CS 681: Computational Number Theory and Algebra **Lecture 31:**
Polynomial Factorization over $\mathbb{Q}$
Lecturer: Manindra Agrawal **Notes by: Arun Iyer**

November 8, 2005.

1 Polynomial Factorization over $\mathbb{Q}$

Given a polynomial $f(x)$ of degree d over $\mathbb{Q}$.
Assume that f is monic and square-free.

1. Choose a small prime p such that f remains square-free in F_p.

   [1.1] For making this choice of p, we can simply iterate over all primes starting from the smallest prime that is 2. We will now try to derive an upper bound on p.

   [1.2] Let k be the largest coefficient in f. Then, the possible largest coefficient in f' would be kd. Now, this would imply that $|Res(f, f')| \leq (2d)!(kd)^{2d} \leq (2kd^2)^{2d} = 2^{2d\log(2kd^2)}$. This would imply that $p = O(d\log(kd)\log(d))$.

2. Factorize $f \; mod \, p$ as $f = f_1 f_2$ where f_1 is irreducible.

   [2.1] Recall that polynomial factorization over field which was discussed in the earlier class was randomized. However, owing to the fact that p here is very small, the process can be made deterministic.

3. Use Modified Hensel Lifting to compute $f = g_1 g_2 (mod \, p^l)$.

   [3.1] Note that g_1 and f_1 have same degree. Also, the way modified hensel lifting is done, if g_1 were reducible mod p^l then it would be reducible mod p and this would imply f_1 to be reducible mod p which is false. Hence g_1 above is irreducible.

   [3.2] The choice of value l, will be decided later.

4. Let $deg(g_1) = d_1$. Define lattice $\mathbb{L}$ as spanned by $[g_1, xg_1, \ldots, x^{d-d_1}g_1, p^l, xp^l, \ldots, x^{d_1-1}p^l]$.

   [4.1] Volume of this lattice, $Vol(\mathbb{L}) = p^{ld_1}$.

5. Use LLL-algorithm (Lenstra, Lenstra and Lovàsz algorithm) to find a short vector in $\mathbb{L}$. Let that vector be $\overrightarrow{u}$.

   [5.1] $|u| \leq 2^{\frac{d-1}{2}}$(length of the actual shortest vector) $\leq 2^{\frac{d-1}{2}}\sqrt{d}p^{\frac{ld_1}{d}}$

   [5.2] Let $u(x)$ be the polynomial give by the $\overrightarrow{u}$. $\overrightarrow{u}$ can written as a linear combination of its basis vectors. Therefore, $u(x)$ can be written as $g_1(x)h(x)(mod \, p^l)$ for some $h(x)$.

[5.3] Let $f = \hat{f}_1\hat{f}_2$ over $\mathbb{Q}$ with $g_1|\hat{f}_1(mod\, p^l)$. $(\hat{f}_1, u(x)) \neq 0(mod\, p^l)$, this implies $|Res(\hat{f}_1, u(x))| = 0(mod\, p^l)$

(To be continued . . .)