Алгебра и теория чисел :: занятие 08 (03.04.2010)

День 1 (03.04.2010)

Задачи 1. Первообразные корни и квадратичные вычеты

A. primroot Первообразный корень

Лекция 1. (Теория+Практика) Первообразные корни и квадратичные вычеты

1. Теорема о цикличности мультипликативной группы поля $\mathbb{Z}/p\mathbb{Z}$
2. Первообразные корни
   a. Теорема о существовании первообразных корней по модулям p^n, $2 \cdot p^n$ и 4
   b. Количество первообразных корней
3. Квадратичные вычеты
   a. Определение квадратичного вычета и квадратичного невычета по произвольному модулю
   b. Число квадратичных вычетов по простому модулю
   c. Символ Лежандра
   d. Формула для символа Лежандра (Критерий Эйлера)
   e. Теорема о $((\frac{p-1}{2})!)^2 \equiv -1 \pmod{p}$ при $p = 4k + 1$
   f. Лемма Гаусса для вычисления квадратичного характера числа по простому модулю
   g. Квадратичный характер числа 2 по простому модулю