Basic Algorithms, Assignment 12

Due by 8 a.m. Wednesdy, April 28.
Send to Jingshuai: jj2903@nyu.edu.

To me, it does not seem unlikely that on some shelf of the universe there lies a total book. I pray the unknown gods that some man - even if only one man, and though it have been thousands of years ago! - may have examined and read it. If honor and wisdom and happiness are not for me, let them be for others. May heaven exist, though my place be in hell. Let me be outraged and annihilated, but may Thy enormous Library be justified, for one instant, in one being.
Jorge Luis Borges, *The Library of Babel*

1. Using the Island-Hopping Method to find 2^{1072} modulo 1073 using a Calculator but NOT using multiple precision arithmetic. (You should never have an intermediate value more than 1072^2.) What does your result tell you about the primality of 1073.

2. `Please try all of these but submit only three -- your choice!` Which of the following problem classes are in P and which are probably not in P. (By probably not we mean that we do not as of today know that it is in P but of course tomorrow somebody might come up with a clever algorithm.)

   (a) `PRIME`. The input here would be an integer n and Yes would be returned iff n is prime. Also: what was the answer when I gave the above problem twenty five years ago?

   (b) `CONNECTED-GRAPH`. The input here would be a graph G and Yes would be returned iff the graph was connected.

   (c) `TRAVELING-SALESMAN`. The input here would be a graph G together with a positive integer weight $w(e)$ for each edge e and an integer B. Yes would be returned iff there was a Hamiltonian Cycle which had total weight at most B.

   (d) `SPANNING-TREE`. The input here would be a graph G together with a positive integer weight $w(e)$ for each edge e and an integer B. Yes would be returned iff there was a spanning tree which had total weight at most B.

   (e) `ALMOSTDAG`. The input here would be a directed graph G. Yes would be returned iff there was a set of at most 10 edges of G that could be removed from G so that the remaining graph is a `DAG`. (Your argument should work with 10 replaced by any *constant* value.)

3. `Please try all of these but submit only three -- your choice!` Show that the following problem classes are in NP. (That is, describe the certificate that the Oracle gives and describe the procedure that Verifier will take. Warning: Do not trust Oracle! For example, if Oracle gives you n distinct vertices you have to verify that they are indeed distinct!)

   (a) `PRIME-INTERVAL` The input here would be integers n, a, b. Yes would be returned iff there was a prime p which divided n and for which $a \leq p \leq b$.

   (b) `TRAVELING-SALESMAN` As described above.

   (c) `RAMANUJAN` We'll call a positive integer n RAMANUJAN if it can be expressed as the sum of two positive cubes in (at least) two different ways. So $1729 = 1^3 + 12^3 = 10^3 + 9^3$ is RAMANUJAN, and comes from a famous story about Ramanujan and Hardy.

   (d) `COMPOSITE` The input here would be an integer n. Yes would be returned if n was composite. For this problem I want two solutions. One (the easier one) uses the Agarwal, Kayal, Saxena algorithm. The second should *not* use the Agarwal, Kayal, Saxena algorithm.

   (e) `3-COLOR`. The input here would be a graph G. Yes would be returned if there was a three coloring of the vertices such that no two adjacent vertices v, w had the same color.

   (f) `NEAR-DAG`. The input here would be a directed graph G and an integer B. Yes would be returned if there was a set of at most B edges that could be removed from G so that the remaining graph was acyclic. (This is like `ALMOST-DAG` with the critical distinction that B is not restricted to 10, or any constant value. Rather, B can depend on the number of vertices of G.)

4. Assume `PRIME-INTERVAL` (defined above) is in P. Using it as a black box give a polynomial time algorithm with input integer $n \geq 2$ that returns some prime factor p. Suppose `PRIME-INTERVAL` takes time $O(d^6)$ where d is the number of digits of n. Give the time of your algorithm as time $O(d^c)$ for some explicit constant c.

Among his co-workers in an Indian named Ganapathy. Ganapathy often arrives late to work; on some days he does not come at all. When he does come, he does not appear to be working very hard; he sits in his cubicle with his feet on the desk, apparently dreaming. For his absences he has only the most cursory of excused ("I was not well") Nevertheless he is not chided. Ganapathy, it emerges, is a particularly valuable aquisition for International Computers. He has studied in America, holds an American degree in computer science.
J.M. Coetzee, *Youth*