Homework 3 : Due Wednesday, February 15

Problem 1: Follow the proof of the Chinese Remainder Theorem (with several moduli) in the notes to find all $x \in \mathbb{Z}$ that simultaneously satisfy the following three congruences:

$$x \equiv 1 \pmod 7 \qquad x \equiv 4 \pmod 9 \qquad x \equiv 3 \pmod 5$$

Problem 2: Show that $n^{91} \equiv n^7 \pmod{91}$ for all $n \in \mathbb{Z}$.

Problem 3: Prove the converse to Wilson's Theorem: If $n \geq 2$ and $(n-1)! \equiv -1 \pmod n$, then n is prime.

Problem 4: Define $\sigma \colon \mathbb{N}^+ \to \mathbb{N}^+$ by letting $\sigma(n)$ be the sum of all positive divisors of n. In other words,

$$\sigma(n) = \sum_{d \mid n} d$$

For example, $\sigma(6) = 1 + 2 + 3 + 6 = 12$.
a. Suppose that m and n are relatively prime. Let $d \in \mathbb{N}^+$ be such that $d \mid mn$. Show that there exist unique $a, b \in \mathbb{N}^+$ such that $d = ab$, $a \mid m$, and $b \mid n$. Avoid using the Fundamental of Arithmetic if possible.
b. Use part a to show that $\sigma(mn) = \sigma(m) \cdot \sigma(n)$ whenever $m, n \in \mathbb{N}^+$ satisfy $\gcd(m, n) = 1$.
c. Give a closed form formula for $\sigma(p^k)$ whenever $p \in \mathbb{N}^+$ is prime and $k \in \mathbb{N}^+$.
d. Use parts b and c to give a formula for $\sigma(n)$ in terms of the prime factorization of n.

Problem 5: Let R be a commutative ring. An *idempotent* of R is an element $e \in R$ such that $e^2 = e$. For example, $0, 1 \in R$ are always idempotents. In $\mathbb{Z}/6\mathbb{Z}$, both $\overline{3}$ and $\overline{4}$ are idempotents distinct from $\overline{0}$ and $\overline{1}$.
a. Show that if R is an integral domain, then the only idempotents of R are 0 and 1.
b. Let p be prime and $k \geq 1$. Show that the only idempotents in $\mathbb{Z}/p^k\mathbb{Z}$ are $\overline{0}$ and $\overline{1}$.
c. Show that if n is not a prime power, then there exists an idempotent in $\mathbb{Z}/n\mathbb{Z}$ other than $\overline{0}$ and $\overline{1}$. Give a formula for the number of such idempotents in terms of the prime factorization of n.
Hint for c: Instead of trying to "build" idempotents in $\mathbb{Z}/n\mathbb{Z}$ directly, work in an isomorphic ring.

Problem 6:
a. Show that $\varphi(n)$ is even for all $n \geq 3$.
b. Show that $\lim_{n \to \infty} \varphi(n) = \infty$. In other words, show that for every $m \in \mathbb{N}^+$, there are only finitely many $n \in \mathbb{N}^+$ with $\varphi(n) \leq m$.