Math 151 Spring 2004

Project A (optional, for extra credit)

Last day to submit solutions: 18 February 2004

The proof of the Chinese Remainder Theorem given in the book (p. 29) gives an algorithm to solve a system

$$x \equiv a (\text{mod } n), \quad x \equiv b (\text{mod } m)$$

where $(n, m) = 1$.

Extend the techniques of the CRT to solve the following systems.
Note: These systems may have no solutions. Under which conditions on a, n, b, m, etc. does each system have a solution? Give an algorithm to solve each system when a solution exists. How many solutions does the system have modulo mn (mnp, $n_1 \ldots n_k$)?

1. $x \equiv a (\text{mod } n), \quad x \equiv b (\text{mod } m), \quad x \equiv c (\text{mod } p)$
   where $\gcd(n, m) = \gcd(n, p) = \gcd(m, p) = 1$.
2. Use your algorithm in part (1) to solve
   $x \equiv 1 (\text{mod } 2), \quad x \equiv 2 (\text{mod } 3), \quad x \equiv 3 (\text{mod } 5)$.
3. $x \equiv a (\text{mod } n), \quad x \equiv b (\text{mod } m)$
   where $(n, m) > 1$.
4. Use your algorithm in part (3) to solve the following systems:
   (a) $x \equiv 11 (\text{mod } 15), \quad x \equiv 6 (\text{mod } 10)$
   (b) $x \equiv 11 (\text{mod } 15), \quad x \equiv 8 (\text{mod } 10)$
5. $x \equiv a (\text{mod } n), \quad x \equiv b (\text{mod } m), \quad x \equiv c (\text{mod } p)$,
   no restrictions on n, m, and p.
6. $\begin{cases} x \equiv a_1 (\text{mod } n_1) \\ \ldots \\ x \equiv a_k (\text{mod } n_k) \end{cases}$
7. $\begin{cases} a_1 x \equiv b_1 (\text{mod } n_1) \\ \ldots \\ a_k x \equiv b_k (\text{mod } n_k) \end{cases}$
8. Do problem 20 on page 31.
9. Do problem 21 on page 31.