федеральное государственное бюджетное образовательное учреждение высшего образования «Мордовский государственный педагогический университет имени М.Е. Евсевьева»

Физико-математический факультет

Кафедра математики и методики обучения математике

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Наименование дисциплины (модуля): Современные проблемы геометрии
Уровень ОПОП: Бакалавриат

Направление подготовки: 44.03.05 Педагогическое образование (с двумя профилями подготовки)
Профиль подготовки: Информатика. Математика.
Форма обучения: Очная

Разработчики:
Ладошкин М. В., канд. физ. – мат наук, зав. кафедрой
Дербеденева Н.Н., канд. пед. наук, доцент

Программа рассмотрена и утверждена на заседании кафедры, протокол № 10 от 24.05.2017 года

Зав. кафедрой _____Ладошкин М. В.

Программа с обновлениями рассмотрена и утверждена на заседании кафедры, протокол № 1 от 31.08.2020 года

Зав. кафедрой Ладошкин М. В.

1. Цель и задачи изучения дисциплины

Цель изучения дисциплины - сформировать представление о будущего учителя о современных проблемах геометрии как разделе математики, ее основных задачах

Задачи дисциплины:

формировать умения студентов решать векторным методом задачи аффинного характера на взаимное расположение точек, прямых и плоскостей, используя куб, пирамиду, параллелепипед

формировать умения студентов решать векторным методом задачи метрического характера на нахождение расстояний, углов, площадей, используя куб, правильную пирамиду, правильный тетраэдр, параллелепипед;

формировать умения студентов в координатной форме, с помощью уравнений прямых и плоскостей, решать аффинные и метрические задачи стереометрии, используя в качестве объектов изучения куб, прямоугольный параллелепипед, правильный тетраэдр, правильную пирамиду, сферу, шар.

2. Место дисциплины в структуре ОПОП ВО

Дисциплина «Современные проблемы геометрии» относится к вариативной части учебного плана.

Дисциплина изучается на 5 курсе, в 10 семестре.

Для изучения дисциплины требуется: владение навыками дифференциального исчисления, знание основных алгебраических понятий, умение представлять математические модели геометрических объектов

Изучению дисциплины «Современные проблемы геометрии» предшествует освоение дисциплин (практик):

Математический анализ;

Алгебра;

Геометрия.

Область профессиональной деятельности, на которую ориентирует дисциплина «Современные проблемы геометрии», включает: образование, социальную сферу, культуру.

Освоение дисциплины готовит к работе со следующими объектами профессиональной деятельности:

- обучение;
- воспитание;
- развитие.

В процессе изучения дисциплины студент готовится к видам профессиональной деятельности и решению профессиональных задач, предусмотренных ФГОС ВО и учебным планом.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование компетенций и трудовых функций (профессиональный стандарт Педагог (педагогическая деятельность в сфере дошкольного, начального общего, основного общего, среднего общего образования) (воспитатель, учитель), утвержден приказом Министерства труда и социальной защиты №544н от 18.10.2013).

Выпускник должен обладать следующими профессиональными компетенциями (ПК) в соответствии с видами деятельности:

ПК-11. готовностью использовать систематизированные теоретические и практические знания для постановки и решения исследовательских задач в области образования
научно-исследовательская деятельность

ПК-11 готовностью использовать систематизированные теоретические и практические знания для постановки и решения исследовательских задач в области образования	знать: основные алгоритмы и протоколы на эллиптических кривых; понятия теории решёток • уметь: применять алгоритмы на эллиптических кривых для решения задач факторизации и дискретного логарифмирования • владеть: алгоритмами криптоанализа, основанными на эллиптических кривых, на теории решёток

4. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов	Десятый семестр
Контактная работа (всего)	**30**	**30**
Практические	30	30
Самостоятельная работа (всего)	**42**	**42**
Виды промежуточной аттестации		
Зачет		+
Общая трудоемкость часы	**72**	**72**
Общая трудоемкость зачетные единицы	**2**	**2**

5. Содержание дисциплины

5.1. Содержание модулей дисциплины

Модуль 1. Эллиптические кривые:

Алгебраические кривые и эллиптические кривые. Группа точек эллиптической кривой. Эллиптические кривые над полями действительных и рациональных чисел. Эллиптические кривые над конечными полями. Теорема Хассе. Структура групп эллиптических кривых. Алгоритм сложения и удвоения точек. Эллиптические кривые над GF(2n). Скалярное умножение на суперсингулярных кривых. Скалярное умножение на несуперсингулярных кривых. Формирование представления об эллиптических кривых в школьном курсе математики.

Модуль 2. Применение эллиптических кривых в защите информации:

Протоколы распределения ключей. Криптосистемы Эль-Гамаля. Протоколы цифровой подписи. Передача с забыванием. Факторизационный алгоритм Ленстры. Дискретный логарифм на эллиптических кривых. Гиперэллиптические кривые. Дивизоры и якобианы. Дзета-функция гиперэллиптической кривой. Дискретный логарифм на якобианах гиперэллиптических кривых. Процесс ортогонализации Грамма – Шмидта. Алгоритм Ленстры – Ленстры – Ловаша и его применение. Общая методика использования эллиптических кривых в криптографии. Задача об укладке ранца.

5.2 Содержание дисциплины: Практические (30 ч.)

Модуль 1. Эллиптические кривые: (16 ч.)

Тема 1. Общие понятия об эллиптических кривых. (2 ч.)

Алгебраические кривые и эллиптические кривые. Группа точек эллиптической кривой.

Тема 2. Эллиптические кривые над полями. (2 ч.)

Эллиптические кривые над полями действительных и рациональных чисел. Эллиптические кривые над конечными полями.

Тема 3. Теорема Хассе. (2 ч.)

Различные формулировки теоремы Хассе. Доказательство теоремы Хассе. Следствия из теоремы

Тема 4. Действия над эллиптическими кривыми. (2 ч.)

Скалярное умножение на суперсингулярных кривых. Скалярное умножение на несуперсингулярных кривых

Тема 5. Структура групп кривых (2 ч.)

Структура групп эллиптических кривых. Эллиптические кривые над GF(2n).

Тема 6. Алгоритм сложения точек на эллиптических кривых (2 ч.)

Алгоритм сложения точек на эллиптических кривых

Тема 7. Алгоритм удвоения точек на эллиптических кривых (2 ч.)

Алгоритм удвоения точек на эллиптических кривых

Тема 8. Понятие об эллиптических кривых в школьном курсе (2 ч.)

Формирование представления об эллиптических кривых в школьном курсе математики

Модуль 2. Применение эллиптических кривых в защите информации: (14 ч.)

Тема 9. Основные протоколы (2 ч.)

Протоколы распределения ключей. Криптосистемы Эль-Гамаля. Протоколы цифровой подписи.

Тема 10. Алгоритмы на кривых. (2 ч.)

Передача с забыванием. Факторизационный алгоритм Ленстры. Дискретный логарифм на эллиптических кривых

Тема 11. Алгоритм Ленстры – Ленстры – Ловаша (2 ч.)

Процесс ортогонализации Грамма – Шмидта. Алгоритм Ленстры – Ленстры – Ловаша и его применение..

Тема 12. Гиперэллиптические кривые (2 ч.)

Гиперэллиптические кривые. Дивизоры и якобианы. Дзета-функция гиперэллиптической кривой.

Тема 13. Функции на эллиптических кривых(2 ч.)

Дискретный логарифм на якобианах гиперэллиптических кривых.

Тема 14. Общая методика использования эллиптических кривых в криптографии (2 ч.)

Общая методика использования эллиптических кривых в криптографии.

Тема 15. Применение в школьном курсе. (2 ч.)

Применение теории эллиптических кривых в простейшем кодировании и в задачах школьной информатики. Задача об укладке ранца.

6. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

6.1 Вопросы и задания для самостоятельной работы Десятый семестр (42 ч.)

Модуль 1. Эллиптические кривые (21 ч.)

Вид СРС: Выполнение индивидуальных заданий

Выполнение индивидуального домашнего задания по теме " Эллиптические кривые"

Вид СРС: Подготовка к контрольной работе

Подготовка к контрольной работе по вычислительным алгоритма теории эллиптических кривых

Модуль 2. Применение эллиптических кривых в защите информации (21 ч.)

Вид СРС: Выполнение индивидуальных заданий

Выполнение индивидуального домашнего задания по теме «Защита информации на основе теории эллиптических кривых"

Вид СРС: Подготовка к контрольной работе

Подготовка к контрольной работе по вычислению гомологий цепных комплексов (при заданной короткой и длинной точных последовательностях)

7. Тематика курсовых работ(проектов)

Курсовые работы (проекты) по дисциплине не предусмотрены.

8. Оценочные средства для промежуточной аттестации

8.1 Компетенции и этапы формирования

Коды компетенций	Этапы формирования		
	Курс, семестр	Форма контроля	Модули (разделы) дисциплины
ПК-11	5 курс, Десятый семестр	Зачет	Модуль 1: Эллиптические кривые
ПК-11	5 курс, Десятый семестр	Зачет	Модуль 2: Применение эллиптических кривых в защите информации.

Сведения об иных дисциплинах, участвующих в формировании данных компетенций:

Компетенция ПК-11 формируется в процессе изучения дисциплин:

Аналитические методы исследования геометрических объектов, Визуализация решений математических задач, Воспитательная работа в обучении математике, Интеграция алгебраического и геометрического методов в обучении математике, Информационные технологии в научных исследованиях, Исследовательская и проектная деятельность в обучении математике, Компьютерная обработка результатов научного исследования, Методика обучения информатике, Методика обучения математике, Методы принятия решений, Научно-исследовательская работа, Общая теория линейных операторов и ее приложение к решению геометрических задач, Основные направления развития топологии, Подготовка учебных и научных документов в LaTe, Современный урок математики, Специальные методы математического моделирования, Экстремальные задачи в школьном курсе математики, Элементы конструктивной геометрии в школьном курсе математики.

8.2 Показатели и критерии оценивания компетенций, шкалы оценивания

В рамках изучаемой дисциплины студент демонстрирует уровни овладения компетенциями:

Повышенный уровень:

знает и понимает теоретическое содержание дисциплины; творчески использует ресурсы (технологии, средства) для решения профессиональных задач; владеет навыками решения практических задач.

Базовый уровень:

знает и понимает теоретическое содержание; в достаточной степени сформированы умения применять на практике и переносить из одной научной области в другую теоретические знания; умения и навыки демонстрируются в учебной и практической деятельности; имеет навыки оценивания собственных достижений; умеет определять проблемы и потребности в конкретной области профессиональной деятельности.

Пороговый уровень:

понимает теоретическое содержание; имеет представление о проблемах, процессах, явлениях; знаком с терминологией, сущностью, характеристиками изучаемых явлений; демонстрирует практические умения применения знаний в конкретных ситуациях профессиональной деятельности.

Уровень ниже порогового:

имеются пробелы в знаниях основного учебно-программного материала, студент допускает принципиальные ошибки в выполнении предусмотренных программой заданий, не способен продолжить обучение или приступить к профессиональной деятельности по окончании вуза без дополнительных занятий по соответствующей дисциплине.

Уровень сформированности компетенции	Шкала оценивания для промежуточной аттестации	Шкала оценивания по БРС
	Зачет	
Повышенный	зачтено	90 – 100%
Базовый	зачтено	76 – 89%
Пороговый	зачтено	60 – 75%
Ниже порогового	не зачтено	Ниже 60%

Критерии оценки знаний студентов по дисциплине

Оценка	Показатели
Зачтено	Студент знает: основные положения эллиптических кривых, понятия алгебраических кривых и эллиптических кривых, владеет вычислительными навыками техники гомологий. Умеет приводить примеры построения эллиптических кривых
Не зачтено	Студент демонстрирует незнание основного содержания дисциплины, обнаруживая существенные пробелы в знаниях учебного материала, допускает принципиальные ошибки в выполнении предлагаемых заданий; затрудняется делать выводы и отвечать на дополнительные вопросы преподавателя.

8.3 Вопросы, задания текущего контроля

Модуль 1: Эллиптические кривые

ПК-11 готовностью использовать систематизированные теоретические и практические знания для постановки и решения исследовательских задач в области образования

1. Сформулируйте определение топологического пространства.
2. Опишите классификацию точек в топологическом пространстве. Приведите примеры в различных топологиях
3. Опишите открытые и замкнутые множества.
4. Сформулируйте определение внутренних, внешних, предельных, граничных и изолированных точек в топологическом пространстве
5. Приведите примеры непрерывных отображений в различных топологических пространствах.

Модуль 2: Применение эллиптических кривых в защите информации:

ПК-11 готовностью использовать систематизированные теоретические и практические знания для постановки и решения исследовательских задач в области образования

1. Приведите два примера клеточного разбиения сферы .
2. Опишите понятие клеточного пространства.
3. Приведите примеры цепных комплексов и точных последовательностей.
4. Опишите понятие гомологий цепных комплексов.
5. Приведите примеры вычисления гомологий.
6. Опишите основные методы вычисления гомологий.

8.4 Вопросы промежуточной аттестации

Десятый семестр (Зачет, ПК-11)

1. Алгебраические кривые и эллиптические кривые
2. Группа точек эллиптической кривой
3. Эллиптические кривые над полями действительных и рациональных чисел
4. Эллиптические кривые над конечными полями
5. Теорема Хассе
6. Структура групп эллиптических кривых
7. Алгоритм сложения и удвоения точек
8. Эллиптические кривые над GF(2n)
9. Скалярное умножение на суперсингулярных кривых
10. Скалярное умножение на несуперсингулярных кривых
11. Протоколы распределения ключей
12. Криптосистемы Эль-Гамаля
13. Протоколы цифровой подписи
14. Передача с забыванием
15. Факторизационный алгоритм Ленстры
16. Дискретный логарифм на эллиптических кривых
17. Гиперэллиптические кривые
18. Дивизоры и якобианы
19. Дзета-функция гиперэллиптической кривой
20. Дискретный логарифм на якобианах гиперэллиптических кривых
21. Процесс ортогонализации Грамма – Шмидта
22. Алгоритм Ленстры – Ленстры – Ловаша и его применение
23. Задача об укладке ранца
24. Формирование представления об эллиптических кривых в школьном курсе математики
25. Общая методика использования эллиптических кривых в криптографии

8.5 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Промежуточная аттестация проводится в форме зачета.

Зачет позволяет оценить сформированность компетенций, теоретическую подготовку студента, его способность к творческому мышлению, готовность к практической деятельности, приобретенные навыки самостоятельной работы, умение синтезировать полученные знания и применять их при решении практических задач.

При балльно-рейтинговом контроле знаний итоговая оценка выставляется с учетом набранной суммы баллов.

Собеседование (устный ответ) на зачете

Для оценки сформированности компетенции посредством собеседования (устного ответа) студенту предварительно предлагается перечень вопросов или комплексных заданий, предполагающих умение ориентироваться в проблеме, знание теоретического материала, умения применять его в практической профессиональной деятельности, владение навыками и приемами выполнения практических заданий.

При оценке достижений студентов необходимо обращать особое внимание на:

– усвоение программного материала;
– умение излагать программный материал научным языком;
– умение связывать теорию с практикой;
– умение отвечать на видоизмененное задание;
– владение навыками поиска, систематизации необходимых источников литературы по изучаемой проблеме;
– умение обосновывать принятые решения;
– владение навыками и приемами выполнения практических заданий;
– умение подкреплять ответ иллюстративным материалом.

Тесты

При определении уровня достижения студентом с помощью тестового контроля необходимо обращать особое внимание на следующее:

– оценивается полностью правильный ответ;

– преподавателем должна быть определена максимальная оценка за тест, включающий определенное количество вопросов;

– преподавателем может быть определена максимальная оценка за один вопрос теста;

– по вопросам, предусматривающим множественный выбор правильных ответов, оценка определяется исходя из максимальной оценки за один вопрос теста.

9. Перечень основной и дополнительной учебной литературы

9.1 Список литературы

Основная литература

1. Глазырина, П.Ю. Нормированные пространства. Типовые задачи [Электронный ресурс] : учебное пособие / П.Ю. Глазырина, М.В. Дейкалова, Л.Ф. Коркина. - Екатеринбург : Издательство Уральского университета, 2012. - 108 с. – Режим доступа:s https://biblioclub.ru/index.php?page=book_red&id=239621&sr=1.

2. Игнаточкина, Л. А. Топология для бакалавров математики [Электронный ресурс] : учебное пособие / Л.А. Игнаточкина. - М. : Прометей, 2016. - 88 с. – Режим доступа:s https://biblioclub.ru/index.php?page=book_red&id=437314&sr=1.

3. Элементарная топология [Электронный ресурс] / О. Я. Виро, О. А. Иванов, Н. Ю. Нецветаев, В. М. Харламов. - Москва : МЦНМО, 2010. - 368 с. - URL https://biblioclub.ru/index.php?page=book_red&id=64196&sr=1

Дополнительная литература

1. Кузовлев, В.П. Курс геометрии: элементы топологии, дифференциальная геометрия, основания геометрии / В.П. Кузовлев. – Москва : Физматлит, 2012. – 207 с. : схем., ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=275554 (дата обращения: 24.09.2019). – Библиогр. в кн. – ISBN 978-5-9221-1360-1. – Текст электронный.

2. Мищенко, А.С. Краткий курс дифференциальной геометрии и топологии / А.С. Мищенко, А.Т. Фоменко. – Москва : Физматлит, 2004. – 300 с. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=69322 (дата обращения: 24.09.2019). – ISBN 978-5-9221-0442-5. – Текст : электронный.

10. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. http://school-collection.edu.ru - Единая коллекция цифровых образовательных ресурсов

2. http://www.matburo.ru/st_subject.php?p=ma - Математический анализ: учебники, лекции сайты, примеры В данном разделе предлагаются ссылки на лучшие материалы по математическому анализу.

3. http://www.allmath.ru/mathan.htm - Вся математика в одном месте. Это математически портал, на котором можно найти любой материал по математическим дисциплинам. Здесь представлены школьная, высшая, прикладная, олимпиадная математика.

11. Методические указания обучающимся по освоению дисциплины (модуля)

При освоении материала дисциплины необходимо:

– спланировать и распределить время, необходимое для изучения дисциплины;

– конкретизировать для себя план изучения материала;

– ознакомиться с объемом и характером внеаудиторной самостоятельной работы для полноценного освоения каждой из тем дисциплины.

Сценарий изучения курса:

– проработайте каждую тему по предлагаемому ниже алгоритму действий;

– изучив весь материал, выполните итоговый тест, который продемонстрирует готовность к сдаче зачета.

Алгоритм работы над каждой темой:

– изучите содержание темы вначале по лекционному материалу, а затем по другим источникам;

– прочитайте дополнительную литературу из списка, предложенного преподавателем;

– выпишите в тетрадь основные категории и персоналии по теме, используя лекционный материал или словари, что поможет быстро повторить материал при подготовке к зачету;

– составьте краткий план ответа по каждому вопросу, выносимому на обсуждение на лабораторном занятии;

– выучите определения терминов, относящихся к теме;

– продумайте примеры и иллюстрации к ответу по изучаемой теме;

– подберите цитаты ученых, общественных деятелей, публицистов, уместные с точки зрения обсуждаемой проблемы;

– продумывайте высказывания по темам, предложенным к лабораторному занятию.

Рекомендации по работе с литературой:

– ознакомьтесь с аннотациями к рекомендованной литературе и определите основной метод изложения материала того или иного источника;

– составьте собственные аннотации к другим источникам на карточках, что поможет при подготовке рефератов, текстов речей, при подготовке к зачету;

– выберите те источники, которые наиболее подходят для изучения конкретной темы.

12. Перечень информационных технологий

Реализация учебной программы обеспечивается доступом каждого студента к информационным ресурсам – электронной библиотеке и сетевым ресурсам Интернет. Для использования ИКТ в учебном процессе используется программное обеспечение, позволяющее осуществлять поиск, хранение, систематизацию, анализ и презентацию информации, экспорт информации на цифровые носители, организацию взаимодействия в реальной и виртуальной образовательной среде.

Индивидуальные результаты освоения дисциплины студентами фиксируются в электронной информационно-образовательной среде университета.

12.1Перечень программного обеспечения

1. Microsoft Windows 7 Pro
2. Microsoft Office Professional Plus 2010
3. 1С: Университет ПРОФ

12.2Перечень информационных справочных систем

1. Информационно-правовая система «ГАРАНТ» (http://www.garant.ru)
2. Справочная правовая система «КонсультантПлюс» (http://www.consultant.ru)

12.3Перечень современных профессиональных баз данных

1. Единое окно доступа к образовательным ресурсам (http://window.edu.ru)
2. Профессиональная база данных «Открытые данные Министерства образования и науки РФ» (http://xn----8sblcdzzacvuc0jbg.xn--80abucjiibhv9a.xn--p1ai/opendata/)

13. Материально-техническое обеспечение дисциплины(модуля)

Для проведения аудиторных занятий необходим стандартный набор специализированной учебной мебели и учебного оборудования, а также мультимедийное оборудование для демонстрации презентаций на лекциях. Для проведения практических занятий, а также организации самостоятельной работы студентов необходим компьютерный класс с рабочими местами, обеспечивающими выход в Интернет.

Индивидуальные результаты освоения дисциплины фиксируются в электронной информационно-образовательной среде университета.

Реализация учебной программы обеспечивается доступом каждого студента к

информационным ресурсам – электронной библиотеке и сетевым ресурсам Интернет. Для использования ИКТ в учебном процессе необходимо наличие программного обеспечения, позволяющего осуществлять поиск информации в сети Интернет, систематизацию, анализ и презентацию информации, экспорт информации на цифровые носители.

Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, курсового проектирования (выполнения курсовых работ).

Школьный кабинет математики.

Помещение укомплектовано специализированной мебелью и техническими средствами обучения.

Основное оборудование:

Наборы демонстрационного оборудования: автоматизированное рабочее место в составе (системный блок, монитор, клавиатура, мышь, гарнитура, проектор, интерактивная доска), магнитно-маркерная доска.

Учебно-наглядные пособия:

Помещения для самостоятельной работы.

Помещение укомплектовано специализированной мебелью и техническими средствами обучения.

Основное оборудование:

Компьютерная техника с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета (персональный компьютер 10 шт.).

Учебно-наглядные пособия:

Презентации.

Помещение для самостоятельной работы.

Читальный зал электронных ресурсов

Помещение укомплектовано специализированной мебелью и техническими средствами обучения

Основное оборудование:

Компьютерная техника с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду университета (компьютер 12 шт., мультимедийный проектор 1 шт., многофункциональное устройство 1 шт., принтер 1 шт.)

Учебно-наглядные пособия:

Презентации

Электронные диски с учебными и учебно-методическими пособиями