Министерство просвещения Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Ульяновский государственный педагогический университет
имени И.Н. Ульянова»
(ФГБОУ ВО «УлГПУ им. И.Н. Ульянова»)

Факультет физико-математического и технологического образования
Кафедра высшей математики

УТВЕРЖДАЮ
Проректор по учебно-методической работе
_____ С.Н. Титов
«25» июня 2021 г.

ЭЛЕМЕНТЫ АЛГЕБРАИЧЕСКОЙ ТЕОРИИ КОДИРОВАНИЯ

Программа учебной дисциплины модуля «Специальные разделы предметной области»

основной профессиональной образовательной программы высшего образования – программы бакалавриата по направлению подготовки
44.03.05 Педагогическое образование (с двумя профилями подготовки),

направленность (профиль) образовательной программы
Информатика. Иностранный язык

(очная форма обучения)

Составитель: Глухова Н.В.,
доцент кафедры высшей математики

Рассмотрено и одобрено на заседании ученого совета факультета физико-математического и технологического образования, протокол от «21» июня 2021 г. № 7

Ульяновск, 2021

Место дисциплины в структуре образовательной программы

Дисциплина «Алгебраические методы теории кодирования» относится к дисциплинам части, формируемой участниками образовательных отношений, Блока 1. Дисциплины (модули) модуля «Специальные разделы предметной области» учебного плана основной профессиональной образовательной программы высшего образования – программы бакалавриата по направлению подготовки 44.03.05 Педагогическое образование (с двумя профилями подготовки), направленность (профиль) образовательной программы «Информатика. Иностранный язык», очной формы обучения.

Дисциплина опирается на результаты обучения, сформированные в рамках дисциплин Вводный курс алгебры, Математическая логика, Дифференциальное и интегральное исчисление, Дискретная математика, Теория чисел.

Результаты изучения дисциплины являются основой для изучения ряда дисциплин и прохождения практик: Теория алгоритмов, Компьютерное моделирование, Численные методы и для прохождения государственной итоговой аттестации

Перечень планируемых результатов обучения (образовательных результатов) по дисциплине

Целью освоения дисциплины является подготовка учителя к будущей профессиональной деятельности: формирование способности к преподаванию учебных предметов по профилю, как в обычных общеобразовательных классах, так и в классах с углубленным изучением математики.

Задачей освоения дисциплины является демонстрация возможностей применения математических методов в информатике, кодировании, закрепление умений проводить математические преобразования выражений с помощью компьютерных технологий, отработка понятийного аппарата математики, техники проведения математических расчетов, формирование и закрепление умения проводить строгие абстрактно-логические доказательства.

В результате освоения программы обучающийся должен овладеть следующими результатами обучения (в таблице представлено соотнесение образовательных результатов обучения по дисциплине с индикаторами достижения компетенций):

Компетенция и индикаторы ее достижения в дисциплине	Образовательные результаты дисциплины (этапы формирования дисциплины)		
	знает	умеет	владеет
ПК-12 - Способен выделять структурные элементы, входящие в систему познания предметной области (в соответствии с профилем и уровнем обучения), анализировать их в единстве содержания, формы и выполняемых функций.			
ПК-12.1. Знает формулировки определений,	ОР-1. Основные понятия дисциплины, определения,	ОР-2 Решать задачи по дисциплине, проводить	

содержательное значение терминов и понятий предметной области, правила и алгоритмы оперирования с объектами предметной области, понимает взаимосвязь между структурными элементами; имеет представление о функциях и практическом применении изучаемых объектов. ПК-12.2. Умеет выделять и анализировать структурные элементы, входящие в систему познания предметной области; определять логическую взаимосвязь между компонентами предметной области; строить логически верные и обоснованные рассуждения; решать задачи предметной области.	содержательное значение терминов и их взаимосвязь, алгоритмы доказательств и решения задач	доказательства, классифицировать и систематизировать основные изучаемые объекты, строить логически верные рассуждения	
ПК-14. Способен устанавливать содержательные, методологические и мировоззренческие связи предметной области (в соответствии с профилем и уровнем обучения) со смежными научными областями ИПК-14.1. Знает роль и возможности применения аппарата предметной области в смежных	ОР-3. возможности применения полученных сведений к решению задач школьного курса, а также в	ОР-4. решать задачи школьного курса повышенной сложности, решать и составлять прикладные задачи	

научных областях, их методологическое и мировоззренческое значение; имеет представление о междисциплинарных связях, научных методах смежных областей ИПК-14.2. Умеет определять роль полученных знаний для смежных областей и для школьного курса, применять полученные знания в решении прикладных задач.	смежных научных областях	по дисциплине	

2. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Номер семестра	Учебные занятия						Форма промежуточной аттестации
	Всего		Лекции, час	Практические занятия, час	Лабораторные занятия, час	Самостоят. работа, час	
	Трудоемк.						
	Зач. ед.	Часы					
3	3	108	18	30	-	33	экзамен (27)
Итого:	3	108	18	30	-	33	

3. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

3.1 .Указание тем (разделов) и отведенного на них количества академических часов и видов учебных занятий

Наименование раздела и тем	Количество часов по формам организации обучения

	Лекционные занятия	Практические занятия	Лабораторные занятия	Самостоятельная работа
3 семестр				
Алгебраические методы помехоустойчивого кодирования	8	16		13
Алгебраические методы в криптографии	10	14		20
Экзамен				27
Всего по дисциплине:	18	-	30	60

3.2. Краткое описание содержания тем (разделов) дисциплины

Краткое содержание курса

1. Алгебраические методы помехоустойчивого кодирования

Основы теории информации. Группы и подгруппы. Сравнимость элементов группы по подгруппе. Нормальные делители. Циклические группы. Расширения полей, алгебраические и конечные расширения. Групповые и линейные коды. Коды с повторениями и коды с проверкой на чётность. Коды Хемминга. Алгоритмы, позволяющие найти и исправить две ошибки. Пути улучшения алгоритмов для исправления большего числа ошибок. Коды Рида-Соломона. Необходимые сведения из теории конечных полей. Поля GF (2^m). Расширенные и укороченные коды Рида-Соломона. Интерактивные формы: деловая игра – лекция проводимая студентами, практическое занятие – групповая дискуссия о преимуществах и недостатках кодов. Отображение РС-кодов над GF (2^m) на двоичные коды. Способы кодирования и декодирования. Алгоритм Берлекэмпа-Месси.

2. Алгебраические методы в криптографии

Основные понятия и определения криптографии. Криптографические системы с закрытым и открытым ключом. Исторические сведения о системах с закрытым ключом. Применение подстановок в криптографии. Кольца классов вычетов (числа и многочлены). Кольца конечной характеристики и конечные кольца. Основы модулярной арифметики. Системы с открытым ключом. Система RSA и её криптостойкость. Типы атак на криптографические системы. Алгоритмы защиты. Интерактивные формы: деловая игра – лекция проводимая студентами, практическое занятие – групповая дискуссия.

4. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Самостоятельная работа студентов является особой формой организации учебного процесса, представляющая собой планируемую, познавательно, организационно и методически направляемую деятельность студентов, ориентированную на достижение конкретного результата, осуществляемую без прямой помощи преподавателя. Самостоятельная работа студентов является составной частью учебной работы и имеет целью закрепление и углубление полученных знаний и навыков, поиск и приобретение новых знаний, а также выполнение учебных заданий, подготовку к предстоящим занятиям и экзамену. Она предусматривает, как правило, разработку рефератов, написание докладов, выполнение творческих, индивидуальных заданий в соответствии с учебной

программой (тематическим планом изучения дисциплины). Тема для такого выступления может быть предложена преподавателем или избрана самим студентом, но материал выступления не должен дублировать лекционный материал. Реферативный материал служит дополнительной информацией для работы на практических занятиях. Основная цель данного вида работы состоит в обучении студентов методам самостоятельной работы с учебным материалом. Для полноты усвоения тем, вынесенных в практические занятия, требуется работа с первоисточниками. Курс предусматривает самостоятельную работу студентов со специальной литературой. Следует отметить, что самостоятельная работа студентов результативна лишь тогда, когда она выполняется систематически, планомерно и целенаправленно.

Задания для самостоятельной работы предусматривают использование необходимых терминов и понятий по проблематике курса. Они нацеливают на практическую работу по применению изучаемого материала, поиск библиографического материала и электронных источников информации, иллюстративных материалов. Задания по самостоятельной работе даются по темам, которые требуют дополнительной проработки.

Общий объем самостоятельной работы студентов по дисциплине включает аудиторную и внеаудиторную самостоятельную работу студентов в течение семестра.

Аудиторная самостоятельная работа осуществляется в форме выполнения тестовых заданий, письменных проверочных работ по дисциплине. Аудиторная самостоятельная работа обеспечена базой тестов, контрольных и самостоятельных работ.

Внеаудиторная самостоятельная работа осуществляется в формах:

- подготовки к устным докладам;
- решение задач (домашних заданий) по изучаемым темам;
- выполнение групповых интерактивных заданий

ОС-1. Самостоятельная работа

Примерный вариант .

1. В поле, полученном присоединением к $\mathbf{Z}_p$ корня θ неприводимого многочлена *f(x),* перечислите все элементы. Вычислите θ^{-1} и θ^2:

а) $f(x) = x^2 + x + 1$, $p = 2$ б) $f(x) = x^2 + 1$, $p = 3$.

2. Найти информационное сообщением в системе, позволяющей найти и исправить одну ошибку, если принято сообщение

а) (5, 3, 2, 9, 14) б) (4, 3, 2, 1, 11, 21)

ОС-2 Контрольная работа

Примерный вариант:

1)Перевести 112_7 и $2(10)5_{12}$ в 9-чную систему счисления и найти в этой системе сумму, разность, произведение этих чисел, а также разделить большее на меньшее с остатком.

2)Найти элемент обратный 12 в поле классов вычетов по модулю 17.

3)Избавится от иррациональности в знаменателе

$$\frac{2\sqrt[3]{5}}{\sqrt[3]{25}+4\sqrt[3]{5}+1}$$

4)Представить подстановку в виде произведения независимых циклов

1 2 3 4 5 6 7

(2 3 4 7 6 5 1)

Групповое интерактивное задание.

Студенты разбиваются на микрогруппы по 4 человека и готовят доклад по темам

1. Нахождение обратных элементов в поле классов вычетов.
2. Расширенные конечные поля.

3. Числа конечного поля. Характеристика поля.
4. Теорема о количестве элементов произвольного конечного поля.
5. Отношение сравнения многочленов по модулю.
6. Фактор-кольцо многочленов по модулю многочлена. Необходимое и достаточное условие того, чтобы оно было полем (с доказательством).
7. Вычислительные аспекты работы с расширенными конечными полями.
8. Приводимость многочленов над конечными полями.
9. Корни уравнений в конечных полях.
10. Коды с повторениями
11. Коды с проверкой на чётность

Для самостоятельной подготовки к занятиям по дисциплине рекомендуется использовать учебно-методические материалы:

Глухова Н.В. Элементы абстрактной и компьютерной алгебры. Учебно-методическое пособие. – Ульяновск: УлГПУ, 2009. – 50 с

5. Примерные оценочные материалы для проведения текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине

Организация и проведение аттестации студента

ФГОС ВО в соответствии с принципами Болонского процесса ориентированы преимущественно не на сообщение обучающемуся комплекса теоретических знаний, но на выработку у бакалавра компетенций – динамического набора знаний, умений, навыков и личностных качеств, которые позволят выпускнику стать конкурентоспособным на рынке труда и успешно профессионально реализовываться.

В процессе оценки бакалавров необходимо используются как традиционные, так и инновационные типы, виды и формы контроля. При этом постепенно традиционные средства совершенствуются в русле компетентностного подхода, а инновационные средства адаптированы для повсеместного применения в российской вузовской практике.

Цель проведения аттестации – проверка освоения образовательной программы дисциплины-практикума через сформированность образовательных результатов.

Промежуточная аттестация осуществляется в конце семестра и завершает изучение дисциплины; помогает оценить крупные совокупности знаний и умений, формирование определенных компетенций.

Оценочными средствами текущего оценивания являются: доклад, тесты по теоретическим вопросам дисциплины, защита практических работ и т.п. Контроль усвоения материала ведется регулярно в течение всего семестра на практических (семинарских, лабораторных) занятиях.

№ п/п	**СРЕДСТВА ОЦЕНИВАНИЯ,** используемые для текущего оценивания показателя формирования компетенции	Образовательные результаты дисциплины
	Оценочные средства для текущей аттестации ОС-1 Самостоятельная работа ОС-2 Контрольная работа ОС-3. Выступление с докладами (интерактивное задание) Составление тестов	ОР-1. Знает оновные понятия дисциплины, определения, содержательное значение терминов и их взаимосвязь, алгоритмы доказательств и решения задач ОР-2. Умеет решать задачи по дисциплине, проводить доказательства, классифицировать и систематизировать основные изучаемые объекты, строить логически верные рассуждения
	Оценочные средства для промежуточной аттестации **зачет (экзамен)** ОС-4 Экзамен в форме устного собеседования	

		ОР-3. знает возможности применения полученных сведений к решению задач школьного курса, а также в смежных научных областях ОР-4. умеет решать задачи школьного курса повышенной сложности, решать и составлять прикладные задачи по дисциплине

Описание оценочных средств и необходимого оборудования (демонстрационного материала), а так же процедуры и критерии оценивания индикаторов достижения компетенций на различных этапах их формирования в процессе освоения образовательной программы представлены в Фонде оценочных средств для текущего контроля успеваемости и промежуточной аттестации по дисциплине.

Материалы, используемые для текущего контроля успеваемости обучающихся по дисциплине

Материалы для организации текущей аттестации представлены в п.5 программы.

Материалы, используемые для промежуточного контроля успеваемости обучающихся по дисциплине

ОС-4 Экзамен в форме устного собеседования
Примерные вопросы к экзамену

1. . Понятие группы, подгруппы
2. Смежные классы по подгруппе, фактор-группы. Теорема Лагранжа
3. Кольцо, подкольцо, идеал
4. Классы вычетов по произвольному идеалу. Фактор-кольцо
5. Кольцо классов вычетов по числовому модулю. Операции над классами вычетов.
6. Кольцо классов вычетов. Необходимое и достаточное условие того, чтобы это кольцо являлось полем (с доказательством)
7. Нахождение обратных элементов в поле классов вычетов
8. Кольцо многочленов от одной переменной, отношение делимости в нём, теорема о делении с остатком, НОД и НОК
9. Алгебраические расширения полей. Теорема о строении простого алгебраического расширения поля
10. Конечные поля, их простейшие свойства
11. Числа в конечных полях, характеристика поля
12. Теорема о количестве элементов произвольного конечного поля
13. Существование примитивного элемента в конечном поле (с доказательством)
14. Отношение сравнения многочленов по модулю
15. Фактор-кольцо многочленов по модулю многочлена. Необходимое и достаточное условие того, чтобы оно было полем (с доказательством)
16. Примеры вычислений над конечными полями
17. Основные понятия теории кодирования. Групповые коды и их свойства, применение теории групп для исправления ошибок
18. Алгоритм кодирования, позволяющий найти и исправить одну ошибку.
19. Алгоритм кодирования, позволяющий найти и исправить две ошибки. Пути улучшения алгоритма
20. Криптография. Системы с открытым ключом (алгоритм RSA).
21. Представление чисел в различных системах счисления. Примеры арифметических действий над числами в позиционных системах
22. Перевод чисел из одной системы счисления в другую для целых чисел

23. Перевод чисел из одной системы счисления в другую для дробных чисел
24. Алгоритмы работы с обыкновенными дробями
25. Перевод периодических дробей в обыкновенные
26. Представление многочленов в компьютере. Разреженные и плотные представления
27. Многочлены от нескольких переменных (способы упорядочения членов, рекурсивные и распределённые представления).
28. Дробно-рациональные выражения (нормальное и каноническое представления, алгоритмы работы)
29. Алгебраические числа. Алгоритмы работы с выражениями, содержащими иррациональность

Примерные практические задания к экзамену

1. Перечислить все элементы поля из 25 элементов. Указать квадраты любых 8 элементов и обратные для них
2. Найти информационное сообщением в системе, позволяющей найти и исправить одну ошибку, если принято сообщение (4, 3, 2, 1, 11, 21);

В конце изучения дисциплины подводятся итоги работы студентов на лекционных и практических занятиях путем суммирования заработанных баллов в течение семестра.

Критерии оценивания знаний обучающихся по дисциплине

Формирование балльно-рейтинговой оценки работы обучающихся

		Посещение лекций	Посещение практических занятий	Работа на практических занятиях	Экзамен
3 семестр	Разбалловка по видам работ	9 х 1=9 баллов	15 х 1=15 баллов	212 баллов	64 балла
	Суммарный макс. балл	9 баллов max	24 балла max	236 баллов max	300 баллов max

Критерии оценивания работы обучающегося по итогам семестра

Оценка	**Баллы (3 ЗЕ)**
«отлично»	271-300
«хорошо»	211-270
«удовлетворительно»	151-210
«неудовлетворительно»	150 и менее

6. Методические указания для обучающихся по освоению дисциплины

Успешное изучение курса требует от обучающихся посещения лекций, активной работы на практических занятиях, выполнения всех учебных заданий преподавателя, ознакомления с основной и дополнительной литературой.

Запись **лекции** – одна из форм активной самостоятельной работы обучающихся, требующая навыков и умения кратко, схематично, последовательно и логично фиксировать основные положения, выводы, обобщения, формулировки. В конце лекции преподаватель оставляет время (5 минут) для того, чтобы обучающиеся имели возможность задать уточняющие вопросы по изучаемому материалу. Из-за недостаточного количества аудиторных часов некоторые темы не удается осветить в полном объеме, поэтому преподаватель, по своему усмотрению, некоторые вопросы выносит на самостоятельную работу студентов, рекомендуя ту или иную литературу. Кроме этого, для лучшего освоения материала и систематизации знаний по дисциплине, необходимо

постоянно разбирать материалы лекций по конспектам и учебным пособиям. В случае необходимости обращаться к преподавателю за консультацией.

Подготовка к практическим занятиям.

При подготовке к практическим занятиям студент должен изучить теоретический материал по теме занятия (использовать конспект лекций, изучить основную литературу, ознакомиться с дополнительной литературой, при необходимости дополнить конспект, делая в нем соответствующие записи из литературных источников). В случае затруднений, возникающих при освоении теоретического материала, студенту следует обращаться за консультацией к преподавателю. Идя на консультацию, необходимо хорошо продумать вопросы, которые требуют разъяснения.

В начале практического занятия преподаватель знакомит студентов с темой, оглашает план проведения занятия, выдает задания. В течение отведенного времени на выполнение работы студент может обратиться к преподавателю за консультацией или разъяснениями. В конце занятия проводится прием выполненных заданий, собеседование со студентом.

Результаты выполнения практических зданий оцениваются в баллах, в соответствии с балльно-рейтинговой системой университета.

Планы лабораторных (практических) занятий

ПЗ-1 Представление чисел в компьютере

1. Запишите первые 20 чисел в системах счисления с основаниями

а) 9, б) 14, в) 4, г) 11

2. Выполните действия сложения и вычитания:

а) $10465_7 + 3351_7$ б) $15(11)3_{12} + 2724_{12}$
в) $10441_5+203_5+4211_5+41030_5$ г) $8051_9 + 12356_9 + 8051_9$
д) $134602_8 – 26415_8$ е) $15(11)3_{16} – 2724_{16}$
ж) $21(11)39_{12} – 37(10)4_{12}$ з) $2304_6 – 425_6$

3. Выполнить действия умножения и деления

а) $32403_7 \cdot 623_7$ б) $545_6 \cdot 3_6$
в) $(10)5(11)_{12} \cdot 9(10)_{12}$ г) $125_7 \cdot 64_7$
д) $1141043_5 : 23_5$ е) $26833_9 : 1823_9$
ж) $4(11)0930_{12} : 6_{12}$ з) $9(10)166_{12} : (10)_{12}$

ПЗ 2. Позиционные системы счисления

1. Перевести число из одной системы счисления в систему с основанием g:

а) 2718_9, g = 7 д) 1927_{10}, g = 7
б) 34014_5, g = 8 е) 41102_7, g = 9
в) $(13)40(10)_{14}$, g =10 ж) $25(11)3_{12}$, g = 10
г) 34022_7, g = 5 з) $4(11)0930_{12}$, g = 6

2. Чему равно основание системы счисления x, в которой

а) $26 = 101_x$ б) $231_x = 123_7$

3. Запишите в двоичной системе счисления

а) 47056_8 в) 51435_8
б) $9(13)5_{16}$ г) $(12)4(11)7_{16}$

4. Запишите числа в восьмеричной и шестнадцатеричной системах

а)$111\ 000\ 101\ 011\ 010_2$ в) $100\ 111\ 010\ 101_2$
б) $1\ 110\ 000\ 011\ 100\ 110_2$ г) $1100\ 0100\ 1011\ 0111_2$

5. Выполните действия в соответствующей системе счисления, а затем переведите в десятичную и проверьте результат

а) $(1001101_2 + 1110001_2)\cdot(1110001_2 - 1001101_2)$
б) $45_8 + 60_9 + 55_{12} = x_{11}$

ПЗ 3. Представление дробей

1. Перевести в десятичную

а) $126{,}34_8$ б) $(10)49{,}62_{16}$

2. Перевести из десятичной в систему с основанием g

а) 634,36 , g = 8 б) 52,37, g = 8
в) 36,6, g = 2 г) 156,5, g = 2
д) 52,21, g = 16 е) 812,32, g = 16

3. Выполните действия:

а) $12{,}034_5 + 3{,}444_5$ б) $2{,}304_6 + 0{,}253_6$
в) $28{,}07_{12} - 8{,}23_{12}$ г) $3{,}04_7 - 2{,}15_7$
д) $23{,}4_5 \cdot 0{,}24_5$ е) $2{,}(10)1_{12} \cdot 3{,}7_{12}$
ж) $0{,}(11)4(11)_{12} : 2{,}7_{12}$ з) $1{,}03_6 : 0{,}43_6$

ПЗ-4 Работа с обыкновенными дробями

1. Можно ли сократить дробь 12/20 записанную в системе счисления , g = 7

2. Выяснить, обращаются ли в конечные систематические дроби по основанию g следующие обыкновенные дроби (записанные в десятичной системе счисления)

а) 7/400, g = 10 б) 23/48, g = 6
в) 25/288, g = 12 г) 5/384, g = 12

Если это возможно, выполните это обращение.

3. Представьте смешанную периодическую дробь в виде несократимого отношения двух целых чисел

а) 0, 233(37) б) 9, (387)
в) 11, (459) г) 7, 4(099)
д) $0{,}(02)_4$ е) $0{,}\ 0(2)_4$
ж) $0{,}\ 000(3)_6$ з) $0{,}\ 4(3)_7$

ПЗ 5. Группы, подгруппы, классы смежности, фактор-группы

1. Доказать, что множество целых чисел, кратных 3 (д/з 5) является подгруппой аддитивной группы всех целых чисел. Найдите правосторонне и левосторонне разложение группы целых чисел по данной подгруппе. Является ли данная подгруппа нормальным делителем?
2. Докажите, что множество самосовмещений правильного треугольника образует группу. Найдите все подгруппы данной группы. Найдите левые и правые классы смежности по всем подгруппам. Укажите те из них, которые являются нормальными делителями.
3. (д/з) Докажите, что множество поворотов квадрата образует подгруппу его самосовмещений. Найдите левые и правые классы смежности. Является ли эта подгруппа нормальным делителем.
4. Доказать, что множество всех чётных подстановок четырёхэлементного множества образует подгруппу всех подстановок данного множества. Докажите, что она является нормальным делителем. Постройте фактор-группу.

5. (д/з) Даны подстановки:

$a_0=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$, $a_1=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$, $a_2=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$, $a_3=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$, $a_4=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$, $a_5=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$

Найти все подгруппы и все нормальные делители данной группы. Построить левые и правые классы смежности по всем нетривиальным подгруппам. Где это возможно, указать фактор-группы.

6. Даны матрицы:

$E=\begin{pmatrix}1&0\\0&1\end{pmatrix}$, $A=\begin{pmatrix}-1&0\\0&-1\end{pmatrix}$, $B=\begin{pmatrix}0&-1\\1&0\end{pmatrix}$, $C=\begin{pmatrix}0&1\\-1&0\end{pmatrix}$,

Найти все подгруппы и все нормальные делители данной группы. Построить левые и правые классы смежности по всем этим подгруппам. Где это возможно, указать фактор-группы.

ПЗ-6. Подстановки и их представление в виде циклов

7. Представьте в виде произведения независимых циклов подстановки:

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

в) $\begin{pmatrix}1&2&3&4&5&6&7&8\\2&1&3&6&8&7&4&5\end{pmatrix}$ г) $\begin{pmatrix}1&2&3&4&5&6&7&8\\8&6&4&3&2&1&7&5\end{pmatrix}$

Найдите порядок и чётность каждой подстановки.

8. Представьте произведения независимых циклов в виде подстановок. Найдите порядок и чётность каждой подстановки.

а) (123)(4568) б) (34)(52618)

9. Вычислить τ^k

а) $\tau=\begin{pmatrix}1&2&3&4&5&6&7\\4&7&1&3&5&2&6\end{pmatrix}$, $k = 137$

б) $\tau=\begin{pmatrix}1&2&3&4&5&6&7&8&9\\9&5&4&3&1&7&6&8&2\end{pmatrix}$, $k = 352$

ПЗ – 7. Работа с многочленами.

1. Расположите члены следующих многочленов в лексикографическом порядке, в порядке «общей степени, затем лексикографическом»:

а) $x_1 + x_2 + x_3$

б) $3x_1^2 + 3x_2^2 + x_2$

в) $x_1 x_2 + x_2x_{13}$

г) $x_1^3 + x_2^3 + x_3^2 - 3x_1x_2x_3$.

2. Укажите старшие члены многочленов:

а) $(x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$

б) $(x_1 - x_2)^2 (x_1 - x_3)^2 (x_2 - x_3)^2$

в) $(x_1 - x_2 - x_3)(x_2 - x_1 - x_3)(x_3 - x_1 - x_2)$

г) $(x_2^3 + x_1^2x_3 - x_3^3)(x_1^2 - x_1^2x_2x_3)(x_1^3x_2^2 - x_1^4 + x_2^2)$

д) $2\sigma_1^4 \sigma_2^3\sigma_3^2$ (σ_i – элементарные симметрические многочлены)

е) $2\sigma_1^2 \sigma_2\sigma_3^3$.

3. Если это возможно, сократите дроби $f(x)/g(x)$:

а) $f(x) = x^4 - 3x^3 + 3x^2 - 3x + 2$, $g(x) = x^3 - 2x^2 - x + 2$

б) $f(x) = x^4 + 2x^3 + 2x^2 + 2x + 2$, $g(x) = x^3 + 3x^2 + 2$

в) $f(x) = x^5 + x^4 + 3x^3 + 4x^2 + 4x + 2$, $g(x) = x^5 + 2x^4 + 3x^3 + 6x^2 + 6x + 2$

г) $f(x) = x^6 + 6x^5 + 2x^3 + 3x^2 + 6x + 1$, $g(x) = x^5 + 6x^4 + 4x^2 + 4x + 6$.

4. Упростите выражения:

а) $\dfrac{1}{x^4 + x^3 + 2x^2 + x + 1} + \dfrac{1}{x^3 + 2x^2 + x - 2}$

б) $\dfrac{x-1}{x^4 + 6x^3 + 17x^2 + 24x + 12} \cdot \dfrac{x^3 - 2x^2 - 13x - 10}{x^2 - 1}$

в) $\dfrac{x^2 + 1}{x^5 + x^3 + 2x^2 + 2x + 2} + \dfrac{x^4 + 2x^2 + 1}{x^4 + 2x^3 + 7x^2 + 2x + 6}$

г) $\dfrac{x^4 + x^3 + 3x^2 + 6x + 3}{x^3 + 2x^2 + 2x + 1} - \dfrac{x^6 + x^5 + 3x^4 + 2x^3 + 4x + 2}{x^5 + 3x^4 + x^3 + 6x^2 + 4x + 6}$.

ПЗ-8. Контрольная работа.

ПЗ-9 Числовые конечные поля

1. Доказать, что кольцо классов вычетов $\mathbf{Z_p}$ является полем тогда и только тогда, когда p – простое число.

2.Найти элемент обратный для элемента a в поле $\mathbf{Z_p}$:

а) a = 10, p = 17 д) a = 11, p = 13

б) a = 7, p = 31 е) a = 19, p = 23

в) a = 12, p = 29 ж) a = 13, p = 17

г) a = 23, p = 41

3.Построить фактор-кольцо кольца многочленов по главному идеалу, порождённому многочленом f(x) над полем $\mathbf{Z_p}$. Является ли данный идеал полем? Найдите квадраты всех его элементов и обратные элементы, когда они существуют.

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

4.Решить систему

а) $\begin{cases} 3x + y + 2z = 1 \\ x + 2y + 3z = 1 \\ 4x + 3y + 2z = 1 \end{cases}$ в $\mathbf{Z}_5$ и $\mathbf{Z}_7$ б) $\begin{cases} x + 2z = 1 \\ y + 2z = x \\ 2x + z = 1 \end{cases}$ в $\mathbf{Z}_3$ и $\mathbf{Z}_5$

ПЗ-10. Конечные поля составной характеристики

1. В поле, полученном присоединением к в $\mathbf{Z}_3$ корня θ неприводимого многочлена f(x) перечислить все элементы. Вычислить θ^{-1} и θ^2

а) $f(x) = x^2 + x + 1$, p = 2 б) $f(x) = x^2 + 1$, p = 3

2. Доказать, что для поля характеристики p

а) $(a+b)^{p^f} = a^{p^f} + b^{p^f}$

б) $(a_1 + a_2 + \ldots + a_n)^p = a_1^p + a_2^p + \ldots + a_n^p$

в) $a^p = a$

ПЗ-11. Работа с иррациональными выражениями

1. Найдите минимальный многочлен для числа над полем рациональных чисел:

а) 1

б) $\sqrt{2}+i\sqrt{3}$

в) $-1+i\sqrt{3}$

г) $\sqrt[4]{1+\sqrt{2}}$

д) $\cos 10^0$

е) i

ж) $1-2\sqrt[3]{4}$

з) $1+\sqrt[5]{11}$

и) $\cos\frac{\pi}{4}+i\sin\frac{\pi}{4}$

к) $\sin 10^0$.

2. Освободитесь от α в знаменателе дроби, где α – корень указанного уравнения:

а) $\frac{\alpha}{\alpha^3+1}$, $\alpha^3-2\alpha+2=0$

б) $\frac{1}{\alpha^3+3\alpha^2+3\alpha+2}$, $\alpha^4+\alpha^3-4\alpha^2-3\alpha+2=0$

в) $\frac{\alpha^2}{\alpha^4+1}$, $\alpha^4+2\alpha+2=0$

г) $\frac{\alpha^2-3\alpha+1}{\alpha^2+2\alpha+1}$, $\alpha^3+\alpha^2+3\alpha+4=0$.

3. Освободитесь от иррациональности в знаменателе дроби:

а) $\frac{7}{1-\sqrt[4]{2}+\sqrt{2}}$

б) $\frac{1}{1+3\sqrt[3]{2}+\sqrt[3]{4}}$

в) $\frac{\sqrt{7}+1}{\sqrt[4]{7}+\sqrt{7}-1}$

г) $\frac{11}{\sqrt[3]{4}+\sqrt[3]{2}-1}$

4. Найти расширение поля рациональных чисел элементами $\sqrt{3}$ и $\sqrt{2}$. Найти примитивный элемент этого поля и выразить через него $\sqrt{3}$ и $\sqrt{2}$.

ПЗ-12.Булевы алгебры

1. Определите, являются ли структурами и булевыми алгебрами следующие множества:

а) множество всех подмножеств некоторого множества с отношением порядка «включение»;

б) множество всех высказываний с операциями «конъюнкция» и «дизъюнкция» в качестве умножения и сложения соответственно;

в) множество целых (действительных) чисел с обычными операциями сложения и умножения;

г) множество натуральных чисел, в которых отношением порядка служит отношение делимости.

2. Докажите, что любое линейно упорядоченное множество является структурой.

3. Докажите, что любой элемент булевой алгебры имеет только одно дополнение.

ПЗ-13. Элементы теории кодирования

1.Сообщение кодируется с проверкой на чётность, указать заведомо ошибочные среди пришедших сообщений:
а) 1 1 1 1 1 1
б) 0 0 0 0 0 0
в) 1 0 1 0 1 0
г) 0 0 1 1 0 0
2. Определите последнюю цифру, добавляемую к сообщению (1 1 1 0 0) при кодировании с проверкой на чётность
3. Информационное сообщение: (1, 1, 2, 3). Определите проверочные символы в алгоритме с исправлением одной и двух ошибок
4. Найти информационное сообщением в системе, позволяющей найти и исправить одну ошибку, если принято сообщение
а) (5, 3, 2, 9, 14) Отв. (5, 3, 1)
б) 4, 3, 2, 1, 11, 21 Отв. (5, 3, 2, 1)
в) 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 6, 29 – верно
г) (1, 2, 2, 4, 5, 15, 55) Отв. (1, 2, 3, 4, 5)
д) 4, 1, 10, 16 Отв. (4, 6)
е) (1, 2, 3, 1, 2, 1, 10, 34) Отв. (1. 2, 1, 1, 2, 1)
ж) 1, 2, 1, 2, 1, 2, 9, 15 – ошибочен s_2
з) (1, 3, 0, -1, 4, 10) – отказ.
и) (1, 0, 1, 0, 2, 4) Отв. 1, 0, 1, 0
5. Найти сообщения, которые не содержат ошибок в системе, позволяющей найти и исправить одну ошибку:
а) 1, 2, 3, 1, 2, 1, 11, 34
б) 1, 1, 1, 0, 0, 0, 3, 6
в) 3, 1, 0, 0, 1, 1, 6, 16
г) 1, 1, 1, 1, 1, 1, 1, 6, 21
6. При кодировании сообщения каждый символ утраивается, какое сообщение согласно принципу наибольшего правдоподобия является правильным, если принято сообщение 111001010111
7. Закодировать сообщение для исправления двух ошибок:
а) 1, 0, 1, 1
б) (4, 3, 2, 1) Отв. (10, 20, 50, 146)
в) (2, 5)
г) (1, 0, 1) Отв. (2, 4, 10, 28)
8. Декодировать сообщение (алгоритм с исправлением двух ошибок):
(2, 1, 1, 0, 1, 1, 6, 16, 68, 352)
Отв. (3, 1, 0, 0, 1, 1)

ПЗ-14. Выступление с докладами

ПЗ 15. Контрольная работа

Основная литература

1. Царев А.В., Шеина Г.В. Элементы абстрактной и компьютерной алгебры. – М.МПГУ, 2016 – 116 с. (Электронный ресурс: «Университетская библиотека онлайн» http://biblioclub.ru/index.php?page=book_view_red&book_id=471787)
2. Титов К.В. Компьютерная математика: Учебное пособие. - М.: ИЦ РИОР, НИЦ ИНФРА-М, 2016. - 261 с (http://znanium.com/bookread2.php?book=523231).
3. Кострикин А.И. Введение в алгебру. – 3-е изд. – М.: Физматлит. – 2001. – 368 с, М.: МЦНМО, 2009. том 3. Основные структуры алгебры – 272 с. (Электронный ресурс http://biblioclub.ru/index.php?page=book_view_red&book_id=62951)

Дополнительная литература

1. Крамарь В.А., Карапетьян В.А., Альчаков В.В. Специальные разделы математики: Практикум / - М.:Вузовский учебник, НИЦ ИНФРА-М, 2017. - 123 с. (http://znanium.com/bookread2.php?book=550621)
2. Кнауб Л. В., Новиков Е. А., Шитов Ю. А. Теоретико-численные методы в криптографии: учебное пособие – Красноярск: Сибирский федеральный университет, 2011. – 160 с. (Электронный ресурс: «Университетская библиотека онлайн» http://biblioclub.ru/index.php?page=book_view_red&book_id=229582)
3. Влэдуц С. Г. , Ногин Д. Ю. , Цфасман М. А. Алгеброгеометрические коды. – М.: , 2003 – 503 с. (http://biblioclub.ru/index.php?page=book_view_red&book_id=62181)
4. Комбинаторные алгоритмы: множества, графы, коды/БыковаВ.В. - Краснояр.: СФУ, 2015. - 152 с. (http://znanium.com/bookread2.php?book=550333)
5. Василенко О. Н. Теоретико-числовые алгоритмы в криптографии. - М.: МЦНМО, 2006 – 336 с. (Электронный ресурс: «Университетская библиотека онлайн» http://biblioclub.ru/index.php?page=book_view_red&book_id=61814)
6. Дадаян А.А. Математика: Учебник / А.А. Дадаян. - 3-е изд. - М.: Форум: НИЦ ИНФРА-М, 2013. - 544 с. (http://znanium.com/bookread2.php?book=397662)
7. Минаев В. А. Простые числа: новый взгляд на закономерности формирования - М.: Логос, 2011 – 79 с. (электронный ресурс: http://biblioclub.ru/index.php?page=book_view_red&book_id=119456)
8. Шевалдина О. Я. , Стрелкова Е. В. Начала математического анализа: учебное пособие. - Издательство Уральского университета, 2014. – 100 с. (http://biblioclub.ru/index.php?page=book_view_red&book_id=276483)
9. Глухова Н.В. Элементы абстрактной и компьютерной алгебры. Учебно-методическое пособие. – Ульяновск: УлГПУ, 2009. – 50 с (библиотека УлГПУ).
10. Бухштаб А.А. Теория чисел. – СПб. и др.: Лань, 2008.- 383 с. (библиотека УлГПУ).
11. Михелович, Ш. Х. Теория чисел / Ш.Х. Михелович. - Москва : Высшая школа, 1962. - 260 с. http://biblioclub.ru/index.php?page=book&id=437366
12. Куликов Л.Я. Алгебра и теория чисел. – М.: Высшая школа, 1979. – 559 с.

Интернет-ресурсы

http://www.mathnet.ru Общероссийский математический портал