МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

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

Механико-математический факультет

УТВЕРЖДАЮ
Декан механико-математического факультета
_____Захаров А.М.
"12" 11 2021 г.

Рабочая программа дисциплины

СПЕЦКУРС 10.1
ЭЛЛИПТИЧЕСКИЕ КРИВЫЕ И КРИПТОГРАФИЯ

Направление подготовки бакалавриата
02.04.01 – Математика и компьютерные науки

Профиль подготовки бакалавриата
Математические основы компьютерных наук

Квалификация (степень) выпускника
Магистр

Форма обучения
очная

Саратов,
2021

Статус	ФИО	Подпись	Дата
Преподаватель-разработчик	Сецинская Е.В.		12.11.2021
Председатель НМК	Тышкевич С.В.		12.11.2021
Заведующий кафедрой	Водолазов А.М.		12.11.2021.
Специалист Учебного управления			

1. Цели освоения дисциплины

Целями освоения дисциплины «Спецкурс 10.1» являются: познакомить студентов механико-математического факультета с некоторыми понятиями и методами алгебраической геометрии; привить навыки применения этих методов для решения отдельных задач; познакомить с основными задачами и методами их решений, встречающихся в теории эллиптических кривых.

2. Место дисциплины в структуре ООП

Дисциплина «Спецкурс 10.1» включена в часть, формируемую участниками образовательных отношений блока 1 «Дисциплины (модули)» ООП магистратуры. На ее изучение отводится 252 часа (72 часа аудиторной работы, 180 часов СР). Согласно учебному плану направления и профиля подготовки данный курс в третьем и четвертом семестрах заканчивается зачетом.

В курсе излагаются основные свойства эллиптических кривых и эллиптических функций, а также доказывается теорема о бирациональной классификации эллиптических кривых, что является необходимой теоретической базой для построения криптографических систем на эллиптических кривых.

Освоение данной дисциплины необходимо для написания выпускных квалификационных работ (магистерских работ).

3. Результаты обучения по дисциплине

Код и наименование компетенции	**Код и наименование индикатора (индикаторов) достижения компетенции**	**Результаты обучения**
УК-1 Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	**1.1_М.УК-1.** Анализирует проблемную ситуацию как систему, выявляя ее составляющие и связи между ними.	**Знать:** – постановку основных задач криптографии; – основные этапы проведения работ по обработке и анализу научно-технической информации и результатов исследований. **Уметь:** – анализировать проблемные ситуации, выделяя ее базовые составляющие; – выявлять связи между составляющими проблемной ситуации. **Владеть:** – навыками анализа проблемных ситуаций с выделением ее базовых составляющих.

	1.2_М.УК-1. Осуществляет поиск алгоритмов решения поставленной проблемной ситуации на основе доступных источников информации. Определяет в рамках выбранного алгоритма вопросы (задачи), подлежащие дальнейшей детальной разработке. Предлагает способы их решения.	**Знать:** – основные алгоритмы криптографии на эллиптических кривых и их применение; – способы решения задач, определенных в рамках выбранного алгоритма решения проблемной ситуации. **Уметь:** – находить и критически анализировать информацию, необходимую для решения поставленной проблемной ситуации. **Владеть:** – навыками поиска алгоритмов решения поставленной проблемной ситуации
	2.1_М.УК-1. Разрабатывает стратегию достижения поставленной цели как последовательность шагов, предвидя результат каждого из них и оценивая их влияние на внешнее окружение планируемой деятельности и на взаимоотношения участников этой деятельности.	**Знать:** – основные методы разработки стратегий достижения поставленной цели. **Уметь:** – оценить достоинства и недостатки различных вариантов решения задач при применении методов теории кодирования на эллиптических кривых. **Владеть:** – навыками выбора оптимального решения для поставленной задачи.
ПК-1 Способен демонстрировать фундаментальные знания математических и естественных наук, программирования и информационных технологий.	**1.1_М.ПК-1.** Понимает основные концепции, принципы, теории и факты, в области математических и (или) естественных наук, программирования и информационных технологий.	**Знать:** – основные концепции, принципы, теории и факты, связанные с эллиптическими кривыми и криптографией. **Уметь:** – использовать основные концепции, принципы, теории и факты, связанные с эллиптическими кривыми и криптографией. **Владеть:** – основными навыками, принципами, теорией и фактами, связанными с эллиптическими кривыми и криптографией.

	2.1_М.ПК-1. Формулирует и решает стандартные задачи в собственной научно- исследовательской деятельности.	**Знать:** – основные методы теории эллиптических кривых и криптографии для решения задач в собственной научно-исследовательской деятельности. **Уметь:** – применять методы теории эллиптических кривых и криптографии для решения задач в собственной научно-исследовательской деятельности. – обрабатывать и анализировать научно-техническую информацию для постановки и решения задач. **Владеть:** – навыками применения методов теории эллиптических кривых и криптографии для решения задач в собственной научно- исследовательской деятельности.
	3.1_М.ПК-1. Проводит научно-исследовательские работы в области математики и компьютерных наук.	**Знать:** – основные методы проведения научно-исследовательской деятельности при помощи задач теории эллиптических кривых и криптографии. **Уметь:** – проводить научно-исследовательскую деятельность при помощи задач теории эллиптических кривых и криптографии. **Владеть:** – навыками научно-исследовательской деятельности с применением задач теории эллиптических кривых и криптографии.

4. Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 7 зачетных единиц 252 часа.

1	2	3	4	5	6	7	8	9	10
№ п/п	**Раздел дисциплины**	**Семестр**	**Неделя семестра**	**Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)**					**Формы текущего контроля успеваемости *(по неделям семестра)* Формы промежуточной аттестации *(по семестрам)***
				Лекции	Практические занятия	КСР	СР	Контроль	
1	Бирациональная эквивалентность алгебраических кривых	3	1-6	6	6		24		Консультация, опрос
2	Эллиптические функции	3	7-12	6	6		24		Консультация, опрос
3	Бирациональная эквивалентность эллиптических кривых	3	13-18	6	6		24		Консультация, опрос
	Промежуточная аттестация	**3**							**Зачет**
	Итого за 3 семестр – *108 ч.*			**18**	**18**	**0**	**72**	**0**	
4	Криптография с открытым ключом	4	1-6	6	6		36		Консультация, опрос
5	Методы факторизации чисел	4	7-12	6	6		36		Консультация, опрос
6	Криптосистемы на эллиптических кривых	4	13-18	6	6		36		Консультация, опрос
	Промежуточная аттестация	**4**							**Зачет**
	Итого за 4 семестр – *144 ч.*			**18**	**18**	**0**	**108**	**0**	
	Общая трудоемкость дисциплины			**252ч.**					

Содержание дисциплины

1. Бирациональная эквивалентность алгебраических кривых.

Аффинные и проективные пространства. Аффинные и проективные алгебраические многообразия, их идеалы, кольца регулярных функций, поля рациональных функций. Неприводимость алгебраических многообразий. Размерность многообразий. Топология Зарисского. Регулярные и рациональные отображения. Различные определения бирациональной эквивалентности алгебраических многообразий. Бирациональная эквивалентность алгебраических кривых (определение и примеры). Особые и неособые алгебраические кривые. Бирациональная классификация неособых кривых 2-го порядка над полями R и C. Рациональность особых кривых 3-го порядка. Эллиптические кривые. Приведение уравнения эллиптической кривой к форме Вейерштрасса.

2. Эллиптические функции.

Теоремы о структуре групп периодов мероморфных функций. Свойства основных периодов. Эллиптические функции. Поле эллиптических функций. Параллелограмм периодов и его свойства. Теоремы, выражающие общие свойства эллиптических функций. Сходимость рядов голоморфных и мероморфных функций. Лемма о сходимости ряда степеней модулей решётки периодов. Определение и простейшие свойства функции Вейерштрасса и её производной. Дифференциальное уравнение для функции Вейерштрасса. Нули и полюса функций Вейерштрасса. Теорема о параметризации эллиптических кривых. Топологическое строение эллиптической кривой. Закон сложения для функций Вейерштрасса. Теорема о структуре поля эллиптических функций.

3. Бирациональная эквивалентность эллиптических кривых.

Первый критерий бирациональной эквивалентности для эллиптических кривых. Второй критерий бирациональной эквивалентности. Описание групп бирациональных автоморфизмов эллиптических кривых.

Приведённая форма параллелограмма периодов. Критерий бирациональной эквивалентности эллиптических кривых в терминах приведённого параллелограмма. Модулярная группа, её действие на верхней полуплоскости и её фундаментальная область (без доказательства). Модулярный инвариант и его основные свойства. Разложение модулярного инварианта в ряд Фурье на бесконечности. Теорема о значениях модулярного инварианта. Основной критерий бирациональной эквивалентности для эллиптических кривых. Теорема о параметризации эллиптических кривых эллиптическими функциями.

4. Криптография с открытым ключом.

Основные понятия и обозначения в криптографии. Некоторые примеры простых криптосистем. Биграммы и их преобразования. Действия с матрицами по модулю N. Шифрующие матрицы. Шифрующие аффинные преобразования. Основные принципы шифрования с открытым ключом. Классическая криптосистема с открытым ключом. Аутентификация отправителя. Хеш-функции. Обмен ключами. Вероятностное шифрование. Криптосистема RSA. Примеры. Задача дискретного логарифмирования. Система Диффи-Хеллмана обмена ключами. Криптосистема Мэсси-Омуры для передачи сообщений. Криптосистема Эль-Гамаля. Стандарты цифровой подписи. Алгоритм дискретного логарифмирования в конечных полях. Индексный алгоритм дискретного логарифмирования. Задача о рюкзаке. Задача о рюкзаке с быстрорастущим набором. Криптосистемы, использующие задачу о рюкзаке. Протоколы с нулевым разглашением и скрытая передача.

5. Методы факторизации чисел

Псевдопростые числа. Критерии псевдопростоты. Число Кармайкла, его свойства. Эйлеровы псевдопростые числа. Тесты на псевдопростоту

числа. Ро-метод факторизации Полларда. Примеры. Факторизация Ферма. Примеры. Факторные базы, их алгоритм. Эвристическая временная оценка. Цепные дроби. Алгоритм разложения на множители с помощью цепных дробей. Метод квадратичного решета. Примеры. Алгоритм решета в числовом поле.

6. Криптосистемы на эллиптических кривых

Кратные точки эллиптической кривой. Представление открытого текста точками эллиптической кривой. Задача дискретного логарифмирования на эллиптической кривой. Аналог ключевого обмена Диффи-Хеллмана. Аналог системы Мэсси-Омуры. Аналог системы Эль-Гамаля. Критерий простоты, использующий эллиптические кривые. Методы разложения на множители при помощи эллиптических кривых: p-1-метод Полларда, метод Ленстры. Примеры.

5. Образовательные технологии, применяемые при освоении дисциплины

Для реализации компетентностного подхода в учебном процессе применяются следующие образовательные технологии:

1) при проведении лекционных занятий: информационные лекции, проблемные лекции, лекции беседы, лекции дискуссии, лекции с заранее запланированными ошибками;

2) при проведении практических занятий: традиционные занятия, занятия исследования, проблемные ситуации, ситуации с ошибкой;

3) при организации самостоятельной работы студентов: поиск и обработка информации, в том числе с использованием информационно-телекоммуникационных технологий; исследование проблемной ситуации; постановка и решение задач из предметной области; отработка навыков применения стандартных методов к решению задач предметной области.

Успешное освоение материала курса предполагает большую самостоятельную работу студентов и руководство этой работой со стороны преподавателей. Применяются следующие формы контроля: устный опрос, проверка решения практических задач.

При обучении лиц с ограниченными возможностями здоровья и инвалидов используются подходы, способствующие созданию безбарьерной образовательной среды: технологии дифференциации и индивидуального обучения, применение соответствующих методик по работе с инвалидами, использование средств дистанционного общения, проведение дополнительных индивидуальных консультаций по изучаемым теоретическим вопросам и практическим занятиям, оказание помощи при подготовке к промежуточной и итоговой аттестации. Подготовка, при необходимости, учебных и контрольно-измерительных материалов в формах, доступных для изучения студентами с особыми образовательными потребностями (для студентов с нарушениями зрения учебные материалы подготавливаются с применением укрупненного шрифта, используются аудиозаписи занятий; для студентов с нарушением слуха предоставляются

электронные лекции, печатные раздаточные материалы с заданиями для самостоятельной работы).

При необходимости, для подготовки к ответу на практическом занятии, студентам с инвалидностью и студентам с ограниченными возможностями здоровья среднее время увеличивается в 1,5–2 раза по сравнению со средним временем подготовки обычного студента.

Для студентов с инвалидностью или с ограниченными возможностями здоровья форма промежуточной аттестации устанавливается с учетом индивидуальных психофизических особенностей (устно, письменно на бумаге, письменно на компьютере, в форме тестирования и т.п.). Промежуточная аттестация по дисциплине может проводиться в несколько этапов в форме рубежного контроля по завершению изучения отдельных тем дисциплины.

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

Самостоятельная внеаудиторная работа студентов проводится в форме изучения и анализа лекционного материала, изучения отдельных теоретических вопросов по предлагаемой литературе, подбора дополнительных источников для извлечения научно-технической информации, связанной с проблемами, изучаемыми в рамках данной дисциплины и решения задач с дальнейшим их разбором или обсуждением на аудиторных занятиях, подготовки к промежуточной аттестации.

Самостоятельная аудиторная работа студентов проводится в форме самостоятельного решения задач на практических занятиях с дальнейшим их разбором и обсуждением; поиска решений проблемных ситуаций, предложенных на лекциях и практических занятиях; поиска и устранения ошибок, заложенных в представлении материала преподавателем и допущенных другими студентами.

Текущий контроль усвоения дисциплины «Спецкурс 10.1» проводится в форме устных опросов на лекционных и практических занятиях, разбора и обсуждения решаемых задач на практических занятиях, контрольных работ.

Промежуточная аттестация по дисциплине «Спецкурс 10.1» проводится в форме *зачета*. Контрольные вопросы готовятся к каждому разделу.

Перечень вопросов для проведения зачета в 3 семестре.

1. Аффинные и проективные пространства.
2. Аффинные и проективные алгебраические многообразия, их идеалы, кольца регулярных функций, поля рациональных функций.
3. Неприводимость алгебраических многообразий.
4. Размерность многообразий.
5. Топология Зарисского.
6. Регулярные и рациональные отображения.

7. Различные определения бирациональной эквивалентности алгебраических многообразий.

8. Бирациональная эквивалентность алгебраических кривых (определение и примеры).

9. Особые и неособые алгебраические кривые. Бирациональная классификация неособых кривых 2-го порядка над полями R и C.

10. Рациональность особых кривых 3-го порядка.

11. Эллиптические кривые. Приведение уравнения эллиптической кривой к форме Вейерштрасса.

12. Теоремы о структуре групп периодов мероморфных функций.

13. Свойства основных периодов.

14. Эллиптические функции. Поле эллиптических функций. Параллелограмм периодов и его свойства.

15. Теоремы, выражающие общие свойства эллиптических функций.

16. Сходимость рядов голоморфных и мероморфных функций. Лемма о сходимости ряда степеней модулей решётки периодов.

17. Определение и простейшие свойства функции Вейерштрасса и её производной.

18. Дифференциальное уравнение для функции Вейерштрасса. Нули и полюса функций Вейерштрасса.

19. Теорема о параметризации эллиптических кривых. Топологическое строение эллиптической кривой.

20. Закон сложения для функций Вейерштрасса.

21. Теорема о структуре поля эллиптических функций.

22. Первый критерий бирациональной эквивалентности для эллиптических кривых.

23. Второй критерий бирациональной эквивалентности. Описание групп бирациональных автоморфизмов эллиптических кривых.

24. Приведённая форма параллелограмма периодов. Критерий бирациональной эквивалентности эллиптических кривых в терминах приведённого параллелограмма.

25. Модулярная группа, её действие на верхней полуплоскости и её фундаментальная область (без доказательства).

26. Модулярный инвариант и его основные свойства.

27. Разложение модулярного инварианта в ряд Фурье на бесконечности.

28. Теорема о значениях модулярного инварианта.

29. Основной критерий бирациональной эквивалентности для эллиптических кривых.

30. Теорема о параметризации эллиптических кривых эллиптическими функциями.

Перечень вопросов для проведения зачета в 4 семестре.

31. Основные понятия и обозначения в криптографии.

32. Некоторые примеры простых криптосистем. Биграммы и их преобразования.
33. Действия с матрицами по модулю N.
34. Шифрующие матрицы. Шифрующие аффинные преобразования.
35. Основные принципы шифрования с открытым ключом.
36. Классическая криптосистема с открытым ключом.
37. Аутентификация отправителя.
38. Хеш-функции.
39. Обмен ключами.
40. Вероятностное шифрование.
41. Криптосистема RSA. Примеры.
42. Задача дискретного логарифмирования.
43. Система Диффи-Хеллмана обмена ключами.
44. Криптосистема Мэсси-Омуры для передачи сообщений.
45. Криптосистема Эль-Гамаля.
46. Стандарты цифровой подписи.
47. Алгоритм дискретного логарифмирования в конечных полях.
48. Индексный алгоритм дискретного логарифмирования.
49. Задача о рюкзаке. Задача о рюкзаке с быстрорастущим набором.
50. Криптосистемы, использующие задачу о рюкзаке.
51. Протоколы с нулевым разглашением и скрытая передача.
52. Псевдопростые числа. Критерии псевдопростоты.
53. Число Кармайкла, его свойства.
54. Эйлеровы псевдопростые числа.
55. Тесты на псевдопростоту числа.
56. Ро-метод факторизации Полларда. Примеры.
57. Факторизация Ферма. Примеры.
58. Факторные базы, их алгоритм.
59. Эвристическая временная оценка.
60. Цепные дроби. Алгоритм разложения на множители с помощью цепных дробей.
61. Метод квадратичного решета. Примеры.
62. Алгоритм решета в числовом поле.
63. Кратные точки эллиптической кривой.
64. Представление открытого текста точками эллиптической кривой.
65. Задача дискретного логарифмирования на эллиптической кривой.
66. Аналог ключевого обмена Диффи-Хеллмана.
67. Аналог системы Мэсси-Омуры.
68. Аналог системы Эль-Гамаля.
69. Критерий простоты, использующий эллиптические кривые.
70. p-1-метод Полларда разложения на множители при помощи эллиптических кривых Примеры.
71. Метод Ленстры разложения на множители при помощи эллиптических кривых. Примеры.

7. Данные для учета успеваемости студентов в БАРС

Таблица 1.1 Таблица максимальных баллов по видам учебной деятельности.

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

Программа оценивания учебной деятельности студента

1 семестр

Лекции

Посещаемость, опрос, активность и др. от 0 до 20 баллов.

Лабораторные занятия

Не предусмотрены.

Практические занятия – от 0 до 20 баллов

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

Самостоятельная работа – от 0 до 20 баллов

Контроль качества и количества выполненных домашних работ – от 0 до 10 баллов, правильность выполнения – от 0 до 10 баллов.

Автоматизированное тестирование

Не предусмотрено.

Другие виды учебной деятельности

Не предусмотрено.

Промежуточная аттестация – зачет – от 0 до 40 баллов

при проведении промежуточной аттестации

ответ на «отлично» оценивается от 36 до 40 баллов;

ответ на «хорошо» оценивается от 31 до 35 баллов;

ответ на «удовлетворительно» оценивается от 25 до 30 баллов;

ответ на «неудовлетворительно» оценивается от 0 до 24 баллов.

Таким образом, максимально возможная сумма баллов за все виды учебной деятельности студента за 3 семестр по дисциплине «Спецкурс 10.1» составляет **100** баллов.

Таблица 2.1 Таблица пересчета полученной студентом суммы баллов по дисциплине «Спецкурс 10.1» в оценку (зачет):

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

4 семестр

Лекции

Посещаемость, опрос, активность и др. от 0 до 20 баллов.

Лабораторные занятия

Не предусмотрены.

Практические занятия – от 0 до 20 баллов

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

Самостоятельная работа – от 0 до 20 баллов

Контроль качества и количества выполненных домашних работ – от 0 до 10 баллов, правильность выполнения – от 0 до 10 баллов.

Автоматизированное тестирование

Не предусмотрено.

Другие виды учебной деятельности

Не предусмотрено.

Промежуточная аттестация – зачет – от 0 до 40 баллов

при проведении промежуточной аттестации

ответ на «отлично» оценивается от 36 до 40 баллов;

ответ на «хорошо» оценивается от 31 до 35 баллов;

ответ на «удовлетворительно» оценивается от 25 до 30 баллов;

ответ на «неудовлетворительно» оценивается от 0 до 24 баллов.

Таким образом, максимально возможная сумма баллов за все виды учебной деятельности студента за 4 семестр по дисциплине «Спецкурс 10.1» составляет **100** баллов.

Таблица 2.1 Таблица пересчета полученной студентом суммы баллов по дисциплине «Спецкурс 10.1» в оценку (зачет):

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

8. Учебно-методическое и информационное обеспечение дисциплины

а) литература:

1. *Фаддеев Д.К.*. Лекции по алгебре. СПб.; М.; Краснодар: Лань, 2007
2. *Виноградов И.М.* Основы теории чисел. СПб.; М.; Краснодар: Лань, 2006
3. *Гурвиц А., Курант Р.* Теория функций. М: «Наука», 1968.
4. *Коблиц Н.* Введение в эллиптические кривые и модулярные формы. М: «Мир», 1988.
5. *Ленг С.* Эллиптические функции. М: «Наука», 1984.

б) программное обеспечение и Интернет-ресурсы:

Лицензионное программное обеспечение:

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

Интернет-ресурсы:

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

9. Материально-техническое обеспечение дисциплины

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

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

Автор:

доцент, к.ф.-м.н., доцент кафедры КАиТЧ Е.В. Сецинская

Программа одобрена на заседании кафедры компьютерной алгебры и теории чисел от 12 ноября 2021 года, протокол № 4.