Алгебра и теория чисел :: занятие 02 (16.02.2010)

День 1 (16.02.2010)

Задачи 1. Основные алгоритмы теории чисел

A.	divmod	Деление остатков по модулю
B.	crt	Китайская теорема об остатках
C.	totient	Функция Эйлера
D.	power	Возведение в степень по модулю

Лекция 1. (Теория) Основные элементы теории чисел

1. Сравнения
   a. Сравнение чисел по модулю. Арифметика по модулю
   b. Полная и приведенная система вычетов
   c. Отсутствие делителей нуля в приведенной системе вычетов
   d. Решение линейных сравнений по модулю, деление остатков
   e. Китайская теорема об остатках, некоструктивное доказательство
   f. Малая теорема Ферма
   g. Теорема Вильсона
2. Теоретико-числовые функции
   a. Функция Эйлера (totient function), мультипликативность функции Эйлера
   b. Теорема Эйлера
   c. Число делителей, сумма делителей, функция Мёбиуса
   d. Свертка Дирихле мультипликативных функций
      - Теорема о мультипликативности свертки Дирихле
      - Теорема об ассоциативности и коммутативности свертки Дирихле
      - Теорема о существовании обратного элемента относительно свертки Дирихле
      - Формула обращения Мёбиуса: обратный элемент для функции Мёбиуса

Лекция 2. (Практика) Основные алгоритмы теории чисел

1. Китайская теорема об остатках, конструктивное доказательство
2. Вычисление мультипликативных функций с помощью решета Эратосфена
3. Быстрое возведение в степень
   a. Метод right-left
   b. Метод left-right
4. Умножение по Монтгомери