15-852 Randomized Algorithms

Homework # 5 **due: April 9, 1997**

Problems:

1. Exercise 14.4 (p. 397) in the book: prove for $n = p_1^{k_1} \cdots p_t^{k_t}$ that

$$\phi(n) = \prod_{i=1}^{t} p_i^{k_i - 1}(p_i - 1).$$

   Thus, given a factorization of n we can compute $\phi(n)$.

2. Problem 14.3 in the book: show that given n and $\phi(n)$ we can compute the factorization of n (note: we did this in class just for the special case $n = pq$).

3. Describe a decision (yes/no) problem that is poly-time equivalent to factoring (given an oracle for solving the decision problem one can factor and vice-versa) and show that your decision problem is in NP $\cap$ co-NP.

4. Problem 12.28 in the book.