CS 70 Discrete Mathematics for CS Spring 2006 Vazirani — HW 4

Please remember to write your section and TA name on your answer sheet. Also check the newsgroup for any corrections/hints.

1. The goal of this question is to generalize the Chinese remainder theorem to the situation where the two moduli m and n do have common factors.

   (a) Suppose that a, b, n are all divisible by d, and let $a' = a/d$, $b' = b/d$ and $n' = n/d$. Show that if $a \equiv b \bmod n$ then $a' \equiv b' \bmod n'$.

   (b) Prove that the congruences $x \equiv a \bmod m$ and $x \equiv b \bmod n$ have no solution if $a \neq b \bmod gcd(m,n)$.

   (c) Now show that if $a \equiv b \bmod gcd(m,n)$ then there is a unique solution for x modulo $lcm(m,n)$. Recall that the $lcm(m,n)$ is the least common multiple of m and n: i.e. the smallest number k such that $m|k$ and $n|k$. Also $gcd(m,n)lcm(m,n) = mn$.

   (d) Now solve the following puzzle from Brahma-Sphuta-Siddhanta (Brahma's Correct System) by Brahmagupta (born 598 AD):

   An old woman goes to market and a horse steps on her basket and crashes the eggs. The rider offers to pay for the damages and asks her how many eggs she had brought. She does not remember the exact number, but when she had taken them out two at a time, there was one egg left. The same happened when she picked them out three, four, five, and six at a time, but when she took them seven at a time they came out even. What is the smallest number of eggs she could have had?

2. This time we will generalize the Chinese remainder theorem as proved in class in a different direction. Suppose that the numbers $n_1, \ldots n_k$ are pairwise relatively prime; i.e. $gcd(n_i, n_j) = 1$. Prove by induction on n that the set of congruences $x \equiv a_i \bmod n_i$ have a unique solution $x \bmod n_1 n_2 \cdots n_k$.