Программа курса

«Основы комбинаторики и теории чисел (весна 2025)»

1. Алгоритм Евклида. Основная теорема арифметики (ОТА): формулировка, существование. Лемма Евклида (док-во, не использующее ОТА). Доказательства ОТА: напрямую, через лемму Евклида.
2. Основы теории сравнений. Системы вычетов. Теоремы Эйлера (2 доказательства) и Ферма (4 доказательства).
3. Линейные сравнения. Китайская теорема об остатках. Вывод формулы для функции Эйлера через остатки.
4. Теорема Лагранжа о числе корней многочлена по простому модулю. Теорема Вильсона.
5. Сравнения второй степени по простому модулю. Квадратичные вычеты и невычеты.
6. Символы Лежандра. Определение, простейшие свойства, формула для (2/p). Квадратичный закон взаимности.
7. Матрицы Адамара. Определение. Нормальная форма. Существование матриц при n = 1 и 2. Необходимость делимости на 4 при n > 3. Гипотеза Адамара. Общие слова про недоказанность. Попытка построить матрицу для n = 2^k путем наложения единиц на минус единицы (получается только k строчек). Решение для n = 2^k. Кронекеровское произведение и общая формулировка про A*B. Конструкция Пэйли с квадратичными вычетами при n = p+1, p = 4m+3.
8. Двоичный код. Расстояние Хэмминга. (n,M,d)-код. Коды, исправляющие ошибки. Верхние границы Хемминга и Плоткина для M. Построение с помощью матриц Адамара кода, который достигает верхней границы Плоткина.
9. Задача о раскрасках с первой лекции первого семестра в терминах уклонения. Верхняя оценка (б/д). Нижняя оценка при помощи матриц Адамара.
10. Распределение простых чисел в натуральном ряде. Функции \pi(x), \theta(x), \psi(x). Теорема о равенстве нижних и верхних пределов. Теорема Чебышёва.
11. Асимптотический закон распределения простых (б/д). «Дырки» между соседними простыми числами (б/д).

12. Показатели. Первообразные корни. Существование по модулю 2, 4, p, p^a, 2p^a. Несуществование по другим модулям. Индексы. Алгоритмические проблемы дискретного логарифмирования.
13. Теорема Дирихле о диофантовых приближениях: случай иррациональных и рациональных чисел. Двумерная теорема Минковского. Ее уточнение для замкнутых множеств (б/д). Применение теоремы Минковского для передоказательства теоремы Дирихле.
14. Конечные цепные дроби. Каноническая запись. Подходящие дроби. Рекуррентные соотношения для числителей и знаменателей подходящих дробей. Следствия: несократимость подходящих дробей, возрастание подходящих дробей с четными номерами и убывание подходящих дробей с нечетными номерами.
15. Бесконечные цепные дроби. Процедура разложения данного числа в цепную дробь. Теорема о сходимости полученной дроби к данному числу. Передоказательство теоремы Дирихле. Уточнение теоремы Дирихле (б/д). Зависимость качества аппроксимации от скорости роста неполных частных: существование чисел с заданным наперед качеством аппроксимации; золотое сечение как самое плохо приближаемое число (б/д). Теорема о периодичности дроби для квадратичной иррациональности (доказательство в одну сторону).
16. Алгебраические и трансцендентные числа. Существование трансцендентных чисел (из соображения мощности). Теорема Лиувилля. Конструкция трансцендентного числа с помощью цепной дроби и теоремы Лиувилля. Сводка результатов о трансцендентности: e, пи, e+пи, пи+e^{пи}, alpha^{beta} (теорема Гельфонда), вывод про e^{пи} из теоремы Гельфонда.
17. Уравнения Пелля (семинары)
18. Иррациональность e. Трансцендентность e.
19. Решетки в пространствах. Базис и определитель. Многомерная теорема Минковского (для произвольной решетки). Теорема Минковского–Главки и история ее улучшений. Доказательство теоремы Минковского-Главки для октаэдра.
20. Равномерно распределенные последовательности mod 1. Исследование р.р. mod 1 последовательностей \sqrt{n}, ln n, a^n, при a < 1. Существование a > 1, при котором последовательность a^n не р.р. mod 1. Интегральные признаки р.р. mod 1 через непрерывную и через комплекснозначную периодическую функцию.

21. Тригонометрические суммы. Критерий Вейля для р.р. mod 1. Теорема Вейерштрасса про приближение непрерывной функции(б/д). Равносильность критерия Вейля и интегрального признака. Исследование р.р. mod 1 последовательности x_n=an при вещественном a, Суммы Гаусса.
22. Тесты на простоту. Тест Ферма. Числа Кармайкла. Символ Якоби, его свойства. Тест Соловея-Штрассена.
23. Тест Миллера-Рабина. Теорема Миллера-Рабина. Сравнение с другими вероятностными тестами. Числа Мерсенна. Тест Люка-Лемера.

Литература:

1. Н.Б. Алфутова, А.В. Устинов. Алгебра и теория чисел (сборник задач). – М.: МЦНМО, 2002.
2. А.М. Райгородский. Линейно-алгебраический метод в комбинаторике. – М.: МЦНМО, 2007.
3. А.М. Райгородский. Задачи о раскрасках. – М.: МЦНМО, 2020.
4. А.И. Галочкин, Ю.В. Нестеренко, А.Б. Шидловский. Введение в теорию чисел. – Изд-во Московского Университета, 1995.
5. И.М. Виноградов. Основы теории чисел. – Москва–Ижевск: НИЦ "Регулярная и хаотическая динамика", 2003.
6. К. Чандрасекхаран. Арифметические функции. – М.: Наука, 1975.
7. Дж.В. Касселс. Введение в геометрию чисел. – М.: Мир, 1965.
8. Хинчин. Цепные дроби.
9. А.А. Глибичук и др. Основы комбинаторики и теории чисел. Сборник задач. Учебное пособие. – М.: Интеллект, 2015
10. Л.Кейперс, Г.Нидеррейтер Равномерные распределения последовательностей. - М.: Наука, 1985.
11. Agrawal M., Kayal N., Saxena N. PRIMES is in P (англ.) // Ann. Math. / J. Bourgain — Princeton University, 2004. — Vol. 160, Iss. 2. — P. 781–793. — ISSN 0003-486X; 1939-8980 — doi:10.4007/ANNALS.2004.160.781