МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Механико-математический факультет

УТВЕРЖДАЮ
Декан механико-математического факультета
_____ Захаров А.М.
"2" 09 2024 г.

Рабочая программа дисциплины

Алгебраические приложения в компьютерных науках

Направление подготовки магистратуры
02.04.01 Математика и компьютерные науки

Профиль подготовки магистратуры
Математические основы компьютерных наук

Квалификация (степень) выпускника
Магистр

Форма обучения
очная

Саратов,
2024

Статус	ФИО	Подпись	Дата
Преподаватель-разработчик	Кривобок В.В.		2.09.2024
Председатель НМК	Тышкевич С.В.		2.09.2024
Заведующий кафедрой	Водолазов А.М.		2.09.2024
Специалист Учебного управления			

1. Цели освоения дисциплины

С помощью теории абстрактной алгебры, изложить теорию конечных полей, описать арифметику многочленов над конечными полями, способы их построения, алгоритмы нахождения элементов конечных полей, описать структуры и группы Галуа конечных полей.

2. Место дисциплины в структуре ООП

Дисциплина «Алгебраические приложения в компьютерных науках» (Б1.О.08) относится к обязательной части блока 1 «Дисциплины (модули)». На ее изучение отводится 108 часов (18 часа аудиторной работы, 90 часов СР). Согласно учебному плану направления и профиля подготовки данный курс в первом семестре и заканчивается зачетом.

В качестве предварительной основы для этого курса необходимо знание абстрактной алгебры, теории конечных полей и теории многочленов над конечными полями, что является важным в теории кодирования и теории защиты информации.

Этот курс тесно связан с теорией конечных полей, арифметики над конечными полями, построения многочленов над конечными полями, нахождение взаимосвязи структур конечных полей. Является курсом, служащим основой для написания выпускных магистерских работ.

3. Результаты обучения по дисциплине.

Код и наименование компетенции	Код и наименование индикатора (индикаторов) достижения компетенции	Результаты обучения
ОПК-2 Способен создавать и исследовать новые математические модели в естественных науках, совершенствовать и разрабатывать концепции, теории и методы	**1.1_М.ОПК-2.** Создает и исследует новые математические модели в естественных науках	**Знать:** – основные модели теории многочленов над конечными полями; **Уметь:** – применять основные модели теории многочленов над конечными полями к исследованиям математических моделей. **Владеть:** – навыками создания и исследования новых математических моделей при помощи моделей теории многочленов над конечными полями.
	2.1_М.ОПК-2. Используя методы математического моделирования, находит эффективные решения	**Знать:** – основные методы математического моделирования, основанные на моделях теории

	научных и прикладных задач.	многочленов над конечными полями. **Уметь:** – использовать основные методы математического моделирования, основанные на моделях теории многочленов над конечными полями для нахождения эффективных решений научных и прикладных задач. **Владеть:** – методами математического моделирования, основанными на моделях теории многочленов над конечными полями для нахождения эффективных решений научных и прикладных задач.
	3.1_М.ОПК-2. Совершенствует и разрабатывает методы математического моделирования, оценивает пригодность модели, ее соответствие практике.	**Знать:** – методы математического моделирования, основанные на методах и моделях теории многочленов над конечными полями. **Уметь:** – совершенствовать и разрабатывать методы математического моделирования, основанные на методах и моделях теории многочленов над конечными полями, оценивать ее пригодность и соответствие практике. **Владеть:** – навыками оценивания пригодности и соответствия практике моделей, основанных на методах теории многочленов над конечными полями.
ПК-1 Способен демонстрировать фундаментальные знания математических и естественных наук, программирования и информационных технологий	**1.1_М.ПК-1.** Понимает основные концепции, принципы, теории и факты, в области математических и (или) естественных наук, программирования и информационных технологий	**Знать:** – основные концепции, принципы, теории и факты, в области математических и (или) естественных наук, программирования и информационных технологий, основанные на

		методах и моделях теории многочленов над конечными полями. **Уметь:** – Понимать основные концепции, принципы, теории и факты, в области математических и (или) естественных наук, программирования и информационных технологий, связанные с моделями теории многочленов над конечными полями. **Владеть:** – основными концепции, принципами, основами теории и фактами, в области математических и (или) естественных наук, программирования и информационных технологий, связанными с теорией многочленов над конечными полями.
	2.1_М.ПК-1. Формулирует и решает стандартные задачи в собственной научно- исследовательской деятельности	**Знать:** – основные методы решения стандартных задач, связанных с моделями и методами из теории многочленов над конечными полями. **Уметь:** – применять модели и методы из теории многочленов над конечными полями при формулировании и решении стандартных задач в собственной научно-исследовательской деятельности. **Владеть:** – навыками формулирования и решения стандартных задач, связанных с моделями и методами из теории многочленов над конечными полями в собственной научно- исследовательской

		деятельности
	3.1_М.ПК-1. Проводит научно-исследовательские работы в области математики и компьютерных наук	**Знать:** – основные методы проведения научно-исследовательские работы в области математики и компьютерных наук, основанные на моделях и методах теории многочленов над конечными полями. **Уметь:** – проводить научно-исследовательские работы в области математики и компьютерных наук, основанные на моделях и методах теории многочленов над конечными полями. **Владеть:** – навыками проведения научно-исследовательских работ в области математики и компьютерных наук, основанные на моделях и методах теории многочленов над конечными полями.

4. Структура и содержание дисциплины.

Общая трудоемкость дисциплины составляет 3 зачетных единиц 108 часов.

№ п/п	Раздел дисциплины	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)				Формы текущего контроля успеваемости *(по неделям семестра)* Формы промежуточной аттестации *(по семестрам)*
				Лек.	Пр.	СРС	КСР	
1	Структура конечных полей	1	1-7		6	20		Консультация, опрос
2	Порядок многочленов над конечными полями	1	8-10		4	20		Консультация, опрос
3	Неприводимые над конечными полями многочлены	1	11-13		4	25		Консультация, опрос
4	Построение неприводимых многочленов над конечными полями	1	14-18		4	25		*Контрольная работа*

	Промежуточная аттестация	**1**						**Зачет**
	Итого за 1 семестр				**18**	**90**		
	Общая трудоемкость дисциплины			**108**				

1. Структура конечных полей.

Характеристики конечных полей и их простые подполя. Порядки конечных полей. Критерий расширения для конечных полей. Нормальность и сепарабельность расширений конечных полей. Критерий подполя. Цикличность мультипликативной группы конечного поля. Примитивный элемент конечного поля. Количество примитивных элементов конечного поля. Существование неприводимых многочленов любой положительной степени над любым конечным полем. Автоморфизм Фробениуса. Группа Галуа расширения конечного поля. Корни неприводимых многочленов над конечным полем. Поля разложений неприводимых многочленов. Порядки сопряженных элементов в мультипликативной группе поля. Следы и нормы элементов расширений конечных полей и их свойства. Характеристические многочлены элементов расширений. Круговые поля и круговые многочлены. Конечные поля как круговые расширения. Три способа представлений элементов конечных полей

2. Порядок многочленов над конечными полями.

Порядок многочленов со свободным членом. Теорема о порядке многочлена и ее следствие для неприводимых многочленов. Теорема о числе неприводимых многочленов данной степени и данного порядка. Формула для порядков многочленов, разложенных в произведение.

3. Неприводимые над конечными полями многочлены.

Теорема о произведении всех неприводимых многочленов данной степени, делящей натуральное число n. Соотношение для количеств неприводимых многочленов. Функция Мебиуса. Сумма значений функций Мебиуса. Формула обращения Мебиуса. Формула для числа нормированных неприводимых многочленов данной степени над конечным полем. Формула для круговых многочленов. Теорема о произведении всех нормированных неприводимых многочленов данной степени над данным полем.

4. Построение неприводимых многочленов над конечными полями.

Теоретико-числовая вспомогательная лемма. Формулы о построении новых неприводимых многочленов по набору заданных неприводимых многочленов. Нахождение минимальных многочленов с помощью характеристических многочленов. Способ построения характеристических многочленов. Прямые способы построения минимальных многочленов. Критерий сохранения неприводимости многочлена при расширении поля коэффициентов.

5. Образовательные технологии, применяемые при освоении дисциплины

При проведении лекционных и практических занятий предусматривается использование информационных технологий, включающих пакеты стандартных

статистических программ: Statistica, SPSS и др. Использование информационных технологий осуществляется, в частности, в процессе реализации активных и интерактивных форм проведения занятий.

При чтении лекций в качестве материала, иллюстрирующего возможности математического моделирования в различных ситуациях, активно используются примеры из практики обработки данных в процессе исследований в предметной области. Информационные и интерактивные технологии используются при обсуждении проблемных и неоднозначных вопросов, требующих выработки решения в ситуации неопределенности.

Удельный вес занятий, проводимых в интерактивных формах, определяется главной целью (миссией) программы, особенностью контингента обучающихся и содержанием конкретных дисциплин, и в целом в учебном процессе они должны составлять не менее 30 % аудиторных занятий.

Практическая подготовка осуществляется путем проведения лабораторных занятий, предусматривающих участие обучающихся в выполнение отдельных элементов работ, связанных с будущей профессиональной деятельностью. По результатам практической подготовки обучающиеся сдают отчет.

По курсу «Алгебраические приложения в компьютерных науках» обучающиеся формируют первичные профессиональные умения и навыки по обработке и анализу научной информации и результатов исследований.

При проведении практической подготовки студенты решают задачи, направленные на формирование исследовательских умений и навыков. Прохождение практики будет способствовать повышению уровня логической культуры обучающихся, научит аргументировано рассуждать и доказывать, что позволит им более осознанно и эффективно осваивать все последующие математические дисциплины, формировать профессиональные компетенции.

Особенности проведения занятий для инвалидов и граждан с ОВЗ

При обучении лиц с ограниченными возможностями используются подходы, способствующие созданию безбарьерной образовательной среды: технологии дифференциации и индивидуализации обучения, применение соответствующих методик по работе с инвалидами, использование средств дистанционного общения.

Для студентов с ограниченными возможностями здоровья предусмотрены следующие формы организации учебного процесса и контроля знаний:

-*для слабовидящих:*

обеспечивается индивидуальное равномерное освещение не менее 300 люкс;

для выполнения контрольных заданий при необходимости предоставляется увеличивающее устройство;

задания для выполнения, а также инструкция о порядке выполнения контрольных заданий оформляются увеличенным шрифтом (размер 16-20);

- *для глухих и слабослышащих:*

обеспечивается наличие звукоусиливающей аппаратуры коллективного пользования, при необходимости студентам предоставляется звукоусиливающая аппаратура индивидуального пользования;

- *для лиц с тяжелыми нарушениями речи, глухих, слабослышащих* все контрольные задания по желанию студентов могут проводиться в письменной форме.

Основной формой организации учебного процесса является интегрированное обучение инвалидов, т.е. все студенты обучаются в смешанных группах, имеют возможность постоянно общаться со сверстниками, легче адаптируются в социуме.

6. Учебно-методическое обеспечение самостоятельной работы студентов. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины.

Самостоятельная работа студентов предполагает индивидуальную работу с учебно-методической литературой: учебниками, задачниками, конспектами лекций, методическими пособиями. Консультации лектора помогают усвоению материала. Контроль за успеваемостью осуществляется в форме бесед учебного и творческого характера, опроса, индивидуальных заданий, контрольных работ, коллоквиумов.

Часть самостоятельных занятий посвящена выполнению домашних заданий и подготовке к семинарам, докладам, обсуждениям, дискуссиям. Проверка домашних заданий проводится на практических занятиях.

Пример контрольной работы

Вариант1.

1. Пусть задан многочлен $f(x) = x^2 + 1 \in F_3[x]$. Сопровождающая матрица для него имеет вид $A = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}$. Найти представления поля F_9.

2. Разложить многочлен $x^7 + x^6 + x^5 - x^3 + x^2 - x - 1$ над полем F_3.

Вариант 2.

1. Пусть задан многочлен $f(x) = x^2 + 1 \in F_3[x]$. Сопровождающая матрица для него имеет вид $A = \begin{pmatrix} 0 & 2 \\ -1 & 0 \end{pmatrix}$. Найти представления поля F_9.

2. Разложить многочлен $x^{12} + x^7 + x^5 + x^4 + x^3 + x^2 + 1$ над полем F_2.

Контрольные вопросы готовятся к каждому разделу.

Примерный перечень вопросов по дисциплине.

1. Характеристика конечного поля.
2. Порядок конечных полей.
3. Нормальность и сепарабельность расширений конечных полей.
4. Цикличность мультипликативной группы конечного поля.
5. Примитивный элемент конечного поля.
6. Неприводимые многочлены над любым конечным полем.
7. Автоморфизм Фробениуса.
8. Группа Галуа расширения конечного поля.
9. Поля разложений неприводимых многочленов.

10. Следы и нормы элементов расширений конечных полей и их свойства.

11. Характеристические многочлены элементов расширений.

12. Круговые поля и круговые многочлены.

13. Порядок многочленов со свободным членом.

14. Теорема о порядке многочлена и ее следствие для неприводимых многочленов.

15. Теорема о числе неприводимых многочленов данной степени и данного порядка.

16. Формула для порядков многочленов, разложенных в произведение.

17. Теорема о произведении всех неприводимых многочленов данной степени, делящей натуральное число n.

18. Функция Мебиуса. Сумма значений функций Мебиуса. Формула обращения Мебиуса.

19. Формула для числа нормированных неприводимых многочленов данной степени над конечным полем.

20. Формула для круговых многочленов.

21. Теорема о произведении всех нормированных неприводимых многочленов данной степени над данным полем.

7. Данные для учета успеваемости студентов в БАРС

Таблица 1.1 Таблица максимальных баллов по видам учебной деятельности.

1	2	3	4	5	6	7	8	9
Семестр	Лекции	Лабораторные занятия	Практические занятия	Самостоятельная работа	Автоматизированное тестирование	Другие виды учебной деятельности	Промежуточная аттестация	Итого
1	0	0	20	10	0	30	40	**100**

Программа оценивания учебной деятельности студента

1 семестр

Лекции

Не предусмотрены.

Лабораторные занятия

Не предусмотрены.

Практические занятия - от 0 до 20 баллов

Самостоятельность и правильность при выполнении работы – от 0 до 10 баллов, активность работы в аудитории – от 0 до 5 баллов, уровень подготовки к занятиям – от 0 до 5 баллов.

Самостоятельная работа - от 0 до 10 баллов

Контроль качества и количества выполненных домашних работ – от 0 до 5 баллов, правильность выполнения – от 0 до 5 баллов.

Автоматизированное тестирование

Не предусмотрено.

Другие виды учебной деятельности - от 0 до 30 баллов

Контрольная работа – от 0 до 30 баллов.

Промежуточная аттестация - от 0 до 40 баллов

при проведении промежуточной аттестации
ответ на «зачтено» оценивается от 16 до 40 баллов;
ответ на «не зачтено» оценивается от 0 до 15 баллов;

Таким образом, максимально возможная сумма баллов за все виды учебной деятельности студента по дисциплине «Алгебраические приложения в компьютерных науках» составляет 100 баллов.

Таблица 2.1 Таблица пересчета полученной студентом суммы баллов по дисциплине «Алгебраические приложения в компьютерных науках» в оценку (зачет):

60 – 100 баллов	«зачтено»
0 – 59 баллов	«не зачтено»

8. Учебно-методическое и информационное обеспечение дисциплины.

На кафедре имеется достаточное количество методических указаний для выполнения индивидуальных заданий.

Имеются экзаменационные билеты для проведения экзамена в каждом семестре.

В библиотеке СГУ имеется достаточное количество учебников, которые рекомендованы в качестве основной и дополнительной литературы.

а) литература:

1. *Виноградов, И.М. Основы теории чисел/ И.М. Виноградов. -Москва: Лань, 2009.-176с.*
2. *Курош, А.Г. Курс высшей алгебры [Электронный ресурс] : учеб. / А.Г. Курош. - Москва: Лань, 2024. - 431 с.* Книга находится в ЭБС "ЛАНЬ"
3. *Лидл Р., Нидеррайтер Г.* Конечные поля. Т.1. - М.: Мир, 1988.
4. *Лидл Р., Нидеррайтер Г.* Конечные поля. Т.2. - М.: Мир, 1988.
5. *Ленг С.* Алгебра – М: Мир, 1968

б) программное обеспечение и Интернет-ресурсы:

Лицензионное программное обеспечение:

1. Операционная система Windows 7, или более поздняя версия
2. Microsoft Office PowerPoint

Интернет-ресурсы:

1. Саратовской государственный университет им. Н.Г. Чернышевского. – Режим доступа: www.sgu.ru/
2. Зональная научная библиотека им. В.А. Артисевич Саратовского государственного университета им. Н.Г. Чернышевского. – Режим доступа: http://library.sgu.ru/
3. Каталог образовательных Интернет-ресурсов. – Режим доступа: http://window.edu.ru/

9. Материально-техническое обеспечение дисциплины

Учебная аудитория с обязательным наличием специализированной доски, мела (маркера), проектора, с возможностью размещения всех обучающихся по данной дисциплине.

Программа составлена в соответствии с требованиями ФГОС по направлению 02.04.01 «Математика и компьютерные науки» и профилю подготовки «Математические основы компьютерных наук».

Автор доцент, к.ф.-м.н., доцент кафедры КАиТЧ В.В. Кривобок

Программа одобрена на заседании кафедры компьютерной алгебры и теории чисел от 2 сентября 2024 года, протокол № 2.