Basic Algorithms, Assignment 10  
Due, TUESDAY, Nov 20

1. A positive integer $n$ is called banana if it can be written as the sum of two integer squares. (E.g., $41 = 16 + 25$.) Argue that the problem class BANANA is in NP.

2. In 2002 Agarwal, Kayal and Saxena showed that PRIME is in P. Call a positive integer $n$ walrus if it is the product of precisely three primes. Given the AKS result, argue that WALRUS is in NP. Argue (harder!) that NOTWALRUS is in NP.

3. Let define 3-SATSMALL to be the same as 3-SAT except that no Boolean variable $x_i$ appears (as either $x_i$ or $\overline{x_i}$) more than 20 times. Our object is to show $3$-SAT$\leq_P 3$-SATSMALL.

   (a) Let $x, y$ be Boolean variables. Find a set of clauses $C_1, \ldots, C_r$ of size 3 using auxiliary Boolean variables $z_1, z_2, \ldots, z_s$ so that $C_1 \land \ldots \land C_r$ can be satisfied if and only if $x, y$ have the same truth value. (Here $r, s$ will be small numbers.)

   (b) Let $x_1, \ldots, x_w$ be Boolean variables. Show that there is a set of clauses $C_1, \ldots, C_v$ using auxiliary variables $z_1, \ldots$ so that $C_1 \land \ldots \land C_v$ can be satisfied if and only if $x_1, \ldots, x_w$ have the same truth value. Further, we require that none of the Boolean variables (neither the original $x$’s nor the auxiliary $z$’s) are used more than ten times. (Idea: Make sure $x_i, x_{i+1}$ have the same truth value for $1 \leq i < w$.)

   (c) Show $3$-SAT$\leq_P 3$-SATSMALL. (Idea: When $x_i$ appears many times replace it with copies $x_i^1, x_i^2, \ldots$, none appearing very often, that all must have the same truth value.)

4. Suppose a graph algorithm with input a graph $G$ takes a time polynomial in $N + M$ where $N$ is the number of vertices and $M$ is the number of edges in $G$. Show that it takes time polynomial in $N$. Suppose a number theoretic algorithm with input a positive integer $x$ takes time polynomial in $x$. What can you say about the time it takes when the input is an $n$-digit number? In particular, explain why you cannot say that the time is polynomial in $n$.

What I tell you three times is true  
– Lewis Carroll in Hunting the Snark