Алгебра и теория чисел :: занятие 09 (20.04.2010)

День 1 (20.04.2010)

Задачи 1. Проверка чисел на простоту

A. mrptest Тест Миллера-Рабина
B. ssptest Тест Соловея-Штрассена

Лекция 1. (Теория) Квадратичные вычеты

1. Квадратичные вычеты
   a. Квадратичный закон взаимности
   b. Символ Якоби, формулы для символа Якоби аналогичные формулам для символа Лежандра
2. Цепные (непрерывные) дроби
   a. Цепные дроби, рекуррентные формулы для числителей и знаменателей дробей
   b. Число слагаемых в полиноме $[a_0; a_1; \ldots; a_n]$
   c. Теорема о том, что $[a_0; a_1; \ldots; a_{n-1}; a_n] = [a_n; a_{n-1}; \ldots; a_1; a_0]$

Лекция 2. (Практика) Вероятностные тесты чисел на простоту

1. Алгоритмы проверки простоты числа
   a. Тест Ферма проверки чисел на простоту, числа Кармайкла
   b. Тест Соловея-Штрассена проверки чисел на простоту, вероятность ошибки
   c. Тест Миллера-Рабина проверки чисел на простоту
      - Формула для числа свидетелей того, что число составное
2. Сложность задачи проверки чисел на простоту и разложения на множители
   a. Принадлежность задачи проверки чисел на простоту классам **NP** и **coNP**
   b. Принадлежность задачи разложения чисел на множители (в подходящей формулировке) классам **NP** и **coNP**