Math 5330 Homework 7

Spring 2009

1. Find (with proof!) all integers n such that $\varphi(n) = 20$.

2. Solve each of the following systems of congruences:

a.
$x \equiv 1 \bmod 3$
$x \equiv 3 \bmod 5$
$x \equiv 5 \bmod 7$

b.
$x \equiv 1 \bmod 2$
$x \equiv 2 \bmod 3$
$x \equiv 3 \bmod 5$
$x \equiv 4 \bmod 7$

c.
$x \equiv 1 \bmod 12$
$x \equiv 4 \bmod 21$
$x \equiv 18 \bmod 35$

d.
$x \equiv 2 \bmod 9$
$x \equiv 8 \bmod 15$
$x \equiv 10 \bmod 25$

3. Find a number n such that $3^2 \mid n$, $4^2 \mid n + 1$, $5^2 \mid n + 2$.

Extra credit problems:

1. Show that for each prime $p \geq 5$, $n_p = \dfrac{4^p - 1}{3}$ is a base 2–pseudoprime.

Hint: You must show that $2^{n_p - 1} \equiv 1 \pmod{n_p}$. To do this, note that $2^{n_p - 1} = 2^{(4^p - 4)/3}$. Since p is a prime, $4^p - 4$ is divisible by p. It is also divisible by 3 (why?), and is even, so $\dfrac{4^p - 4}{3} = 2kp$ for some integer k.

Use all this information to show that $2^{n_p - 1} \equiv 1 \pmod{n_p}$.

2. Prove that for every integer $b \geq 2$, there are infinitely many pseudoprimes base b. (That is, show that there are infintely many n such that n is not prime but $b^{n-1} \equiv 1 \pmod{n}$.) Hint: mimic the proof to 1.