

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
Методы 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.

1. Цели освоения дисциплины

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

2. Место дисциплины в структуре образовательной программы

Данная дисциплина относится к базовой части образовательной и является дисциплиной специализации.

Она опирается на знания, полученные студентами в ходе изучения дисциплин «Алгебра», «Геометрия», «Избранные вопросы алгебры», «Алгебраическая алгоритмика», «Общая алгебра», «Алгебраические структуры».

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)	Перечень планируемых результатов обучения
Профессионально-специализированные компетенции	
ПСК-2.3 Обладает способностью строить математические модели для оценки безопасности компьютерных систем и анализировать компоненты системы безопасности с использованием современных математических методов	Знать: основные понятия и результаты теории эллиптических кривых Уметь: применять алгоритмы, использующие групповую структуру на эллиптической кривой Владеть навыками: формального дифференцирования в алгебре полиномов, вычислений в полях конечной характеристики, работы с проективным заданием кривой

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	СР	

			лекции	практические	лабораторные	консультации	аттестационные испытания		
1	Вводная лекция: алгебраическая геометрия и защита информации	9	8	8		2		20	
2	Эллиптические кривые. Гиперэллиптическая кривая и ее якобиан	9	14	14		2		20	Контрольная работа
3	Некоторые алгоритмы с использованием эллиптических кривых	9	14	14		3		20	
							0,3	4,7	зачёт
	ИТОГО		36	36		7	0,3	64,7	

Содержание разделов дисциплины:

1. Вводная лекция: алгебраическая геометрия и защита информации. Современный подход к геометрии. Предмет алгебраической геометрии. Зачем специалисту по защите информации нужна алгебраическая геометрия? Проективное пространство над произвольным полем. Открытые и замкнутые подмножества аффинного и проективного пространств (топология Зариского). Аффинные карты на проективной плоскости и проективное замыкание плоской алгебраической кривой. Пример: проективные коники. Представление о групповом алгебраическом многообразии (сложение точек на конике). Кольцо регулярных и поле рациональных функций замкнутого алгебраического множества. Регулярное отображение и изоморфизм замкнутых алгебраических множеств. Представление о бирациональном изоморфизме.

2. Эллиптические кривые. Гиперэллиптическая кривая и ее якобиан. Касательные и точки перегиба плоской кривой над произвольным полем. Точки перегиба кубической кривой, их расположение. Сложение точек на плоской кубике. Нормальные формы уравнения неособой плоской кубической кривой. Особые кубические кривые. Группа неособых точек особой кубической кривой и ее характеристика. Нерациональность эллиптической кривой. Дискриминант и j -инвариант кубической кривой. Случай нулевого дискриминанта. Сложение точек эллиптической кривой в координатах. Эллиптические функции. Функция Вейерштрасса. Параметризация комплексной эллиптической кривой. Сложение точек и сложение значений параметра. 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-функция гиперэллиптической кривой.

3. Некоторые алгоритмы с использованием эллиптических кривых. Факторизация целого числа с использованием эллиптической кривой: метод Ленстры. Дискретное логарифмирование на эллиптической кривой: метод Полларда. Влияние комплексного умножения на сложность логарифмирования. Функция Вейля и метод ее вычисления. 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 изложение материала, осуществляемое преимущественно в виде монолога преподавателя. 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. 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>

2. Тимофеева Н. В. Алгебраические структуры Ч. 1 - Ярославль: ЯрГУ, 2021. <http://www.lib.uniyar.ac.ru/edocs/iuni/20210203.pdf>

б) дополнительная литература

1. Мартынов Л. М. Алгебра и теория чисел для криптографии: учебное пособие для вузов — Санкт-Петербург: Лань, 2022. <https://reader.lanbook.com/book/189446>

2. М. Атья, И. Макдональд Введение в коммутативную алгебру. – М.: Мир, 1972.

3. Кокс Д., Литтл Дж., О’Ши Д. Идеалы, многообразия и алгоритмы. Введение в вычислительные аспекты алгебраической геометрии и коммутативной алгебры - М.: Мир, 2000. <https://djvu.online/file/eiimwj1ccBbs6?ysclid=ljzq1a9rn920127368>

4. Ишмухаметов Ш.Т. Методы факторизации натуральных чисел: учебное пособие – Казань, Казанский ун-т, 2011. <http://mathscinet.ru/files/IshmuxametovST.pdf>

5. Рид, М. Алгебраическая геометрия для всех / М. Рид. Пер. с англ. - М.: Мир, 1991. <https://djvu.online/file/rfNKtbiiu4tHp?ysclid=ljzq45udvh161710909>

6. Ростовцев, А. Г. Алгебраические основы криптографии. - СПб.: Мир и семья, 2000.

7. Алгебраическая геометрия и ее приложения. / отв. ред. С. М. Никольский - М.: Наука, 1984. - 229 с.

8. Шафаревич И. Р. Основы алгебраической геометрии. / И. Р. Шафаревич - 3-е изд., доп. - М.: МЦНМО, 2007. - 588 с.

9. Cox D., Little J., O’Shea D. Using Algebraic Geometry, 2nd ed., Graduate texts in Math, vol.185, Springer, 2004.

<https://djvu.online/file/jwTY9oNhPWp1?ysclid=ljzq65rgok496841099>

10. Gallian J. Contemporary Abstract Algebra. Cengage Learning, 2010.

<https://djvu.online/file/E2gpfrHdFjRgr?ysclid=ljzq70vucm862792622>

11. 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
«Методы алгебраической геометрии в криптографии»**

**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**

Примеры задач для самостоятельного решения (в качестве домашних заданий)

1. Дана кривая, определенная над полем характеристики $\neq 2,3$: $y^2 + 2xy = x^3 - x^2$
А) Выясните любым известным вам способом, особа она или нет.
Б) Если кривая особа, определите координаты особой точки.
2. Дана кривая, определенная над полем характеристики 2: $y^2 + y = x^3 + x^2$
А) Выпишите явные формулы сложения точек на такой кривой.
Б) Вычислите координаты точки $2P$, если $P(1,1)$.
3. Охарактеризовать особые точки кубической кривой (характеристика произвольная)
 $x^3 - y^2z - yz^2 - x^2z = 0$.
4. Вычислите координаты точек перегиба кривой (характеристика произвольная)
 $x^3 - y^2z - yz^2 = 0$.
5. Вычислите дискриминант и j -инвариант эллиптической кривой (в характеристике 0)
6. 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.
7. В точке перегиба эллиптической кривой проведена касательная. В какой еще точке она пересечет кривую?
8. Кубическая кривая над алгебраически замкнутым полем совпадает со своим гессианом. Что собой представляет такая кривая?
9. Покажите, что точки кручения эллиптической кривой образуют группу.

Вариант контрольной работы

1. Дана кривая, определенная над полем характеристики $\neq 2,3$: $y^2 + 2xy = x^3 - x^2$
А) Выясните любым известным вам способом, особа она или нет.
Б) Если кривая особа, определите координаты особой точки и тип особенности.
2. Дана кривая, определенная над полем характеристики 2: $y^2 + y = x^3 + x^2$
А) Выпишите явные формулы сложения точек на такой кривой.
Б) Вычислите координаты точки $2P$, если $P(1,1)$.

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

Прием зачета проводится (по выбору студента) либо в виде собеседования по вопросам прилагаемого списка, либо на основании подготовленной студентом заранее программной реализации одного из алгоритмов (см. список задач для программирования).

Список вопросов к зачету

1. Аффинные алгебраические множества и плоские алгебраические кривые над полем.
2. Проективная плоскость. Проективные алгебраические множества. Проективное замыкание плоской аффинной кривой. Бесконечно удаленные точки проективной кривой.
3. Аффинные и проективные коники. Аффинная и проективная классификации коник над полем действительных чисел. Сложение точек на конике.
4. Касательные и точки перегиба плоской кривой над произвольным полем. Точки перегиба кубической кривой, их расположение.
5. Сложение точек на плоской кубике.
6. Нули формы степени d на проективной прямой.
7. Нормальные формы уравнения неособой плоской кубической кривой.
8. Особые кубические кривые. Группа неособых точек особой кубической кривой и ее характеристика.
9. Нерациональность эллиптической кривой.
10. Дискриминант и j -инвариант кубической кривой. Случай нулевого дискриминанта.
11. Сложение точек эллиптической кривой в координатах.
12. Эллиптические функции.
13. Функция Вейерштрасса.
14. Параметризация комплексной эллиптической кривой. Сложение точек и сложение значений параметра.
15. Эллиптические кривые над полем рациональных чисел. Теоремы Морделла – Вейля и Мазура. Каноническая высота точки и спаривание Нерона – Тейта.
16. Изоморфизмы эллиптических кривых. Изоморфизмы над полями характеристики, отличной от 2 и 3.
17. Изоморфизмы эллиптических кривых над полями характеристик 2 и 3.
18. Рациональное отображение и бирациональный изоморфизм кривых.
19. Эндоморфизмы групповой структуры эллиптической кривой. Кривые с комплексным умножением.
20. Изогения эллиптических кривых.
21. Изоморфизмы эллиптических кривых в форме Лежандра.
22. Дивизоры на алгебраической кривой. Группа дивизоров. Линейная эквивалентность. Якобиан кривой. Критерий того, что дивизор на эллиптической кривой является дивизором функции.
23. Спаривание Вейля и метод его вычисления.
24. Норма и след в конечных полях.
25. Эллиптические кривые над конечными полями. Дзета-функция неособой алгебраической кривой.
26. Гиперэллиптические кривые и дивизоры на них.
27. Якобиан и дзета-функция гиперэллиптической кривой.
28. Факторизация целого числа с использованием эллиптической кривой: метод Ленстры.
29. Дискретное логарифмирование на эллиптической кривой: метод Полларда.
30. Влияние комплексного умножения на сложность логарифмирования.
31. Функция Вейля и метод ее вычисления.
32. Сложение в якобиане гиперэллиптической кривой.
33. Логарифмирование с использованием функции Вейля.
34. Логарифмирование в якобиане гиперэллиптической кривой.

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. Расчет числа точек на эллиптической кривой: алгоритм Чуфа.
5. Генерация эллиптической кривой с $j=0$ над полем длины p , с указанием циклической подгруппы в ней.
6. Генерация эллиптической кривой с $j=1728$ над полем длины p , с указанием циклической подгруппы в ней.
7. Генерация эллиптической кривой с комплексным умножением.

3. Методические рекомендации преподавателю по процедуре оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Целью процедуры оценивания является определение степени овладения студентом ожидаемыми результатами обучения (знаниями, умениями, навыками и (или) опытом деятельности).

Процедура оценивания степени овладения студентом ожидаемыми результатами обучения осуществляется с помощью методических материалов, представленных в разделе «Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций»

Пороговый уровень (общие характеристики):

- владение основным объемом знаний, умений и навыков по программе дисциплины;
- знание основной терминологии данной области знаний, стилистически грамотное, логически правильное изложение ответа на вопросы без существенных ошибок;
- владение инструментарием дисциплины, умение его использовать в решении стандартных (типовых) задач;
- способность самостоятельно применять типовые решения в рамках рабочей программы дисциплины;
- усвоение основной литературы, рекомендованной рабочей программой дисциплины;
- знание базовых теорий, концепций и направлений по изучаемой дисциплине;
- самостоятельная работа на практических и лабораторных занятиях, периодическое участие в групповых обсуждениях, достаточный уровень культуры исполнения заданий.

Продвинутый уровень (общие характеристики):

- достаточно полные и систематизированные знания в объеме программы дисциплины;
- использование основной терминологии данной области знаний, стилистически грамотное, логически правильное изложение ответа на вопросы, умение делать выводы;
- владение инструментарием дисциплины, умение его использовать в решении учебных и профессиональных задач;
- способность самостоятельно решать сложные задачи (проблемы) в рамках рабочей программы дисциплины;
- усвоение основной и дополнительной литературы, рекомендованной рабочей программой дисциплины;

- умение ориентироваться в базовых теориях, концепциях и направлениях по изучаемой дисциплине и давать им сравнительную оценку;
- самостоятельная работа на практических и лабораторных занятиях, участие в групповых обсуждениях, высокий уровень культуры исполнения заданий.

Высокий уровень (общие характеристики):

- систематизированные, глубокие и полные знания по всем разделам дисциплины;
- точное использование терминологии данной области знаний, стилистически грамотное, логически правильное изложение ответа на вопросы, умение делать обоснованные выводы;
- безупречное владение инструментарием дисциплины, умение его использовать в постановке и решении научных и профессиональных задач;
- способность самостоятельно и творчески решать сложные задачи (проблемы) в рамках рабочей программы дисциплины;
- полное и глубокое усвоение основной и дополнительной литературы, рекомендованной рабочей программой дисциплины;
- умение ориентироваться в основных теориях, концепциях и направлениях по изучаемой дисциплине и давать им критическую оценку;
- активная самостоятельная работа на практических и лабораторных занятиях, творческое участие в групповых обсуждениях, высокий уровень культуры исполнения заданий.

Описание процедуры выставления оценки

В зависимости от уровня сформированности компетенции по окончании освоения дисциплины студенту выставляется оценка «зачтено» или «не зачтено».

Оценка «зачтено» выставляется студенту, проявившему на мероприятии промежуточной аттестации умения и навыки, соответствующие уровню, не ниже чем на пороговом уровне:

- **знает** понятие плоской алгебраической кривой, эллиптической кривой, понятие рациональной кривой и факт нерациональности эллиптической кривой, теорему Пуанкаре, канонические формы уравнений эллиптической кривой, понятие дискретного логарифмирования.
- **умеет** находить особые точки и точки перегиба алгебраической кривой, переходить от аффинного к проективному уравнению кривой и обратно, вычислять сумму точек на эллиптической кривой в форме Вейерштрасса (формулы сложения помнить не требуется).
- **владеет** навыками формального дифференцирования в алгебре полиномов, вычислений в полях конечной характеристики
- **ориентируется** в вычислительных приложениях эллиптических кривых: может перечислить некоторые из этих приложений.

Оценка «не зачтено» выставляется студенту, проявившему на мероприятии промежуточной аттестации умения и навыки, соответствующие уровню, ниже чем на пороговом уровне:

- **не знает** понятие плоской алгебраической кривой, эллиптической кривой, понятие рациональной кривой и факт нерациональности эллиптической кривой, теорему Пуанкаре, канонические формы уравнений эллиптической кривой, понятие дискретного логарифмирования.
- **не умеет** находить особые точки и точки перегиба алгебраической кривой, переходить от аффинного к проективному уравнению кривой и обратно, вычислять сумму точек на эллиптической кривой в форме Вейерштрасса (формулы сложения помнить не требуется).

-не может выполнить формальное дифференцирование в алгебре полиномов, вычисления в полях конечной характеристики.

-не ориентируется в вычислительных приложениях эллиптических кривых: не может назвать/описать ни одного из этих приложений.

Оценка «не зачтено» выставляется также студенту, получившему на зачете задание, но отказавшемуся отвечать.

Студентам, выбравшим для сдачи зачета программную реализацию алгоритма, оценка «зачтено» выставляется в случае, когда программа, составленная студентом, работает корректно, а студент может пояснить логику ее работы. В противном случае выставляется оценка «не зачтено».

Приложение № 2 к рабочей программе дисциплины «Методы алгебраической геометрии в криптографии»

Методические указания для студентов по освоению дисциплины

Дисциплина «Методы алгебраической геометрии в криптографии» имеет двустороннюю направленность. С одной стороны, в ходе ее освоения происходит знакомство студентов с одной из наиболее технически насыщенных и быстро развивающихся отраслей «чистой» математики, которое не может даваться 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.