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

Кафедра алгебры и математической логики

УТВЕРЖДАЮ
Декан математического факультета

Нестеров П.Н.
20 июня 2023 г.

Рабочая программа дисциплины
Дополнительные главы алгебраической геометрии в криптографии

Направление подготовки (специальности)
10.05.01 Компьютерная безопасность

Направленность (профиль)
«Математические методы защиты информации»

Форма обучения очная

Программа рассмотрена
на заседании кафедры
от 18 апреля 2023 г., протокол № 8

Программа одобрена НМК
математического факультета
протокол № 9 от 3 мая 2023 г.

Ярославль

1. Цели освоения дисциплины

Целью освоения дисциплины «Дополнительные главы алгебраической геометрии в криптографии» является углубление знакомства студентов с основами теории эллиптических кривых и её приложениями к алгоритмам, используемым для защиты информации

2. Место дисциплины в структуре образовательной программы

Дисциплина относится к обязательной части Блока 1 и является дисциплиной по выбору (Б1.О.ДВ.02.01). Она углубляет знания, полученные студентами при изучении курса «Методы алгебраической геометрии в криптографии», а также их общеалгебраическую подготовку.

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 приобретения следующих знаний, умений, навыков и (или) опыта деятельности:

Формируемая компетенция (код и формулировка)	**Индикатор достижения компетенции (код и формулировка)**	**Перечень планируемых результатов обучения**
Общепрофессиональные компетенции		
ОПК-3 Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности;	И-ОПК-3_4 знает основные понятия, результаты и методы современной математики и сценарии их применения в задачах профессиональной деятельности И-ОПК-3_8 умеет распознать математические структуры, возникающие в задачах профессиональной деятельности, конструировать, анализировать объекты и выполнять вычисления, формулировать требования к свойствам математических объектов, необходимым для решения профессиональной задачи	**Знает** основные понятия, результаты и методы из алгебры и алгебраической геометрии **Умеет** распознать математические структуры, исследовать их свойства **Имеет навыки** вычислений в факторкольцах, конечных полях, на эллиптических кривых, в т.ч. над полями конечной характеристики
ОПК-2.1 Способен разрабатывать алгоритмы, реализующие современные математические методы защиты информации	**И-ОПК-2.1_5** знает принципиальные закономерности применения математических методов и результатов в задачах защиты информации **И-ОПК-2.1_6** умеет понимать и анализировать работу вычислительного алгоритма, использующего современные математические методы **ИД-ОПК-2.1_2** Способен разрабатывать алгоритмы, используемые в современных математических методах защиты информации	**Знает** принципиальные закономерности применения математических методов и результатов в задачах защиты информации **Умеет** понимать и анализировать работу вычислительного алгоритма, использующего вычисления на эллиптических и гиперэллиптических кривых **Имеет опыт** программной реализации алгоритмов, использующих вычисления на эллиптических и гиперэллиптических кривых

4. Объем, структура и содержание дисциплины

Общая трудоемкость дисциплины составляет _3_ зачетных единицы, _108_ 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)* Формы ЭО и ДОТ *(при наличии)*
			Контактная работа					самостоятельная работа	
			лекции	практические	лабораторные	консультации	аттестационные испытания		
1	**Кольца**	10	4	10		2		12	
2	**Модули и алгебры**	10	4	10		2		12	Задание для самостоятельной работы № 1
3	**Эллиптические и гиперэллиптические кривые**	10	4	10		2		12	Задание для самостоятельной работы № 2
4	**Некоторые алгоритмы с использованием эллиптических и гиперэллиптических кривых**	10	4	2				17,7	Реализация алгоритма (Задача для программирования)
							0,3		зачёт
	ИТОГО		16	32		6		53,7	

4.Содержание разделов дисциплины

1. **Кольца.** Сумма и пересечение подколец и идеалов. Идеал, порожденный подмножеством. Операции над идеалами в коммутативном кольце, радикал идеала. Теорема Гильберта о нулях. Поля и тела, их простейшие свойства. Тело кватернионов. Поля вычетов. Поле частных целостного кольца. Поле рациональных дробей. Поле К((x)) формальных рядов Лорана от одной переменной. Поле частных кольца К[[x]]. Подполя. Простое подполе и его связь с характеристикой поля. Гомоморфизм и изоморфизм полей. Расширения полей. Типы расширений: конечные, алгебраические, трансцендентные, конечно порожденные, простые. Теоремы о башнях для конечных и алгебраических расширений. Описание и изоморфизм простых расширений поля. Вид элементов конечного расширения поля, вычисления в конечном расширении. Символическое присоединение. Построение поля разложения многочлена. Изоморфизм полей разложения многочлена. Алгебраически замкнутые поля. Алгебраическое замыкание поля. Поля Галуа: их существование и единственность. Подполя конечного поля. Цикличность мультипликативной группы конечного поля. Цикличность мультипликативной группы кольца вычетов по модулю p^n. Норма и след. Автоморфизмы конечных полей.
2. **Модули и алгебры.** Подмодули, фактормодули, гомоморфизмы модулей. Прямые произведения и прямые суммы модулей. Образующие модуля. Циклические подмодули и модули. Свободные модули. Базис и размерность свободного модуля. Гомоморфизмы свободных модулей. Условия конечности для модулей. Конечная порожденность и конечная представимость. Замена кольца коэффициентов (тензорное умножение). Алгебры над полем. Конечномерные алгебры с делением. Теорема Фробениуса.
3. **Эллиптические и гиперэллиптические кривые**. Эллиптические кривые над полем рациональных чисел. Теоремы Морделла – Вейля и Мазура. Каноническая высота точки и

спаривание Нерона – Тейта. Изоморфизмы эллиптических кривых. Изоморфизмы над полями характеристики, отличной от 2 и 3. Изоморфизмы эллиптических кривых над полями характеристик 2 и 3. Рациональное отображение и бирациональный изоморфизм кривых. Эндоморфизмы групповой структуры эллиптической кривой. Кривые с комплексным умножением. Изогения эллиптических кривых. Изоморфизмы эллиптических кривых в форме Лежандра. Дивизоры на алгебраической кривой. Группа дивизоров. Линейная эквивалентность. Якобиан кривой. Критерий того, что дивизор на эллиптической кривой является дивизором функции. Спаривание Вейля и метод его вычисления. Норма и след в конечных полях. Эллиптические кривые над конечными полями. Дзета-функция неособой алгебраической кривой. Гиперэллиптические кривые и дивизоры на них. Якобиан и дзета-фунция гиперэллиптической кривой.

4. **Некоторые алгоритмы с использованием эллиптических и гиперэллиптических кривых.** Логарифмирование методами Полларда и Гельфонда—Сильвера—Поллига—Хеллмана. Влияние комплексного умножения на сложность логарифмирования. Функция Вейля и метод ее вычисления. Криптографические требования к эллиптической кривой. Логарифмирование с использованием функции Вейля. Логарифмирование в якобиане гиперэллиптической кривой.

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:

Вводная лекция – дает первое целостное представление о дисциплине и ориентирует студента в системе изучения данной дисциплины. Студенты знакомятся с назначением и задачами курса, его ролью и местом в системе учебных дисциплин и в системе подготовки в целом. Дается краткий обзор курса, история развития науки и практики, достижения в этой сфере, имена известных ученых, излагаются перспективные направления исследований. На этой лекции высказываются методические и организационные особенности работы в рамках данной дисциплины, а также дается анализ рекомендуемой учебно-методической литературы.

Академическая лекция с элементами лекции-беседы – последовательное изло-жение 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

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

а) основная литература

. Зяблицева, Л. В. Алгебраические структуры и их приложения / Зяблицева Л. В. , Корабельщикова С. Ю. , Кузнецова И. В. , Тихомиров С. А. - Архангельск : ИД САФУ, 2015. - 169 с. - ISBN 978-5-261-01074-6. - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : https://www.studentlibrary.ru/book/ISBN9785261010746.html (дата обращения: 01.02.2022). - Режим доступа : по подписке.

2. Тимофеева Н.В. Алгебраические структуры / Н. В. Тимофеева; Яросл. гос. ун-т им. П. Г. Демидова. - Ярославль: ЯрГУ, 2021. Ч. 1 [Электронный ресурс]: учебное пособие. - Б.м.: Б.и., 2021. - 79 с. http://www.lib.uniyar.ac.ru/edocs/iuni/20210203.pdf

3. Ростовцев, А. Г. Алгебраические основы криптографии. - СПб.: Мир и семья, 2000.-354с

б) дополнительная литература

1. Мартынов, Л. М. Алгебра и теория чисел для криптографии : учебное пособие для вузов / Л. М. Мартынов. — 2-е изд., стер. — Санкт-Петербург : Лань, 2022. — 456 с. — ISBN 978-5-8114-9346-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/189446 (дата обращения: 01.02.2022). — Режим доступа: для авториз. пользователей.

2. Атья М. Введение в коммутативную алгебру / М. Атья, И.Макдональд. Пер. с англ. – М.: Мир, 1972. – 161 с.

3. Кокс Д., Литтл Дж., О'Ши Д. Идеалы, многообразия и алгоритмы. Введение в вычислительные аспекты алгебраической геометрии и коммутативной алгебры / Д. Кокс; Пер. с англ. --- М. : Мир, 2000. http://www.bookre.org/reader?file=1221440

4. Ишмухаметов Ш.Т. Методы факторизации натуральных чисел: учебное пособие / Ш.Т. Ишмухаметов. – Казань, Казанский ун-т, 2011. – 190 с.

в) ресурсы сети «Интернет» (при необходимости)

1. Острик, В. В. Алгебраическая геометрия и теория чисел: рациональные и эллиптические кривые : учебное пособие / В. В. Острик, М. А. Цфасман. — Москва : МЦНМО, 2001. — 48 с. — ISBN 5-900916-71-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/9381 (дата обращения: 29.11.2021). — Режим доступа: для авториз. пользователей. https://e.lanbook.com/book/9381?category=908

2. Шафаревич, И. Р. Основы алгебраической геометрии : учебное пособие / И. Р. Шафаревич. — 3-е изд. — Москва : МЦНМО, 2007. — 589 с. — ISBN 978-5-94057-085-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/9441 — Режим доступа: для авториз. пользователей. https://e.lanbook.com/book/9441?category=908

3. Cox D., Little J., O'Shea D. Using Algebraic Geometry, 2nd ed., Graduate texts in Math, vol.185, Springer, 2004. http://bookre.org/reader?file=741076

4. Gallian J. Contemporary Abstract Algebra. Cengage Learning, 2010. https://notendur.hi.is/mbh6/html/_downloads/Contemporary%20Abstract%20Algebra%20-%20Joseph%20Gallian%20(2012).pdf

5. Eisenbud D. Commutative Algebra with a View Towards Algebraic Geometry, Graduate texts in Math,vol.150. https://www.math.ens.psl.eu/~benoist/refs/Eisenbud.pdf

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 АМЛ, д.ф.-м.н. Н.В. Тимофеева

Приложение № 1 к рабочей программе дисциплины
« Дополнительные главы алгебраической геометрии в криптографии »
наименование дисциплины

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

Задание для самостоятельной работы № 1 (**И-ОПК-3_4, И-ОПК-3_8**)

1. Найдите центр матричной алгебры над полем (любым доступным вам способом).
2. Найти радикал идеала в предложенном полиномиальном кольце от нескольких переменных над полем
3. Перечислите все гомоморфизмы кольца Z_{12} в $Z_2 \oplus Z_3$
4. Вычислите норму и след предложенного элемента в конечном поле, заданном в виде факторкольца кольца полиномов
5. Найдите следующие степени расширений: $[Q(\sqrt{2}, \sqrt[3]{3}) : Q]$ и $[Q(\sqrt{6}) : Q(\sqrt{2})]$.
6. Составляют ли алгебры 1) над полем действительных чисел: а) вещественные полиномы от одной переменной? б) вещественные полиномы от двух переменных? в) вещественные полиномы от переменных, занумерованных натуральными числами? г) вещественные полиномы от двух переменных, имеющие чётные степени? Нечётные степени? д) целочисленные полиномы от одной переменной? е) комплексные числа? ж) комплексные полиномы от фиксированного набора переменных? з) кватернионы? 2) над полем комплексных чисел а) комплексные полиномы от любого фиксированного набора переменных? б) формальные степенные ряды от одной переменной с комплексными коэффициентами?
7. Составляют ли подалгебру / идеал классы полиномов, кратных *x*, в факторкольце $k[x]/ < x^2 - 1 >$?
8. Выполните действия в предложенном факторкольце кольца полиномов; в качестве ответа укажите представитель смежного класса, имеющий наименьшую степень.
9. Есть ли ненулевые делители нуля / нильпотенты в данных факторкольцах (даётся список из 3 примеров)?
10. Расклассифицируйте данные алгебраические множества (3 множества) по признаку неприводимости, используя простоту / непростоту определяющих их идеалов.
11. Укажите какую-нибудь систему образующих образа идеала $(x^2, x + y, y^2)$ в факторкольце $k[x, y]/(x - y)$. Можно ли задать этот образ двумя образующими? Одной образующей? То же самое для образов идеалов (x^2, y^2), $(x^2, x + y)$.

Задание для самостоятельной работы № 2 (**И-ОПК-3_4, И-ОПК-3_8**)

1. Укажите, какие из данных алгебраических множеств изоморфны? Бирационально изоморфны?
2. Касательные в двух различных точках P и Q эллиптической кривой, заданной в форме Вейерштрасса, пересекаются в точке R эллиптической кривой. Покажите, что точка P-Q имеет нулевую ординату.
3. В точке перегиба эллиптической кривой проведена касательная. В какой еще точке она пересечет кривую?

4. Кубическая кривая над алгебраически замкнутым полем совпадает со своим гессианом. Что собой представляет какая кривая?
5. Покажите, что точки кручения эллиптической кривой образуют группу.

В теме 4 предполагается программная реализация одного из алгоритмов на эллиптической или гиперэллиптической кривой (см. список задач для программирования, приведённый ниже, **И-ОПК-3_4, И-ОПК-3_8, И-ОПК-2.1._5, И-ОПК-2.1._6, И-ОПК-2.1_2**). Эта работа выполняется студентами в мини-группах.

Список задач для программирования

1. Разложить на множители составное число вида pq (p и q простые) с помощью эллиптической кривой.

2. Дискретное логарифмирование на эллиптической кривой: метод Гельфонда – Силвера – Поллига – Хеллмана.

3. Дискретное логарифмирование на эллиптической кривой: метод Полларда.

4. Генерация эллиптической кривой с j=0 над полем длины p, с указанием циклической подгруппы в ней.

5. Генерация эллиптической кривой с j=1728 над полем длины p, с указанием циклической подгруппы в ней.

6. Генерация эллиптической кривой с комплексным умножением.

7. Умножение точки на число в расширенном поле.

Зачёт выставляется по итогам сдачи студентами задачи для программирования и выборочной проверки задач для самостоятельной работы.

Приложение № 2 к рабочей программе дисциплины
« Дополнительные главы алгебраической геометрии в криптографии »
наименование дисциплины

Методические указания для студентов по освоению дисциплины

Дисциплина «Дополнительные главы алгебраической геометрии в криптографии» имеет двустороннюю направленность. С одной стороны, в ходе ее освоения происходит углубление знакомства студентов с одной из наиболее технически насыщенных и быстро развивающихся отраслей «чистой» математики, которое не может даться без усилий. С другой стороны, такое знакомство не является самоцелью, а лишь служит базой для изложения алгоритмов. Как правило, «прикладной» аспект воспринимается студентами с большей готовностью, несмотря на громоздкость самих алгоритмов. Основная трудность курса – обилие теоретического материала, поэтому разбор теории при самоподготовке необходим. Круг учебных задач, предлагаемых студентам, весьма узок; задачи в основном несложны и совершенно посильны при некотором усердии со стороны добросовестного студента. Курс готовит базу для разбора и применения алгоритмов, в него не вошедших, а быть может, приоткрывает возможность для разработки новых.