

МИНОБРНАУКИ РОССИИ
Ярославский государственный университет им. П.Г. Демидова

Кафедра алгебры и математической логики

УТВЕРЖДАЮ

Декан математического факультета

Нестеров П.Н.

21 мая 2024 г.

Рабочая программа дисциплины
Вычислительные методы в алгебре и теории чисел

Направление подготовки (специальности)
02.04.01 Математика и компьютерные науки

Направленность (профиль)
«Компьютерная математика»

Форма обучения очная

Программа рассмотрена
на заседании кафедры
от 12.04.2024, протокол № 8

Программа одобрена НМК
математического факультета
протокол № 9 от 03.05.2024

1. Цели освоения дисциплины

Целями освоения дисциплины «Вычислительные методы в алгебре и теории чисел» являются: овладение основными вычислительными методами классической и современной алгебры и теории чисел; освоение основных методов разработки алгоритмов для решения задач, возникающих в алгебре, теории чисел и в криптографии; обеспечение подготовки в одной из важных областей применения алгебраических и теоретико-числовых алгоритмов для решения задач, возникающих в различных приложениях.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Вычислительные методы в алгебре и теории чисел» относится к части образовательной программы, формируемой участниками образовательных отношений, и является элективной дисциплиной. Для ее успешного изучения необходимы знания, умения и навыки, приобретенные в ходе изучения таких базовых и специальных курсов, как «Теория чисел», «Алгебра», «Фундаментальные алгебраические структуры», «Алгебраическая алгоритмика», «Криптография». Эта дисциплина закладывает знание основных методов и алгоритмов, используемых в криптографии и других приложениях.

3. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы

Процесс изучения дисциплины направлен на формирование следующих компетенций в соответствии с ФГОС ВО, ООП ВО и приобретение следующих знаний, умений, навыков и (или) опыта деятельности:

Формируемая компетенция (код и формулировка)	Индикатор достижения компетенции (код и формулировка)	Перечень планируемых результатов обучения
Профессиональные компетенции		
ПК-1 Способен создавать и исследовать новые математические модели в естественных науках, промышленности и бизнесе, с учетом возможностей современных информационных технологий, программирования и компьютерной техники	И-ПК-1.1 Способен построить математическую модель, учитывая основные этапы построения, формулирует требования к ней.	Уметь: использовать изученные методы для решения алгебраических и теоретико-числовых задач.
	И-ПК-1.2 Исследует новые математические модели в естественных науках, промышленности и бизнесе, с учетом возможностей современных информационных технологий и программирования и компьютерной техники.	Владеть: основными методами работы и алгоритмами решения задач, возникающих в приложениях.
	И-ПК-1.3 Обладает фундаментальными знаниями, полученными в области математического моделирования.	Знать: основные проблемы, возникающие в алгебре, теории чисел и основные подходы к их решению.

4. Объем, структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 4 зачетных единицы, 144 акад. часов.

№ п/п	Темы (разделы) дисциплины, их содержание	Семестр	Виды учебных занятий, включая самостоятельную работу студентов, и их трудоемкость (в академических часах)						Формы текущего контроля успеваемости Форма промежуточной аттестации (по семестрам)
			Контактная работа					самостоятельная работа	
			лекции	практические	лабораторные	консультации	аттестационные испытания		
1	Наибольший общий делитель чисел и многочленов		3	2				18	Задачи для самостоятельной работы
2	Разложение многочленов на множители над кольцом целых чисел		3	7		2		18	Задачи для самостоятельной работы Домашняя контрольная работа №1
3	Разложение многочлена на множители над конечным полем		4	7		2		12	Задачи для самостоятельной работы
4	Проверка чисел на простоту		3					12	Задачи для самостоятельной работы Домашняя контрольная работа №2
5	Алгоритмы факторизации целых чисел		3					12	Задачи для самостоятельной работы
						2	0,5	33,5	экзамен
	ИТОГО		16	16		6	0.5	105.5	

Содержание разделов дисциплины:

Тема 1. Наибольший общий делитель чисел и многочленов.

Деление многочленов и метод Гаусса. Алгоритм Доджсона. Лемма Лейдекера. Теорема Лейдекера. Расширенный алгоритм Евклида для чисел. Расширенный алгоритм Евклида для многочленов над полем. Алгоритм Евклида и псевдоделение, нахождение наибольшего общего делителя многочленов над кольцом.

Тема 2. Разложение многочленов на множители над кольцом целых чисел.

Модулярный алгоритм нахождения наибольшего общего делителя многочленов. Метод Кронекера - Шуберта.

Тема 3. Разложение многочлена на множители над конечным полем.

Разложение многочлена на неприводимые множители над полем Галуа. Разложение на свободные от квадратов множители над конечным полем. Теорема о производной многочлена над конечным полем. Необходимые и достаточные условия обращения производной в нуль над конечным полем. Алгоритм Кантора и Цассенхауза. Вероятностная оценка нахождения нетривиального сомножителя многочлена над конечным полем. Алгоритм Берлекэмп

разложения многочлена над конечным полем. Подъём разложения в конечном поле до разложения в кольце целых чисел. Алгоритм линейного подъёма Гензеля.

Тема 4. Проверка чисел на простоту.

Решето Эратосфена. Теорема Вильсона. Тест на основе малой теоремы Ферма. Псевдопростые числа и числа Кармайкла. Тест Соловея - Штрассена. Эйлеровы псевдопростые числа. Сильно псевдопростые числа. Тест Рабина - Миллера.

Тема 5. Алгоритмы факторизации целых чисел.

Метод Полларда. Факторизация Ферма. Алгоритм Диксона. $(p-1)$ -метод факторизации Полларда.

5. Образовательные технологии, в том числе технологии электронного обучения и дистанционные образовательные технологии, используемые при осуществлении образовательного процесса по дисциплине

В процессе обучения используются следующие образовательные технологии:

Академическая лекция с элементами лекции-беседы – последовательное изложение материала, осуществляемое преимущественно в виде монолога преподавателя. Требования к академической лекции: современный научный уровень и насыщенная информативность, убедительная аргументация, доступная и понятная речь, четкая структура и логика, наличие ярких примеров, научных доказательств, обоснований, фактов.

Элементы лекции-беседы обеспечивают контакт преподавателя с аудиторией, что позволяет привлекать внимание студентов к наиболее важным темам дисциплины, активно вовлекать их в учебный процесс, контролировать темп изложения учебного материала в зависимости от уровня его восприятия.

Практическое занятие – занятие, посвященное освоению конкретных умений и навыков по закреплению полученных на лекции знаний.

Консультации – вид учебных занятий, являющийся одной из форм контроля самостоятельной работы студентов. На консультациях по просьбе студентов рассматриваются наиболее сложные моменты при освоении материала дисциплины, преподаватель отвечает на вопросы студентов, которые возникают у них в процессе самостоятельной работы.

6. Перечень лицензионного и (или) свободно распространяемого программного обеспечения, используемого при осуществлении образовательного процесса по дисциплине

В процессе осуществления образовательного процесса по дисциплине используются: для формирования материалов для текущего контроля успеваемости и проведения промежуточной аттестации, для формирования методических материалов по дисциплине:

- программы Microsoft Office;
- издательская система LaTeX;
- Adobe Acrobat Reader.

7. Перечень современных профессиональных баз данных и информационных справочных систем, используемых при осуществлении образовательного процесса по дисциплине (при необходимости)

В процессе осуществления образовательного процесса по дисциплине используются:

- Автоматизированная библиотечно-информационная система «БУКИ-NEXT»

http://www.lib.uniyar.ac.ru/opac/bk_cat_find.php

- Электронная библиотечная система «Лань» <https://e.lanbook.com>
- Электронная библиотечная система «Юрайт» <https://urait.ru>
- Электронная библиотечная система «Консультант студента»
<https://www.studentlibrary.ru>

8. Перечень основной и дополнительной учебной литературы, ресурсов информационно-телекоммуникационной сети «Интернет» (при необходимости), рекомендуемых для освоения дисциплины

а) основная литература

1. Яблокова С.И. Основы алгебраической алгоритмики. Ч.1 - Ярославль, 2008.
<http://www.lib.uniyar.ac.ru/edocs/iuni/20080290.pdf>
2. Яблокова С.И. Основы алгебраической алгоритмики. Ч.2 - Ярославль, 2009.
<http://www.lib.uniyar.ac.ru/edocs/iuni/20090237.pdf>

б) дополнительная литература

1. Берлекэмп Э. Алгебраическая теория кодирования. – М.: Мир, 1971.
2. Биркгоф Г. Современная прикладная алгебра. / Г. Биркгоф, Т. К. Бартти; пер. с англ. Ю. И. Манина - 2-е изд., стереотип. - СПб.: Лань, 2005. - 400 с.
3. Дэвенпорт Д., Сирэ И., Турнье Э. Компьютерная алгебра. - М.: Мир, 1991.
4. Ноден П., Китте К. Алгебраическая алгоритмика. – М.: Мир, 1999.
5. Акритас А. Основы компьютерной алгебры с приложениями. – М.: Мир, 1994.

в) ресурсы сети Интернет

1. Глава 7. Криптосистемы с открытыми ключами. Глава 8. Тестирование чисел на простоту и выбор параметров rsa: <https://studfile.net/preview/5367570/>
2. Лекция 8: Разложение многочленов на неприводимые множители по модулю p. Лемма Гензеля: <https://intuit.ru/studies/curriculums/15814/courses/196/lecture/5102>
3. Тест простоты Миллера-Рабина: <https://foxford.ru/wiki/informatika/test-prostoty-millera-rabina>

9. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине включает в свой состав специальные помещения:

- учебные аудитории для проведения занятий лекционного типа;
- учебные аудитории для проведения практических занятий (семинаров);
- учебные аудитории для проведения групповых и индивидуальных консультаций;
- учебные аудитории для проведения текущего контроля и промежуточной аттестации;
- помещения для самостоятельной работы;
- помещения для хранения и профилактического обслуживания технических средств обучения.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде ЯрГУ.

Автор(ы):

Профессор кафедры алгебры и математической логики, д.ф.-м.н

Н.В. Тимофеева

**Приложение № 1 к рабочей программе дисциплины
«Вычислительные методы в алгебре и теории чисел»**

**Фонд оценочных средств
для проведения текущего контроля успеваемости
и промежуточной аттестации студентов
по дисциплине**

**1. Типовые контрольные задания и иные материалы,
используемые в процессе текущего контроля успеваемости**

Задачи для самостоятельной работы (И-ПК-1.1, И-ПК-1.2)

1. Найти наибольший общий делитель чисел $a=126$ и $b=39$ и коэффициенты Безу, т. е. представить НОД в виде : $\text{НОД}(a, b) = au + bv$.
2. Найти наибольший общий делитель многочленов в $\mathbb{Z}_7[x]$
 $f(x) = x^4 + 4x^3 + 6x^2 + 5x + 2$ и $g(x) = x^3 + 5x^2 + 2x + 6$.
Представить его в виде $\text{НОД}(f(x), g(x)) = f(x)u(x) + g(x)v(x)$.
3. Найти целочисленные решения уравнения $185x + 74y = 111$.
4. Найти наибольший общий делитель многочленов
 $f(x) = 6x^5 - 6x^4 - 18x^2 - 6x - 12$ и $g(x) = 3x^4 - 15x^2 + 12$
над кольцом целых чисел, используя псевдоделение.
5. Используя модулярный алгоритм, найти наибольший общий делитель многочленов
 $f(x) = 9x^5 + 6x^4 + 3x^3 + 3x^2 + 2x + 1$ и $g(x) = 3x^4 + 5x^3 + 6x^2 + 3x + 1$
над кольцом целых чисел.
6. Используя метод Кронекера - Шуберта, разложить многочлен с целыми коэффициентами на множители
 $f(x) = x^4 + 3x^3 + 5x^2 + 4x + 2$
7. Разложить на свободные от квадратов множители многочлен
 $f(x) = x^{14} + x^{13} + x^{12} + x^{10} + x^8 + x^7 + x^6 + x^4$
в кольце $\mathbb{Z}_2[x]$.
8. Используя алгоритм Берлекэмпса, в кольце $\mathbb{Z}_{13}[x]$ разложить многочлен
 $f(x) = 5x^4 + 5x^3 + 11x^2 + 9$
на неприводимые множители.
9. Разложить на неприводимые множители многочлен $f(x) = x^{64} - x$
в кольце $\mathbb{Z}_2[x]$.
10. Является ли число 2047 по основанию 2 : а) псевдопростым? б) эйлеровым псевдопростым? в) сильно псевдопростым?
11. Найти все основания a , по которым число 63 является псевдопростым.
12. Является ли 2 примитивным элементом по модулю 239? Найти порядок элемента 2 в мультипликативной группе кольца \mathbb{Z}_{239} .
13. Является ли число 2465 числом Кармайкла? Ответ обосновать.

Домашняя контрольная работа № 1 (И-ПК-1.1, И-ПК-1.2)

1. Реализовав расширенный алгоритм Евклида в кольце целых чисел, найдите $\text{НОД}(745, 320)$ и его линейное выражение.
2. Решите в целых числах уравнение $188x + 208y = 16$.
3. Реализовав расширенный алгоритм Евклида над полем \mathbb{Z}_7 , найдите $\text{НОД}(x^3 + 6x^2 + 5x + 2, x^4 + x^3 + 5x^2 + 5x)$.

4. Используя псевдоделение, найдите НОД многочленов над кольцом целых чисел:
 $f(x) = 3x^3 + 9x^2 + 3x - 3$, $g(x) = 3x^4 + 3x^3 - 6x - 6$.

Домашняя контрольная работа № 2 (ИД-ПК-1.1, ИД-ПК-1.2)

1. Используя модулярный алгоритм, вычислите НОД многочленов
 $f(x) = x^4 + 7x^3 + 9x^2 + x - 2$, $g(x) = x^4 + 2x^3 - 3x^2 - 8x - 4$.
2. Методом Кронеккера --- Шуберта разложите на множители многочлен
 $f(x) = x^4 + 2x^3 + 4x^2 + 2x + 3$.

Замечание. Интерполяционные формулы Лагранжа предназначены для вычислений над полем; поэтому интерполяционные вычисления следует проводить в поле частных кольца Z , т.е. в поле рациональных чисел. Необходимо, чтобы искомым полином-делитель имел целочисленные коэффициенты. Полином-делитель с нецелыми коэффициентами не годится, т.к. необходимо найти разложение над кольцом целых чисел.

3. Методом Берлекэмпа разложите на множители многочлен над полем Z_3 (считайте известным, что он свободен от квадратов): $f(x) = 2x^3 + 2x^2 + 2$.

2. Список вопросов и (или) заданий для проведения промежуточной аттестации

Вопросы к экзамену (И-ПК-1.3)

1. Деление многочленов и метод Гаусса. Алгоритм Доджсона.
2. Лемма Лейдекера. Теорема Лейдекера.
3. Расширенный алгоритм Евклида для чисел.
4. Расширенный алгоритм Евклида для многочленов над полем.
5. Алгоритм Евклида и псевдоделение, нахождение наибольшего общего делителя многочленов над кольцом
6. Модулярный алгоритм нахождение наибольшего общего делителя многочленов.
7. Метод Кронекера - Шуберта.
8. Разложение многочлена на неприводимые множители над полем Галуа.
9. Разложение на свободные от квадратов множители над конечным полем. Теорема о производной многочлена над конечным полем.
10. Необходимые и достаточные условия обращения производной в нуль над конечным полем. Алгоритм Кантора и Цассенхауза.
11. Вероятностная оценка нахождения нетривиального сомножителя многочлена над конечным полем.
12. Алгоритм Берлекэмпа разложения многочлена над конечным полем.
13. Подъём разложения в конечном поле до разложения в кольце целых чисел. Алгоритм линейного подъёма Гензеля.
14. Проверка чисел на простоту. Решето Эратосфена. Теорема Вильсона. Тест на основе малой теоремы Ферма. Псевдопростые числа и числа Кармайкла.
15. Тест Соловея - Штрассена. Эйлеровы псевдопростые числа.
16. Сильно псевдопростые числа. Тест Рабина - Миллера.
17. Алгоритмы факторизации целых чисел. Метод Полларда.
18. Алгоритм Диксона.
19. Метод факторизации Ферма.
20. (p-1)-метод факторизации Полларда.

Приложение № 2 к рабочей программе дисциплины «Вычислительные методы в алгебре и теории чисел»

Методические указания для студентов по освоению дисциплины

Основной формой изложения учебного материала по дисциплине «Вычислительные методы в алгебре и теории чисел» являются лекции. По большинству тем предусмотрены практические занятия, на которых происходит закрепление лекционного материала путем применения его к конкретным задачам.

Для успешного освоения дисциплины очень важно решение задач, как в аудитории, так и самостоятельно в качестве домашних заданий. Примеры решения задач разбираются на лекциях и практических занятиях. Большое внимание должно быть уделено выполнению домашней работы.

Для успешного усвоения данного курса необходимо знание следующих вопросов из других математических дисциплин:

- сравнения по модулю целого числа, свойства сравнений;
- функция Эйлера и ее основные свойства;
- теорема Эйлера и малая теорема Ферма;
- кольцо и поле вычетов по модулю натурального числа;
- мультипликативная группа кольца вычетов;
- строение мультипликативных групп колец вычетов по модулю простого числа, по модулю степени простого числа и по модулю степени двойки;
- алгоритм Евклида для чисел и многочленов над полем;
- понятие примитивного элемента поля Гауа;
- понятие минимального многочлена алгебраического над полем элемента.

Экзамен принимается по экзаменационным билетам. На самостоятельную подготовку к экзамену выделяется 3 дня, во время подготовки к экзамену предусмотрена групповая консультация.