CS 681: Computational Number Theory and Algebra **Lecture 26**

Analysis of Discrete Log Problem using Index Calculus and Number Field Sieve

Lecturer: Manindra Agrawal **Scribe: Sudeepa Roy**

October 10, 2005

1 Introduction

In this lecture we will first do the analysis of the algorithm to solve discrete log problem using index calculus stated in the last lecture. Next we will briefly discuss *Number Field Sieve*.

2 Analysis of Discrete Log Problem

Here we use the same notations as in the previous lecture. To recapitulate, the problem was to compute m from the equation $e = g^m$ given g and e, and the idea was to find r and s, such that

1. $g^r e^s = 1$
2. $\gcd(s, order(g)) = 1$

After the step 4 of the algorithm, we have k triples (r_i, s_i, u_i) with $u_i = \prod_{j=1}^{t} {p_j}^{\alpha_{ij}}$, where $p_1, \cdots, p_t$ are all the primes $\leq k$.

We know $\vec{\beta}$ is such that $\sum_{i=1}^{k} \beta_i \alpha_{ij} = 0 \ (\mod p-1)$

$r = \sum_{i=1}^{k} \beta_i r_i$ and $s = \sum_{i=1}^{k} \beta_i s_i$

Then

$g^r e^s$

$= g^{\sum_i \beta_i r_i} e^{\sum_i \beta_i s_i}$

$= \prod_{i=1}^{k} (g^{r_i} e^{s_i})^{\beta_i}$

$$= \prod_{i=1}^{k} u_i^{\beta_i}$$
$$= \prod_{i=1}^{k} \prod_{j=1}^{t} {p_j}^{\alpha_{ij}\beta_i}$$
$$= \prod_{j=1}^{t} \prod_{i=1}^{k} {p_j}^{\alpha_{ij}\beta_i}$$
$$= \prod_{j=1}^{t} {p_j}^{\sum_{i=1}^{k} \alpha_{ij}\beta_i}$$
$$= 1 \ (\mod p)$$

We also need $\gcd(s, p-1) = 1$.
$Pr[\gcd(s, p-1) = 1] = \frac{\phi(p-1)}{p-1} \geq \frac{1}{2}$.

Time complexity of the algorithm is
$O(e^{2(\ln p)^{\frac{1}{2}}(\ln \ln p)^{\frac{1}{2}}})$.

3 Number Field Sieve

Number Field Sieve is a very fast method to factor integer n and improvement over quadratic sieve reducing the exponent. The time complexity is $O(e^{c(\ln n)^{\frac{1}{3}}(\ln \ln n)^{\frac{2}{3}}})$ where $c \approx 1.93$.