МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Государственное образовательное учреждение

высшего профессионального образования

«САМАРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Механико-математический факультет

Кафедра алгебры и геометрии

УТВЕРЖДАЮ

Проректор по учебной работе

_____В.П.Гарькин

«_____»_____2011 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Теория чисел

(блок «Общие математические и естественнонаучные дисциплины»; раздел «Федеральный компонент»; основная образовательная программа специальности 090102 Компьютерная безопасность)

Самара

2011

Рабочая программа составлена на основании Государственного образовательного стандарта высшего профессионального образования специальности 090102 Компьютерная безопасность, утвержденного 05.04.2000г. (номер государственной регистрации 283 ИНФ/СП) и типовой (примерной) программы дисциплины «Теория чисел», одобренной Советом УМО по образованию в области информационной безопасности.

Составитель рабочей программы: канд. ф.-м. н., доцент Азовская Т.В.
Рецензенты: д. ф.-м. н., профессор Панов А.Н. **,** канд. ф.-м. н., доцент Воскресенская Г.В.

Рабочая программа утверждена на заседании кафедры алгебры и геометрии (протокол № 6 от «17» января 2011 г.)

Заведующий кафедрой
17 января 2011 г. _____ А.Н.Панов

СОГЛАСОВАНО
Декан
факультета
″____″ _____ 2011 г. _____ С.Я.Новиков

Начальник
методического отдела
″____″ _____ 2011 г. _____ Н.В.Соловова

ОДОБРЕНО
Председатель
методической
комиссии факультета
″____″ _____ 2011 г. _____ Е.Я.Горелова

1. **Цели и задачи дисциплины, ее место в учебном процессе, требования к уровню освоения содержания дисциплины.**

1.1. Цели и задачи изучения дисциплины

Цель дисциплины - изучение стандартного базового курса теории чисел и некоторых простейших алгоритмов, применяемых в криптографии. Формирование у студентов знаний и умений, позволяющих использовать теоретический материал в решении задач.

Задачи дисциплины:

- обозначить классические вопросы теории чисел и указать пути и способы их разрешения;
- научить пользоваться алгоритмами, предусмотренными курсом, ознакомить с арифметикой конечных колец и полей;
- подготовить студентов к восприятию современных алгоритмов теории чисел, применяемых в криптографии.

1.2. Требования к уровню подготовки студента, завершившего изучение данной дисциплины

Студенты, завершившие изучение данной дисциплины, должны:

Иметь представление:

- об основных задачах, решаемых в рамках классической теории чисел, о принципах, понятиях и теоремах лежащих в основе изучаемого курса;
- о теоретико-числовых проблемах, связанных с криптографией и теорией кодирования;
- об истории предмета.

Знать:

- базовую терминологию, основные понятия и теоремы, предусмотренные курсом.

Уметь:

- решать и анализировать задачи по данной дисциплине;
- формулировать и решать теоретико-числовые задачи на языке теории сравнений, в терминах конечных колец и полей;
- доказывать теоремы, формулировать свойства, применять возможности теории на практике.

1.3. Связь с предшествующими дисциплинами

Для усвоения курса по теории чисел требуются хорошие знания школьных разделов математики.

1.4. Связь с последующими дисциплинами

Основные понятия, теоремы и методы, курса теории чисел, являются базовыми при изучении современных методов теории чисел в криптографии, теории кодирования, дисциплинах специализации.

2. Содержание дисциплины

2.1. Объем дисциплины в виде учебной работы (в часах)

ОЧНАЯ ФОРМА ОБУЧЕНИЯ, 3-й семестр - экзамен

Вид учебных занятий	Количество часов
	семестр
Всего часов аудиторных занятий	**34**
Лекции	**34**
Всего часов самостоятельной работы	**46**
Подготовка к практическим занятиям	**46**
Всего часов по дисциплине	**80**

2.2. Разделы дисциплины и виды занятий

№ п/п	Название раздела дисциплины	Часы лекций
1	Делимость чисел	8
2	Арифметические функции	4
3	Числовые сравнения	4
4	Сравнения с неизвестным	4
5	Первообразные корни и индексы	4
6	Квадратичные вычеты	4
7	Кольца и поля классов вычетов	4
8	Приложение к криптографии	2
	Итого:	*34*

2.3. Лекционный курс

Раздел 1. Теория делимости в кольце целых чисел.

Делимость нацело, свойства. Деление с остатком, теорема существования и единственности, метод остатков. Наибольший общий делитель и наименьшее общее кратное, их свойства. Эквивалентность определений НОД и НОК на языке делимости и языке абсолютных величин. Алгоритм Евклида. Характеристическое представление НОД, алгоритм Кнута. Взаимно-простые числа, их свойства. Критерий взаимной простоты чисел. Простые числа, их свойства. Теорема о бесконечности множества простых чисел (минимум 2 доказательства). Теорема Дирихле о простых числах в арифметической прогрессии (доказательство простейших случаев). Отсутствие полиномиальных формул простых чисел. Числа Мерсенна и числа Ферма, их свойства. Доказательства бесконечности множества простых чисел с помощью свойств функции Эйлера и чисел Ферма. Решето Эратосфена. Существование сколь угодно больших промежутков ,не содержащих простых чисел. Основная теорема арифметики. Алгоритмы разложения в произведение (метод проб, алгоритм Ферма), их эффективность. Представление рационального числа непрерывной дробью, подходящие дроби, их свойства, их применение к решению теоретико-числовых задач.

Раздел 2. Мультипликативные функции и их свойства.

Важнейшие функции в теории чисел: определения, формулы, свойства: число делителей, сумма делителей, функция Мебиуса, функция Эйлера. Формула обращения Мебиуса, ее приложения.

Раздел 3. Числовые сравнения и их свойства.

Понятие сравнимости чисел, условия эквивалентные равноостаточности. Арифметические свойства числовых сравнений. Метод числовых сравнений и метод выбора модуля в решении задач на делимость. Признаки делимости. Классы вычетов и их свойства. Полная и приведенная системы вычетов, свойства. Теорема Эйлера. Малая теорема Ферма. Применение теоремы Ферма: псевдопростые числа, числа Кармайкла, теорема Корселта. Тест Миллера.

Раздел 4. Сравнения с одним неизвестным.

Основные понятия. Сравнения первой степени: анализ, способы решения. Системы линейных сравнений. Китайская теорема об остатках. Диофантовы уравнения первой степени. Сравнения любой степени по простому модулю.

Раздел 5. Первообразные корни и индексы.

Показатели, их свойства. Первообразные корни. Существование первообразных корней по простому модулю, способы отыскания. Индексы и их свойства. Решение степенных сравнений методом индексирования.

Раздел 6. Квадратичные вычеты и символ Лежандра.

Степенные вычеты. Критерий степенного вычета по простому модулю. Квадратичные вычеты. Символ Лежандра и его свойства. Квадратичный закон взаимности. Символ Якоби.

Раздел 7. Кольца и поля классов вычетов.

Кольцо классов вычетов по модулю: таблица сложения и умножения, противоположный и обратный элементы, делители нуля, порядок элемента. Поле классов вычетов по простому модулю. Мультипликативная группа поля.

Раздел 8. Приложения к криптографии.

Система шифрования RSA, проблема подписи.

2.4.Практические (семинарские) занятия

Курсом не предусмотрены.

2.5.Лабораторный практикум

Курсом не предусмотрен.

3. Организация текущего и промежуточного контроля знаний

3.1.Контрольные работы

Тематика контрольных работ	Сроки проведения	Разделы и темы дисциплины
Итоговая(домашняя)	13-ое занятие	2,3,4,5.

3.2.Комплекты тестовых заданий

- Комплект тестовых заданий по темам курса. Тестирование проводится на 10-м занятии.

3.3.Самостоятельная работа

3.3.1. Поддержка самостоятельной работы (сборники тестов, задач, упражнений и др.)

3.3.2. Тематика рефератов

- Написание рефератов по курсу не предусмотрено.

3.4.Курсовая работа, ее характеристика; примерная тематика

- Написание курсовых работ не предусмотрено.

Итоговый контроль проводится в виде экзамена. Экзаменационная оценка ставится на основании письменного и устного ответа по экзаменационному билету.

4. Технические средства обучения и контроля, использование ЭВМ

Нет.

5. Активные методы обучения (деловые игры, научные проекты)

Лекционным курсом не предусмотрены.

6. Материальное обеспечение дисциплины

Нет.

7. Литература

7.1.Основная

1. Виноградов И.М. Основы теории чисел. – Москва-Ижевск: НИЦ «Регулярная и хаотическая динамика» 2003.

7.2.Дополнительная

1. Айерлэнд К., Роузен М. Классическое введение в современную теорию чисел. М., 1987.
2. Окунев Л.Я. Краткий курс теории чисел. М., 1956.

7.3.Учебно-методические материалы по дисциплине

1. Задачи по теории чисел / для студентов 2 курса механико-математического факультета, издательство «Самарский университет» - 1996