WRITTEN HW #5

(1) (10 points) Solve the following systems of congruences (5 each):
  (a) $x \equiv 3 \bmod 4, x \equiv 5 \bmod 7, x \equiv 1 \bmod 9$.
  (b) $2x \equiv 3 \bmod 5, 3x \equiv 4 \bmod 7$.

(2) (10 points) Solve the following systems of congruences (5 each):
  (a) $x \equiv 4 \bmod 6, x \equiv 7 \bmod 15$.
  (b) $3x \equiv 4 \bmod 10, x \equiv 12 \bmod 14$.

(3) (10 points) Suppose you are given a system of linear congruences

$$x \equiv a_1 \bmod n_1, \ldots, x \equiv a_k \bmod n_k,$$

where the a_i are arbitrary integers and the n_i are positive integers. Show that there are either no solutions to this system, or all the solutions can be described by $x \equiv a \bmod \operatorname{lcm}(n_1, \ldots, n_k)$, for some integer a.

(4) (10 points) Show, using basic methods (in particular, without citing Lemma 4.8 of the text), that 1105 and 1729 are Carmichael numbers.

(5) (10 points) In this problem, we will check that 703 is a strong pseudoprime to base 3.
  (a) (5 points) Carry out the fast-exponentiation method by hand to compute 3^{351} and 3^{702} mod 703. You should show work when you calculate the binary expansion of 351 and also the results of computing successive squares of 3 mod 703.
  (b) (5 points) Based on your answers to the previous part, explain why 703 is a strong psuedoprime to base 3. Is 703 a strong psuedoprime to base 2? (You should carry out the same calculations as in the previous part, except this time you can just use your computer to calculate $2^{351}, 2^{702}$ mod 703.)