CS 681: Computational Number Theory and Algebra	**Lecture 29**
Lecturer: Manindra Agrawal	**Notes by: Ashwini Aroskar**
	October 28, 2005.

Idea: Given v_1, v_2, ..., v_n, compute v_1^*, v_2^*, ..., v_n^* and sort v_1, v_2, ..., v_n in increasing order of $|v_n^*|$

The reordered sequence v_1', v_2', ..., v_n' is a reduced basis, but as we cannot claim $v_1' = v_1'^*$, the proof of the earlier lemma about a reduced basis does not go through. Hence, we cannot get the shortest vector in this manner.

First Algorithm proposed

Input: v_1, v_2, ..., v_n

Step 1: Compute u_1, u_2, ..., u_n from v_1, v_2, ..., v_n using 'approximate orthogonalization' process

Step 2: Check if u_1, u_2, ..., u_n is a reduced basis

If not suppose the first violation occurs at index i.

Step 3: Swap u_i and u_{i+1}, rename the sequence v_1, v_2, ..., v_n and goto Step 1

This algorithm stops only if we have a reduced basis.

Analysis of the above algorithm

$u_i^* = u_i - \sum_{j<i} \lceil \mu_{ij} \rfloor u_j$

Denote the sequence as $\hat{u}_1, \hat{u}_2, ...\hat{u}_n$ after the swap.

But we want $\hat{u}_j^* = u_j^*$ for all $j < i$ and $j > i$

Therefore we modify the above algorithm.

Modified Algorithm

Input: v_1, v_2, ..., v_n

Step 0: Let $u_i = v_i$

Step 1: for($i = 1; i \leq n;$) {

Step 2: Compute $u_i = v_i - \sum_{j<i} \lceil \mu_{ij} \rfloor u_j$

& $u_i^* = v_i^* - \sum_{j<i} \lceil \mu_{ij} \rfloor u_j^*$

Step 3: Check if $|u_{i+1}^*| \leq 2|u_i^*|^2$

Step 4: If not, swap u_{i+1} and u_i and let $i = i - 1$
Step 5: else let $i = i + 1$
}
The analysis of the modified algorithm will follow in the next class.