МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
Факультет математики и компьютерных наук

УТВЕРЖДАЮ:
Проректор по учебной работе,
качеству образования – первый
проректор
_____ Т.А. Хагуров
подпись
«26» мая 2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.О.13 ДОПОЛНИТЕЛЬНЫЕ ГЛАВЫ ФУНДАМЕНТАЛЬНОЙ МАТЕМАТИКИ

Направление подготовки 01.04.01 Математика

Направленность (профиль) Алгебраические методы защиты информации

Преподавание математики и информатики

Форма обучения очная

Квалификация магистр

Краснодар 2023

Рабочая программа дисциплины Дополнительные главы фундаментальной математики
составлена в соответствии с федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по направлению подготовки / специальности
01.04.01 Математика Алгебраические методы защиты информации
код и наименование направления подготовки

Программу составил(и):
А.В. Рожков, профессор, д.ф.-м.н., профессор
И.О. Фамилия, должность, ученая степень, ученое звание _____ подпись

Рабочая программа дисциплины Дополнительные главы фундаментальной математики
утверждена на заседании кафедры функционального анализа и алгебры
протокол № 8 «18» апреля 2023 г.
Заведующий кафедрой функционального анализа и алгебры
Барсукова В.Ю. _____
фамилия, инициалы подпись

Утверждена на заседании учебно-методической комиссии факультета/института математики и компьютерных наук
протокол № 8 «27» апреля 2023 г.
Председатель УМК факультета/института Шмалько С.П. _____
фамилия, инициалы подпись

Рецензенты:
Чубырь Н.О., кандидат физико-математических наук, доцент, доцент кафедры прикладной математики КубГТУ
Лазарев В.А., доктор педагогических наук, профессор, заведующий кафедрой теории функций КубГУ

2

1 Цели и задачи изучения дисциплины

1.1 Цель дисциплины

Целями освоения дисциплины «Дополнительные главы фундаментальной математики» являются формирование математической культуры студентов; формирование способностей к алгоритмическому и логическому мышлению, овладение современным аппаратом алгоритмической математики, освоение приложений теории алгоритмов алгебры в различных областях математики, информатики и защиты информации; творческое овладение основными методами теории алгебраических вычислений.

1.2 Задачи дисциплины

Дать студентам знания о различных подходах к построению алгебраических и теоретико-числовых алгоритмов, об основных понятиях теории колец и теории чисел. Ознакомить студентов современными математическими методами в фундаментальных и прикладных задачах анализа и применения алгоритмов.

1.3 Место дисциплины в структуре образовательной программы

Дисциплина «Дополнительные главы фундаментальной математики» включена в обязательную часть Блока 1. Дисциплины и модули. и является обязательной дисциплиной Б1.О.13.

Для успешного освоения дисциплины обучающийся должен владеть знаниями, умениями и навыками по программе дисциплин «Алгебра», «Теория алгоритмов». Дисциплина изучается в 4 семестре.

1.4 Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

Изучение данной учебной дисциплины направлено на формирование у обучающихся следующих компетенций:

Код и наименование индикатора* достижения компетенции	Результаты обучения по дисциплине (знает, умеет, владеет (навыки и/или опыт деятельности))
ОПК-2 Способен строить и анализировать математические модели в современном естествознании, технике, экономике и управлении	
ОПК-2.1 Знает математические модели стандартных задач в области профессиональной деятельности ОПК-2.2 Выбирает необходимые методы исследования, модифицирует существующие и разрабатывает новые методы, исходя из задач конкретного исследования ОПК-2.3 Применяет полученные результаты, представляет итоги проделанной работы	Знать: о целях, задачах, принципах и основных направлениях обеспечения информационной безопасности государства; о методологии создания систем защиты информации; Уметь: выбирать и анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации; пользоваться современной научно-технической информацией по исследуемым проблемам и задачам; Владеть: анализом информационной инфраструктуры государства; формальной постановкой и решением задачи обеспечения информационной безопасности компьютерных систем.
ПК-1 Способен формулировать и решать актуальные и значимые задачи фундаментальной и прикладной математики	

Код и наименование индикатора* достижения компетенции	Результаты обучения по дисциплине (знает, умеет, владеет (навыки и/или опыт деятельности))
ПК-1.1 Знает основные понятия, идеи и методы фундаментальных математических дисциплин для решения базовых задач ПК-1.2 Умеет передавать результаты проведенных теоретических и прикладных исследований в виде конкретных предметных рекомендаций в терминах предметной области ПК-1.3 Самостоятельно и корректно решает стандартные задачи фундаментальной и прикладной математики ПК-1.4 Имеет навыки решения математических задач, соответствующих квалификации, возникающих при проведении научных и прикладных исследований	Знать: О компьютерной реализации информационных объектов. Связи компьютерной алгебры и численного анализа Уметь: Применять основные математические методы, используемые в анализе типовых алгоритмов Владеть навыками: использования библиотеки алгоритмов и пакетов расширения; поиска и использования современной научно-технической литературой в области символьных вычислений.

Результаты обучения по дисциплине достигаются в рамках осуществления всех видов контактной и самостоятельной работы обучающихся в соответствии с утвержденным учебным планом.

Индикаторы достижения компетенций считаются сформированными при достижении соответствующих им результатов обучения.

2. Структура и содержание дисциплины

2.1 Распределение трудоёмкости дисциплины по видам работ

Изучение курса «Дополнительные главы фундаментальной математики» рассчитано на 1 семестр. Общая трудоемкость дисциплины составляет 3 зачетных единицы, 108 академических часа (из них 24,3 контактных). Программой дисциплины предусмотрены 8 часов лекционных занятий, 16 часов практических занятий, а также 57 часов самостоятельной работы, 26,7 часов отводится на подготовку к экзамену.

Вид учебной работы	Всего часов	Семестры
		4
Контактная работа, в том числе:		
Аудиторные занятия (всего)	**24**	**24**
В том числе:		
Занятия лекционного типа	8	8
Занятия семинарского типа (семинары, практические занятия)	16	16
Иная контактная работа:		
Промежуточная аттестация (ИКР)	0,3	0,3
Самостоятельная работа (всего)	**57**	**57**
В том числе:		
Проработка учебного (теоретического) материала	25	25
Выполнение домашних заданий (решение задач)	20	20
Подготовка к текущему контролю	12	12
Контроль:		
Подготовка к экзамену	26,7	16,7

Общая трудоемкость	**час.**	**108**	**108**
	в том числе контактная работа	**24,3**	**24,3**
	зач. ед.	**3**	**3**

2.2 Структура дисциплины:

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.

Разделы дисциплины, изучаемые в 4 семестре.

№ раздела	Наименование разделов	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
				ПЗ		СРС
1	**2**	**3**		**5**		**7**
1	Кольца вычетов. Китайская теорема об остатках.	24		4		20
2	Решение уравнений в кольцах. В кольцах матриц над полем и в кольце целых чисел. Регистры сдвига с обратной связью.	24		6		18
3	Поля Галуа. Структура полей. Неприводимые многочлены над полями Галуа. Эллиптические кривые.	25		6		19
	Итого:			**16**		**57**

2.3 Содержание разделов дисциплины:

2.3.1 Занятия лекционного типа

№ п/п	Наименование раздела	Содержание раздела	Форма текущего контроля
1	**2**	**3**	**4**
1	Кольца вычетов. Китайская теорема об остатках.	Теория делимости в кольцах. НОД и НОК. Алгоритм Евклида. Решение модульных уравнений. Решение систем по разным модулям. Квадратичный закон взаимности.	Проверка домашнего задания, устный опрос
2	Решение уравнений в кольцах. В кольцах матриц над полем и в кольце целых чисел.	Обратимые матрицы. Решение систем линейных уравнений в кольце целых чисел. Приложения в криптографии. Эллиптические кривые.	Проверка домашнего задания, контрольная работа
3	Поля Галуа. Структура полей. Неприводимые многочлены над полями Галуа.	Простое поле Галуа. Расширение полей Галуа. Автоморфизмы полей Галуа. Неприводимые многочлены над полем Галуа. Регистры сдвига с обратной связью.	Проверка домашнего задания

2.3.2 Занятия семинарского типа

№ п/п	Наименование раздела	Содержание раздела	Форма текущего контроля
1	2	3	4
1	Кольца вычетов. Китайская теорема об остатках.	НОД и НОК. Алгоритм Евклида. Решение модульных уравнений. Решение систем по разным модулям.	Проверка домашнего задания, устный опрос
2	Кольца вычетов. Китайская теорема об остатках.	Решение систем линейных уравнений в кольце целых чисел. Приложения в криптографии. Эллиптические кривые.	Проверка домашнего задания, контрольная работа
3	Кольца вычетов. Китайская теорема об остатках.	Простое поле Галуа. Расширение полей Галуа. Неприводимые многочлены над полем Галуа. Регистры сдвига с обратной связью.	Проверка домашнего задания

2.3.3 Лабораторные работы не предусмотрены.

2.3.4 Примерная тематика курсовых работ (проектов) курсовые работы не предусмотрены.

2.4 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

1. Методические указания для подготовки к занятиям лекционного и семинарского типа. Утверждены на заседании Совета факультета математики и компьютерных наук ФГБОУ ВО «КубГУ». Протокол № 5 от 05 мая 2022 г.

2. Методические указания по выполнению самостоятельной работы обучающихся. Утверждены на заседании Совета факультета математики и компьютерных наук ФГБОУ ВО «КубГУ». Протокол № 5 от 05 мая 2022 г.

3. Методические указания по использованию интерактивных методов обучения. Утверждены на заседании Совета факультета математики и компьютерных наук ФГБОУ ВО «КубГУ». Протокол № 5т от 05 мая 2022 г.

4. Методические указания по подготовке эссе, рефератов, курсовых работ. Утверждены на заседании Совета факультета математики и компьютерных наук ФГБОУ ВО «КубГУ». Протокол № 5т от 05 мая 2022 г.

5. Методические указания по выполнению лабораторных работ. Утверждены на заседании Совета факультета математики и компьютерных наук ФГБОУ ВО «КубГУ». Протокол № 5 от 05 мая 2022 г.

6. Методические указания по выполнению расчетно-графических заданий. Утверждены на заседании Совета факультета математики и компьютерных наук ФГБОУ ВО «КубГУ». Протокол № 5 от 05 мая 2022 г.

Учебно-методические материалы для самостоятельной работы обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья (ОВЗ) предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

– в печатной форме увеличенным шрифтом,

– в форме электронного документа,

Для лиц с нарушениями слуха:

– в печатной форме,

– в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

– в печатной форме,

– в форме электронного документа.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

3 Образовательные технологии

При изучении данного курса используются традиционные лекции и практические занятия.

Цель практических занятий – научить студента применять полученные на лекциях теоретические знания к решению и исследованию конкретных задач. В каждом семестре проводятся контрольные работы для проверки усвоения материала студентами.

Для лиц с ограниченными возможностями здоровья предусмотрена организация консультаций с использованием электронной почты.

Самостоятельная работа студентов является неотъемлемой частью процесса подготовки. Под самостоятельной работой понимается часть учебной планируемой работы, которая выполняется по заданию и при методическом руководстве преподавателя, но без его непосредственного участия.

Самостоятельная работа направлена на усвоение системы научных и профессиональных знаний, формирования умений и навыков, приобретение опыта самостоятельной творческой деятельности. СРС помогает формировать культуру мышления студентов, расширять познавательную деятельность.

Виды самостоятельной работы по курсу:

по характеру работы: изучение литературы; поиск литературы в библиотеке; конспектирование рекомендуемой для самостоятельного изучения научной литературы; решение задач.

4. Оценочные средства для текущего контроля успеваемости и промежуточной аттестации

Учебная деятельность проходит в соответствии с графиком учебного процесса. Процесс самостоятельной работы контролируется во время аудиторных занятий и индивидуальных консультаций.

Оценочными средствами дисциплины являются средства текущего контроля (ответ у доски и проверка домашних заданий) и промежуточной аттестации (экзамен).

Оценка успеваемости осуществляется по результатам устного опроса, ответа на экзамене, в ходе которого выявляются уровень знаний и понимания теоретического материала.

Фонд оценочных средств для проведения текущей аттестации

Структура оценочных средств для текущей и промежуточной аттестации

№ п/п	Код и наименование индикатора (в соответствии с п. 1.4)	Результаты обучения (в соответствии с п. 1.4)	Наименование оценочного средства	
			Текущий контроль	Промежуточная аттестация
1	ОПК-1.1 Проводит поиск и обработку научной и научно-технической информации, необходимой для решения исследовательских задач ОПК-1.2 Обладает навыками проведения исследований под руководством более квалифицированного работника	Знать: основные педагогические методы и идеи	Тест по теме, разделу Круглый стол, Кейс Защита персональных данных	Методы правовой защиты информации. Правовые основы защиты государственной, коммерческой, служебной, профессиональной и личной тайны. Защита персональных данных.

	ОПК-1.3 Оценивает полученные результаты и формулирует выводы по итогам проведенных исследований			Правовая основа допуска и доступа персонала к защищаемым сведениям.
2	ПК-1.1 Способен решать актуальные и важные задачи фундаментальной и при-кладной математики ПК-1.2 Демонстрирует навыки программирования подготовленных алгоритмов решения вычислительных задач, разработки структуры и программирования реляционных баз данных, а также экспертных систем ПК-1.4 Собирает и анализирует научно- техническую информацию с учетом базовых представлений, полученных в области фундаментальной математики, механики, естественных наук, программирования и информационных технологий	Владеть: анализом информационной инфраструктуры государства; формальной постановкой и решением задачи обеспечения информационной безопасности компьютерных систем.	Индивидуальная работа работа Система правовой ответственности за утечку информации и утрату носителей информации.	Система правовой ответственности за утечку информации и утрату носителей информации. Правовые основы деятельности подразделений защиты информации

4.1 Примерные задания контрольной работы

1. Нахождение примитивного элемента конечного поля.
2. Построение таблицы логарифма Якоби конечного поля.
3. Решение систем линейных уравнений над конечным полем.
4. Алгоритм быстрого возведения в степень.
5. Нахождение обратных элементов в конечном поле.
6. Расширения конечных полей.
7. Алгоритм шифрования AES: структура поля $GF(2^8)$, нахождение обратных элементов.
8. Алгоритм RSA – выбор секретных параметров p,q,d, вычисление открытого ключа n,e.
9. Рюкзачная система шифрования. Быстрорастущий вектор. Сокрытие быстрорастущего вектора после преобразования умножения по модулю.
10. Решение систем линейных уравнений по разным модулям.
11. Решение систем линейных уравнений в кольце целых чисел.
12. Линейный регистр сдвига с обратной связью

$$S_{n+k} = a_{k-1}S_{n+k-1} + a_{k-2}S_{n+k-2} + ... + a_1S_{n+1} + a_0S_n + a, n = 0,1,2,...$$

4.2 Фонд оценочных средств для проведения промежуточной аттестации

Перечень вопросов к экзамену.

1. Построение конечного поля GF(5^2).
2. Построение неприводимых полиномов степеней 2, 3, 4 над GF(2), GF(3), GF(5).
3. Нахождение примитивного элемента конечного поля.
4. Нахождение обратного элемента в конечном поле.
5. Расширение конечных полей.
6. Структура поля GF(2^8).
7. Факторизация круговых полиномов над GF(p).
8. Нахождение примитивных полиномов над GF(2).
9. Квадратичный закон взаимности.
10. Нахождение порождающих элементов конечного поля.

Теоретические вопросы для экзамена

1. Решение систем линейных уравнений над полем. Алгоритм Гаусса.
2. Линейные отображения векторных пространств. Матричная запись.
3. Собственные и корневые вектора. Определение и свойства.
4. Алгоритм нахождения собственных векторов: вычисление определителя, задающего характеристический многочлен; для каждого корня нахождение собственных векторов.
5. Алгоритм нахождения жордановой формы над полем комплексных чисел и над полем разложения характеристического многочлена в случае полей Галуа.
6. Алгоритм решение систем линейных уравнений над кольцом целых чисел.
7. Определение и примеры евклидовых колец: кольцо целых чисел и кольцо многочленов над полем P[x].
8. Существование НОД и НОК в евклидовых кольцах.
9. Алгоритм Евклида деления с остатком. Нахождение НОД, как последнего ненулевого остатка.
10. Следствие из алгоритма Евклида, нахождение обратного элемента по модулю натурального числа.
11. Кольцо вычетов Z_n по модулю n. Решение линейных уравнений в кольце Z_n.
12. Решение систем линейных уравнений по разным модулям.
13. Китайская теорема об остатках.
14. Кольцо вычетов по простому модулю. Проверка, что $Z_p \cong GF(\text{p})$ - поле, простое поле Галуа.
15. Расширение полей Галуа. Расширение, как поле разложения неприводимого многочлена.
16. Башня расширений полей Галуа.
17. След и норма элементов в поле Галуа.
18. Связь корней неприводимого многочлена степени n над полем Галуа характеристики p: $\alpha_1 = \alpha; \alpha_2 = \alpha^p; ...; \alpha_n = \alpha^{p^{n-1}}$.
19. Теорема о существовании примитивного элемента в поле Галуа.
20. Логарифм Якоби в поле Галуа и его нахождение.
21. Алгоритм нахождения примитивного элемента и логарифма Галуа.
22. Эллиптическая кривая над полем Галуа. Приведение к каноническому виду.
23. Подсчет числа точек эллиптической кривой над полем Галуа.
24. Операция сложения на эллиптической кривой над полем Галуа.
25. Линейные регистры сдвига с обратной связью над полями Галуа. Определение и оценка минимального периода.
26. Линейные регистры сдвига – матричная запись. Импульсная функция.
27. Линейные регистры сдвига – характеристический многочлен. Явная формула для n-го члена регистра, выраженная через корни характеристического многочлена.
28. Квадратичный закон взаимности – формулировка и примеры применения.
29. Описание алгоритма RSA и его анализ.
30. Описание алгоритма AES и его анализ.
31. Алгоритм быстрого возведения в степень.
32. Алгоритм нахождения обратных элементов в поле Галуа.
33. Многочлен как функция – интерполяционная формула Лагранжа.
34. Симметрический многочлен. Основная теорема о симметрических многочленах. Симметрический многочлен однозначно выражается через элементарные симметрические.
35. Второе раундовое преобразование шифра AES. Нахождение жордановой формы матрицы линейного преобразования.
36. Основные алгебраические конструкции пакета Nemo языка программирования Julia.

Типовые задачи, выносимые на экзамен

1. Подсчет количества точек на эллиптической кривой.

2. Операция сложения на эллиптической кривой.
3. Схема алгоритма RSA.
4. Нахождение примитивного элемента конечного поля.
5. Построение таблицы логарифма Якоби конечного поля.
6. Решение систем линейных уравнений над конечным полем.
7. Алгоритм быстрого возведения в степень.
8. Нахождение обратных элементов в конечном поле.
9. Расширения конечных полей.
10. Алгоритм шифрования AES: структура поля $GF(2^8)$, нахождение обратных элементов.
11. Алгоритм шифрования AES: фактор кольцо $GF(2^8)[x]/\text{ид}((x+1)^4)$, преобразование столбцов.
12. Алгоритм шифрования AES: Линейное преобразование, собственные значения матрицы.
13. Алгоритм RSA – выбор секретных параметров p,q,d, вычисление открытого ключа n,e.
14. Рюкзачная система шифрования. Быстрорастущий вектор. Сокрытие быстрорастущего вектора после преобразования умножения по модулю.
15. Решение систем линейных уравнений по разным модулям.
16. Решение систем линейных уравнений в кольце целых чисел.
17. Линейный регистр сдвига с обратной связью
$S_{n+k} = a_{k-1}S_{n+k-1} + a_{k-2}S_{n+k-2} + ... + a_1S_{n+1} + a_0S_n + a, n = 0,1,2,...$
18. Характеристический многочлен регистра сдвига $x^k = a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + ... + a_1x + a_0$
19. Нахождение явного вида значений регистра сдвига
$S_n = \beta_1\alpha_1^{\,n} + \beta_2\alpha_2^{\,n} + ... + \beta_k\alpha_k^{\,n}, n = 0,1,2,...$, где $\alpha_1, \alpha_2, ..., \alpha_k$ - корни характеристического многочлена, коэффициенты $\beta_1, \beta_2, ..., \beta_k \in P$ являются решениями системы
$$\begin{cases} \beta_1\alpha_1^{\,0} + \beta_2\alpha_2^{\,0} + ... + \beta_k\alpha_k^{\,0} = S_0 \\ \beta_1\alpha_1^{\,1} + \beta_2\alpha_2^{\,1} + ... + \beta_k\alpha_k^{\,1} = S_1 \\ ... \\ \beta_1\alpha_1^{\,k-1} + \beta_2\alpha_2^{\,k-1} + ... + \beta_k\alpha_k^{\,k-1} = S_{k-1} \end{cases}.$$
20. Матрица линейного регистра сдвига ее собственные значения и жорданова форма.
21. Квадратичный закон взаимности. Вычисление квадратичных вычетов и невычетов.

Оценочные средства для инвалидов и лиц с ограниченными возможностями здоровья выбираются с учетом их индивидуальных психофизических особенностей.

– при необходимости инвалидам и лицам с ограниченными возможностями здоровья предоставляется дополнительное время для подготовки ответа на экзамене;

– при проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья предусматривается использование технических средств, необходимых им в связи с их индивидуальными особенностями;

– при необходимости для обучающихся с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения по дисциплине может проводиться в несколько этапов.

Процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине (модулю) предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

– в печатной форме увеличенным шрифтом,
– в форме электронного документа.
Для лиц с нарушениями слуха:
– в печатной форме,
– в форме электронного документа.
Для лиц с нарушениями опорно-двигательного аппарата:
– в печатной форме,
– в форме электронного документа.
Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

Типовые билеты к экзамену

Билет № 1
Дополнительные главы фундаментальной математики
1. Решение систем линейных уравнений над полем. Алгоритм Гаусса.
2. Основные алгебраические конструкции пакета Nemo языка программирования Julia.
3. Найти группу обратимых элементы кольца

Билет № 2
Дополнительные главы фундаментальной математики
1. Второе раундовое преобразование шифра AES. Нахождение жордановой формы матрицы линейного преобразования.
2. Линейные отображения векторных пространств. Матричная запись
3. В кольце решить уравнение .

Билет № 3
Дополнительные главы фундаментальной математики
1. Собственные и корневые вектора. Определение и свойства.
2. Симметрический многочлен. Основная теорема о симметрических многочленах. Симметрический многочлен однозначно выражается через элементарные симметрические многочлены.
3. Найти примитивный элемент поля .

Билет № 4
Дополнительные главы фундаментальной математики
1. Многочлен как функция – интерполяционная формула Лагранжа.
2. Алгоритм нахождения собственных векторов: вычисление определителя, задающего характеристический многочлен; для каждого корня нахождение собственных векторов
3. Над полем решить систему

Билет № 5
Дополнительные главы фундаментальной математики
1. Китайская теорема об остатках.
2. Алгоритм нахождения жордановой формы над полем комплексных чисел и над полем разложения характеристического многочлена в случае полей Галуа.
3. Решить систему

Билет № 6
Дополнительные главы фундаментальной математики
1. Алгоритм решение систем линейных уравнений над кольцом целых чисел.
2. Алгоритм нахождения обратных элементов в поле Галуа.

3. Методом Евклида решить уравнение .

Билет № 7
Дополнительные главы фундаментальной математики
1. Алгоритм быстрого возведения в степень.
2. Определение и примеры евклидовых колец: кольцо целых чисел и кольцо многочленов над полем P[x].
3. Разложить в сумму простейших дробей .

Билет № 8
Дополнительные главы фундаментальной математики
1. Существование НОД и НОК в евклидовых кольцах.
2. Описание алгоритма AES и его анализ.
3. Разложить в сумму простейших в кольце дробь .

Билет № 9
Дополнительные главы фундаментальной математики
1. Описание алгоритма RSA и его анализ.
2. Алгоритм Евклида деления с остатком. Нахождение НОД, как последнего ненулевого остатка.
3. Существует ли дифференцирование в кольце , такое, что .

Билет № 10
Дополнительные главы фундаментальной математики
1. Решение систем линейных уравнений по разным модулям.
2. Следствие из алгоритма Евклида, нахождение обратного элемента по модулю натурального числа.
3. Найти .

Билет № 11
Дополнительные главы фундаментальной математики
1. Кольцо вычетов по модулю n. Решение линейных уравнений в кольце .
2. Квадратичный закон взаимности – формулировка и примеры применения
3. Найти над

Билет № 12
Дополнительные главы фундаментальной математики
1. Линейные регистры сдвига с обратной связью.
2. Кольцо вычетов по простому модулю. Проверка, что - поле, простое поле Галуа.
3. Используя производную найти кратные множители многочлена над .

Билет № 13
Дополнительные главы фундаментальной математики
1. Линейные регистры сдвига – характеристический многочлен. Явная формула для n-го члена регистра, выраженная через корни характеристического многочлена.
2. Расширение полей Галуа. Расширение, как поле разложения неприводимого многочлена.
3. Найти все неприводимые многочлены третьей степени в кольце .

Билет № 14
Дополнительные главы фундаментальной математики
1. Башня расширений полей Галуа.

2. Линейные регистры сдвига – матричная запись. Импульсная функция.
3. Построить поле разложения многочлена .

Билет № 15
Дополнительные главы фундаментальной математики
1. Линейные регистры сдвига с обратной связью над полями Галуа. Определение и оценка минимального периода.
2. След и норма элементов в поле Галуа.
3. Является ли отображение линейным , если да, то найти его матрицу в стандартном базисе, над полем GF(5)

Билет № 16
Дополнительные главы фундаментальной математики
1. Связь корней неприводимого многочлена степени n над полем Галуа характеристики p:
.
2. Операция сложения на эллиптической кривой над полем Галуа.
3. Найти все неприводимые многочлены второй степени в кольце .

Билет № 17
Дополнительные главы фундаментальной математики
1. Подсчет числа точек эллиптической кривой над полем Галуа.
2. Логарифм Якоби в поле Галуа и его нахождение.
3. Построить поле разложения многочлена .

Билет № 18
Дополнительные главы фундаментальной математики
1. Алгоритм нахождения примитивного элемента и логарифма Галуа.
2. Эллиптическая кривая над полем Галуа. Приведение к каноническому виду.
3. Является ли отображение линейным , если да, то найти его матрицу в стандартном базисе над полем GF(7).

Критерии оценивания по промежуточной аттестации

Критерии оценивания результатов обучения

Оценка	Критерии оценивания по экзамену
Высокий уровень «5» (отлично)	оценку «отлично» заслуживает студент, освоивший знания, умения, компетенции и теоретический материал без пробелов; выполнивший все задания, предусмотренные учебным планом на высоком качественном уровне; практические навыки профессионального применения освоенных знаний сформированы.
Средний уровень «4» (хорошо)	оценку «хорошо» заслуживает студент, практически полностью освоивший знания, умения, компетенции и теоретический материал, учебные задания не оценены максимальным числом баллов, в основном сформировал практические навыки.
Пороговый уровень «3» (удовлетворительно)	оценку «удовлетворительно» заслуживает студент, частично с пробелами освоивший знания, умения, компетенции и теоретический материал, многие учебные задания либо не выполнил, либо они оценены числом баллов близким к минимальному, некоторые практические навыки не сформированы.

Минимальный уровень «2» (неудовлетво-рительно)	оценку «неудовлетворительно» заслуживает студент, не освоивший знания, умения, компетенции и теоретический материал, учебные задания не выполнил, практические навыки не сформированы.

Критерии оценивания по зачету:

«зачтено»: студент владеет теоретическими знаниями по данному разделу, знает формы допускает незначительные ошибки; студент умеет правильно объяснять материал, иллюстрируя его примерами

«не зачтено»: материал не усвоен или усвоен частично, студент затрудняется привести примеры, довольно ограниченный объем знаний программного материала.

Оценочные средства для инвалидов и лиц с ограниченными возможностями здоровья выбираются с учетом их индивидуальных психофизических особенностей.

– при необходимости инвалидам и лицам с ограниченными возможностями здоровья предоставляется дополнительное время для подготовки ответа на экзамене;

– при проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья предусматривается использование технических средств, необходимых им в связи с их индивидуальными особенностями;

– при необходимости для обучающихся с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения по дисциплине может проводиться в несколько этапов.

Процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине (модулю) предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

– в печатной форме увеличенным шрифтом,

– в форме электронного документа.

Для лиц с нарушениями слуха:

– в печатной форме,

– в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

– в печатной форме,

– в форме электронного документа.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

5. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

1. Мартынов Л.М. Алгебра и теория чисел для криптографии: учебное пособие, 2-е изд. [Электронный ресурс]. - СПб.: Лань, 2022. - URL: https://reader.lanbook.com/book/189446
2. Глухов М.М., Круглов И.А., Пичкур А.Б., Черемушкин А.В. Введение в теоретико-числовые методы криптографии. [Электронный ресурс]. - СПб.: Лань, 2021. - URL: https://e.lanbook.com/reader/book/153680

5.2 Дополнительная литература:

1. Виноградов И.М. Основы теории чисел. 14-е изд. [Электронный ресурс]. - СПб.: Лань, 2020. - URL: https://e.lanbook.com/reader/book/139285
2. Бухштаб А.А. Теория чисел, 6-е изд. [Электронный ресурс]. - СПб.: Лань, 2022. - https://reader.lanbook.com/book/189329

5.3. Интернет-ресурсы, в том числе современные профессиональные базы данных и информационные справочные системы

Электронно-библиотечные системы (ЭБС):

1. ЭБС «ЮРАЙТ» https://urait.ru/

2. ЭБС «УНИВЕРСИТЕТСКАЯ БИБЛИОТЕКА ОНЛАЙН» www.biblioclub.ru
3. ЭБС «BOOK.ru» https://www.book.ru
4. ЭБС «ZNANIUM.COM» www.znanium.com
5. ЭБС «ЛАНЬ» https://e.lanbook.com

Профессиональные базы данных:

1. Web of Science (WoS) http://webofscience.com/
2. Scopus http://www.scopus.com/
3. ScienceDirect www.sciencedirect.com
4. Журналы издательства Wiley https://onlinelibrary.wiley.com/
5. Научная электронная библиотека (НЭБ) http://www.elibrary.ru/
6. Полнотекстовые архивы ведущих западных научных журналов на Российской платформе научных журналов НЭИКОН http://archive.neicon.ru
7. Национальная электронная библиотека (доступ к Электронной библиотеке диссертаций Российской государственной библиотеки (РГБ) https://rusneb.ru/
8. Президентская библиотека им. Б.Н. Ельцина https://www.prlib.ru/
9. Электронная коллекция Оксфордского Российского Фонда https://ebookcentral.proquest.com/lib/kubanstate/home.action
10. Springer Journals https://link.springer.com/
11. Nature Journals https://www.nature.com/siteindex/index.html
12. Springer Nature Protocols and Methods https://experiments.springernature.com/sources/springer-protocols
13. Springer Materials http://materials.springer.com/
14. zbMath https://zbmath.org/
15. Nano Database https://nano.nature.com/
16. Springer eBooks: https://link.springer.com/
17. "Лекториум ТВ" http://www.lektorium.tv/
18. Университетская информационная система РОССИЯ http://uisrussia.msu.ru

Информационные справочные системы:

1. Консультант Плюс - справочная правовая система (доступ по локальной сети с компьютеров библиотеки)

Ресурсы свободного доступа:

1. Американская патентная база данных http://www.uspto.gov/patft/
2. Полные тексты канадских диссертаций http://www.nlc-bnc.ca/thesescanada/
3. КиберЛенинка (http://cyberleninka.ru/);
4. Министерство науки и высшего образования Российской Федерации https://www.minobrnauki.gov.ru/;
5. Федеральный портал "Российское образование" http://www.edu.ru/;
6. Информационная система "Единое окно доступа к образовательным ресурсам" http://window.edu.ru/;
7. Единая коллекция цифровых образовательных ресурсов http://school-collection.edu.ru/ .
8. Федеральный центр информационно-образовательных ресурсов (http://fcior.edu.ru/);
9. Проект Государственного института русского языка имени А.С. Пушкина "Образование на русском" https://pushkininstitute.ru/;
10. Справочно-информационный портал "Русский язык" http://gramota.ru/;

11. Служба тематических толковых словарей http://www.glossary.ru/;
12. Словари и энциклопедии http://dic.academic.ru/;
13. Образовательный портал "Учеба" http://www.ucheba.com/;
14. Законопроект "Об образовании в Российской Федерации". Вопросы и ответы http://xn--273--84d1f.xn--p1ai/voprosy_i_otvety

Собственные электронные образовательные и информационные ресурсы КубГУ:

1. Среда модульного динамического обучения http://moodle.kubsu.ru
2. База учебных планов, учебно-методических комплексов, публикаций и конференций http://mschool.kubsu.ru/
3. Библиотека информационных ресурсов кафедры информационных образовательных технологий http://mschool.kubsu.ru;
4. Электронный архив документов КубГУ http://docspace.kubsu.ru/
5. Электронные образовательные ресурсы кафедры информационных систем и технологий в образовании КубГУ и научно-методического журнала "ШКОЛЬНЫЕ ГОДЫ" http://icdau.kubsu.ru/

6. Методические указания для обучающихся по освоению дисциплины (модуля).

Согласно учебному плану дисциплины «Информационная безопасность» итоговой формой контроля является зачет. Для сдачи зачета студент должен научиться на лабораторных занятиях решать практические задания по темам разделов 1-3, выполнять домашние задания. Типы практических заданий на зачет соответствуют заданиям. Также на зачете студентам предлагаются и теоретические задания, состоящие в письменном ответе на один из вопросов. Количество практических и теоретических заданий зависит от активности и результативности работы студента в течение семестра.

Важнейшим этапом курса является самостоятельная работа по дисциплине (модулю).

Для подготовки к ответам на теоретические вопросы в ходе контрольных работ и на зачете студентам достаточно использовать материал лекций. Весь этот теоретический материал содержится в учебных пособиях из списка основной литературы. Для изучения теоретического материала, необходимого для подготовки реферативного доклада, кроме основных источников литературы возможно использование дополнительных источников и Интернет-ресурса. В случае затруднений, возникающих у студентов в процессе самостоятельного изучения теории, преподаватель разъясняет сложные моменты на консультациях.

7. Материально-техническое обеспечение по дисциплине (модулю)

По всем видам учебной деятельности в рамках дисциплины используются аудитории, кабинеты и лаборатории, оснащенные необходимым специализированным и лабораторным оборудованием.

При заполнении таблицы учитывать все виды занятий, предусмотренные учебным планом по данной дисциплине: лекции, занятия семинарского типа (практические занятия, лабораторные работы), а также курсовое проектирование, консультации, текущий контроль и промежуточную аттестацию.

При использовании лаборатории указать ее наименование «Лаборатория…».

Наименование специальных помещений	Оснащенность специальных помещений	Перечень лицензионного программного обеспечения
Учебные аудитории для проведения занятий лекционного типа	Мебель: учебная мебель Технические средства обучения: экран, проектор, компьютер	
Учебные аудитории для проведения занятий семинарского типа, групповых и индивидуальных	Мебель: учебная мебель Технические средства обучения: экран, проектор, компьютер	

консультаций, текущего контроля и промежуточной аттестации	Оборудование:	
Учебные аудитории для проведения лабораторных работ. Лаборатория…	Мебель: учебная мебель Технические средства обучения: экран, проектор, компьютер Оборудование:	
Учебные аудитории для курсового проектирования (выполнения курсовых работ)	Мебель: учебная мебель Технические средства обучения: экран, проектор, компьютер Оборудование:	

Для самостоятельной работы обучающихся предусмотрены помещения, укомплектованные специализированной мебелью, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Наименование помещений для самостоятельной работы обучающихся	Оснащенность помещений для самостоятельной работы обучающихся	Перечень лицензионного программного обеспечения
Помещение для самостоятельной работы обучающихся (читальный зал Научной библиотеки)	Мебель: учебная мебель Комплект специализированной мебели: компьютерные столы Оборудование: компьютерная техника с подключением к информационно-коммуникационной сети «Интернет» и доступом в электронную информационно-образовательную среду образовательной организации, веб-камеры, коммуникационное оборудование, обеспечивающее доступ к сети интернет (проводное соединение и беспроводное соединение по технологии Wi-Fi)	
Помещение для самостоятельной работы обучающихся (ауд._____)	Мебель: учебная мебель Комплект специализированной мебели: компьютерные столы Оборудование: компьютерная техника с подключением к информационно-коммуникационной сети «Интернет» и доступом в электронную информационно-образовательную среду образовательной организации, веб-камеры, коммуникационное оборудование, обеспечивающее доступ к сети интернет (проводное соединение и беспроводное соединение по технологии Wi-Fi)	

№	Вид работ	Материально-техническое обеспечение дисциплины (модуля) и оснащенность
1.	Лекционные занятия	Лекционная аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук) и соответствующим программным обеспечением (ПО) Программы, демонстрации видео материалов (проигрыватель «Windows Media Player»). Программы для демонстрации и создания презентаций («Microsoft Power Point»).

2.	Семинарские занятия	Не предусмотрены
3.	Лабораторные занятия	Лаборатория, укомплектованная специализированной мебелью и техническими средствами обучения – компьютерами с предустановленными GAP и Sage
4.	Курсовое проектирование	Не предусмотрено
5.	Групповые (индивидуальные) консультации	Аудитория для групповых занятий
6.	Текущий контроль, промежуточная аттестация	Аудитория для групповых занятий
7.	Самостоятельная работа	Кабинет для самостоятельной работы, оснащенный компьютерной техникой с возможностью подключения к сети «Интернет», программой экранного увеличения и обеспеченный доступом в электронную информационно-образовательную среду университета.

Рецензия

на рабочую программу дисциплины «Дополнительные главы фундаментальной математики» для направления подготовки 02.04.01 Математика и компьютерные науки (квалификация «магистр»)

Изучение разделов анализа и их приложений является важным для формирования квалифицированного специалиста в области математики, в частности.

Рабочая программа дисциплины «Дополнительные главы фундаментальной математики» включает в себя необходимые структурные части. Все основные разделы программы нашли свое отражение в перечне представленных в программе необходимых знаний, умений и компетенций. Распределение времени, отводимого на изучение различных разделов курса, включая самостоятельную работу, соответствует их трудоемкости.

Содержание разделов, их разделение по видам занятий, и трудоемкость в часах отвечают целям и задачам курса. В программе сформулированы темы самостоятельной внеаудиторной работы, примеры заданий для контрольных работ, билеты для экзаменов, перечень основной и дополнительной литературы, доступной для обучающихся.

В целом, рабочая программа по дисциплине «Дополнительные главы фундаментальной математики» составлена в соответствии с требованиями ФГОС ВО, отвечает современным требованиям к качественному образовательному процессу и может быть использована для обеспечения основной образовательной программы по направлению подготовки 01.04.01 Математика.

Рецензент
кандидат физ.-мат. наук,
доцент кафедры прикладной математики КубГТУ Чубырь Н.О.

Рецензия

на рабочую программу дисциплины «Дополнительные главы фундаментальной математики» для направления подготовки 02.04.01 Математика и компьютерные науки (квалификация «магистр»)

Изучение вопросов фундаментальной математики и их применение в приложениях является важным для формирования квалифицированного специалиста в области математики, в частности.

Рабочая программа по курсу «Дополнительные главы фундаментальной математики» предусматривает формирование у обучающихся математического аппарата, включающего в себя математические знания, умения и навыки необходимые для дальнейшей профессиональной деятельности.

Программа отвечает современным требованиям к обучению и отражает современные тенденции в обучении и воспитании личности. Содержание рабочей программы охватывает весь материал, необходимый для обучения студентов высших учебных заведений по направлению магистратуры «Математика».

Рабочая программа дает целостное представление о дисциплине. Структура и содержание курса взаимно дополняют друг друга. Также в программе приведены примеры заданий для промежуточной аттестации, перечень вопросов, выносимых на экзамен, перечень основной и дополнительной литературы, доступной обучающимся.

В целом, рабочая программа по дисциплине «Дополнительные главы фундаментальной математики» соответствует ФГОС ВО и отвечает современным требованиям к качественному образовательному процессу. Данная рабочая программа может быть использована для обеспечения основной образовательной программы по направлению подготовки магистров 01.04.01 Математика.

Рецензент
доктор педагогических наук, профессор,
зав. кафедрой теории функций КубГУ Лазарев В.А.