ПОЛУГОДОВОЙ СПЕЦКУРС "НЕКОТОРЫЕ РАЗДЕЛЫ ТЕОРИИ ЧМСЕЛ"

для студентов 1–5 курсов начинает читать профессор А.И.Галочкин по пятницам с 18 час 30 мин до 20 часов по Zoom. Номер конференции 81708926798 код доступа 371774 Для понимания материала достаточно знать элементарную теорию чисел в объеме материала 1 курса. Первая лекция состоится 26 февраля.

ПРОГРАММА КУРСА

1) Алгоритмы нахождения общего наибольшего делителя. Оценка числа арифметических операций.

2) Алгоритм быстрого возведения в степень.

3) Проверка разрешимости квадратичного сравнения по простому модулю.

4) Методы решения полиномиальных сравнений по простому и составному модулям.

5) Методы отбрасывания составных чисел с оценкой сложности алгоритмов и вероятности их реализации.

6) Построение "больших"простых чисел.

7) Методы разложени многочленов на множители.

8) Шифрация по методу RSA, электронная подпись.

9) Алгоритмы дискретного логарифмирования.

10) Субэкспоненциальные методы разложения чисел на множители.

11) Уравнение Пелля. Уравнение Туэ.

12) Представление чисел в виде суммы квадратов.