Белорусский государственный университет

УТВЕРЖДАЮ
Проректор по учебной работе и
образовательным инновациям
_____ О.И. Чуприс
"26" 06 2018 г.
Регистрационный № УД-5775/уч.

ЭЛЛИПТИЧЕСКИЕ КРИВЫЕ

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

2018 г.

Учебная программа составлена на основе ОСВО 1-31 03 01-2013 (30.08.2013) и учебного плана № G31-140/уч. 2013 г. (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.

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ:

Кафедрой высшей алгебры и защиты информации
(протокол № 10 от 30.05.2018)

Учебно-методической комиссией механико-математического факультета Белорусского государственного университета
(протокол № 8 от 19.06.2018)

Зав.кафедрой ВАиЗИ /В.В. Беняш-Кривец/

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

В настоящее время преобразования в эллиптических кривых положены в основу методов криптографической защиты информации с открытым ключом. Кроме того, аппарат теории эллиптических кривых оказывается полезным и при анализе криптографических алгоритмов, основанных на задачах факторизации целых чисел и дискретного логарифмирования в конечном поле.

Цель дисциплины «Эллиптические кривые»: изложить основы теории эллиптических кривых.

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 Зарисского;
- 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.

В результате изучения дисциплины специализации «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; Самостоятельно приобретать с помощь информационных технологий и использовать в практической деятельности новые знания и умения, в том числе в новых областях знаний, непосредственно не связанных со сферой деятельности.

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

ПК-13. Составлять документацию (графики работ, инструкции, планы, заявки, деловые письма и т.п.), а также отчетную документацию по установленным формам.

ПК-16. Разрабатывать и согласовывать представляемые материалы.

ПК-22. Осваивать и реализовывать управленческие инновации в сфере высоких технологий.

ПК-27. Разрабатывать новые информационные технологии на основе математического моделирования и оптимизации.

Дисциплина «Эллиптические кривые» является дисциплиной специализации и использует изученные ранее сведения из дисциплин «Алгебра и теория чисел» и «Дополнительные главы алгебры».

Учебная программа предназначена для студентов 4 курса (8 семестр) очной формы получения образования.

В соответствии с учебным планом специальности на изучение дисциплины отводится 100 часов, в том числе 36 часов аудиторных занятий. Распределение аудиторных часов по видам занятий: лекции – 32 часа, УСР – 4 часа. Текущая аттестация – 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

Номер раздела, темы	Название раздела, темы	Количество ауд. ч.					Количество часов УСР	Форма контроля знаний
		Лекции	Практические занятия	Семинарские занятия	Лабораторные занятия	Иное		
1	2	3	4	5	6	7	8	9
1.	**Алгебраические основы**	**10**						
1.1	Группа. Подгруппа. Факторгруппа	2						
1.2	Кольцо. Идеал. Простые и максимальные идеалы. Факторкольцо. Теорема о гомоморфизме колец	2						Экспресс-опрос
1.3	Поле. Характеристика поля. Степень расширения полей	2						
1.4	Конечные поля. Число элементов в конечном поле. Мультипликативная группа конечного поля	4						Проверка индивидуальных заданий
2	**Основы алгебраической геометрии**	**8**						
2.1	Топология Зариского. Аффинные и проективные многообразия	4						
2.2	Кольцо регулярных функций. Поле рациональных функций. Гладкие многообразия	2						Экспресс-опрос
2.3	Алгебраические кривые	2						Проверка индивидуальных

								заданий
3	**Уравнение Вейерштрасса**	**4**						
3.1	Дискриминант. Уравнение Вейерштрасса над полями различной характеристики	4						Экспресс-опрос
4.	**Эллиптические кривые. Групповой закон**	**4**					**2**	
4.1	Обоснование группового закона	2						Экспресс-опрос
4.2	Формулы сложения точек в аффинных и проективных координатах. Вычисление кратной точки	2						
	Проверка знаний по темам 1-4.						2	Контрольная работа
5	**Вычисление порядка групп точек эллиптических кривых над конечными полями**	**4**					**2**	
5.1	Теорема Хассе о порядке группы точек эллиптической кривой над конечным полем	2						Экспресс-опрос
5.2	Дзета-функция эллиптической кривой. Теорема Вейля для эллиптической кривой	2						
	Проверка знаний по теме 5.						2	Контрольная работа
6	**Применение эллиптических кривых в криптографии с открытым ключом**	**2**						
6.1	Протокол обмена ключами Диффи–Хеллмана. Задача дискретного логарифмирования. Электронная цифровая подпись	2						Экспресс-опрос
Итого		**32**					**4**	

ИНФОРМАЦИОННАЯ ЧАСТЬ

Основная литература:

1. Шафаревич И.Р. Основы алгебраической геометрии, изд. 3-е, испр. и доп., МЦНМО, М., 2007.

2. Коблиц Н. Введение в эллиптические кривые и модулярные формы. М.: Мир. 1988.

Дополнительная литература:

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.

4. Silverman J.H., Tate J. Rational points on elliptic curves. 2nd ed. Springer. 2015.

ОРГАНИЗАЦИЯ УПРАВЛЯЕМОЙ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

Управляемая самостоятельная работа студентов по дисциплине «Эллиптические кривые» проводится преподавателем во время аудиторных занятий. Контроль осуществляется в виде проведения экспресс-опросов, проверки индивидуальных заданий и контрольных работ. Полученные студентом количественные результаты УСР учитываются как составная часть оценки по дисциплине на экзамене.

ПРИМЕРНЫЙ ПЕРЕЧЕНЬ ЗАДАНИЙ УПРАВЛЯЕМОЙ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

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: $\mathbf{C}\backslash\mathbf{Z}$, $\mathbf{Z}/16\mathbf{Z}$, $M_2(\mathbf{Q})$?
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 $|E(\mathbf{F}_{16})|$.

ПРИМЕРНЫЙ ПЕРЕЧЕНЬ ИСПОЛЬЗУЕМЫХ СРЕДСТВ ДИАГНОСТИКИ РЕЗУЛЬТАТОВ УЧЕБНОЙ ДЕЯТЕЛЬНОСТИ

При чтении лекционного курса непосредственно в аудитории необходимо контролировать усвоение материала основной массой студентов путем проведения экспресс-опросов, проверки индивидуальных заданий по конкретным темам. Кроме того, предусматривается проведение контрольных работ. По итогам семестра проводится экзамен.

МЕТОДИКА ФОРМИРОВАНИЯ ИТОГОВОЙ ОЦЕНКИ

Итоговая оценка формируется на основе 3-х документов:

1. Правила проведения аттестации (Постановление №53 от 29.05.2012 г.).
2. Положение о рейтинговой системе БГУ (ред. 2015 г.).
3. Критерии оценки студентов (10 баллов).

ПРОТОКОЛ
СОГЛАСОВАНИЯ УЧЕБНОЙ ПРОГРАММЫ ПО ИЗУЧАЕМОЙ УЧЕБНОЙ ДИСЦИПЛИНЕ С ДРУГИМИ ДИСЦИПЛИНАМИ СПЕЦИАЛЬНОСТИ

Название учебной дисциплины, с которой требуется согласование	Название кафедры	Предложения об изменениях в содержании учебной программы учреждения высшего образования по учебной дисциплине	Решение, принятое кафедрой, разработавшей учебную программу (с указанием даты и номера протокола)
Дополнительные главы алгебры	Кафедра высшей алгебры и защиты информации	нет	Вносить изменения не требуется (протокол № 10 от 30.05.2018)

ДОПОЛНЕНИЯ И ИЗМЕНЕНИЯ К УЧЕБНОЙ ПРОГРАММЕ УВО
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

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

УТВЕРЖДАЮ
Декан факультета

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