HOMEWORK ASSIGNMENT #4, DUE FRIDAY, 10/22/2010

(1) (a) Find all simultaneous solutions to the system $x \equiv 7 \mod 20, x \equiv 2 \mod 3$.
    (b) Find all simultaneous solutions to the system $x \equiv 3 \mod 7, x \equiv 2 \mod 8, x \equiv 1 \mod 5$.

(2) (a) Find all simultaneous solutions to the system $x^2 + 3x + 1 \equiv 0 \mod 5, 3x \equiv 2 \mod 7$.
    (b) Find all simultaneous solutions to the system $x^2 \equiv 1 \mod 8, 5x \equiv 15 \mod 20, 5x \equiv 1 \mod 6$.

(3) Consider the simultaneous system $x \equiv a_1 \mod n_1, x \equiv a_2 \mod n_2$. Prove the following special case of Theorem 3.12 in the textbook: this system has a solution if and only if $\gcd(n_1, n_2) \mid (a_1 - a_2)$, and if there is a solution, it is unique mod $\operatorname{lcm}(n_1, n_2)$. (Obviously, you should not be just citing Theorem 3.12. However it might be worthwhile to look at the proof and try to unwind the ideas in the proof to the special situation in this problem.)

(4) Let $f(x)$ be a polynomial with integer coefficients. Consider the equation $f(x) \equiv 0 \mod n$. If $f(x)$ is a linear polynomial, is it possible for $x \equiv 1, 4, 7, 11 \mod 12$ to be the solution set of the linear congruence $f(x) \equiv 0 \mod n$?

(5) (a) Compute the remainder when 4^{6303} is divided by 31.
    (b) Compute the remainder when 7^{7^7} is divided by 11.

(6) Let p be a prime, and let a be an integer relatively prime to p. Suppose that d is the smallest positive integer such that $a^d \equiv 1 \mod p$. Show that $d|(p-1)$. (This d is sometimes called the *order* of a mod p; the terminology comes from abstract algebra.)