МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Ярославский государственный университет им. П.Г. Демидова

Математический факультет

УТВЕРЖДАЮ

Проректор по развитию образования
_____Е.В.Сапир

"_____"_____2012г.

Рабочая программа дисциплины
послевузовского профессионального образования
(аспирантура)

Теория чисел

по специальности научных работников

01.01.06 Математическая логика, алгебра и теория чисел

Ярославль 2012

1. Цели освоения дисциплины.

Целями освоения дисциплины **«Теория чисел»** в соответствии с общими целями основной профессиональной образовательной программы послевузовского профессионального образования (аспирантура) (далее - образовательная программа послевузовского профессионального образования) являются:

- усвоение аспирантами знаний об основных результатах в теории чисел;
- формирование математической культуры аспиранта, фундаментальная подготовка в области теории чисел и ее приложений;
- овладение основными понятиями и методами теории чисел для дальнейшего использования при решении теоретических и прикладных задач.

2. Место дисциплины в структуре образовательной программы послевузовского профессионального образования

Данная дисциплина относится к разделу обязательные дисциплины (подраздел дисциплины по выбору аспиранта) образовательной составляющей образовательной программы послевузовского профессионального образования по специальности научных работников 01.01.06 Математическая логика, алгебра и теория чисел.

Для ее успешного изучения необходимы «входные» знания и умения, полученные в процессе обучения по программам специалитета или бакалавриата-магистратуры, а также алгебраических специальных курсов/

Теория чисел относится к числу основных разделов современной математики. Знание основ этих разделов является важной составляющей общей математической культуры. Эти знания необходимы как при проведении теоретических исследований в различных областях математики, так и при решении задач из разнообразных прикладных областей, таких как математическая физика, математическая экономика, криптография и др.

3. Требования к результатам освоения содержания дисциплины « Теория чисел»

В результате освоения дисциплины «Теория чисел» обучающийся должен:

Знать: основные понятия теории чисел, определения и свойства математических объектов, используемых в этой области математики, формулировки утверждений, методы их доказательства, возможные сферы их приложений.

Уметь: решать задачи теоретического характера из различных разделов теории чисел, доказывать утверждения, строить примеры основных объектов и понятий.

Владеть: математическим аппаратом теории чисел, методами доказательства теорем и основными теоретико – числовыми алгоритмами.

4. Структура и содержание дисциплины « Теория чисел»

Общая трудоемкость дисциплины составляет 3 зачетных единицы (108 часов)

№ п/п	Раздел Дисциплины	Курс	Неделя	Виды учебной работы, включая самостоятельную работу обучающихся, и трудоемкость (в часах) Форма обуч.: Очная/заочная	Формы текущего контроля успеваемости (по неделям) Форма промежуточной аттестации

				Лекций	Лабораторных	Практических	Сам. работа	работыКонтроль сам.	
1	**Тема 1.**	1	1	1			12/13		реферат
2	**Тема 2.**	1	2-3				12/13		реферат
3	**Тема 3.**	1	4-5	1			13		реферат
4	**Тема 4.**	1	6-7	1/0			13		реферат
5	**Тема 5.**	1	8-9	1			13		реферат
6	**Тема 6.**	1	10-11		4		13		контрольная работа
7	**Тема 7.**	1	12-13	1/0			13		реферат
8	**Тема 8.**	1	14-15	1			13		реферат
	Всего			**6/4**			**102/ 104**		**Зачет**

Содержание дисциплины

Тема 1.

Предмет, цели и задачи курса. Основная терминология. Приложения теории чисел в обработке сигналов и изображений и криптографии.

Тема 2.

Элементарная теория чисел. Делимость и простота. Диофантовы уравнения первой и второй степени. Кубические уравнения. Приближения и непрерывные дроби.

Тема 3.

Разложение на множители и несимметричное шифрование. Достоверные тесты простоты. Разложение больших чисел на множители. Диофантовы приближения и иррациональность некоторых чисел.

Тема 4.

Арифметика алгебраических чисел. Разложения простых идеалов. Дедекиндовы кольца и нормирования. Теория полей классов. Группа Галуа в арифметических задачах.

Тема 5.

Элементарная теория чисел с точки зрения логики. Диофантовы множества. Частично рекурсивные функции и перечислимые множества. Диофантовы множества и алгоритмическая неразрешимость.

Тема 6.

Алгебраические многообразия. Схемы конечного типа над кольцом целых чисел. Геометрические методы изучения диофантовых уравнений. Основные классы диофантовых уравнений. Диофантовы уравнения и представления Галуа. Теорема Фалтингса и проблемы конечности в диофантовой геометрии.

Тема 7.

Дзета-функции и модулярные формы. Модулярные формы и эйлеровы произведения. Модулярные формы и представления Галуа. Идея доказательства Уайлса теоремы Ферма.

Тема 8.

Теория чисел и обработка сигналов и изображений. Быстрые алгоритмы обработки сигналов и вычисления свертки. Эллиптические кривые и криптографические алгоритмы.

5. Образовательные технологии

В преподавании используются мультимедийные презентации, иллюстрации, таблицы, методические пособия.

В преподавании курса используются активные и интерактивные технологии проведения занятий в сочетании с внеаудиторной работой.

Используются компьютерные классы.

6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы обучающихся

В качестве средств текущего контроля используется 1 контрольных работы, а также написание в течение семестра 1 реферата на выбранную тему. Итоговая форма контроля (зачет) дает возможность выявить уровень профессиональной подготовки аспиранта по данной дисциплине.

Контрольная работа

Вариант 1. Программирование алгоритмов проверки числа на простоту.
Вариант 2. Программирование нахождения решений Диофантовых уравнений.

<u>Темы рефератов:</u>

1. Диофантовы уравнения первой и второй степени.
2. Кубические уравнения.
3. Приближения и непрерывные дроби.
4. Достоверные тесты простоты. Разложение больших чисел на множители.
5. Диофантовы приближения и иррациональность некоторых чисел.
6. Частично рекурсивные функции и перечислимые множества.
7. Диофантовы множества и алгоритмическая неразрешимость.

8. Алгебраические числа и геометрия.

9. Дедекиндовы кольца и нормирования.

10. Теория полей классов.

11. Группа Галуа в арифметических задачах.

12. Алгебраические многообразия. Схемы конечного типа над кольцом целых чисел.

13. Геометрические методы изучения диофантовых уравнений. Основные классы диофантовых уравнений.

14. Диофантовы уравнения и представления Галуа.

15. Теорема Фалтингса и проблемы конечности в диофантовой геометрии.

16. Дзета-функции и модулярные формы. Модулярные формы и эйлеровы произведения.

17. Модулярные формы и представления Галуа.

18. Идея доказательства Уайлса теоремы Ферма.

19. Быстрые алгоритмы обработки сигналов и вычисления свертки.

20. Эллиптические кривые и криптографические алгоритмы.

Вопросы к зачету

1. Приложения теории чисел в обработке сигналов и изображений и криптографии.
2. Диофантовы уравнения первой и второй степени. Кубические уравнения.
3. Приближения и непрерывные дроби.
4. Достоверные тесты простоты. Разложение больших чисел на множители
5. Диофантовы приближения и иррациональность некоторых чисел.
6. Диофантовы множества. Частично рекурсивные функции и перечислимые множества.
7. Диофантовы множества и алгоритмическая неразрешимость.
8. Алгебраические многообразия. Схемы конечного типа над кольцом целых чисел.
9. Основные классы диофантовых уравнений. Диофантовы уравнения и представления Галуа.
10. Теорема Фалтингса и проблемы конечности в диофантовой геометрии.
11. Дзета-функции и модулярные формы.
12. Модулярные формы и эйлеровы произведения.

13. Модулярные формы и представления Галуа.

14. Идея доказательства Уайлса теоремы Ферма.

15. Быстрые алгоритмы обработки сигналов и вычисления свертки.

16. Эллиптические кривые и криптографические алгоритмы.

7. Учебно-методическое и информационное обеспечение дисциплины

а) основная литература*:*

1.Манин Ю.А., Панчишкин А.А., Введение в теорию чисел. Современные проблемы математики. Фундаментальные направления. Итоги Науки и Техники, т.49, М., 1990, - 345 с.

2.О.Н.Василенко, Теоретико-числовые алгоритмы в криптографии, М.: МЦНМО, 2006, -333 с.

б) дополнительная литература:

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.: Из-д-во МГУ, 1995.
3. Ленг С. Алгебра. – М.: Мир, 1968. – 564 с.
4. Ноден П., Китте К., Алгебраическая алгоритмика, М.:»Мир», 1999, - 719 с.
5. Кострикин А.И. Основные структуры алгебры. Часть III. – М.: Физматлит, 2000.
6. Винберг Э.Б. Курс алгебры. – М.: Факториал Пресс, 2002.

в) программное обеспечение и Интернет-ресурсы:

- для демонстрации презентаций используются программы *Windows* и *MS Office*.
- в качестве вспомогательных **интернет-ресурсов** по дисциплине используется:

Портал Math-Net.ru

8. Материально-техническое обеспечение дисциплины

- компьютерный класс;
- набор теоретико-групповых программ GAP..
- аудитории для лекций и практических занятий (с необходимым материальным оснащением).

Наличие рекомендованной литературы. Наличие электронных версий методических материалов.

Программа составлена в соответствии с федеральными государственными требованиями к структуре основной профессиональной образовательной программы послевузовского профессионального образования (аспирантура) (приказ Минобрнауки от 16.03.2011 г. № 1365) с учетом рекомендаций, изложенных в письме Минобрнауки от 22.06.2011 г. № ИБ – 733/12.

Программа одобрена на заседании кафедры алгебры и математической логики 22.10.2012 (протокол № 2).

Заведующий кафедрой Л.С.Казарин, доктор физ-мат.наук, профессор

Автор В.Л.Дольников, доктор физ-мат.наук, профессор