

**Math 104A, Number Theory, Fall 2002.**  
**Summary of Lecture 23.**

**Midterm Grades.** The exam was graded out of 100. To assign grades to this particular exam, A- starts in the high seventies, B+ starts around 70, B- starts around 55 and C- starts around 30. If you got below 40 you should make arrangements to discuss with Kate Okikiolu or Michele Schuman your strategy for reviewing the material and passing the class.

This lecture we covered Proposition 5.3.1, Examples 5.3.8 and 5.3.9, and Proposition 5.3.3.

**Theorem.** If  $n = pq$  is a product of distinct primes and  $ed = 1 \pmod{\phi(n)}$ , where  $\leq e, d < n$ , then from knowing  $n, e, d$  one can compute  $p$  with probability  $1 - 2^{-k}$  in time  $Ck(\log n)^\ell$ . Here  $C$  and  $\ell$  are constant.

To prove this, we start by proving Lagrange's Theorem 4.4.1. We make the following definition.

**Definition.** The polynomials  $f(x) = a_n x^n + \cdots + a_0$  and  $g(x) = b_n x^n + \cdots + b_0$  are congruent as polynomials modulo  $m$  (written  $f \equiv g \pmod{m}$ ) if  $a_j \equiv b_j \pmod{m}$  for each  $j$  with  $0 \leq j \leq n$ .

To prove Lagrange's Theorem we will show

**Theorem.** For any polynomial  $f(x) = a_n x^n + \cdots + a_0$ , if  $r_1, \dots, r_k$  are the distinct roots of  $f$  modulo  $m$ , then there exist exponents  $e_1, \dots, e_k$  and a polynomial  $g(x) = b_\ell x^\ell + \cdots + b_0$ , such that  $g$  has no roots modulo  $m$  and

$$f(x) \equiv (x - r_1)^{e_1} \cdots (x - r_k)^{e_k} g(x) \pmod{m}.$$

Here  $e_1 + \cdots + e_k + \ell = n$ . Moreover the exponent  $e_k$  is well defined and is called the *multiplicity* of the root  $r_k$ .