Белорусский государственный университет

УТВЕРЖДАЮ
Проректор по учебной работе и
образовательным инновациям
_____ О.Н. Здрок
«___» _____ 2020 г.

Регистрационный № УД-_9357_/уч.

ЭЛЛИПТИЧЕСКИЕ КРИВЫЕ

Учебная программа учреждения высшего образования
по учебной дисциплине для специальности:
1-31 03 01 Математика (по направлениям)
направление специальности:
1-31 03 01-01 Математика (научно-производственная деятельность)

2020 г.

Учебная программа составлена на основе образовательного стандарта ОСВО 1-31 03 01-2013 и учебного плана G31-140/уч. от 30.05.2013.

СОСТАВИТЕЛИ:

Тихонов Сергей Викторович – доцент кафедры высшей алгебры и защиты информации механико-математического факультета Белорусского государственного университета, кандидат физико-математических наук, доцент.

РЕЦЕНЗЕНТ:

Васильев Д.В., заведующий отделом теории чисел Института математики Национальной Академии Наук Республики Беларуси, кандидат физико-математических наук.

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ:

Кафедрой высшей алгебры и защиты информации
Белорусского государственного университета
(протокол № 11 от 25.05.2020);

Научно-методическим советом
Белорусского государственного университета
(протокол № 5 от 17.06.2020).

Зав. кафедрой высшей алгебры
и защиты информации, профессор В.В. Беняш-Кривец

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Цели и задачи учебной дисциплины

Целью дисциплины «Эллиптические кривые» является расширение, систематизация и закрепление у студентов знаний, методов и приемов их использования, связанных с теорией эллиптических кривых, повышение уровня профессиональной компетентности студентов, формирование понятия о возможностях одного из разделов современных алгебры и криптографии.

Образовательная цель: знакомство с основными понятиями алгебраической геометрии, а также теории эллиптических кривых, изучение свойств эллиптических кривых, изучение основных методов вычисления порядков групп точек эллиптических кривых над конечными полями.

Развивающая цель: формирование у студентов основ математического мышления, знакомство с методами математических доказательств, изучение алгоритмов решения конкретных математических задач, привитие студентам умения самостоятельно изучать учебную и научную литературу в области математики.

Основные задачи, решаемые в рамках изучения дисциплины «Эллиптические кривые»:

- ознакомить студентов с фундаментальными понятиями теории алгебраических многообразий такими, как аффинные и проективные многообразия, топология Зарискoго;
- изучить основы теории эллиптических кривых.
- ознакомить студентов со свойствами эллиптических кривых, используемыми в криптографических преобразованиях;
- развить у студентов аналитическое мышление и общую математическую культуру;
- привить студентам умение самостоятельно изучать учебную и научную литературу в области математики и ее приложений.

В результате изучения учебной дисциплины студент должен:

знать:

– основные понятия теории алгебраических многообразий;

– методы доказательств важнейших результатов, изучаемых в рамках учебной дисциплины «Эллиптические кривые»;

– алгоритмы решения задач по дисциплине «Эллиптические кривые»;

уметь:

– выполнять вычисления в группах точек эллиптических кривых над конечными полями;

– вычислять порядки групп точек специальных эллиптических кривых;

владеть:

– основными навыками решения задач, связанных с эллиптическими кривыми;

– методами доказательств основных теорем, встречающихся в курсе «Эллиптические кривые»;

– навыками самообразования и способами использования аппарата алгебры и теории чисел для проведения математических и междисциплинарных исследований.

Место учебной дисциплины в системе подготовки специалиста с высшим образованием.

Учебная дисциплина относится **к циклу** дисциплин специализаций компонента учреждения высшего образования.

Связи с другими учебными дисциплинами, включая учебные дисциплины компонента учреждения высшего образования, дисциплины специализации и др. Данная дисциплина опирается и использует изученные ранее сведения из дисциплин «Алгебра и теория чисел» и «Дополнительные главы алгебры».

Требования к компетенциям специалиста

В результате изучения дисциплины «Эллиптические кривые» студент должен обладать следующими компетенциями:

Академические компетенции:

АК-1. Уметь применять базовые научно-теоретические знания для решения теоретических и практических задач.

АК-2. Владеть системным и сравнительным анализом.

АК-3. Владеть исследовательскими навыками.

АК-4. Уметь работать самостоятельно.

АК-5. Быть способным вырабатывать новые идеи (обладать креативностью).

АК-6. Владеть междисциплинарным подходом при решении проблем.

АК-7. Иметь навыки, связанные с использованием технических устройств, управлением информацией и работой с компьютером.

АК-8. Обладать навыки устной и письменной коммуникаций.

АК-9. Уметь учиться, повышать свою квалификацию в течение всей жизни.

Социально-личностные компетенции:

СЛК-2. Быть способным к социальному взаимодействию.

СЛК-3. Обладать способностью к межличностным коммуникациям.

СЛК-5. Быть способным к критике и самокритике.

СЛК-6. Уметь работать в команде.

Профессиональные компетенции:

ПК-1. Разрабатывать практические рекомендации по использованию научных исследований, планировать и проводить экспериментальные исследования, исследовать патентоспособность и показатели технического уровня разработок программного обеспечения информационных систем.

ПК-2. Владеть основными методами, способами и средствами получения, хранения, переработки информации. Применять современные методы

проектирования информационных систем, использовать веб-сервисы, оформлять техническую документацию.

ПК-3. Применять методы математического анализа и моделирования, теоретического и экспериментального исследования в профессиональной деятельности и в областях знаний, непосредственно не связанных со сферой деятельности.

ПК-4. Разрабатывать и тестировать информационные системы, осуществлять защиту приложений и данных.

ПК-5. Заниматься аналитической и научно-исследовательской деятельностью в области математики и информационных технологий.

ПК-6. Использовать и развивать современные информационные технологии и средства автоматизации управленческой деятельности.

ПК-7. Проводить исследования в области эффективности решения производственных задач.

ПК-8. Работать с научной, нормативно-справочной и специальной литературой.

ПК-9. Осуществлять выбор оптимального варианта проведения научно-исследовательских работ.

ПК-13. Взаимодействовать со специалистами смежных профилей.

ПК-16. Готовить доклады, материалы к презентациям.

ПК-22. Работать с научной, технической и патентной литературой.

ПК-27. Реализовывать инновационные проекты в профессиональной деятельности.

Структура учебной дисциплины.

Дисциплина изучается в 8 семестре очной формы получения образования.

Всего на изучение учебной дисциплины «Эллиптические кривые» отведено 100 часов, в том числе: 36 аудиторных часов, из них: лекции – 32 часа, управляемая самостоятельная работа – 4 часа.

Трудоемкость учебной дисциплины составляет 3 зачетные единицы.

Форма текущей аттестации по учебной дисциплине – экзамен.

СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

Тема 1. Алгебраические основы

Группа. Подгруппа. Факторгруппа. Кольцо. Идеал. Простые и максимальные идеалы. Факторкольцо. Теорема о гомоморфизме колец. Поле. Характеристика поля. Степень расширения полей. Конечные поля. Число элементов в конечном поле. Мультипликативная группа конечного поля.

Тема 2. Основы алгебраической геометрии

Топология Зариского. Аффинные и проективные многообразия. Кольцо регулярных функций. Поле рациональных функций. Гладкие многообразия. Алгебраические кривые.

Тема 3. Уравнение Вейерштрасса

Дискриминант. Уравнение Вейерштрасса над полями различной характеристики.

Тема 4. Эллиптические кривые. Групповой закон

Обоснование группового закона. Формулы сложения точек в аффинных и проективных координатах. Вычисление кратной точки.

Тема 5. Вычисление порядка групп точек эллиптических кривых над конечными полями

Теорема Хассе о порядке группы точек эллиптической кривой над конечным полем. Дзета-функция эллиптической кривой. Теорема Вейля для эллиптической кривой.

Тема 6. Применение эллиптических кривых в криптографии с открытым ключом

Протокол обмена ключами Диффи–Хеллмана. Задача дискретного логарифмирования. Электронная цифровая подпись.

УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА УЧЕБНОЙ ДИСЦИПЛИНЫ

Дневная форма получения высшего образования

Номер раздела, темы	Название раздела, темы	Количество аудиторных часов					Количество часов по УСР	Формы контроля знаний
		лекции	практические занятия	семинарские занятия	лабораторные занятия	Иное		
1.	Алгебраические основы	10					2	Экспресс-опрос
2	Основы алгебраической геометрии	8						Экспресс-опрос
3	Уравнение Вейерштрасса	4						Экспресс-опрос
4.	Эллиптические кривые. Групповой закон	4					2	Контрольная работа
5	Вычисление порядка групп точек эллиптических кривых над конечными полями	4						Контрольная работа
6	Применение эллиптических кривых в криптографии с открытым ключом	2						Экспресс-опрос
	Итого	**32**					**4**	

ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

Перечень основной литературы

1. Knapp A.W. Elliptic Curves. Mathematical Notes. Princeton University Press. 2018.
2. Silverman J.H., Tate J. Rational points on elliptic curves. 2nd ed. Springer. 2015.
3. Шафаревич И.Р. Основы алгебраической геометрии, изд. 3-е, испр. и доп., МЦНМО, М., 2007.
4. Коблиц Н. Введение в эллиптические кривые и модулярные формы. М.: Мир. 1988.

Перечень дополнительной литературы

1. Ростовцев А.Г., Маховенко Е.Б. Теоретическая криптография. АНО НПО Профессионал. 2005.
2. Koblitz N. Algebraic aspects of cryptography. Springer. 2004.
3. Silverman J.H. The arithmetic of elliptic curves. 2nd ed. Springer. 2009.

Перечень рекомендуемых средств диагностики и методика формирования итоговой оценки

Формой текущей аттестации по дисциплине «Эллиптические кривые» учебным планом предусмотрен экзамен.

Контроль работы студента проходит в форме собеседования, выполнения самостоятельных работ и практических упражнений в аудитории, а также самостоятельной работы вне аудитории с предоставлением отчета с его устной защитой. Задания к самостоятельным работам составляются согласно содержанию учебного материала.

Рейтинговая оценка предусматривает использование весовых коэффициентов для текущего контроля знаний и текущей аттестации студентов по дисциплине.

Примерные весовые коэффициенты, определяющие вклад текущего контроля знаний и текущей аттестации в рейтинговую оценку:

Формирование оценки за текущую успеваемость:

– выполнение контрольной работы – 50 %;

– экспресс-опрос– 50 %.

Итоговая оценка формируется на основе 3-х документов:

1. Правила проведения аттестации студентов, курсантов, слушателей при освоении содержания образовательных программ высшего образования (Постановление Министерства образования Республики Беларусь №53 от 29.05.2012 г.).

2. ПОЛОЖЕНИЕ о рейтинговой системе оценки знаний студентов по дисциплине в Белорусском государственном университете (Приказ ректора БГУ №189-ОД от 31.03.2020).

3. Критерии оценки знаний и компетенций студентов по 10-балльной шкале (Письмо Министерства образования Республики Беларусь от 22.12.2003 г. № 21-04-1/105).

Рейтинговая оценка по дисциплине рассчитывается на основе оценки текущей успеваемости и экзаменационной оценки с учетом их весовых коэффициентов. Вес оценки по текущей успеваемости составляет 40%, экзаменационная оценка – 60%.

Примерный перечень заданий для управляемой самостоятельной работы

Тема 1. Алгебраические основы.

1. Сколько элементов в мультипликативной группе кольца $\mathbf{Z}/81\mathbf{Z}$?
2. Сколько элементов в поле, являющемся расширением степени 3 поля F_4?
3. Сколько корней в поле F_{32} имеет многочлен x^3+x+1?
4. Содержит ли поле F_{25} поле F_4?
5. Содержит ли поле F_{27} поле F_9?
6. Найти порядок группы $(\mathbf{Z}/121\mathbf{Z})^*$?
7. Какая характеристика у расширения степени 2 поля F_{25}?
8. Являются ли полями следующие множества с естественными операциями: $\mathbf{C}\backslash\mathbf{Z}$, $\mathbf{Z}/16\mathbf{Z}$, $M_2(\mathbf{Q})$?

   Форма контроля – экспресс-опрос

Тема 4. Эллиптические кривые. Групповой закон

9. Является ли проективная кривая, заданная над полем рациональных чисел уравнением $zy^2=x^3-xz^2$, эллиптической кривой?
10. Какой порядок точки P = (1,0) в группе точек эллиптической кривой, заданной над полем рациональных чисел уравнением $y^2=x^3-1$?
11. Сколько элементов второго порядка в группе $E(\mathbf{Q})$, где E — эллиптическая кривая, заданная над полем рациональных чисел уравнением $y^2=x^3-8$?
12. Сколько элементов второго порядка в группе $E(\mathbf{C})$, где E — эллиптическая кривая, заданная над полем комплексных чисел уравнением $y^2=x^3-9$?
13. Найдите порядок точки P = (2,3) эллиптической кривой, заданной уравнением $y^2=x^3+1$ над полем $\mathbf{F}_5$.
14. Найдите все $\mathbf{F}_4$-точки эллиптической кривой, заданной уравнением $y^2+y=x^3$.
15. Найдите все точки порядка 2 на эллиптической кривой, заданной уравнением $y^2=x^3+x$ над полем $\mathbf{F}_5$.
16. Найдите координаты точки -P для P = (0,1) на эллиптической кривой, заданной уравнением $y^2=x^3+x+1$ над полем F_3.
17. Пусть эллиптическая кривая E задана над полем $\mathbf{F}_2$ уравнением $y^2-xy=x^3+x^2-x$. Найти $|E(\mathbf{F}_{16})|$.

    Форма контроля – контрольная работа

Описание инновационных подходов и методов к преподаванию учебной дисциплины (эвристический, проектный, практико-ориентированный)

При организации образовательного процесса используется ***эвристический подход,*** который предполагает**:**

– осуществление студентами личностно-значимых открытий окружающего мира;

– демонстрацию многообразия решений большинства профессиональных задач и жизненных проблем;

– творческую самореализацию обучающихся в процессе создания образовательных продуктов;

– индивидуализацию обучения через возможность самостоятельно ставить цели, осуществлять рефлексию собственной образовательной деятельности.

При организации образовательного процесса используется ***практико-ориентированный подход,*** который предполагает***:***

– освоение содержание образования через решения практических задач;

– приобретение навыков эффективного выполнения разных видов профессиональной деятельности;

– ориентацию на генерирование идей, реализацию групповых студенческих проектов, развитие предпринимательской культуры;

– использованию процедур, способов оценивания, фиксирующих сформированность профессиональных компетенций.

При организации образовательного процесса ***используется метод проектного обучения,*** который предполагает***:***

– способ организации учебной деятельности студентов, развивающий актуальные для учебной и профессиональной деятельности навыки планирования, самоорганизации, сотрудничества и предполагающий создание собственного продукта;

– приобретение навыков для решения исследовательских, творческих, социальных, предпринимательских и коммуникационных задач.

Методические рекомендации по организации и выполнению самостоятельной работы студентов

Самостоятельная работа студентов - это любая деятельность, связанная с воспитанием мышления будущего профессионала. В широком смысле под самостоятельной работой следует понимать совокупность всей самостоятельной деятельности студентов как в учебной аудитории, так и вне её, в контакте с преподавателем и в его отсутствии.

Самостоятельная работа реализуется:

1. Непосредственно в процессе аудиторных занятий - на лекциях.

2. В контакте с преподавателем вне рамок расписания - на консультациях по учебным вопросам, в ходе творческих контактов, при ликвидации задолженностей, при выполнении индивидуальных заданий и т.д.

3. В библиотеке, дома, в общежитии, на кафедре при выполнении студентом учебных и творческих задач.

При изучении дисциплины организация самостоятельной работы студентов должна представлять единство трех взаимосвязанных форм:

1. Внеаудиторная самостоятельная работа;

2. Аудиторная самостоятельная работа, которая осуществляется под непосредственным руководством преподавателя;

3. Творческая, в том числе научно-исследовательская работа.

Примерный перечень вопросов к экзамену

1. Группа. Подгруппа.
2. Факторгруппа.
3. Кольцо. Идеал.
4. Простые и максимальные идеалы.
5. Факторкольцо.
6. Теорема о гомоморфизме колец.
7. Поле. Характеристика поля.
8. Степень расширения полей.
9. Конечные поля. Число элементов в конечном поле.
10. Мультипликативная группа конечного поля.
11. Топология Зариского. Аффинные и проективные многообразия.
12. Кольцо регулярных функций.
13. Поле рациональных функций.
14. Гладкие многообразия. Алгебраические кривые.
15. Уравнение Вейерштрасса.
16. Эллиптические кривые.
17. Формулы сложения точек в аффинных и проективных координатах.
18. Вычисление кратной точки.
19. Теорема Хассе о порядке группы точек эллиптической кривой над конечным полем.
20. Дзета-функция эллиптической кривой.
21. Теорема Вейля для эллиптической кривой.
22. Протокол обмена ключами Диффи–Хеллмана.
23. Задача дискретного логарифмирования.
24. Электронная цифровая подпись.

ПРОТОКОЛ СОГЛАСОВАНИЯ УЧЕБНОЙ ПРОГРАММЫ УВО

Название дисциплины, с которой требуется согласование	Название кафедры	Предложения об изменениях в содержании учебной программы по изучаемой учебной дисциплине	Решение, принятое кафедрой, разработавшей учебную программу (с указанием даты и номера протокола)

ДОПОЛНЕНИЯ И ИЗМЕНЕНИЯ К УЧЕБНОЙ ПРОГРАММЕ ПО ИЗУЧАЕМОЙ УЧЕБНОЙ ДИСЦИПЛИНЕ
на _____/_____ учебный год

№ п/п	Дополнения и изменения	Основание

Учебная программа пересмотрена и одобрена на заседании кафедры Высшей алгебры и защиты информации (протокол № ____ от _____ 20__ г.)

Заведующий кафедрой

_____ _____ _____
(степень, звание) (подпись) (И.О.Фамилия)

УТВЕРЖДАЮ
Декан факультета

_____ _____ _____
(степень, звание) (подпись) (И.О.Фамилия)