Homework 2 : Due Wednesday, February 10

Problem 1: Follow the proof of the Chinese Remainder Theorem to find all $x \in \mathbb{Z}$ which simultaneously satisfy the following three congruences:

$$x \equiv_7 1 \qquad x \equiv_9 4 \qquad x \equiv_5 3$$

Problem 2: Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ be a polynomial in $\mathbb{Z}[x]$. Suppose that a_0 and $a_n + a_{n-1} + \cdots + a_1 + a_0$ are both odd. Show that $f(x)$ has no integer roots.

Problem 3: Show that $n^{91} \equiv_{91} n^7$ for all $n \in \mathbb{Z}$.

Problem 4: Define $\sigma \colon \mathbb{N}^+ \to \mathbb{N}^+$ by letting $\sigma(n)$ be the sum of all positive divisors of n. 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 $b \mid n$.
b. Show that $\sigma(mn) = \sigma(m) \cdot \sigma(n)$ whenever m and n are relatively prime.
c. Give a closed form formula for $\sigma(p^\alpha)$ whenever p is prime and $\alpha \geq 1$.
d. Use parts b and c to give a formula for $\sigma(n)$ in terms of the prime factorization of n.

Problem 5: Let p be prime.
a. Show that $p \mid \binom{p}{k}$ whenever $1 \leq k \leq p-1$ (where $\binom{p}{k} = \frac{p!}{k!(p-k)!}$).
b. Deduce from part a (i.e. don't use Fermat's Little Theorem) that $(a+1)^p \equiv_p a^p + 1$ for all $a \in \mathbb{Z}$.
c. Derive Fermat's Little Theorem from part b.

Problem 6: Suppose that p is prime.
a. Show that if $a^2 \equiv_p b^2$, then either $a \equiv_p b$ or $a \equiv_p -b$.
b. Suppose that p is odd. Show that for exactly half of the integers $a \in \{1, 2, 3, \dots, p-1\}$, the equation $x^2 \equiv_p a$ has a solution in $\mathbb{Z}$.

Problem 7:
a. Show that if p is an odd prime and $k \geq 1$, then $x^2 = 1$ has 2 solutions in $\mathbb{Z}/p^k\mathbb{Z}$.
b. Show that $x^2 = 1$ has 1 solution in $\mathbb{Z}/2\mathbb{Z}$, 2 solutions in $\mathbb{Z}/4\mathbb{Z}$, and 4 solutions in $\mathbb{Z}/2^k\mathbb{Z}$ for every $k \geq 3$..

Problem 8:
a. Find, with explanation, all $n \in \mathbb{N}^+$ such that $\varphi(n)$ is odd.
b. Find, with explanation, all $n \in \mathbb{N}^+$ such that $\varphi(2n) = \varphi(n)$.
c. Find, with explanation, all $n \in \mathbb{N}^+$ such that $\varphi(n) = 24$.