alpha^2 & \alpha^6 & \alpha^3 \end{pmatrix}$.

Вариант 15

1. $p(x) = x^4 + x^3 + 1.$

2. $\begin{cases} (\alpha^3 + \alpha + 1)x + (\alpha^3 + 1)y = \alpha^2 + 1, \\ (\alpha^3 + \alpha^2 + 1)x + (\alpha^2 + \alpha + 1)y = \alpha^3 + \alpha + 1. \end{cases}$

4. $(\alpha^3 + 1)x^2 + (\alpha^2 + \alpha + 1)x + (\alpha^3 + \alpha + 1) = 0.$

5. $\overline{a} = (\alpha, \alpha^2, 1, \alpha^2, \alpha^5, 0, 1),$

$$H = \begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha & \alpha^3 & \alpha^5 \\ 1 & \alpha^3 & \alpha^6 & \alpha^2 & \alpha^5 & \alpha & \alpha^4 \\ 1 & \alpha^4 & \alpha & \alpha^5 & \alpha^2 & \alpha^6 & \alpha^3 \end{pmatrix}.$$

Литература

1. Айерлэнд, К. Классическое введение в современную теорию чисел / К. Айерлэнд, М. Роузен. – М. : Мир, 1987. – 416 с.

2. Аршинов, Н. Н. Коды и математика / Н. Н. Аршинов, Л. Е. Садовский. – М. : Наука, 1983. – 124 с.

3. Бейкер, А. Введение в теорию чисел / А. Бейкер. – Минск : Выш. шк., 1995. – 127 с.

4. Биркгоф, Г. Современная прикладная алгебра / Г. Биркгоф, Т. Барти. – М. : Мир, 1976. – 400 с.

5. Живые числа. Пять экскурсий / В. Боро [и др.]. – М. : Мир, 1985. – 128 с.

6. Василенко, О. Н. Теоретико-числовые алгоритмы в криптографии / О. Н. Василенко. – М. : МЦНМО, 2003. – 326 с.

7. Вернер, М. Основы кодирования : учеб. для вузов / М. Вернер. – М. : Техносфера, 2006. – 288 с.

8. Виноградов, И. М. Основы теории чисел / И. М. Виноградов. – М. : Наука, 1982. – 168 с.

9. Зензин, О. С. Стандарт криптографической защиты AES. Конечные поля / О. С. Зензин, М. А. Иванов. – М. : Кудиц-Образ, 2002. – 168 с.

10. Золотарёв, В. В. Помехоустойчивое кодирование. Методы и алгоритмы : справочник / В. В. Золотарёв, Г. В. Овечкин. – М. : Горячая линия – Телеком, 2004 – 126 с.

11. Каргополов, М. И. Основы теории групп / М. И. Каргополов, Ю. И. Мерзляков. – М. : Наука, 1972. – 240 с.

12. Прикладная теория кодирования. В 2 т. / В. К. Конопелько [и др.]. – Минск : БГУИР, 2004. – 688 с.

13. Коутинхо, С. Введение в теорию чисел. Алгоритм RSA / С. Коутинхо. – М. : Постмаркет, 2001.– 324 с.

14. Липницкий, В. А. Современная прикладная алгебра. Математические основы защиты информации от помех и несанкционированного доступа : учеб.-метод. пособие / В. А. Липницкий. – Минск, 2005. – 88 с.

15. Липницкий, В. А. Современная прикладная алгебра. Математические основы защиты информации от помех и несанкционированного доступа : учеб.-метод. пособие / В. А. Липницкий . – Минск, 2006. – 88 с.

16. Лиддл, Р. Конечные поля. В 2 т. / Р. Лиддл, Г. Ниддеррайтер.– М. : Мир, 1988. – 882 с.

17. Логачев, О. А. Булевы функции в теории кодирования и криптологии / О. А. Логачев, А. А. Сальников, В. В. Ященко. – М. : Изд-во МЦНМО, 2004. – 470 с.

18. Нечаев, В. И. Элементы криптографии. Основы теории защиты информации / В. И. Нечаев. – М. : Высш. шк., 1999. – 110 с.

19. Мак-Вильямс, Ф. Дж. Теория кодов, исправляющих ошибки / Ф. Дж. Мак-Вильямс, Н. Дж. А. Слоэн. – М. : Связь, 1979. – 744 с.

20. Мальцев, А. И. Алгебраические системы / А. И. Мальцев. – М. : Наука, 1970. – 392 с.

21. Муттер, В. М. Основы помехоустойчивой телепередачи информации / В. М. Муттер. – Л. : Энергоатомиздат, 1990. – 286 с.

22. Ноден, П. Алгебраическая алгоритмика / П. Ноден, К. Китте. – М. : Мир, 1999. – 720 с.

23. Прасолов, В. В. Многочлены / В. В. Прасолов. – М. : МЦНМО, 2000. – 336 с.

24. Теория информации и кодирование / Б. Б. Самсонов [и др.]. – Ростов н/Д. : Феникс, 2002. – 288 с.

25. Серр, Ж.-П. Курс арифметики / Ж.-П. Серр. – М. : Мир, 1972. – 184 с.

26. Соловьев, Ю. П. Эллиптические кривые и современные алгоритмы теории чисел / Ю. П. Соловьев. – Москва ; Ижевск : Ин-т компьютер. исслед., 2003. – 192 с.

27. Сушкевич, А. К. Теория чисел. Элементарный курс / А. К. Сушкевич. – Харьков : ХГУ, 1954. – 204 с.

28. Черемушкин, А. В. Лекции по арифметическим алгоритмам в криптографии / А. В. Черемушкин. – М. : МЦНМО, 2002. – 104 с.

29. Математические и компьютерные основы криптологии : учеб. пособие / Ю. С. Харин [и др.]. – Минск : ООО «Новое знание», 2003. – 382 с.

30. Харин, Ю. С. Компьютерный практикум по математическим методам защиты информации / Ю. С. Харин, С. В. Агиевич. – Минск : БГУ, 2001. – 190 с.

31. Холл, М. Теория групп / М. Холл. – М. : ИЛ, 1962. – 468 с.

32. Введение в криптографию / В. В. Ященко [и др.]. – М. : МЦНМО, 1999. – 272 с.

СОДЕРЖАНИЕ

Св. план 2010, поз. 61

Учебное издание

Липницкий Валерий Антонович
Спичекова Наталья Викторовна
Данцевич Светлана Федоровна
Олешкевич Дмитрий Николаевич

ПРИКЛАДНАЯ МАТЕМАТИКА

Методическое 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»
дневной формы обучения

Редактор Л. А. Шичко
Корректор Е. Н. Батурчик
Компьютерная верстка Г. М. Кореневская, Е. Г. Бабичева

Подписано в печать	Формат 60×84 1/16.	Бумага офсетная.
Гарнитура «Таймс».	Отпечатано на ризографе.	Усл. печ. л.
Уч.-изд. л. 5,1.	Тираж 150 экз.	Заказ 4.

Издатель и полиграфическое исполнение: учреждение образования
«Белорусский государственный университет информатики и радиоэлектроники»
ЛИ № 02330/0494371 от 16.03.2009. ЛП № 02330/0494175 от 03.04.2009.
220013, Минск, П. Бровки, 6