МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования

«Воронежский государственный педагогический университет»

УТВЕРЖДАЮ
Проректор по учебной работе _____Г.П. Иванова

«____»_____20___г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Абстрактная и компьютерная алгебра

Уровень основной образовательной программы: ***бакалавриат***

Направление подготовки	***050100.62 Педагогическое образование***
Профиль	***Математика. Информатика***
Форма обучения	***очная***
Срок освоения ООП	***5 лет***
Кафедра	***Информатики и методики преподавания математики***

Разработчики:

Доцент кафедры информатики и МПМ М.В. Богданова

Доцент кафедры информатики и МПМ Р.Х. Вахитов

Начальник учебно-методического управления _____ Т.В. Майзель

Рабочая программа учебной дисциплины одобрена на заседании кафедры
информатики и методики преподавания математики
от «***31***» августа 20***11*** г. Протокол № ***1***

Заведующий кафедрой _____ А.С. Потапов

г. Воронеж – 2011 г.

Лист переутверждения рабочей программы учебной дисциплины

Рабочая программа:

одобрена на 20__/20__ учебный год. Протокол № ___ заседания кафедры

от “___”_____ 20___ г.

Ведущий преподаватель_____

Зав. кафедрой_____

одобрена на 20__/20__ учебный год. Протокол № ___ заседания кафедры

от “___”_____ 20___ г.

Ведущий преподаватель_____

Зав. кафедрой_____

одобрена на 20__/20__ учебный год. Протокол № ___ заседания кафедры

от “___”_____ 20___ г.

Ведущий преподаватель_____

Зав. кафедрой_____

одобрена на 20__/20__ учебный год. Протокол №___ заседания кафедры

от “___”_____ 20___ г.

Ведущий преподаватель_____

Зав. кафедрой_____

одобрена на 20__/20__ учебный год. Протокол № ___заседания кафедры

от “___”_____ 20___ г.

Ведущий преподаватель_____

Зав. кафедрой_____

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цели освоения дисциплины «Абстрактная и компьютерная алгебра»:

- усвоение студентами основных фактов общей (абстрактной) алгебры и символьных вычислений (компьютерной алгебры);
- овладение методами решения математических задач при помощи компьютерных систем (математических пакетов);
- повышение познавательного интереса к изучению компьютерной алгебры, используя активные методы и современные технические средства обучения;
- развитие самостоятельности, элементов поисковой деятельности, творческого подхода к решению задач;
- формирование умений и навыков обобщения информации, выделения главного в изученном материале, построения сообщения, умения высказывать предположения, объяснять и обосновывать их, выдвигать проблемы и переформулировать задачи.

В процессе освоения данной дисциплины студент формирует и демонстрирует следующие **компетенции:**

готов применять знания теоретической информатики, фундаментальной и прикладной математики для анализа и синтеза информационных систем и процессов (СК-8);

способен использовать математический аппарат, методологию программирования и современные компьютерные технологии для решения практических задач получения, хранения, обработки и передачи информации (СК-9).

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВПО

2.1. Учебная дисциплина «Абстрактная и компьютерная алгебра» (Б3.В.ОД.16) относится к обязательным дисциплинам вариативной части профессионального цикла.

2.2. Для изучения данной учебной дисциплины необходимы знания, умения и навыки, формируемые предшествующими дисциплинами*: алгебра и геометрия, математическая логика и теория алгоритмов, дискретная математика, теория чисел и числовые системы, теоретические основы информатики.*

2.3. Перечень последующих учебных дисциплин, для которых необходимы знания, умения и навыки, формируемые данной учебной дисциплиной: *ИКТ в образовании, методы и средства защиты информации, исследование операций и методы оптимизации.*

3. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

3.1. В результате изучения учебной дисциплины «Абстрактная и компьютерная алгебра» студенты овладевают следующими знаниями, умениями и навыками:

Знания:

- основные структуры абстрактной алгебры: группы, кольца, поля;
- основные понятия теории делимости в области целостности;
- алгебраические основы криптографии;
- основные понятия компьютерной алгебры.

Умения:

- применять математические пакеты к решению задач;
- использовать методы решения основных типов задач компьютерной алгебры;
- применять методы общей алгебры и теории чисел (теории делимости и теории сравнений) к изучению математических основ криптосистем.

Навыки:

- соблюдения основных требований информационной безопасности;
- алгебраических, теоретико-числовых, вычислительных преобразований;
- владения представлением о связи со школьной алгеброй.

3.2. Изучение данной учебной дисциплины направлено на формирование у обучающихся следующих компетенций:

СК-8 *готов применять знания теоретической информатики, фундаментальной и прикладной математики для анализа и синтеза информационных систем и процессов*

Структура компетенции	**Основные признаки уровня**	
	Базовый уровень	**Повышенный уровень**
Знает основные структуры абстрактной алгебры: группы, кольца, поля	знать теорию делимости в кольцах целых чисел и многочленов	знать теорию делимости в произвольных кольцах целостности
	знать теорию сравнений, включая теорему Эйлера и квадратичные вычеты	знать решение сравнений первого порядка с одной переменной
	знать компьютерные системы (математические пакеты) для анализа и синтеза информационных систем и процессов	знать основы компьютерной алгебры и основы представления данных знаний информатики и математики в компьютерных системах
Умеет применять математические пакеты к решению задач	уметь применять алгоритм Евклида при решении задач в кольцах целых чисел и многочленов	уметь применять алгоритм Евклида при решении задач в евклидовых кольцах
	уметь производить арифметические действия над сравнениями	уметь доказывать теорему Эйлера и свойства квадратичных вычетов
	уметь применять знания теоретической информатики, фундаментальной и прикладной математики при помощи компьютерных систем	уметь применять основы компьютерной алгебры при использовании знаний теоретической информатики, фундаментальной и прикладной математики для анализа и синтеза информационных систем и процессов
Владеет навыками соблюдения основных требований информационной безопасности	владеть терминологией простых и составных элементов и разложения на простые множители в кольцах целых чисел и многочленов	владеть терминологией простых и составных элементов и разложения на простые множители в произвольных кольцах целостности
	таблицами сложения и умножения классов вычетов	владеть теоретико-числовой терминологией теории сравнений
	владеть терминологией функций и команд компьютерных систем	владеть программированием в компьютерных системах

СК-9 *способен использовать математический аппарат, методологию программирования и современные компьютерные технологии для решения практических задач получения, хранения, обработки и передачи информации*

Структура компетенции	**Основные признаки уровня**	
	Базовый уровень	**Повышенный уровень**
Знает основные понятия теории делимости в области целостности, алгебраические основы криптографии	знать алгебраические операции и отношения, алгебраические системы	знать теоремы о гомоморфизмах алгебраических систем
	знать понятие криптосистемы (шифра)	знать аддитивную и мультипликативную группы классов вычетов
	знать работу со списками в компьютерных системах	знать представление об односторонней функции
Умеет использовать методы решения основных типов задач компьютерной алгебры	уметь выполнять абстрактные алгебраические операции	уметь строить конечные и бесконечные алгебраические системы
	уметь применять сравнения для изучения криптосистем с секретным ключом, с открытым ключом, электронную подпись	уметь применять квадратичные вычеты для изучения криптосистемы с бессознательным разглашением информации
	уметь использовать компьютерные системы с целью применения математического аппарата для решения практических задач получения, хранения, обработки и передачи информации	уметь применять алгебраические и теоретико-числовые методы к компьютерной алгебре и криптографии
Владеть навыками представления связи со школьной алгеброй	владеть терминологией основных понятий алгебраических систем	владеть методами построения изоморфизмов алгебраических систем
	владеть начальными основными понятиями криптографии	владеть алгебраическим и теоретико-числовым аппаратом для решения практических задач получения и защиты информации
	владеть методологией программирования в компьютерных системах	владеть современными компьютерными технологиями с применением компьютерных систем (математических пакетов) для решения практических задач получения, хранения, обработки и передачи информации

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1. ОБЪЕМ УЧЕБНОЙ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Вид учебной работы		**Всего часов**
Аудиторные занятия (всего)		36
В том числе:		-
Лекции (Л)		12
Практические занятия (ПЗ), Семинары (С)		
Лабораторные работы (ЛР)		24
Самостоятельная работа студента (СРС)		72
СРС в период промежуточной аттестации		
Вид промежуточной аттестации	зачет (З)	8 семестр
	экзамен (Э)	
ИТОГО: Общая трудоемкость	**часов**	108
	зач. ед.	3

4.2. СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

4.2.1. Разделы дисциплины, виды учебной деятельности и формы контроля

№ п/п	**Наименование раздела учебной дисциплины**	**Виды учебной деятельности, включая самостоятельную работу студентов (в часах)**					**Форма текущего контроля**
		Л	**ЛР**	**ПЗ**	**СРС**	**всего**	
1	Алгебраические системы	4	8		24	36	письменный опрос
2	Компьютерные системы	4	8		24	36	тест, контр. задания по ЛР
3	Математические основы криптографии	4	8		24	36	

4.2.2. Содержание разделов учебной дисциплины

№ п/п	Наименование раздела учебной дисциплины (модуля)	Содержание раздела в дидактических единицах
1	Алгебраические системы	1. Алгебраические операции и отношения. 2. Группы, кольца, поля. 3. Подгруппы группы. 4. Подкольца, идеалы колец. 5. Изоморфизмы групп и колец. 6 Конечные поля. 7. Теория делимости в области целостности.
2	Компьютерные системы	1. Математические пакеты: Mathematica, Mathcad 2. Представление данных. 3. Работа с математическими функциями. 4. Типовые средства программирования.
3	Математические основы криптографии	1. Теоретико-числовые методы в криптографии. 2. Шифры с секретным ключом. 3. Современная криптография: односторонние функции.

4.2.3. Образовательные технологии

№ п/п	Наименование раздела учебной дисциплины	Образовательные технологии
1	Алгебраические системы	Лекции: вводная лекция, проблемная лекция. Лабораторные работы: ситуация-упражнение, исследовательская ЛР с обсуждением.
2	Компьютерные системы	Лекции: вводная лекция, проблемная лекция. Лабораторные работы: ситуация-упражнение, исследовательская ЛР с обсуждением.
3	Математические основы криптографии	Лекции: лекция-информация, проблемная лекция, тематический зачет. Лабораторные работы: ситуация-упражнение, исследовательская ЛР с обсуждением.

____25____% - интерактивных занятий от объема аудиторных занятий

4.2.4. Лабораторный практикум

№ п/п	Наименование раздела учебной дисциплины	Наименование лабораторных работ	Всего часов
1	Алгебраические системы	1. Генерация простых чисел	2
		2. Разложение на простые множители	2
2	Компьютерные системы	3. Символьные вычисления	4
		4. Работа со списками	4
		5. Программирование на языке компьютерной алгебры MATHEMATICA (и др.)	4

3	Математические основы криптографии	6. Криптосистема с секретным ключом	2
		7. Криптосистема с открытым ключом	2
		8. Электронная подпись	2
		9. Бессознательное разглашение	2
	ИТОГО:		**24**

4.2.5. Примерная тематика курсовых работ

1. Применение компьютерных систем при преподавании теории чисел и теоретико-числовых методов криптографии
2. Применение компьютерных систем при преподавании высшей алгебры и алгебраических методов криптографии
3. Применение компьютерных систем при изучении дискретной математики.
4. Применение компьютерных систем при изучении математической логики и теории алгоритмов.
5. Применение компьютерных систем при изучении математического анализа и дифференциальных уравнений и уравнений математической физики.
6. Применение программирования при исследовании конечных алгебраических систем, в частности, группоидов и неассоциативных колец.
7. Применение программирования при исследовании конечномерных неассоциативных алгебр.

4.3. САМОСТОЯТЕЛЬНАЯ РАБОТА СТУДЕНТА

4.3.1. Планирование СРС

№ п/п	Наименование раздела учебной дисциплины	Виды СРС	Всего часов
1	Алгебраические системы	Решение задач по следующим темам: примеры и простейшие свойства групп, колец и полей и их подалгебр и гомоморфизмов.	24
2	Компьютерные системы	Изучение встроенной графики компьютерной системы MATHEMATICA. Изучение функционального и процедурного программирования на языке компьютерной алгебры MATHEMATICA (и др.)	24
3	Математические основы криптографии	Составление мини-пакетов различных исторических и современных криптосистем. Изучение основ теории сложности в криптографии и проблемы идентификации	24
	ИТОГО:		**72**

Обязательные задания для СРС по всем разделам дисциплины:
- подготовка к лекциям и лабораторным работам;
- поиск теоретического и иллюстративного материала в сети Интернет;
- выполнение индивидуальных заданий.

5. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ КОНТРОЛЯ УСПЕВАЕМОСТИ И РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

5.1. Текущий контроль

В ходе текущего контроля оцениваются достижения студентов в процессе освоения дисциплины. Текущий контроль осуществляется с использованием накопительной балльно-рейтинговой системы и включает оценку самостоятельной (внеаудиторной) и аудиторной работы (в том числе рубежный контроль). В качестве оценочных средств используются:

· различные виды устного и письменного контроля (отчет по лабораторной работе, выступление с докладом, эссе и т.д.);

· компьютерное и/или бланочное тестирование;

· индивидуальные и/или групповые домашние задания, творческие работы, проекты, презентации, портфолио и т.д.;

· контрольные лабораторные работы.

5.2. Промежуточная аттестация по дисциплине

Промежуточная аттестация студентов по дисциплине предполагает зачет, который выставляется в соответствии с «Положением о балльно-рейтинговой системе ВГПУ».

Вопросы для подготовки к зачету

1. Основные понятия общей алгебры: алгебраические системы, алгебры, модели, гомоморфизмы и подсистемы алгебраических систем.
2. Бинарные отношения, их графы, графики. Свойства бинарных отношений.
3. Отношения эквивалентности и порядка.
4. Бинарные алгебраические операции, их свойства. Группоиды. Полугруппы.
5. Группы. Простейшие свойства и примеры конечных и бесконечных групп.
6. Подгруппы, нормальные подгруппы, фактор-группы. Гомоморфизмы групп.
7. Кольца. Простейшие свойства и примеры конечных и бесконечных колец.
8. Подкольца, идеалы колец, фактор-кольца. Гомоморфизмы колец.
9. Поля. Простейшие свойства и примеры конечных и бесконечных полей.
10. Кольцо многочленов. Делимость в кольце многочленов.
11. Кольцо целых чисел. Делимость в кольце целых чисел.
12. Сравнения. Простейшие свойства.
13. Классы вычетов по модулю. Теорема Эйлера.
14. Квадратичные вычеты и невычеты. Символы Лежандра и Якоби.
15. Символьные вычисления в компьютерных системах (Mathematica и др.)
16. Встроенная графика в компьютерных системах (Mathematica и др.)
17. Работа со списками в компьютерных системах (Mathematica и др.)
18. Функциональное программирование в компьютерных системах (Mathematica и др.)
19. Процедурное программирование в компьютерных системах (Mathematica и др.)
20. Вычисление выражений в компьютерных системах (Mathematica и др.)

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

6.1. Основная литература

1. Матрос Д.Ш., Поднебесова Г.Б. Элементы абстрактной и компьютерной алгебры. – М.: Академия, 2004. – 240 с.
2. Панкратьев Е.В. Элементы компьютерной алгебры. – М.: Бином, 2007. – 247 с.

3. Земор Ж. Курс криптографии. – Ижевск: Институт компьютерных исследований, 2006. – 256 с.
4. Дьяконов В.П. Mathematica 5.1/5.2/6 в математических и научно-технических расчетах. – М.:СОЛОН-Пресс, 2008. – 256 с.

6.2. Дополнительная литература

1. Кострикин А.И. Введение в алгебру. Часть 1. Основы алгебры. – М.: Физматлит, 2004. – 272 с.
2. Шмидский Я. К. Mathematica 5. Самоучитель. – М.: Издательский дом «Вильямс». 2004. – 592 с.
3. Нечаев В.И. Элементы криптографии. Основы защиты информации. – М.: Высшая школа, 1999. – 256 с.

6.3. Программное обеспечение и Интернет-ресурсы:

1. ПО для лабораторных работ: компьютерные системы Mathematica, Mathcad, Maple.
2. Образовательный математический сайт. – www.exponenta.ru.
3. Электронные библиотеки по математике. – www.4tivo.com/education/; www.matburo.ru/literat.php; www.plib.ru; http://nehudlit.ru; www.gaudeamus.omskcity.com; www.alleng.ru; www.symplex.ru; www.math.ru.

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

7.1. Требования к аудиториям (помещениям, местам) для проведения занятий:

Лекционные аудитории и компьютерные классы для проведения лабораторных работ должны быть оснащенные мультимедийным оборудованием для проведения интерактивных занятий[1].

Подключение к сети Интернет в компьютерном классе – обязательно, в лекционной аудитории – желательно.

7.2. Требования к оборудованию рабочих мест преподавателя и обучающихся:

РМП: Мультимедийное оборудование (ноутбук, или компьютер, с аудиоколонками, видеопроектор, интерактивный экран).

РМО: компьютеры с аудионаушниками (в соответствии с наполняемостью подгрупп), подключенные к сети Интернет. Необходимо наличие общедоступного сетевого диска для обмена информацией.

В компьютерном классе должно быть установлено следующее программное обеспечение:

- ОС Windows (не ниже XP);
- MS Office 2007 (2010): Word, Excel, PowerPoint и др.;
- проигрыватели мультимедийных файлов: FLV Player, KMPlayer, Windows Media Player и др.;
- Web-браузеры: Internet Explorer, Mozilla Firefox, Opera и др. с поддержкой Flash и Java (TM);
- ПО для проведения телеконференций: Skype, QIP Infium, Mail.Ru Агент.