Math 523 Assignment #2 Due Wednesday February 9

1. Consider the following two recognition problems:

PRIME

instance: given an integer k ($k > 1$), is k prime?

COMPOSITE

instance: given an integer k ($k > 1$), is k composite i.e. does it have non trivial factors?

The 2002 paper by M.Agrawal, N.Kayal and N.Saxena established that the problem PRIME is in P (and hence COMPOSITE is in P but not factoring). Thus a record of the running of that algorithm would provide a certificate. I'll accept that approach only if you can give a good description of why there algorithm works (which would be showing that the certificate is polynomial).

a) Show COMPOSITE$\in$NP (easy)

b) Show PRIME$\in$NP (hard) by showing that the following idea yields a certificate of primality: An integer n is prime if and only if there exists an integer a such that

i)$a^{n-1} \equiv 1(\text{modulo } n)$

ii)$a^{(n-1)/p} \not\equiv 1(\text{modulo } n)$ for all primes p which are divisors of $n-1$.

Don't forget to include certificates of the primality of the various primes p. And no doubt those certificates will involve yet more primes which are mercifully smaller. You will have to develop a recurrence that upper bounds the size of the certificate and the time to verify it.

2. It would be helpful to read concerning polynomial transformations between problems. An instance of the problem ILP has m, n, A, b given and the questions is whether there is an $\mathbf{x} \in Z^n$ with $A\mathbf{x} \le \mathbf{b}$. Show that SAT polynomially transforms into ILP. Does this make ILP an NP-complete problem? Discuss.

3. The formulas for the Ellipsoid algorithm as given will not yield a polynomial algorithm using the ideas of bit complexity.

$$B_{i+1} = \frac{n^2}{n^2-1}\left(B_i - \frac{2}{n+1}\frac{(B_ia)(B_ia)^T}{a^TB_ia}\right)$$

$$t_{i+1} = t_i - \frac{1}{n+1}\frac{B_ia}{\sqrt{a^TB_ia}}$$

We might imagine computing successive B_i with exact rational arithmetic. Explain why we are concerned that the fractions could increase in size to exponential in the input size.

4.(Graph Theory) Let $D = (N, A)$. We refer to a flow cycle C of size k for a directed cycle C, as a flow $\mathbf{x}_C = (x_C(e) : e \in A)$ which has

$$x_C(e) = \begin{cases} k & \text{if } e \in C \\ 0 & \text{if } e \notin C \end{cases}$$

A *circulation* is a flow with conservation of flow at every vertex, namely

$$\sum_j x(i,j) - \sum_j x(j,i) = 0 \text{ for all } i \in N$$

Show that a flow $\mathbf{x}$ on D is a circulation if and only if $\mathbf{x}$ is a sum of flow cycles, in fact at most $m = |A|$ flow cycles. If $\mathbf{x}$ has $x(e) \in Z$ for all $e \in A$, then $\mathbf{x}$ can be written as a sum of flow cycles where all the sizes k are integers.