МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Ярославский государственный университет им. П.Г. Демидова

Математический факультет

УТВЕРЖДАЮ

Проректор по развитию образования
___________________Е.В.Сапир

"_____"___________________2012 г.

Рабочая программа дисциплины
послевузовского профессионального образования
(аспирантура)

<u>Математическая логика, алгебра и теория чисел</u>

по специальности научных работников

01.01.06 Математическая логика, алгебра и теория чисел

Ярославль 2012

1. Цели освоения дисциплины.

Целями освоения дисциплины **« Математическая логика, алгебра и 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 изучаемой области;
- формирование математической культуры аспиранта, фундаментальная подготовка в области математической логики, алгебры и теории чисел 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 специальные дисциплины отрасли науки и научной специальности) 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-магитсратуры по направлению математика, а также алгебраических специальных курсов.

Специальность «Математическая логика, алгебра и теория чисел» –область науки, исследующая свойства целых чисел, изучающая множества с заданными на них алгебраическими операциями и отношениями; исследующая свойства множеств решений систем алгебраических уравнений; изучающая общее строение математических теорий, их моделей и алгоритмических процессов. Целью алгебры является изучение алгебраических структур, возникающих в математике и ее приложениях.

Целью математической логики являются: изучение синтаксических и семантических свойств формализованных математических теорий и структурных свойств их семантических моделей; исследование алгоритмических процессов с заданными свойствами, нахождение взаимосвязей между доказуемостью, истинностью и вычислимостью.

Целью теории чисел является исследование арифметических свойств математических объектов.

Области исследований:

1. Теория алгебраических структур (полугрупп, групп, колец, полей, модулей и т.д.).
2. Алгебраическая геометрия.
3. Алгебраическая и аналитическая теории чисел.
4. Геометрия чисел.
5. Группы и алгебры Ли.
6. Теория представлений.
7. Теория категорий и функторов.
8. Теория моделей: изучение свойств семантических моделей для математических теорий.
9. Теория доказательств (в том числе неклассические логики).
10. Теория алгоритмов и вычислимых функций (в том числе алгоритмическая теория информации и теория сложности).

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 « Математическая логика, алгебра и теория чисел». В результате освоения дисциплины обучающийся должен:

Знать: основные понятия математической логики, алгебры и 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 дисциплины, доказывать утверждения, строить примеры основных объектов и понятий.

Владеть: математическим аппаратом, используемым в математической логике, алгебре и теории чисел, методами доказательства
теорем и основными алгебраическими и теоретико – числовыми алгоритмами.

4. Структура и содержание дисциплины « Математическая логика, алгебра и теория чисел»

Общая трудоемкость дисциплины составляет 4 зачетных единицы (144 часа)

№ 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	Контроль сам. работы	
1	**Тема 1.** Понятие алгоритма и его уточнения**.**	1	1	1			8		реферат
2	**Тема 2.** Построение полугруппы с неразрешимой проблемой распознавания равенства.	1	2				8		реферат
3	**Тема 3.** Логика высказываний.	1	3	1			8		реферат
4	**Тема 4.** Разрешимые теории. Теория плотного линейного порядка.	1	4				8		реферат
5	**Тема 5.** Конечные группы.	1	5	1			8		реферат

6	**Тема 6.** Теорема о конечно порожденных модулях над евклидовым кольцом и ее следствия для групп и линейных операторов.	1	6		4		8		контрольная работа
7	**Тема 7.** Алгебраические расширения полей.	1	7	1			8		реферат
8	**Тема 8.** Радикал кольца.	1	8				8		реферат
9	**Тема 9.** Нетеровы кольца и модули.	1	9	1			8		реферат
10	**Тема 10.** Основы теории представлений**.**	1	10				8		реферат
11	**Тема 11.** Алгебраические системы.	1	11	1			8/9		реферат
12	**Тема 12.** Решетки.	1	12				8/9		реферат
13	**Тема 13.** Квадратичный закон взаимности.	1	13	1			9		реферат
14	**Тема 14.** Неравенства Чебышева для функции *$\pi(x)$*.	1	14	1/0			9		контрольная работа
15	**Тема 15.** Тригонометрические суммы.	1	15	1/0			10		реферат
16	**Тема 16.** Приближение вещественных чисел рациональными дробями.	1	16	1			10		
		1		**10/8**	**4**		**134/ 136**		**Зачет**

Содержание дисциплины

Тема 1.

Понятие алгоритма и его уточнения. Вычислимость по Тьюрингу, частично рекурсивные функции, рекурсивно перечислимые и рекурсивные множества. Тезис Чёрча.

Универсальные вычислимые функции. Существование перечислимого неразрешимого множества. Алгоритмические проблемы.

Тема 2.

Построение полугруппы с неразрешимой проблемой распознавания равенства.

Классы *P* и *NP*. Полиномиальная сводимость и *NP*-полные задачи. Теорема об *NP*-полноте задачи выполнимость.

Тема 3.

Логика высказываний. Представимость булевых функций формулами логики высказываний. Конъюнктивные и дизъюнктивные нормальные формы. Исчисление высказываний. Полнота и непротиворечивость. Логика предикатов. Приведение формул логики предикатов к предварённой нормальной форме. Исчисление предикатов. Непротиворечивость. Теорема о дедукции

Тема 4.

Разрешимые теории. Теория плотного линейного порядка. Формальная арифметика. Теорема о представимости вычислимых функций в формальной арифметике (без доказательства).

Тема 5.

Конечные группы. Теоремы Силова. Простота группы A_n, $n > 5$ и SO_3. Разрешимые и нильпотентные группы.

Тема 6.

Теорема о конечно порожденных модулях над евклидовым кольцом и ее следствия для групп и линейных операторов. Свободные группы и определяющие соотношения.

Тема 7.

Алгебраические расширения полей. Теорема о примитивном элементе. Поле разложения многочлена. Основная теорема теории Галуа. Конечные поля, их подполя и автоморфизмы.

Тема 8.

Радикал кольца. Структурная теорема о полупростых кольцах с условием минимальности. Группа Брауэра. Теорема Фробениуса.

Тема 9.

Нетеровы кольца и модули. Теорема Гильберта о базисе. Алгебры Ли. Простые и разрешимые алгебры. Теорема Ли о разрешимых алгебрах. Теорема Биркгофа-Витта.

Тема 10.

Основы теории представлений. Теорема Машке. Одномерные представления. Соотношения ортогональности.

Тема 11.

Алгебраические системы. Свободные алгебры. Многообразие алгебр. Теорема Биркгофа.

Тема 12.

Решетки. Дедекиндовы решетки. Теорема Стоуна о булевых алгебрах.

Тема 13.

Квадратичный закон взаимности. Первообразные корни и индексы.

Тема 14.

Неравенства Чебышева для функции $\pi(x)$. Дзета-функция Римана. Асимптотический закон распределения простых чисел. Характеры и L-функции. Теорема Дирихле о простых числах в арифметической прогрессии.

Тема 15.

Тригонометрические суммы. Модуль гауссовой суммы. Полные тригонометрические суммы и число решений сравнений. Модулярная группа и модулярные функции. Теорема о строении алгебры модулярных форм. Представление целых чисел унимодулярными квадратичными формами.

Тема 16.

Приближение вещественных чисел рациональными дробями. Теорема Лиувилля о приближении алгебраических чисел рациональными дробями. Примеры трансцендентных чисел. Трансцендентность чисел e и π.

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.

Часть практических занятий проводится в компьютерных классах с использованием системы GAP.

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 2 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 № 1

Вариант 1. Нахождение таблиц характеров конечных групп, заданных преподавателем.

Вариант 2. Нахождение фрагментов таблиц характеров, исходя из информации о вложении подгруппы в группу.

Вариант 3. Доказательства NP-полноты некоторых комбинаторных задач.

Вариант 4. Нахождение ступени разрешимости заданной группы.

Вариант 5. Представление булевских функций в одной из канонических форм.

Контрольная работа № 2

Вариант 1. Решение задач на нахождение идеалов колец.

Вариант 2. Программирование критериев проверки простоты натурального числа.

Вариант 3. Решение задач из теории чисел.

Вариант 4. Программирование нахождения решений Диофантовых уравнений.

<u>Темы рефератов:</u>

1. Приложения алгебраических структур в физике, комбинаторных задачах оптимизации и обработке сигналов.
2. Алгебраические и трансцендентные расширения. Теория Галуа.
3. Модули над кольцами главных идеалов.

4. Нормированные поля.
5. Задание групп порождающими элементами и соотношениями
6. Теорема о представимости вычислимых функций в формальной артифметике
7. Абелевы группы.
8. Теоремы Силова.
9. Решетки. Дедекиндовы решетки. Теорема Стоуна о булевых алгебрах Группы подстановок.
10. Классические полупростые кольца.
11. Радикал кольца с условием минимальности.
12. Структура простых колец.
13. Тензорные произведения представлений и модулей.
14. Лемма Шура и теорема Машке.
15. Теоремы Бернсайда и Фробениуса.
16. Теоремы о линейных группах.
17. Классы *P* и *NP*. Полиномиальная сводимость и *NP*-полные задачи. Теорема об *NP*-полноте задачи ВЫПОЛНИМОСТЬ.
18. Квадратичный закон взаимности. Первообразные корки и индексы.
19. Неравенства Чебышева для функции $\pi(x)$.
20. Модулярная группа и модулярные функции. Теорема о строении алгебры модулярных форм.
21. Дзета-функция Римана. Асимптотический закон распределения простых чисел.
22. Теорема Дирихле о простых числах в арифметической прогрессии.
23. Представление целых чисел унимодулярными квадратичными формами.
24. Теорема Лиувилля о приближении алгебраических чисел рациональными дробями. Примеры трансцендентных чисел.
25. Трансцендентность чисел e и π.

Вопросы к зачету

1. Понятие алгоритма и его уточнения. Вычислимость по Тьюрингу, частично рекурсивные функции, рекурсивно перечислимые и рекурсивные множества. Тезис Чёрча.
2. Универсальные вычислимые функции. Существование перечислимого неразрешимого множества. Алгоритмические проблемы.
3. Построение полугруппы с неразрешимой проблемой распознавания равенства.
4. Классы *P* и *NP*. Полиномиальная сводимость и *NP*-полные задачи. Теорема об *NP*-полно-

те задачи ВЫПОЛНИМОСТЬ.

5. Логика высказываний. Представимость булевых функций формулами логики высказываний. Конъюнктивные и дизъюнктивные нормальные формы. Исчисление высказываний. Полнота и непротиворечивость.
6. Логика предикатов. Приведение формул логики предикатов к предварённой нормальной форме. Исчисление предикатов. Непротиворечивость. Теорема о дедукции
7. Разрешимые теории. Теория плотного линейного порядка. Формальная артифметика. Теорема о представимости вычислимых функций в формальной артифметике (без доказательства).
8. Теорема о конечно порожденных модулях над евклидовым кольцом и ее следствия для групп и линейных операторов. Свободные группы и определяющие соотношения.
9. Алгебраические множества. Нормированные поля.
10. Группы. Периодические и свободные группы. Задание групп порождающими элементами и соотношениями.
11. Конечные группы. Теоремы Силова. Разрешимые и нильпотентные группы.
12. Ассоциативные кольца. Классические полупростые кольца.
13. Групповая алгебра конечной группы и представление группы. Структура простых колец.
14. Нетеровы кольца и модули. Теорема Гильберта о базисе. Алгебры Ли. Простые и разрешимые алгебры. Теорема Ли о разрешимых алгебрах. Теорема Биркгофа-Витта.
15. Характеры групп. Лемма Шура и теорема Машке. Соотношения ортогональности.
16. Алгебраические системы. Свободные алгебры. Многообразие алгебр. Теорема Биркгофа.
17. Решетки. Дедекиндовы решетки. Теорема Стоуна о булевых алгебрах.
18. Квадратичный закон взаимности. Первообразные корни и индексы.
19. Неравенства Чебышева для функции $\pi(x)$. Дзета-функция Римана. Асимптотический закон распределения простых чисел.
20. Теорема Дирихле о простых числах в арифметической прогрессии.
21. Тригонометрические суммы. Модуль гауссовой суммы. Полные тригонометрические суммы и число решений сравнений.
22. Модулярная группа и модулярные функции. Теорема о строении алгебры модулярных форм. Представление целых чисел унимодулярными квадратичными формами.
23. Фундаментальная система корней. Группа Вейля. Классификация комплексных простых алгебр Ли.
24. Группы лиева типа. Базис Шевалле и определение групп Шевалле. Коммутаторная формула Шевалле. Унипотентные подгруппы. Диагональная и мономиальная подгруппы.
25. Разложение Брюа. Группы с BN-парой. Порядки групп Шевалле. Простота групп Шевалле.
26. Автоморфизмы групп Шевалле. Скрученные группы Шевалле. Порождающие и соотношения.
27. Классификация конечных простых групп (основные идеи и техника).

7. Учебно-методическое и информационное обеспечение дисциплины

а) основная литература*:*

1. Ершов Ю.Л., Палютин Е.А. Математическая логика. 2-е изд. М.: Наука. 1987.
2. Мальцев А.И. Алгоритмы и рекурсивные функции. 2-е изд. М.: Наука, 1986.
3. Мендельсон Э. Введение в математическую логику. 3-е изд. М.: Наука, 1984.
4. Кострикин А.И. Введение в алгебру. Ч. 3. Основные структуры алгебры. М.:

Физматлит, 2000.

5. Винберг Э.Б. М. Курс алгебры. М.: Факториал Пресс, 2001.
6. Виноградов И.М. Основы теории чисел. М.: Наука, 1981.
7. Боревич З.И., Шафаревич И.Р. Теория чисел. М.: Наука, 1985.
8. Галочкин А.И., Нестеренко Ю.В. Шидловский А.Б. Введение в теорию чисел. М.: Изд-во МГУ, 1995.

б) дополнительная литература:

1. Ноден П., Китте К., Алгебраическая алгоритмика, М.:»Мир», 1999, - 719 с.
2. 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.
3. Ершов Ю.Л. Проблемы разрешимости и конструктивные модели М.: Наука, 1980.
4. Ван дер Варден Б.Л. Алгебра. М.: Наука, 1976.
5. Новиков П.С. Элементы математической логики. 2-е изд. М.: Наука, 1973.
6. Серр Ж.П. Курс арифметики. М.: Мир, 1972.
7. Мальцев А.И. Алгебраические системы. М.: Наука, 1970.
8. Ленг С. Алгебра. М.: Мир, 1968.
9. Джекобсон Н. Алгебры Ли. М.: Мир, 1964.
10. Гэри М., Джонсон Д. Вычислительные машины и труднорешаемые задачи. М.; Мир, 1982.
11. Кейперс Л., Нидеррейтер Г. Равномерное распределение последовательностей. М.: Наука, 1985.
12. Коробков Н.М. Тригонометрические суммы и их приложения. М.: Наука, 1989.
13. Чандрасекхаран К. Введение в аналитическую теорию чисел. М.: Мир, 1974.
14. Скорняков Л.А. Элементы обшей алгебры. М.: Наука, 1983.
15. Карацуба А.А. Основы аналитической теории чисел. М.: Наука, 1983.
16. О.Н.Василенко, Теоретико-числовые алгоритмы в криптографии, М.: МЦНМО, 2006, -333 с.

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..

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