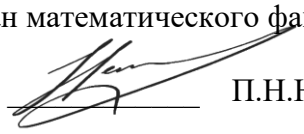
МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Ярославский государственный университет им. П.Г. Демидова

Кафедра алгебры и математической логики

УТВЕРЖДАЮ

Декан математического факультета



П.Н.Нестеров

«18» мая 2021 г.

Рабочая программа дисциплины
«Математическая логика, алгебра и теория чисел»

Направление подготовки
01.06.01 Математика и механика

Направленность (профиль)
«Математическая логика, алгебра и теория чисел»

Форма обучения очная

Программа рассмотрена
на заседании кафедры алгебры и математической логики
от «16» апреля 2021 года, протокол № 8

Ярославль

1. Цели освоения дисциплины Целью изучения дисциплины «Математическая логика, алгебра и теория чисел» является обеспечение фундаментальной подготовки в одной из основных областей современной математики, освоение языка и методов одного из наиболее мощных инструментов современной математики. Курс лежит в основе большей части современной электронной техники, численных методов алгебры и математических методов защиты информации, имеющих применение во многих областях естествознания. Его главной задачей является обучение основным методам решения задач в указанной области, ознакомление с историей развития математической логики, алгебры и теории чисел и вкладом в неё российских математиков.

Основная задача дисциплины – научить студентов пониманию языка математической логики, алгебры и теории чисел, воспитанию культуры вычислений с помощью алгебры логики и теории чисел, умениям применять основной аппарат и алгоритмы математической логики, алгебры и теории чисел в различном контексте. Содержание курса является базой для дальнейшего развития содержания дисциплины в специальных курсах.

2. Место дисциплины в структуре программы аспирантуры

Дисциплина «Математическая логика, алгебра и теория чисел» является обязательной дисциплиной вариативной части Блока 1. Данная дисциплина направлена на подготовку к сдаче кандидатского экзамена по научной специальности 01.01.06 «Математическая логика, алгебра и теория чисел».

3. Планируемые результаты обучения по дисциплине – знания, умения, навыки и (или) опыт деятельности, характеризующие этапы формирования компетенций и обеспечивающие достижение планируемых результатов освоения программы аспирантуры, и критерии их оценивания

Процесс изучения дисциплины направлен на формирование следующих компетенций:

Профессиональные компетенции:

- готовностью к исследованию в области алгебраической геометрии, алгебраической и аналитической теории чисел, геометрии чисел, групп и алгебр Ли (ПК-2).
- способность к разработке и совершенствованию теоретических и методологических подходов в теории представлений, теории категорий и функторов, теории моделей (изучение свойств семантических моделей для математических теорий), теории доказательств (в том числе неклассические логики), теории алгоритмов и вычислимых функций (в том числе алгоритмическая теория информации и теория сложности) (ПК-3).

Код компе-тенции	Планируемые результаты обучения	Критерии оценивания результатов обучения		
		Пороговый уровень	Продвинутый уровень	Высокий уровень

ПК-2	ЗНАТЬ: Основные понятия математической логики, различные уточнения понятия алгоритма; классы P и NP, полиномиальная сводимость; логику высказываний и предикатов; разрешимые теории; формальную арифметику; представимость вычислимых функций в формальной арифметике; теорема Геделя о неполноте	Фрагментарные (неполные) представления об основных концепциях математической логики, уточнениях понятия алгоритма; логики высказываний и предикатов; разрешимые теории; классы P и NP; формальную арифметику; теорему Геделя о неполноте; теорему Тарского о невыразимости истины	Сформированные, но содержащие отдельные пробелы представления об основных концепциях математической логики, уточнениях понятия алгоритма; логики высказываний и предикатов; разрешимые теории; класссы P и NP; формальную арифметику; теорему Геделя о неполноте; теорему Тарского о невыразимости	Систематические представления об основных концепциях математической логики, уточнениях понятия алгоритма; логики высказываний и предикатов; разрешимые теории; классы P и NP; формальную арифметику; теорему Геделя о неполноте; теорему Тарского о невыразимости истины
	УМЕТЬ: Использовать различные формы представления алгоритма; определять принадлежность проблемы к классу P или NP; представлять булевы функции формулами логики высказываний; пользоваться трансфинитной индукцией	В целом успешное, но не систематическое использование различных форм представления алгоритмов; определять принадлежность проблемы к классу P или NP; представлять булевы функции формулами логики высказываний; использование трансфинитной индукции	Успешное, но содержащее пробелы, использование различных форм представления алгоритмов; определять принадлежность проблемы классу P или NP; представлять булевы функции формулами логики высказываний; использование трансфинитной индукции	Сформированное умение использовать различные формы представления алгритмов; определять принадлежность проблемы классу P или NP; представлять булевы функции формулами логики высказываний; использование трансфинитной
	ВЛАДЕТЬ: навыками работы с различными формами алгоритмов; методами определения сложности алгоритмических проблем; вычислительными навыками работы с логическими выражениями, определять мощности различных множеств	В целом успешное, но не систематическое применение навыков работы с формами алгоритмов; методами определения сложности алгоритмических проблем; вычислительными навыками работы с логическими выражениями, определять мощности различных множеств	В целом успешное, но содержащее пробелы, применение навыков работы с формами алгоритмов; методами определения сложности алгоритмических проблем; вычислительными методами работы с логическими выражениями, определять мощности различных множеств	Успешное и систематическое применение навыков работы с формами алгоритмов; методами определения сложности алгоритмических проблем; вычислительными методами работы с логическими выражениями, определять мощности различных множеств

ППК-3	ЗНАТЬ: Основные понятия математической логики и теории сложности алгоритмов, полиномиальную сводимость алгоритмов; методы теории представлений групп и ассоциативных алгебр; следствия теоремы Геделя о неполноте; методы приближения трансцендентных и алгебраических чисел.	Фрагментарные (неполные) представления об основных концепциях математической логики, полиномиальной сводимости алгоритмов; методах теории представлений групп и ассоциативных алгебр; приближениях трансцендентных и алгебраических чисел	Сформированные, но содержащие отдельные пробелы представления об основных концепциях математической логики; теории полиномиальной сводимости алгоритмов; следствиях теоремы Геделя; приближениях трансцендентных и алгебраических чисел.	Успешное и систематическое применение знаний о методах работы с логическими и алгоритмическими проблемами; определения сложности алгоритмических задач в ассоциативных алгебрах и числовых системах; знание перспектив модернизации алгоритмов
	УМЕТЬ: применять концепции и структуры математической логики для анализа сложности алгоритмов ; методы теории представлений групп и ассоциативных алгебр для определения свойств алгебраических и числовых структур; разработки адекватных ситуации методов работы с ними.	В целом успешное, но не систематическое использование математической логики для анализа сложности алгоритмов ; методы теории представлений групп и ассоциативных алгебр для определения свойств алгебраических и числовых структур; разработки методов работы с ними.	Успешное, но содержащее пробелы, использование структур математической логики для анализа сложности алгоритмов ; методов теории представлений групп и ассоциативных алгебр для определения свойств алгебраических и числовых структур; разработки методов работы с ними.	Сформированное умение использо-структуры математической логики для анализа сложности алгоритмов ; методов теории представлений групп и ассоциативных алгебр для определения свойств алгебраических и числовых структур; разработки оптимальных алгоритмов работы с ними.
	ВЛАДЕТЬ: навыками работы с различными логическими структурами; методами определения сложности алгоритмических проблем; навыками работы с ассоциативными алгебрами и числовыми структурами, в том числе, с использованием алгоритмов модулярной арифметики	В целом успешное, но не систематическое применение навыков работы с различными логическими структурами; методами определения сложности алгоритмических проблем; навыками работы с ассоциативными алгебрами и числовыми структурами, в том числе, с использованием алгоритмов модулярной арифметики	Успешное, но содержащее пробелы, использование навыков работы с различными логиическими структурами; методами определения сложности алгоритмических проблем; навыками работы с ассоциативными алгебрами и числовыми структурами, в том числе, с использованием алгоритмов модулярной арифметики	Успешное и систематическое применение навыков работы с различными логиическими структурами; методами определения сложности алгоритмических проблем; навыками работы с ассоциативными алгебрами и числовыми структурами, в том числе, с использованием алгоритмов модулярной арифметики

4. Объем, структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 6 зачетных единиц, 216 акад.часов

Дисциплина изучается в течение четырех семестров. Формой итоговой промежуточной аттестации по дисциплине во втором и четвертом семестрах ее изучения является зачет, в последнем семестре - кандидатский экзамен.

№ п/п	Темы (разделы) дисциплины, их содержание	Семестр	Виды учебных занятий и их трудоемкость (в академических часах)					Формы текущего контроля успеваемости Форма промежуточной аттестации *(по семестрам)*
			лекции	практические	лабораторные	консультации	самостоятельная работа	
1.	Математическая логика и теория алгоритмов.Часть 1	2	4			2	32	Задания для самостоятельной работы
2.	Теория чисел	2	4				30	
	Всего за 2 семестр		**8**			**2**	**62**	**Зачет**
3.	Алгебра	3	6				30	
	Всего за 3 семестр		**6**				**30**	
4.	Математическая логика и теория алгоритмов. Часть 2	4	6			2	28	Задания для самостоятельной работы
	Всего за 4 семестр		**6**			**2**	**28**	**Зачет**
5	Математическая логика. Алгебра	5	6			2	64	
	Всего за 5 семестр		**6**			**2**	**64**	**Экзамен**
	Всего		**26**			**6**	**184**	

Содержание разделов дисциплины:

1. Математическая логика и теория алгоритмов. Часть 1.

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-полноте задачи выполнимость.
5. Логика высказываний. Представимость булевых функций формулами логики высказываний. Конъюнктивные и дизъюнктивные нормальные формы.
6. Исчисление высказываний. Полнота и непротиворечивость.
7. Логика предикатов. Приведение формул логики предикатов к предварённой нормальной форме.
8. Исчисление предикатов. Непротиворечивость. Теорема о дедукции.

2. Теория чисел

1. Квадратичный закон взаимности .
2. Первообразные корни и индексы.
3. Неравенства Чебышева для функции $\pi(x)$.
4. Дзета-функция Римана. Асимптотический закон распределения простых чисел.
5. Характеры и L-функции. Теорема Дирихле о простых числах в арифметической прогрессии.
6. Тригонометрические суммы. Модуль гауссовой суммы. Полные тригонометрические суммы и число решений сравнений.
7. * Критерий Вейля равномерного распределения. Теорема Вейля о последовательности значений многочлена.
8. Модулярная группа и модулярные функции. Теорема о строении алгебры модулярных форм.
9. Представление целых чисел унимодулярными квадратичными формами. ([16]).
10. Приближение вещественных чисел рациональными дробями. Теорема Лиувилля о приближении алгебраических чисел рациональными дробями. Примеры трансцендентных чисел.
11. Трансцендентность чисел e и π.

3. Алгебра

1. Теоремы Силова.
2. Простота группы A_n , $n \geq 5$ и SO_3.
3. Теорема о конечно порожденных модулях над евклидовым кольцом и ее следствия для групп и линейных операторов.
4. Свободные группы и определяющие соотношения.
5. Алгебраические расширения полей. Теорема о примитивном элементе. Поле разложения многочлена. Основная теорема теории Галуа .
6. Конечные поля, их подполя и автоморфизмы .
7. Радикал кольца. Структурная теорема о полупростых кольцах с условием минимальности .
8. Группа Брауэра. Теорема Фробениуса .
9. Нетеровы кольца и модули. Теорема Гильберта о базисе.
10. Алгебры Ли. Простые и разрешимые алгебры. Теорема Ли о разрешимых алгебрах. Теорема Биркгофа-Витта.
11. * Основы теории представлений. Теорема Машке. Одномерные представления. Соотношения ортогональности.
12. * Алгебраические системы. Свободные алгебры. Многообразие алгебр. Теорема Биркгофа.
13. * Решетки. Дедекиндовы решетки. Теорема Стоуна о булевых алгебрах.

1. Математическая логика и теория алгоритмов. Часть 2.

1. * Полнота исчисления предикатов. Теорема Мальцева о компактности.
2. * Элементарные теории классов алгебраических систем. Категоричные в данной мощности теории. Теорема о полноте теории, не имеющей конечных моделей и категоричной в бесконечной мощности.
3. Разрешимые теории. Теория плотного линейного порядка.
4. Формальная арифметика. Теорема о представимости вычислимых функций в формальной арифметике (без доказательства).
5. * Теорема Гёделя о неполноте формальной арифметики. Теорема Тарского о невыразимости арифметической истинности в арифметике.

6. * Неразрешимость алгоритмической проблемы выводимости для арифметики и логики предикатов.
7. * Аксиоматическая теория множеств. Порядковые числа, принцип трансфинитной индукции. Аксиома выбора.

5. Образовательные технологии, используемые при осуществлении образовательного процесса по дисциплине

Академическая лекция (или лекция общего курса) – последовательное изложение материала, осуществляемое преимущественно в виде монолога преподавателя. Требования к академической лекции: современный научный уровень и насыщенная информативность, убедительная аргументация, доступная и понятная речь, четкая структура и логика, наличие ярких примеров, научных доказательств, обоснований, фактов. Академическая лекция, как правило, состоит из трех частей: вступления (введения), изложения и заключения:

- *вступление* (введение) определяет тему, план и цель лекции. Оно призвано заинтересовать и настроить аудиторию, сообщить, в чём заключается предмет лекции и (или) её актуальность, основная идея (проблема, центральный вопрос), связь с предыдущими и последующими занятиями, поставить её основные вопросы. Введение должно быть кратким и целенаправленным.
- *изложение* является основной частью лекции, в которой реализуется научное содержание темы, ставятся все узловые вопросы, приводится вся система доказательств с использованием наиболее целесообразных методических приемов. Каждое теоретическое положение должно быть обосновано и доказано, приводимые формулировки и определения должны быть четкими, насыщенными глубоким содержанием.
- *заключение* обобщает в кратких формулировках основные идеи лекции, логически ее завершая. В заключении могут даваться рекомендации о порядке дальнейшего изучения основных вопросов лекции самостоятельно по указанной литературе.

Вводная лекция – дает первое целостное представление о дисциплине (или ее разделе) и ориентирует студента в системе изучения данной дисциплины. Обучающиеся знакомятся с назначением и задачами курса, его ролью и местом в системе учебных дисциплин и в системе подготовки специалиста. Дается краткий обзор курса, история развития науки и практики, достижения в этой сфере, имена известных ученых, излагаются перспективные направления исследований. На этой лекции высказываются методические и организационные особенности работы в рамках курса, а также дается анализ рекомендуемой учебно-методической литературы.

6. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень лицензионного программного обеспечения и информационных справочных систем (при необходимости).

В процессе осуществления образовательного процесса используются:
-- программное обеспечение для создания и демонстрации презентаций, иллюстраций и других учебных материалов:

- Microsoft Windows (в составе Microsoft Imagine Premium Electronic Software Delivery).
- Microsoft OfficeSTD 2013 RUS OLP NL Acdmc 021-10232 Microsoft Open License №0005279522
- MikTeX (свободно распространяемое ПО);
- GAP (GNU GPL).

-- для поиска учебной литературы библиотеки ЯрГУ -- Автоматизированная библиотечная информационная система "БУКИ - NEXT" (АБИС "БУКИ - NEXT""БУКИ - NEXT").

-- для работы с алгебраическими структурами используется система алгоритмов GAP, имеющаяся в свободном доступе в Интернете.

7. Перечень основной и дополнительной учебной литературы, необходимых для освоения дисциплины

а) основная литература

1. Винберг Э.Б. М., Курс алгебры. М., "Факториал Пресс", 2001.
2. Кострикин А.И. Введение в алгебру. Часть 3. Основные структуры алгебры. М.: Физматлит, 2000.
3. Ленг С. Алгебра. М., Мир, 1968.
4. Боревич З.И., Шафаревич И.Р., Теория чисел. М., Наука, 1985.
5. Виноградов И.М. Основы теории чисел. М., Наука, 1981.
6. Ершов Ю.Л, Палютин Е.А. Математическая логика. Изд. 2. М.: Наука, 1987.
7. Новиков П.С. Элементы математической логики. Изд. 2. М.: Наука, 1973

б) дополнительная литература

8. Гэри М, Джонсон Д. Вычислительные машины и труднорешаемые задачи. М.: Мир, 1982..
9. Мальцев А.И. Алгоритмы и рекурсивные функции. Изд. 2. М.: Наука, 1986.
10. Мендельсон Э. Введение в математическую логику. Изд. 3. М.: Наука, 1984.
11. Ершов Ю.Л.. Проблемы разрешимости и конструктивные модели. Наука, 1980.
12. Ван дер Варден Б.Л. Алгебра. М.: Наука, 1976.
13. Скорняков Л.А. Элементы общей алгебры. М.: Наука, 1983.
14. Мальцев А.И. Алгебраические системы. М.: Наука, 1970
15. Джекобсон Н. Алгебры Ли. М., Мир, 1964.
16. Галочкин А.И., Нестеренко Ю.В., Шидловский А.Б. Введение в теорию чисел. М., МГУ, 1995.
17. Карацуба А.А. Основы аналитической теории чисел. М., Наука, 1983.
18. Кейперс Л., Нидеррейтер Г. Равномерное распределение последовательностей. М., Наука, 1985.
19. Кондратьев А.С. Группы и алгебры Ли, Екатеринбург: УрО РАН, 2009
20. Коробков Н.М. Тригонометрические суммы и их приложения. М., Наука, 1989.
21. Владимиров Д.А., Булевы алгебры. М., Наука, 1969
22. Сарнак П. Модулярные формы и х приложения, М.:ФАЗИС, 1998
23. Серр Ж.П., Курс арифметики. М., Мир, 1972.
24. Чандрасекхаран К. Введение в аналитическую теорию чисел. М., Мир, 1974.

в) ресурсы сети «Интернет»

1. Электронная библиотека учебных материалов ЯрГУ
2. Электронная библиотека ЯрГУ: http://www.lib.uniyar.ac.ru/
3. http://mech.math.msu.su/department/

(**http://www.lib.uniyar.ac.ru/opac/bk_cat_find.php**).

4. Информационная система "Единое окно доступа к образовательным ресурсам" (http://www.edu.ru раздел Учебно-методическая библиотека) или по прямой ссылке (http://www.edu.ru/library).

5. Электронно-библиотечная система "Университетская библиотека online" (www.biblioclub.ru).
6. http:// www.tc26.ru
7. http:// www.nist.gov/manuscript-publicftion-search.cfm?pub_id=919061
6. http://habrahabr.ru/post/210684/
8. http://www.nist.gov/customcf/get pdf.cfm?pub id=919061
9. http://www.streebog.info/news/opredeleny-pobediteli-konkursa-po issledovaniyu-khesh-funksii-stribog/

8. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине включает в свой состав специальные помещения:
-учебные аудитории для проведения занятий лекционного типа, практических занятий (семинаров); групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации;
-помещения для самостоятельной работы;
-помещения для хранения и профилактического обслуживания оборудования.

Специальные помещения укомплектованы специализированной мебелью и техническими средствами обучения, служащими для представления информации большой аудитории.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду организации.

Число посадочных мест в лекционной аудитории больше либо равно списочному составу потока, а в аудитории для практических занятий (семинаров) – списочному составу группы обучающихся.

Автор :
Заведующий кафедрой алгебры и математической логики
профессор, д.ф-м.н. Казарин Л.С

Приложение к №1 рабочей программе дисциплины
«Математическая логика, алгебра и теория чисел»

Оценочные средства
для проведения текущей и/или промежуточной аттестации аспирантов
по дисциплине

1. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

1.1 Список вопросов и (или) заданий для проведения промежуточной аттестации

Список вопросов к экзамену:
Математическая логика и теория алгоритмов.
Список вопросов формирующих компетенцию ПК-2:

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-полноте задачи выполнимость.
5. Логика высказываний. Представимость булевых функций формулами логики высказываний. Конъюнктивные и дизъюнктивные нормальные формы.

Список вопросов формирующих компетенцию ППК-3:

6. Исчисление высказываний. Полнота и непротиворечивость.
7. Логика предикатов. Приведение формул логики предикатов к предварённой нормальной форме.
8. Исчисление предикатов. Непротиворечивость. Теорема о дедукции.
9. Формальная арифметика. Теорема о представимости вычислимых функций в формальной арифметике (без доказательства).
10. Аксиоматическая теория множеств. Порядковые числа, принцип трансфинитной индукции. Аксиома выбора.

Алгебра
Список вопросов формирующих компетенцию ПК-2:

1.Теоремы Силова.
2. Простота группы A_n , $n \geq 5$ и SO_3.
3. Теорема о конечно порожденных модулях над евклидовым кольцом и ее следствия для групп и линейных операторов.
4. Свободные группы и определяющие соотношения.
5.Алгебраические расширения полей. Теорема о примитивном элементе. Поле разложения многочлена. Основная теорема теории Галуа .

Список вопросов формирующих компетенцию ППК-3:

6. Конечные поля, их подполя и автоморфизмы .

7.Радикал кольца. Структурная теорема о полупростых кольцах с условием минимальности .
8. Группа Брауэра. Теорема Фробениуса .
9. Нетеровы кольца и модули. Теорема Гильберта о базисе.
10. Алгебры Ли. Простые и разрешимые алгебры. Теорема Ли о разрешимых алгебрах. Теорема Биркгофа-Витта.

3. Теория чисел
Список вопросов формирующих компетенцию ПК-2:

1. Квадратичный закон взаимности .
2. Первообразные корни и индексы.
3. Неравенства Чебышева для функции $\pi(x)$.
4. Дзета-функция Римана. Асимптотический закон распределения простых чисел.

Характеры и L-функции. Теорема Дирихле о простых числах в арифметической прогрессии.
Тригонометрические суммы. Модуль гауссовой суммы. Полные тригонометрические суммы и число решений сравнений.

5. Критерий Вейля равномерного распределения. Теорема Вейля о последовательности значений многочлена.

Список вопросов формирующих компетенцию ППК-3:

6.
7. Модулярная группа и модулярные функции. Теорема о строении алгебры модулярных форм.
8. Представление целых чисел унимодулярными квадратичными формами. ([16]).
9. Приближение вещественных чисел рациональными дробями. Теорема Лиувилля о приближении алгебраических чисел рациональными дробями. Примеры трансцендентных чисел.
10. Трансцендентность чисел *e* и π.

Задания для зачета
Список заданий формирующих компетенцию ПК-2:

1. Доказать, что группа порядка 15 циклическая.
2. Показать, что неразрешимая группа наименьшего порядка будет иметь порядок 60.
3. Доказать, что число элементов конечного поля -- степень его характеристики.
4. В каком случае поле $GF(p^m)$ содержит подполе, изоморфное $GF(p^n)$?
5. Доказать теорему о строении конечнопорожденных абелевых групп.
6. Предложить алгоритм нахождения примитивного элемента в конечном поле, заданном вычетами по модулю неприводимого многочлена $g(x)$.
7. Какова группа Галуа уравнения $x^4+2x^2+x+3=0$?
8. Доказать, что полное матричное кольцо P_n является центральной простой алгеброй над полем P.
9. Доказать, что если многообразие M содержится в объединении многообразий M_1 и M_2, то M содержится в M_1 или M_2.
10. Является ли идеал $(x_1 x_1 - x_2^2, x_2 x_3 - x_1^3, x_3^2 - x_1^2 x_2)$ кольца $K[x_1, x_2, x_3]$ простым?
11. Как устроена простая алгебра без единицы?
12. В любом подмножестве M кольца $S= R[x_1, x_2, \dots x_m]$ с коэффициентами в поле R существует такой конечный набор элементов $m_1, m_2, \dots m_r$, что любой элемент S представим в виде линейной комбинации элементов $m_1, m_2, \dots m_r$ с коэффициентами из S.
13. Пусть L—алгебра Ли и X – элемент из L. Покажите, что ad X – дифференцирование алгебры L.

14. Пусть L—алгебра Ли и H,K – ее нильпотентные идеалы. Доказать, что H+K – нильпотентный идеал L.

Список заданий формирующих компетенцию ППК-3:

15. Показать, что по таблице неприводимых комплексных характеров конечной группы можно определить порядки классов сопряженных элементов группы, порядок центра и коммутанта группы.
16. Будет ли решетка нормальных подгрупп группы модулярной?
17. Построить полную решетку разбиений множества из четырех элементов.
18. Если группа G порождается конечным множеством X, то в любом ее порождающем множестве имеется конечное подмножество, также порождающее G.
19. Доказать, что все идеалы групповой алгебры бесконечной циклической группы главные.
20. Найти мощность множества всех алгебраических чисел
21. Доказать с помощью неравенства Чебышева постулат Бертрана.
22. Пусть p – нечетное простое число и a – первообразный корень по модулю p^2. Докажите, что a – первообразный корень по модулю p^k для любого $k>2$.
23. Докажите, что нечетное натуральное число n является простым тогда и только тогда, когда оно единственным образом представляется в виде разности квадратов целых неотрицательных чисел.
24. Найти основные единицы в полях $Q((19)^{1/2})$ и $Q((37)^{1/2})$.
25. Какие простые числа представляются формами x^2+5y^2 и $2x^2+2xy+3y^2$?
26. Показать, что для алгебраически замкнутых полей показателей не существует.
27. Определить группу классов Витта для квадратичных форм над полем вещественных чисел и над полем комплексных чисел.
28. Изложить примеры субэкспоненциальных алгоритмов факторизации натуральных чисел.

1.2 Контрольные задания и иные материалы, используемые в процессе текущей аттестации

Задания для самостоятельного решения по теме «Математическая логика и теория алгоритмов. Часть 1.»

Список заданий формирующих компетенцию ПК-2:

1.Докажите, что класс языков NP замкнут относительно объединения, пересечения, конкатенации и *-операции Клини.

2.Можно ли за полиномиальное время определить выполнимость булевой формулы, заданной в дизъюнктивной нормальной форме? А для формулы в конъюктивной нормальной форме?

3. Доказать, что множество дизъюнктов S невыполнимо, когда существует резолютивный вывод пустого дизъюнкта из S.

Список заданий формирующих компетенцию ППК-3:

4. Сформулировать определение независимости аксиомы от остальных аксиом системы. Предложить (возможный) план доказательства независимости аксиомы.

5. Пусть формула A, содержит n предикатов, которые зависят только от одной (и той же) переменной и является истинной для всякой области, содержащей не более 2^n элементов, то формула A тождественно истинна. Доказать.

6. Доказать, что если формула A выводима в исчислении высказываний, то не(не A) выводима в интуиционистском исчислении высказываний. Верно ли, что любая формула, выводимая в интуиционистском исчислении высказываний, выводима в исчислении высказываний?

Задания для самостоятельного решения по теме «Математическая логика и теория алгоритмов. Часть 2.»

Список заданий формирующих компетенцию ПК-2:

1. Доказать, что если для любого x из F(x) следует G(x), то из справедливости для любого x F(x) следует справедливость для любого x G(x).
2. Операции с кванторами в логике предикатов и примитивные формулы. Описать применения.
3. Доказать непротиворечивость ограниченной арифметики.

Список заданий формирующих компетенцию ППК-3:

4.
5. Мощность множества алгебраических чисел.
6. Доказать, что булева алгебра является дистрибутивной решеткой.
7. Каждый максимальный фильтр D на булевой алгебре является простым. Доказать.

Приложение № 2 к рабочей программе дисциплины
«Математическая логика, алгебра и теория чисел»

Методические указания для аспирантов по освоению дисциплины

Учебно-методическое обеспечение самостоятельной работы аспирантов по дисциплине

В качестве учебно-методического обеспечения рекомендуется использовать литературу, указанную в разделе № 7 данной рабочей программы.

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», рекомендованных к использованию при освоении дисциплины

Электронные ресурсы ЯрГУ (http://lib.uniyar.ac.ru)
1.Библиографические записи всех видов документов, составляющих фонд библиотеки, на русском и иностранных языках и поступивших позже 1995 года:
http://www.lib.uniyar.ac.ru/opac/bk_cat_find.php (в открытом доступе)
2. Электронная библиотека учебных материалов ЯрГУ:
http://www.lib.uniyar.ac.ru/opac/bk_cat_find.php
3. Электронная картотека «Книгообеспеченность»:
http://www.lib.uniyar.ac.ru/opac/bk_bookreq_find.php
4. Электронно-библиотечная система «Университетская библиотека Online»:
www.biblioclub.ru
5. Проект МАРС: http://mars.arbicon.ru.
6. Электронно-библиотечная система «Лань: http://e.lanbook.com/
7. Научная электронная библиотека eLIBRARY.ru: http://elibrary.ru
8. Англоязычные библиотеки в сети университета:
а) MathSciNet: http://www.ams.org/snhtml/annser.csv - с платформы издателя
http://search.ebscohost.com/ - с платформы Ebscohost
б) Web of Science: http://webofscience.com
в) Scopus: http://www.scopus.com
г) Science The American Association for the Advancement of Science:
http://www.sciencemag.org
д) Ресурсы Springer
SpringerJournals: http://link.springer.com/
SpringerProtocols: http://www.springerprotocols.com/
SpringerMaterials: http://materials.springer.com/
SpringerReference: http://link.springer.com
zbMATH: http://zbmath.org/