Федеральное государственное автономное образовательное учреждение высшего профессионального образования

Национальный исследовательский университет Высшая школа экономики

Факультет **БИЗНЕС-ИНФОРМАТИКИ**

Отделение Прикладная математика и информатика

Программа дисциплины

«Теория чисел и ее приложения»

для направления 010400.62 «**Прикладная математика и информатика**» подготовки бакалавров

Автор: Чеповский А.А. (aachepovsky@hse.ru)

Рекомендована секцией УМС
«Прикладная математика
и информатика»

Председатель
_____ Кузнецов С.О.
«_____» _____ 200___ г.

Одобрена на заседании кафедры
Анализа данных
и искусственного интеллекта

Зав. кафедрой
_____ Кузнецов С.О.
«_____» _____ 200___ г.

Утверждена УС факультета
бизнес-информатики

Ученый секретарь
_____ Фомичев В.А.
« ____» _____200___ г.

Москва

I. Пояснительная записка

Авторы программы

доцент, к.ф.-м.н. Чеповский А.А.

Требования к студентам

Изучение курса «Теория чисел и ее приложения» требует предварительных знаний по дисциплинам: «Основы информатики и программирования», «Алгоритмы и структуры данных», «Геометрия и алгебра».

Аннотация

Дисциплина «Теория чисел и ее приложения» предназначена для подготовки бакалавров 010400.62 – Прикладная математика и информатика.

Курс предназначен для:

- изучения основных теоретико-числовых объектов и задач теории чисел;
- выработки навыков и умений по решению конкретных задач;
- изучение основ алгоритмов и методов реализаций различных алгоритмов криптографии.

Основные формы обучения – лекции по теории чисел и ее алгоритмическим приложениям; практикумы по программированию с отработкой реализации изучаемых алгоритмов.

Учебные задачи курса

Цель курса.

В результате изучения дисциплины студенты должны:

- знать основы и современные результаты теории чисел;
- понимать принципы реализации основных криптографических алгоритмов;
- иметь навыки решения ряда конкретных теоретико-числовых задач некоторых разделов теории чисел;

II. Тематический план курса «Теория чисел и ее приложения»

№	Название темы	Всего часов по дисциплине	Аудиторные часы		Самостоятельная работа
			Лекции	практические занятия	
Первый модуль (20 часов/8 + 12)					
1	**Тема 1. Введение в теорию чисел.**	**12**	**2**	**2**	**8**
2	**Тема 2. Квадратичные сравнения.**	**17**	**2**	**3**	**12**
3	**Тема 3. Вероятностные методы отсеивания составных чисел.**	**10**	**2**	**2**	**6**
4	**Тема 4.. Строение мультипликативной группы кольца вычетов.**	**21**	**2**	**5**	**14**
Второй модуль (38 часов/22 + 16)					
5	**Тема 5. Дискретное логарифмирование.**	**22**	**4**	**4**	**14**
6	**Тема 6. Детерминированные алгоритмы проверки на простоту.**	**20**	**4**	**4**	**12**
7	**Тема 7. Факторизация натуральных чисел.**	**22**	**4**	**4**	**14**
8	**Тема 8. Распределение простых чисел и дзета-функция Римана**	**12**	**6**	**-**	**6**
9	**Тема 9. Характеры Дирихле.**	**26**	**4**	**4**	**18**
	Итого	**162**	**30**	**28**	**104**

III. Источники информации

Базовый учебник

Манин Ю.И., Панчишкин А.А. Введение в современную теорию чисел. — М.: МЦНМО, 2009

Список литературы

Основная литература

1. Виноградов И.М. Основы теории чисел — М. Наука 1981
2. Василенко О.Н., Галочкин А.И. Сборник задач по теории чисел — М.: МГУ, 1995
3. Галочкин А.И., Нестеренко Ю.В., Шидловский А.Б. Введение в теорию чисел — М.: МГУ, 1995
4. Применко Э.А. Алгебраические основы криптографии — М.: ЛИБРОКОМ, 2013

Дополнительная литература

1. Введение в криптографию/ Под общей редакцией Ященко В.В. — М.: МЦНМО, 1998

IV. Формы контроля и структура итоговой оценки

Текущий контроль – выполнение практических заданий и лабораторных работ.

Промежуточный контроль – 1 контрольная работа (в конце второго модуля).

Итоговый контроль – экзамен (60 мин.).

Преподаватель оценивает работу студентов на семинарских и практических занятиях путём проведения самостоятельных работ. Оценки за работу на семинарских и практических занятиях преподаватель выставляет в рабочую ведомость. Результирующая оценка по 10-ти балльной шкале за работу на семинарских и практических занятиях определяется перед промежуточным или итоговым контролем - $O_{аудиторная}$.

Преподаватель оценивает самостоятельную работу студентов: выполнение домашних заданий. Оценки за самостоятельную работу студента преподаватель выставляет в рабочую ведомость. Результирующая оценка по 10-ти балльной шкале за самостоятельную работу определяется перед промежуточным или итоговым контролем – $O_{сам.\ работа}$.

Результирующая оценка за промежуточный контроль $O_{промежуточный}$ в форме контрольной работы выставляется непосредственно по результатам контрольной работы.

Результирующая оценка за итоговый контроль в форме экзамена выставляется по следующей формуле, где $O_{экзамен}$ – оценка за работу непосредственно на экзамене:

$$O_{итоговый} = 0{,}7 \cdot O_{экзамен} + 0{,}2 \cdot O_{сам.\ работа} + 0{,}1 \cdot O_{аудиторная}$$

На пересдаче студенту не предоставляется возможность получить дополнительный балл для компенсации оценки за текущий контроль.

В диплом выставляет результирующая оценка по учебной дисциплине, которая формируется по следующей формуле:

$$O_{дисциплина} = 0{,}2 \cdot O_{промежуточный} + 0{,}8 \cdot O_{итоговый}$$

Таблица соответствия оценок по десятибалльной и системе зачет/незачет

Оценка по 10-балльной шкале	Оценка по 5-балльной шкале
1	Незачет
2	
3	
4	Зачет
5	
6	
7	
8	
9	
10	

Таблица соответствия оценок по десятибалльной и пятибалльной системе

По десятибалльной шкале	По пятибалльной системе
1 – неудовлетворительно 2 – очень плохо 3 – плохо	неудовлетворительно – 2
4 – удовлетворительно 5 – весьма удовлетворительно	удовлетворительно – 3
6 – хорошо 7 – очень хорошо	хорошо – 4
8 – почти отлично 9 – отлично 10 - блестяще	отлично – 5

V. Программа курса « Теория чисел и ее приложения»

Тема 1. Введение в теорию чисел.

Сравнения по модулю. Алгоритм Евклида. Теорема Эйлера. Малая теорема Ферма. Китайская теорема об остатках.

Литература по разделу:

1. Виноградов И.М. Основы теории чисел — М. Наука 1981
2. Галочкин А.И., Нестеренко Ю.В., Шидловский А.Б. Введение в теорию чисел — М.: МГУ, 1995

Тема 2. Квадратичные сравнения.

Квадратичные сравнения, Символы Лежандра и Якоби. Алгоритмы вычисления символа Якоби. Быстрое возведение в степень. Алгоритмы решения квадратичных сравнений.

Литература по разделу:

3. Виноградов И.М. Основы теории чисел — М. Наука 1981
4. Галочкин А.И., Нестеренко Ю.В., Шидловский А.Б. Введение в теорию чисел — М.: МГУ, 1995
5. Василенко О.Н., Галочкин А.И. Сборник задач по теории чисел — М.: МГУ, 1995

Тема 3. Вероятностные методы отсеивания составных чисел.

Простые числа, псевдопростые числа, числа Кармайкла. Тесты Миллера-Рабина и Соловея-Штрассена.

Литература по разделу:

1. Пиотровский Р.Г., Бектаев К.Б., Пиотровская А.А. Математическая лингвистика. – М.: Высшая школа, 1977. — 383 с.
6. Чатуев М., Чеповский А. М. Частотные методы в компьютерной лингвистике. Учебное пособие. — М.: МГУП, 2011.

Тема 4. Строение мультипликативной группы кольца вычетов.

Порядок мультипликативной группы кольца вычетов. Первообразные корни. Полная система образующих.

Литература по разделу:

1. Виноградов И.М. Основы теории чисел — М. Наука 1981
2. Галочкин А.И., Нестеренко Ю.В., Шидловский А.Б. Введение в теорию чисел — М.: МГУ, 1995
3. Василенко О.Н., Галочкин А.И. Сборник задач по теории чисел — М.: МГУ, 1995

Тема 5. Дискретное логарифмирование.

Индекс. Алгоритмы дискретного логарифмирования по простому модулю.

Литература по разделу:

1. Манин Ю.И., Панчишкин А.А. Введение в современную теорию чисел. — М.: МЦНМО, 2009
2. Применко Э.А. Алгебраические основы криптографии — М.: ЛИБРОКОМ, 2013

Тема 6. Детерминированные алгоритмы проверки на простоту.

Полиномиальные детерминированные алгоритмы проверки на простоту.

Литература по разделу:

1. Манин Ю.И., Панчишкин А.А. Введение в современную теорию чисел. — М.: МЦНМО, 2009
2. Применко Э.А. Алгебраические основы криптографии — М.: ЛИБРОКОМ, 2013

Тема 7. Факторизация натуральных чисел.

Субэкспоненциальные алгоритмы факторизации.

Литература по разделу:

3. Манин Ю.И., Панчишкин А.А. Введение в современную теорию чисел. — М.: МЦНМО, 2009
4. Применко Э.А. Алгебраические основы криптографии — М.: ЛИБРОКОМ, 2013

Тема 8. Распределение простых чисел и дзета-функция Римана

Ассимптотика $\pi(x)$. Функция Чебышева. Дзета-функция Римана. Гипотеза Римана.

Литература по разделу:

1. Виноградов И.М. Основы теории чисел — М. Наука 1981
2. Галочкин А.И., Нестеренко Ю.В., Шидловский А.Б. Введение в теорию чисел — М.: МГУ, 1995

Тема 9.Характеры Дирихле

Характеры Дирихле. *L*-функции Дирихле. Теорема Дирихле о простых числах в арифметических прогрессиях.

Литература по разделу:

3. Виноградов И.М. Основы теории чисел — М. Наука 1981
4. Галочкин А.И., Нестеренко Ю.В., Шидловский А.Б. Введение в теорию чисел — М.: МГУ, 1995

Автор программы: _____/ Чеповский А.А. /