Белорусский государственный университет

УТВЕРЖДАЮ
Проректор по учебной работе

_____ А.Л. Толстик
«_____»_____2015 г.

Регистрационный № УД-_1206_/уч.

ЭЛЛИПТИЧЕСКИЕ КРИВЫЕ НАД КОНЕЧНЫМИ ПОЛЯМИ

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)

2015г.

Учебная программа составлена на основе ОСРБ 1-31 03 01-2012, 30.08.2012 и учебного плана, регистрационный № G31-104/уч., 30.05.2012; по специальности 1-31 03 01 Математика (по направлениям) 1-31 03 01-01 Математика (научно-производственная деятельность).

СОСТАВИТЕЛЬ:

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 № 11 от 22.05.2015)

Учебно-методической комиссией механико-математического факультета Белорусского государственного университета
(протокол № 6 от 26.05.2015)

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. Целью спецкурса является ознакомление студентов с основными понятиями теории алгебраических многообразий, а также с основами теории эллиптических кривых.

Программа дисциплины «Эллиптические кривые над конечными полями» составлена в соответствии с требованиями образовательного стандарта высшего образования по специальности 1-31 03 01 «Математика» (по направлениям) и рассчитана на изучение дисциплины в седьмом семестре студентами очной формы обучения.

Цель дисциплины «Эллиптические кривые над конечными полями»: 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 над конечными полями»:

- 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, необходимыми для дальнейшего изучения криптографических преобразований, связанных с эллиптическими кривыми;
- 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 над конечными полями»;
– алгоритмы решения задач по дисциплине «Эллиптические кривые над конечными полями»;

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 над конечными полями»;
– навыками самообразования и способами использования аппарата алгебры и теории чисел для проведения математических и междисциплинарных исследований.

В соответствии с учебным планом специальности на изучение дисциплины отводится 70 часов, в том числе 34 часа аудиторных занятий. Распределение аудиторных часов по видам занятий: лекции – 22 часа, практические занятия – 8 часов, УСР – 4 часа. Рекомендуемая форма отчетности – экзамен.

СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

Тема 1. Основы алгебраической геометрии
Топология Зарискoго. Аффинные и проективные многообразия. Кольцо регулярных функций. Поле рациональных функций. Гладкие многообразия. Алгебраические кривые.

Тема 2. Уравнение Вейерштрасса
Дискриминант. Уравнение Вейерштрасса над полями различной характеристики.

Тема 3. Эллиптические кривые. Групповой закон
Обоснование группового закона. Формулы сложения точек в аффинных и проективных координатах. Вычисление кратной точки.

Тема 4. Морфизмы и эндоморфизмы эллиптических кривых
Изогении. Дуальные изогении. Кольцо эндоморфизмов.

Тема 5. Спаривание Вейля
Определение и свойства.

Тема 6. Вычисление порядка групп точек эллиптических кривых над конечными полями
Теорема Хассе. Дзета-функция. Гипотезы Вейля.

УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА

Номер раздела, темы, занятия	Название раздела, темы, занятия; перечень изучаемых вопросов	Количество аудиторных часов				Материальное обеспечение занятия (наглядные, методические пособия и др.)	Литература	Форма контроля знаний
		лекции	практические (семинарские) занятия	лабораторные занятия	контролируемая самостоятельная работа студента			
1	2	3	4	5	6	7	8	9
1	**Основы алгебраической геометрии**	**6**					1,2,3	
1.1	Топология Зариского. Аффинные и проективные многообразия	2						
1.2	Кольцо регулярных функций. Поле рациональных функций. Гладкие многообразия	2						
1.3	Алгебраические кривые	2						
2	**Уравнение Вейерштрасса**	**2**					3	
2.1	Дискриминант. Уравнение Вейерштрасса над полями различной характеристики	2						
3.	**Эллиптические кривые. Групповой закон**	**4**	**4**		**2**		3	
3.1	Обоснование группового закона	2	2					
3.2	Формулы сложения точек в аффинных и проективных координатах. Вычисление кратной точки	2	2		2			Самостоятельная работа
4	**Морфизмы и эндоморфизмы эллиптических кривых**	**2**					3	
4.1	Изогении. Дуальные изогении. Кольцо эндоморфизмов	2						
5	**Спаривание Вейля**	**2**					3	
5.1	Определение и свойства	2						
6	**Вычисление порядка групп точек эллиптических кривых над конечными полями**	**6**	**4**		**2**		3	

6.1	Теорема Хассе	2						
6.2	Дзета-функция	2	2		2			Самостоятельная работа
6.3	Гипотезы Вейля	2	2					
	Итого	**22**	**8**		**4**			

ИНФОРМАЦИОННАЯ ЧАСТЬ

ОСНОВНАЯ ЛИТЕРАТУРА

1. Шафаревич И.Р. Основы алгебраической геометрии. М.: Наука. 1972.
2. Хартсхорн Р. Алгебраическая геометрия. М.: Наука. 1977.
3. Silverman J.H. The arithmetic of elliptic curves. Springer-Verlag. 1985.

ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА

4. Ростовцев А.Г., Маховенко Е.Б. Теоретическая криптография. АНО НПО Профессионал. 1985.
5. Коблиц Н. Введение в эллиптические кривые и модулярные формы. М.: Мир. 1988.
6. Koblitz N. Algebraic aspects of cryptography. Springer-Verlag. 1998.

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

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)