Theoretical Cryptography	Manuel Blum and Steven Rudich
HW4	Due: 4/26/06

Who to Blame: Ryan. That is, tell him if you find errors, and ask him for clarifications.

Rules: As usual, please cite all sources that you may use.

For the first two questions, you need not prove your answer. A reference suffices.

1. True or false? *For all primes p and integers $e \geq 1$, $\mathbb{Z}^*_{p^e}$ has a generator.*

2. True or false? *For all odd primes p and integers $e \geq 1$, $\mathbb{Z}^*_{p^e}$ has a generator.*

3. Give a polynomial time algorithm that takes a number N as input, and outputs "yes" if and only if $N = p^e$ for some prime p and positive integer e.

4. Let n be a positive integer. Recall that the prime density function, $\pi(n)$, is defined as the number of prime numbers less than or equal to n. The Prime Number Theorem states that $\lim_{n\to\infty} \frac{\pi(n)}{n/\ln n} = 1$. Here, you will prove a weaker statement: $\pi(n) = \Omega(n/\log n)$. Sophisticated number theory is not required to prove this.

   (a) Let p be a prime in the following. Show that p divides $n!$, at least $\sum_{i=1}^{\infty} \lfloor \frac{n}{p^i} \rfloor$ times.
   Hint: First, count the numbers between 1 and n that can be divided by p at least once. Then count the number that can be divided by p at least twice, and so forth.

   (b) Define $r(p)$ as the natural number such that $p^{r(p)} \leq 2n < p^{r(p)+1}$.
   Prove that p does not divide $\binom{2n}{n}$ more than $r(p)$ times.
   Conclude that
   $$2^n \leq \binom{2n}{n} \leq \prod_{\text{prime } p \leq 2n} p^{r(p)} \leq (2n)^{\pi(2n)}.$$

   (c) Prove that $\pi(n) \geq \frac{n}{2\log_2 n}$.