Math 567, Assignment #8

(due Tuesday, April 4)

This assignment covers material up through section 8.2.

1. Establish each of the statements below, and in each case, determine whether the converse of the statement is true as well:
   (a) If a has order hk modulo n, then a^h has order k modulo n.
   (b) If a has order $2k$ modulo the odd prime p, then $a^k \equiv -1 \pmod{p}$.
   (c) If a has order $n-1$ modulo n, then n is prime.

2. Assume that the order of a modulo n is h and the order of b modulo n is k. Show that the order of ab modulo n is a divisor of hk; and show in particular that if $\gcd(h,k) = 1$ then ab has order hk.

3. Prove that, for each odd prime p, there are infinitely many primes of the form $2kp + 1$.

4. Determine all the primitive roots of the primes $p = 11$, 19, and 23, expressing each as a power of some one of the primitive roots.

5. Use the fact that each prime p has a primitive root to give a different proof of Wilson's theorem. [Hint: If p has a primitive root r, then you can use Theorem 8.4 to show that $(p-1)! \equiv r^{1+2+\cdots+(p-1)} \pmod{p}$.]