Project A (optional, for extra credit, up to 15 points)

Last day to submit solutions: 17 September 2008

The proof of the Chinese Remainder Theorem given in the book (p. 31) gives an algorithm to solve a system

$$x \equiv a \pmod{n}, \quad x \equiv b \pmod{m}$$

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, $n_1 \dots n_k$)?

1. $x \equiv a \pmod{n}, \quad x \equiv b \pmod{m}, \quad x \equiv c \pmod{p}$
   where $\gcd(n, m) = \gcd(n, p) = \gcd(m, p) = 1$.
2. Use your algorithm in part (1) to solve
   $x \equiv 1 \pmod{2}, \quad x \equiv 2 \pmod{3}, \quad x \equiv 3 \pmod{5}$.
3. $x \equiv a \pmod{n}, \quad x \equiv b \pmod{m}$
   where $(n, m) > 1$ (hint: see exercise 23 on page 34).
4. Use your algorithm in part (3) to solve the following systems:
   (a) $x \equiv 11 \pmod{15}, \quad x \equiv 6 \pmod{10}$
   (b) $x \equiv 11 \pmod{15}, \quad x \equiv 8 \pmod{10}$
5. $x \equiv a \pmod{n}, \quad x \equiv b \pmod{m}, \quad x \equiv c \pmod{p}$,
   no restrictions on n, m, and p.
6. $\begin{cases} x \equiv a_1 \pmod{n_1} \\ \dots \\ x \equiv a_k \pmod{n_k} \end{cases}$
7. $\begin{cases} a_1 x \equiv b_1 \pmod{n_1} \\ \dots \\ a_k x \equiv b_k \pmod{n_k} \end{cases}$
8. Do problem 20 on page 34.
9. Do problem 22 on page 34.