Программа вступительных экзаменов в аспирантуру МИАН

специальность 1.1.5 – *Математическая логика, алгебра, теория чисел и дискретная математика*

Раздел 1. «Алгебра»

1. Векторные пространства, подпространства, двойственное векторное пространство, размерность. Линейные отображения, их ядра и образы. Базис, матрица линейного отображения, ранг матрицы. Теорема Кронекера–Капелли. Характеристический многочлен, теорема Гамильтона–Кэли. Собственные векторы и собственные значения. Жорданова нормальная форма линейного оператора.

2. Билинейные и квадратичные формы, их матрицы. Ортогональные и самосопряженные линейные операторы, их матрицы. Классификация конечномерных квадратичных форм над полем вещественных чисел. Приведение к главным осям квадратичной формы в евклидовом пространстве, разложение матрицы в произведение ортогональной и верхнетреугольной матриц.

3. Группы и подгруппы, гомоморфизмы групп, их ядра и образы. Факторгруппы, теорема о гомоморфизмах. Задание группы образующими и соотношениями. Порядок элемента, циклические группы. Коммутант группы, разрешимые группы. Классы сопряженности, центр группы. Действие групп на множестве, стабилизаторы, орбиты. Примеры групп: симметрическая группа, знакопеременная группа, группа обратимых матриц (полная и специальная).

4. Три теоремы Силова.

5. Теорема о строении конечнопорожденных абелевых групп.

6. Теорема о простоте знакопеременной группы степени не менее 5.

7. Ассоциативные кольца, идеалы, гомоморфизмы колец, их ядра и образы. Факторкольца, теорема о гомоморфизмах для колец. Прямое произведение колец. Простота алгебры матриц над полем. Тело кватернионов, теорема Фробениуса.

8. Коммутативные кольца, простые и максимальные идеалы. Факториальность евклидовых коммутативных колец. Примеры коммутативных колец: гауссовы целые числа, кольца вычетов, кольца многочленов и степенных рядов.

9. Поля, характеристика. Конечные расширения полей, присоединение к полю корня неприводимого многочлена. Нормальные и сепарабельные расширения, основная теорема теории Галуа.

10. Структура конечных полей. Теорема о цикличности группы обратимых элементов в конечном поле.

11. Представления групп. Неприводимые представления, лемма Шура, теорема Машке.

Список литературы

[1] Э.Б. Винберг, Курс алгебры, М.: МЦНМО, 2013.

[2] А.И. Кострикин, Введение в алгебру, части 1,2,3 – М.: Физматлит, 2003.

[3] А.И. Кострикин, Ю.И. Манин, Линейная алгебра и геометрия, М.: Наука, 1986.

[4] И.Р. Шафаревич, Основные понятия алгебры, Алгебра–1, Итоги науки и техн. Сер. Соврем. пробл. мат. Фундам. направления, 11, М.: ВИНИТИ, 1986, 5–279.

Раздел 2. «Теория чисел»

1. Алгоритм Евклида нахождения наибольшего общего делителя двух чисел. Представление рациональных чисел в виде цепных дробей. Верхние оценки количества шагов в алгоритме Евклида и длины разложения рационального числа в цепную дробь. Разложение иррационального числа в бесконечную цепную дробь. Подходящие дроби. ([2, гл. I], [6, гл. I, IV], [5, гл. I])

2. Простые числа. Бесконечность множества простых чисел. Решето Эратосфена. Основная теорема арифметики о единственности разложения натурального числа на простые множители. Расходимость ряда, составленного из чисел, обратных простым. ([2, гл. I, §§4, 5], [4, гл. I, §§2,3], [6, гл. I])

3. Мультипликативные функции и их простейшие свойства. Суммы по делителям. Функция Мебиуса $\mu(n)$. Основное свойство функции Мебиуса:

$$\sum_{d|n} \mu(d) = \begin{cases} 1, n = 1, \\ 0, n > 1. \end{cases}$$

Функция Эйлера $\varphi(n)$. Явные формулы для $\varphi(n)$. Формула обращения Мебиуса и примеры ее применения. Формула

$$\sum_{d|n} \varphi(d) = n.$$

Функция $\tau(n)$, равная числу делителей натурального числа n, ее обобщения. ([2, гл. II])

4. Сравнения и их основные свойства. Достаточное условие разрешимости линейного сравнения с одной переменной. Классы вычетов по заданному модулю. Полная и приведенная системы вычетов. Теорема Эйлера: $a^{\varphi(m)} \equiv 1 \pmod{m}$ для любого целого a, взаимно простого с модулем m. Малая теорема Ферма: $a^p \equiv a \pmod{p}$, где p — простое число. ([2, гл. III], [6, гл. II])

5. Китайская теорема об остатках. Решение полиномиальных сравнений по составному модулю. Выражение количества решений полиномиального сравнения по модулю $m = m_1 \dots m_k$, где $(m_i, m_j) = 1$, через числа решений того же сравнения по модулям m_j, $j = 1, \dots, k$. ([2, гл. IV, §§3, 5])

6. Теорема Лагранжа о том, что количество решений полиномиального сравнения по простому модулю не превосходит степени полинома. Разложение на множители многочлена $x^{p-1} - 1$ по простому модулю p. Теорема Вильсона. ([2, гл. IV, §4], [6, гл. II])

7. Квадратичные вычеты и невычеты. Символ Лежандра $\left(\frac{a}{p}\right)$, его простей-

шие свойства. Критерий Эйлера:

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}.$$

Лемма Гаусса:

$$\left(\frac{a}{p}\right) = (-1)^{\Delta}, \quad \Delta = \sum_{n=1}^{(p-1)/2} \left[\frac{2an}{p}\right].$$

Значение символа Лежандра $\left(\frac{2}{p}\right)$. Закон взаимности квадратичных вычетов. ([2, гл. V, §§1-2], [6, гл. III])

8. Показатель, которому принадлежит данный вычет по модулю m; его простейшие свойства. Первообразные корни по модулю m. Существование первообразного корня по простому модулю. Первообразные корни по модулям p^α, $2p^\alpha$, где $p \geqslant 3$ — простое число, $\alpha \geqslant 1$. Необходимое и достаточное условие того, чтобы заданное число было первообразным корнем. Индексы по модулям p^α, $2p^\alpha$. ([2, гл. VI, §§1-4])

9. Отсутствие первообразных корней по модулям $m \neq 2, 4, p^\alpha, 2p^\alpha$, где $p \geqslant 3$ — простое число, $\alpha \geqslant 1$. Показатель, которому принадлежит число 5 по модулю 2^α, $\alpha \geqslant 3$. Представление чисел из приведенной системы вычетов по модулю 2^α, $\alpha \geqslant 3$, в виде $(-1)^\gamma \cdot 5^{\gamma_1}$. Система индексов по модулю 2^α, $\alpha \geqslant 3$. ([2, гл. VI, §§6-7])

10. Функция Мангольдта $\Lambda(n)$. Функция Чебышева $\psi(x)$. Интегральная формула суммирования Абеля. Неравенства Чебышева для функции $\pi(x)$. Асимптотический закон распределения простых чисел (формулировка). ([4, гл. I, §§4], [9, гл. I])

11. Дзета-функция Римана: определение и ее простейшие свойства. Тождество Эйлера. Дзета-функция Римана как производящая функция теории чисел: доказательство формул

$$\zeta^2(s) = \sum_{n=1}^{+\infty} \frac{\tau(n)}{n^s}, \quad \frac{1}{\zeta(s)} = \sum_{n=1}^{+\infty} \frac{\mu(n)}{n^s}, \quad \frac{\zeta'(s)}{\zeta(s)} = -\sum_{n=1}^{+\infty} \frac{\Lambda(n)}{n^s} \quad (\Re s > 1),$$

$$\frac{\zeta(s-1)}{\zeta(s)} = \sum_{n=1}^{+\infty} \frac{\varphi(n)}{n^s} \quad (\Re s > 2).$$

([3, гл. II, §1-2])

12. Характеры Дирихле по заданному модулю. L-функции Дирихле: определение и простейшие свойства. Тождество Эйлера. ([2, гл. VII]; [7, гл. VIII, §§1-2])

13. Алгебраические числа. Замкнутость множества алгебраических чисел относительно арифметических операций. Целые алгебраические числа и их свойства. Теорема о примитивном элементе. Степень конечного расширения. Алгебраическая замкнутость множества алгебраических чисел. ([4, гл. 4, §1], [1, гл. 6])

14. Теорема Дирихле о приближении действительных чисел рациональными. Теорема Лиувилля о приближении алгебраических чисел рациональными. Иррациональность числа e. ([4, гл. 4, §§2-3])

Список литературы

[1] Б.Л. Ван-дер-Варден, Алгебра. М., Наука, 1976.

[2] И.М. Виноградов, Основы теории чисел. Изд. 9-е. М., Наука, 1981.

[3] С.М. Воронин, А.А. Карацуба, Дзета-функци Римана. М., Физматлит, 1994.

[4] А.И. Галочкин, Ю.В. Нестеренко, А.Б. Шидловский, Введение в теорию чисел. Изд. 2-е. М., Изд-во Московского ун-та, 1995.

[5] О.Н. Герман, Ю.В. Нестеренко, Теоретико-числовые методы в криптографии. - Academia, 2012.

[6] Г. Дэвенпорт, Высшая арифметика. М., Наука, 1965.

[7] А.А. Карацуба, Основы аналитической теории чисел. Изд. 2-е. М., Наука, 1983.

[8] А.И. Кострикин, Введение в алгебру, ч.1: Основы алгебры - Мир (1987).

[9] К. Прахар, Распределение простых чисел. М., Мир, 1967.

[10] К. Айерленд, М. Роузен, Классическое введение в современную теорию чисел. - Мир (1987).

Раздел 3. «Математическая логика и дискретная математика»

Логика высказываний

1. Язык классической логики высказываний, истинностные таблицы. Выполнимые формулы, алгоритм распознавания выполнимости. Приведение формул логики высказываний к совершенной дизъюнктивной (конъюнктивной) нормальной форме.

2. Гильбертовское исчисление высказываний. Теорема о полноте.

3. Интуиционистская логика высказываний. Теорема о полноте интуиционистской логики высказываний относительно семантики Крипке.

4. Финитная аппроксимируемость и дизъюнктивное свойство интуиционистской логики высказываний. Теорема Гливенко. Теорема о том, что интуиционистская логика высказываний не является конечнозначной.

Основы теории множеств

5. Система аксиом Цермело–Френкеля с аксиомой выбора, ZFC. Построение натуральных, целых, рациональных и вещественных чисел в теории множеств.

6. Равномощность. Теорема Кантора. Теорема Кантора–Бернштейна.

7. Вполне упорядоченные множества. Ординалы. Трансфинитная индукция и рекурсия.

8. Теорема Цермело. Лемма Цорна. Кардиналы. Теорема о равномощности бесконечного множества своему декартову квадрату.

Основы теории вычислимости

9. Модели вычислений. Понятие (частичной) вычислимой функции. Тезис Черча–Тьюринга.

10. Универсальные и главные универсальные вычислимые функции. Частичная вычислимая функция, которую нельзя расширить до всюду определенной вычислимой функции. Теорема Клини о неподвижной точке.

11. Разрешимые множества, перечислимые множества. Теорема Поста. M-сводимость и m-полнота. Теорема об m-полноте проблемы остановки для машины Тьюринга. Теорема Успенского–Райса. Пары перечислимых множеств, не отделимых разрешимым множеством.

12. Классы P и NP. Полиномиальная сводимость и NP-полнота. Теорема Кука–Левина об NP-полноте проблемы распознавания выполнимости булевых формул.

Логика предикатов

13. Язык логики предикатов первого порядка. Теории первого порядка и их модели.

14. Аксиомы и правила вывода исчисления предикатов. Теорема о дедукции для исчисления предикатов.

15. Теорема Геделя о полноте исчисления предикатов. Теорема о компактности для логики предикатов. Нестандартные модели арифметики. Описание порядковых типов счетных нестандартных моделей.

16. Элементарные подмодели. Теорема Левенгейма–Скулема. Теорема Мальцева о повышении мощности.

17. Разрешимые теории. Метод элиминации кванторов. Теория плотных линейных порядков без наибольшего и наименьшего элементов, ее разрешимость и полнота.

Формальная арифметика и теорема Геделя о неполноте

18. Формальная арифметика (система PA, ее язык и аксиомы). Ограниченные формулы и сигма-формулы в языке арифметики.

19. Теорема о сигма-определимости перечислимых множеств в стандартной модели арифметики. Представимость вычислимых функций в арифметике.

20. Первая теорема Геделя о неполноте в форме Россера. Неразрешимость алгоритмической проблемы выводимости для формальной арифметики и для логики предикатов (теорема Черча).

21. Лемма о диагонализации в арифметике. Теорема Тарского о неопределимости истины в арифметике.

Список литературы

[1] Дж. Булос и Р. Джеффри. Вычислимость и логика. Мир, 1994.

[2] Н.К. Верещагин и А. Шень. Математическая логика и теория алгоритмов. В трех частях, изд. 4-е. М.: МЦНМО, 2012.

[3] М. Гэри и Д. Джонсон. Вычислительные машины и труднорешаемые задачи. М.: Мир, 1982.

[4] Ю.Л. Ершов и Е.А. Палютин. Математическая логика. Изд. 2. М.: Наука, 1987.

[5] В.Н. Крупский и В.Е. Плиско. Математическая логика и теория алгоритмов. М.: Академия, 2013.

[6] Э. Мендельсон. Введение в математическую логику. Изд. 3-е. М.: Наука, 1984.

[7] С.П. Одинцов, С.О. Сперанский и С.А. Дробышевич. Введение в неклассические логики. Новосибирск: РИЦ НГУ, 2014.