ASSIGNMENT 6 ECE 103 (Spring 2009)

Due in tutorial on Monday, June 29.

1. Solve the simultaneous linear congruences

$$\begin{aligned} 11x &\equiv 1 \pmod{21} \\ 15x &\equiv 20 \pmod{40}. \end{aligned}$$

2. Solve the polynomial congruence $x^3 + x^2 \equiv 42 \pmod{72}$. (Hint: $72 = 8 \cdot 9$, and $\mathrm{GCD}(8, 9) = 1$.)

3. (a) Prove that for all $n \in \mathbb{N}$, $7 \mid 5n^7 + 7n^5 + 23n$.
   (b) Prove that for all $n \in \mathbb{N}$, $5n^7 + 7n^5 + 23n \equiv 0 \pmod{35}$.

4. Let p be a prime number, and let a be a positive integer that is not a multiple of p. Fermat's Little Theorem says that $a^{p-1} \equiv 1 \pmod{p}$, but $p - 1$ might not be the lowest power of a with this property.
   (a) Let s be the smallest positive integer such that $a^s \equiv 1 \pmod{p}$. By the Division Algorithm, write $p - 1 = qs + r$, where $q, r \in \mathbb{Z}$ with $0 \leq r < s$. Prove that $a^r \equiv 1 \pmod{p}$.
   (b) Explain why it must be the case that $r = 0$, i.e., that $s \mid p - 1$.
   (c) Find the smallest positive integer s such that $8^s \equiv 1 \pmod{17}$.