Math 25, Homework 6, November 3, 2008

1. Suppose that n is a positive integer and that a, h are positive integers with a coprime to n. Prove that the order of a in U_n is h if and only if

$$a^h \equiv 1 \pmod{n} \quad \text{and} \quad a^{h/q} \not\equiv 1 \pmod{n} \quad \text{for all primes} \quad q \mid h.$$

2. Show that an integer a coprime to 13 is a primitive root for 13 if and only if $a^4 \not\equiv 1 \pmod{13}$ and $a^6 \not\equiv 1 \pmod{13}$.

3. Show that 2 is a primitive root for 101.

4. For a positive integer n, let $\lambda(n)$ denote the largest order of any element in U_n. So, for example, n has a primitive root if and only if $\lambda(n) = \varphi(n)$. For each integer n with $2 \le n \le 20$, find $\lambda(n)$ and exhibit an element in U_n with order $\lambda(n)$.

5. Suppose a is coprime to the positive integer n and that the order of a in U_n is h. Show that the order of a^j in U_n is $h/\gcd(j,h)$ for every integer j.

6. Prove or give a counterexample: If a, b in U_n have orders h, k respectively, and $\gcd(h,k) = 1$, then ab has order hk.

7. Prove or give a counterexample: If a, b in U_n have orders h, k respectively, then ab has order $\operatorname{lcm}[h,k]$.

8. Show that if n is a positive integer and $\gcd(a,n) = 1$, then $a^{\lambda(n)} \equiv 1 \pmod{n}$, where λ is defined in problem 4.

   Solution: Suppose that b has order $\lambda(n)$ and a is an integer coprime to n. Let h be the order of a. We would like to show that $h \mid \lambda(n)$. If $h \nmid \lambda(n)$, then there is a prime p and a positive integer j such that $p^j \mid h$, yet $p^j \nmid \lambda(n)$. By problem 5, the order of $A := a^{h/p^j}$ is $u := h/(h, h/p^j) = p^j$, and the order of $B := b^{p^j}$ is $v := \lambda(n)/(\lambda(n), p^j)$. Since $p^j \nmid \lambda(n)$, it follows that v is not divisible by p, so that u, v are coprime. By problem 6, we have the order of AB is uv. But $v = \lambda(n)/p^i$ for some integer $i < j$, and $u = p^j$, so that $uv \ge p\lambda(n) > \lambda(n)$. This contradicts the definition of $\lambda(n)$, so we are done.

9. Show that if $n > 1$ is an integer,

$$a^{n-1} \equiv 1 \pmod{n} \quad \text{and} \quad a^{(n-1)/q} \not\equiv 1 \pmod{n} \quad \text{for all primes} \quad q \mid n-1,$$

   then n is prime.