**Правительство Российской Федерации**

**Федеральное государственное автономное образовательное учреждение высшего профессионального образования
«Национальный исследовательский университет
«Высшая школа экономики»**

Факультет Компьютерных наук

Департамент больших данных и информационного поиска

Базовая кафедра Яндекс

УТВЕРЖДАЮ

Академический руководитель

образовательной программы

«Науки о данных»

по направлению 01.04.02

 «Прикладная математика и информатика»

С.О. Кузнецов

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

«\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_ 2014 г.

**Программа дисциплины** «Прикладная алгебра»

для направления 01.04.02 "Прикладная математика и информатика" подготовки магистра

для магистерской программы "Науки о данных"

**Автор программы:**

Гайфуллин С.А., к.ф.-м.н. (sgayf@yandex.ru)

Одобрена на заседании базовой кафедры Яндекс «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_ 2014  г.

Заведующий кафедрой \_\_\_\_\_\_\_\_\_\_\_\_\_\_ М.А. Бабенко

Рекомендована Академическим советом образовательной программы

«Науки о данных» «\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_ 2014  г.

Менеджер базовой кафедры Яндекс \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Е.Ф. Баулин

Москва, 2014

*Настоящая программа не может быть использована другими подразделениями университета и другими вузами без разрешения подразделения разработчика программы.*

Пояснительная записка

## Автор программы

 Кандидат физико-математических наук С.А. Гайфуллин.

## Требования к студентам

## Изучение курса «Прикладная алгебра» требует предварительных знаний по линейной алгебре в объеме обязательного курса «Геометрия и алгебра».

## Аннотация

Дисциплина «Прикладная алгебра» предназначена для подготовки магистров по направлению 01.04.02.

Первая часть включает в себя теорию кодирования. Рассказываются необходимые понятия общей алгебры. Вводятся понятия линейного кода над конечным полем, кода, исправляющего ошибки. Доказываются оценки на параметры кода, называемые границами Синглтона, Хемминга и Плоткина. Рассмотрены конструкции кодов наилучших с точки зрения этих границ. Построены коды Хемминга, Рида-Соломона и Рида-Маллера. Рассказан алгоритм Берлекампа разложения многочлена над конечным полем на множители.

Вторая часть курса посвящена криптографии. Рассказаны криптосистемы с открытым ключом. Основной упор сделан на криптосистемы, использующие эллиптические кривые. Рассказаны методы проверки чисел на простоту и разложения их на множители с использованием эллиптических кривых.

Программа курса предусматривает лекции (26 часов), практические занятия (38 часов).

## Учебные задачи курса

Одной из основных целей курса является знакомство студентов с основными конструкциями абстрактной алгебры, теории кодирования и криптографии. В результате изучения курса «Прикладная алгебра» студенты должны:

– иметь представление об основных алгебраических структурах, используемых в перечислительных и алгоритмических задачах, в том числе о конечных группах и полях Галуа;

– понимать конструкции основных типов линейных кодов и знать алгоритмы декодирования некоторых кодов;

– изучить понятие группы точек эллиптической кривой и понимать, как эта группа используется в криптографии.

**Тематический план дисциплины «Прикладная алгебра»**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№** | **Название темы** | **Всего часов по дисциплине** | **Аудиторные часы** | **Самосто-ятельная работа** |
| **Лекции** | **Сем. и практика занятия** |
| 1 | Основные алгебраические структуры: группы, кольца, поля | 24 | 4 | 4 | 16 |
| 2 | Конечные поля | 10 | 2 | 4 | 4 |
| 3 | Линейные коды, границыпараметров | 10 | 2 | 4 | 4 |
| 4 | Коды Рида-Соломона и код Хемминга | 22 | 4 | 4 | 14 |
| 5 | Коды Рида-Маллера | 8 | 2 | 2 | 4 |
| 6 | Алгоритм Берлекампа | 10 | 2 | 4 | 4 |
| 7 | Криптосистемы с открытым ключом | 6 | 2 | 2 | 2 |
| 8 | Группа точек эллиптической кривой | 22 | 4 | 6 | 12 |
| 9 | Алгоритм Гольдвассера-Килиана проверки числа на простоту | 16 | 2 | 4 | 10 |
| 10 | Алгоритм Ленстры разложения чисел на множители | 16 | 2 | 4 | 10 |
|  | Итого | 144 | 26 | 38 | 80 |

# Литература

## По темам 1-2:

### Базовые учебники

1. Кострикин А.И. Введение в алгебру часть 3, М. ФИЗМАТЛИТ, 2004б –272с.

2. Под редакцией Кострикина А.И. Сборник задач по алгебре, М., МЦНМО, 2009, – 403с.

### Дополнительные учебники

3. Винберг Э. Б. Курс алгебры. М., Факториал, 1999. – 528 с.

4. Курош А. Г. Курс высшей алгебры. М., Наука, 1971. – 432 с.

## По темам 3-6:

### Базовые учебники

1. Влэдуц С.Г., Ногин Д.Ю., Цфасман М.А. Алгеброгеомертические коды, М., МЦНМО, 2003, – 503с.

2. Биркгоф Г., Барти Т., Современная прикладная алгебра, М., Лань, 2005 – 400 с.

3. Василенко О.Н. Теоретико-числовые алгоритмы в криптографии, М, МЦНМО, 2003, – 325 с.

### Дополнительные учебники

4. Коблиц Н. Курс теории чисел и криптографии, ТВП, 2001, – 260 c.

## По темам 7-10:

### Базовые учебники

1. Коблиц Н. Курс теории чисел и криптографии, ТВП, 2001, – 260 c.

### Дополнительные учебники

2. Washington C.L. Elliptic curves, number theory and cryptography, Taylor & Francis Group, LLC, 2008, – 513 p.

3. Василенко О.Н. Теоретико-числовые алгоритмы в криптографии, М, МЦНМО, 2003, – 325 с.

**Содержание программы**

**Тема 1. Основные алгебраические структуры: группы, кольца, поля**

Алгебраические системы, их гомоморфизмы и изоморфизмы.

Полугруппа, левый (правый) нейтральный и обратный элементы. Группа, подгруппа.

Примеры конечных групп, группы симметрий. Теорема Кэли. Циклическая группа, ее подгруппы. Абелевы группы. Прямые суммы групп.

Разбиение группы на смежные классы по подгруппе, теорема Лагранжа. Действия группы на множестве, группы симметрий. Перечисление орбит.

Кольцо, тело, поле. Кольцо вычетов, кольцо матриц. Кольцо формальных степенных рядов, кольцо многочленов над кольцом.

**Основная литература**

1. Винберг Э. Б., Курс алгебры. М., Факториал, 1999.

**Дополнительная литература**

1. Кострикин А.И. Введение в алгебру часть 3, М. ФИЗМАТЛИТ, 2004, –272с.

2. Курош А. Г. Курс высшей алгебры. М., Наука, 1971.

**Тема 2. Конечные поля**

Характеристика поля. Простое подполе. Теорема о строении конечных полей.

**Основная литература**

1. Кострикин А.И. Введение в алгебру часть 3, М. ФИЗМАТЛИТ, 2004, –272с.

**Дополнительная литература**

1. Винберг Э. Б., Курс алгебры. М., Факториал, 1999

**Тема 3. Линейные коды, границы параметров.**

Кодирование. Коды, исправляющие ошибки. Матричное кодирование. Линейные коды.

Метрика Хемминга. Неравенства на параметры кодов.

**Основная литература**

1. Влэдуц С.Г., Ногин Д.Ю., Цфасман М.А. Алгеброгеомертические коды, М., МЦНМО, 2003, – 503с.

**Дополнительная литература**

2. Биркгоф Г., Барти Т., Современная прикладная алгебра, М., Лань, 2005 – 400 с.

**Тема 4. Коды Рида-Соломона и код Хемминга**

Построение кодов Рида-Соломона. Двойственный код. Код Хемминга. Декодирование кода, двойственного к коду Рида-Соломона.

**Основная литература**

1. Влэдуц С.Г., Ногин Д.Ю., Цфасман М.А. Алгеброгеомертические коды, М., МЦНМО, 2003, – 503с.

2. Биркгоф Г., Барти Т., Современная прикладная алгебра, М., Лань, 2005.

**Тема 5. Коды Рида-Маллера**

Коды Рида-Маллера. Граница Плоткина. Код Хемминга как двойственный к коду Рида-

Маллера.

**Основная литература**

1. Влэдуц С.Г., Ногин Д.Ю., Цфасман М.А. Алгеброгеомертические коды, М., МЦНМО, 2003, – 503с.

**Дополнительная литература**

2. Биркгоф Г., Барти Т., Современная прикладная алгебра, М., Лань, 2005.

**Тема 6. Алгоритм Берлекампа.**

Разложение многочлена над конечным полем на множители. Избавление от кратных корней. Алгоритм Берликампа.

**Основная литература**

1. Василенко О.Н. Теоретико-числовые алгоритмы в криптографии, М, МЦНМО, 2003, – 325 с.

**Дополнительная литература**

2. Коблиц Н. Курс теории чисел и криптографии, ТВП, 2001, – 260 c.

**Тема 7. Криптосистемы с открытым ключом**

Криптосистемы Диффи-Хелманифма, Месси-Омуры и Эль-Гамаля. Задача дискретного

логарирования.

**Основная литература**

1. Коблиц Н. Курс теории чисел и криптографии, ТВП, 2001, – 260 c.

**Дополнительная литература**

2. Washington C.L. Elliptic curves, number theory and cryptography, Taylor & Francis Group, LLC, 2008, – 513 p.

**Тема 8. Группа точек эллиптической кривой**

Понятие эллиптической кривой. Групповой закон на эллиптической кривой. Явные формулы для сложения точек эллиптической кривой. Теорема Вейля. Теоремы Дойринга-Ватерхауза.

**Основная литература**

1. Прохоров Ю.Г. Эллиптические кривые и криптография, М., ФАКТОРИАЛ, 2009

**Дополнительная литература**

2. Washington C.L. Elliptic curves, number theory and cryptography, Taylor & Francis Group, LLC, 2008, – 513 p.

3. Коблиц Н. Курс теории чисел и криптографии, ТВП, 2001, – 260 c.

**Тема 9. Алгоритм Гольдвассера-Килиана проверки числа на простоту**

Методы проверки чисел на простоту. Метод Поклингтона. Алгоритм Гольдвассера-Килиана проверки числа на простоту с использованием эллиптических кривых.

**Основная литература**

1. Коблиц Н. Курс теории чисел и криптографии, ТВП, 2001, – 260 c.

**Дополнительная литература**

2. Washington C.L. Elliptic curves, number theory and cryptography, Taylor & Francis Group, LLC, 2008, – 513 p.

**Тема 10. Алгоритм Ленстры разложения чисел на множители**

Методы разложения чисел на простые множители. p-1 - метод Полларда. Алгоритм Ленстры разложения числа на простые множители с использованием эллиптических кривых.

**Основная литература**

1. Коблиц Н. Курс теории чисел и криптографии, ТВП, 2001, – 260 c.

**Дополнительная литература**

2. Washington C.L. Elliptic curves, number theory and cryptography, Taylor & Francis Group, LLC, 2008, – 513 p.

# Формы контроля и структура итоговой оценки

Текущий контроль - контрольная работа в первом модуле, контрольная работа во втором модуле.

Итоговый контроль – письменный экзамен (120 мин.)

Итоговая оценка вычисляется следующим образом:

0,2\*оценка за первую контрольную+0,2\*оценка за вторую контрольную+0,6\*оценка за

экзамен.

**Вопросы для оценки качества освоения дисциплины**

**Тема 1**.

1. Постройте инъективный гомоморфизм групп (Z\_5, +) -> (C^\*, x).

2. Опишите все подгруппы а) в циклических группах порядков 7, 4 и 12; б) в прямом

произведении S\_2 x S\_3.

3. Докажите, что в абелевой группе множество ее элементов конечного порядка образует группу.

4. Постройте тело из 4 элементов. Докажите, что все такие тела изоморфны между собой и являются полями.

**Тема 2.**

1. Найти неприводимый многочлен степени 2 над полем из 3 элементов.

2. Постройте поле порядка 9.

**Тема 3.**

1. Сколько ошибок может исправить групповой двоичный код с кодовым расстоянием 5? Сколько ошибок он гарантированно устанавливает?

2. Докажите, что [2^r – 1,2^r – r – 1,3]2 -код является совершенным.

**Тема 4.**

1. Постройте порождающую матрицу для (7,3)-кода Хемминга.

2. Декодируйте сообщение (1,1, 0, 0, 1, 1, 1) в коде Хемминга с r=3, если известно, что было допущено не более 1 ошибки.

3. Декодируйте сообщение (0,2,2,2,0) в коде Рида-Соломона с параметрами [5,3,3]5 c X1=0, X2=1, X3=2, X4=3, X5=4, если известно, что было допущено не более 1 ошибки.

**Тема 5.**

1. Показать, что код Рида-Маллера обращает неравенство в границе Плоткина в равенство.

2. Показать, что код Хемминга эквивалентен коду, двойственному к некоторому коду Рида-Маллера.

**Тема 6.**

Разложить на множители над полем F\_3 на неприводимые множители многочлен x4 + 2x3 + 2x + 1.

**Темы 7-10**

1) Найти количество точек на кривой y2 + y = x3 + x + 1 над полем из 3r элементов.

2) Найти тип кривой y2 = x3 – 1 над F25.

3) Какое количество чисел (1,2,…) можно закодировать точками на кривой y2 = x3 – 1 над полем из 71 элемента так, чтобы вероятность неудачи была равна 1/210 ? Какая точка кривой будет при этом соответствовать числу 5?

**Типовой вариант контрольной работы (1-й модуль)**

1. Какое количество ошибок может гарантированно обнаружить двоичный групповой код с минимальным расстоянием 7?

2. Докажите, что в если x и y — два элемента некоторой группы, то элементы xy и yx этой группы имеют один и тот же порядок.

3. Сколько существует абелевых групп порядка 200?

4. Декодируйте сообщение (1,1,1, 0, 0, 0, 1) в коде Хемминга с r=3, если известно, что было допущено не более 1 ошибки.

5. Декодируйте сообщение (1,2,2,3,1) в коде Рида-Соломона с параметрами [5,3,3]5 c X1=0, X2=1, X3=2, X4=3, X5=4, если известно, что было допущено не более 1 ошибки.

**Типовой вариант контрольной работы (2-й модуль)**

1. Описать алгоритм передачи данных Эль-Гамаля и его аналог для эллиптических кривых.

2. Сформулировать теорему Вейля (и дать определения всех входящих в формулировку понятий).

3. Описать алгоритм Ленстры разложения числа на множители. В чём заключается его преимущество перед (p-1)-методом Полларда?

4. Найти количество точек на кривой y2 + y = x3 + x + 1 над полем из 2r элементов.

5. Найти тип кривой y2 = x3 – 1 над F27.

6. Мы хотим закодировать числа 1,2,3,4,5,6,7 точками на кривой над полем из 71 элемента. Какова минимальная возможная вероятность неудачи? Какая точка кривой будет при этом соответствовать числу 3?

Автор программы: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_С.А. Гайфуллин