MATH 3070
Assignment # 5
Due Thursday, October 30, 2008

1. (a) Find all primitive roots mod 23.
   (b) Determine all residue classes mod 23 of the following orders, or state why none exist: order 2, order 5, order 11.

2. Existence of primitive roots for composite moduli.
   In this problem, the letter p will always denote an odd prime.

   (a) Let $(m, n) = (a, mn) = 1$. Let $\text{ord}_m(a) = k$ and $\text{ord}_n(a) = \ell$.
   Prove that $\text{ord}_{mn}(a) = \dfrac{k\ell}{\gcd(k, \ell)} = \text{lcm}(k, \ell)$.

   (b) Explain why unless $m = 2$ or $n = 2$, there are no primitive roots mod mn. This shows that if N is composite, there are no primitive roots mod N unless N is a prime power or two times a prime power.

   (c) Let a be a primitive root mod p^k, where p is an odd prime and $k \geq 1$. Show that $\text{ord}_{p^{k+1}}(a)$ must be a multiple of $\varphi(p^k)$.

   (d) Let a be a primitive root mod p. Prove that either $\text{ord}_{p^2}(a^{p-1}) = 1$ or a is a primitive root mod p^2.

   (e) Let a be a primitive root mod p. If $\text{ord}_{p^2}(a^{p-1}) = 1$ then prove that $a + p$ is a primitive root mod p^2.

   (f) Let a be a primitive root mod p^2. Prove that a is also a primitive root mod p^k for $k > 2$.

   Hint: Induct on k. Using the inductive hypothesis, first show that if $a^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^k}$ then a must be a primitive root mod p^k. Next show $a^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^k}$ by contradiction. You might find the factorization

   $$a^{p^{k-2}(p-1)} - 1 = (a^{p^{k-3}(p-1)} - 1)(a^{p^{k-3}(p-1)(p-1)} + a^{p^{k-3}(p-1)(p-2)} + \cdots a^{p^{k-3}(p-1)(1)} + 1)$$

   useful. Think about how many factors of p can divide each of these factors.

   (g) Use the results of the previous parts to construct a primitive root mod $2p^k$.

3. Use indices to find all solutions to the following congruences

   (a) $4x^4 \equiv 9 \pmod{23}$
   (b) $x^{10} \equiv 45 \pmod{76}$