MATH 2610
Discrete Mathematics for Computer Science
Thursday March, 3 2005

I will collect the homework from this week Wednesday March 9, 2005.

(1) Find a solution to the following system of linear congruences.

$$x \equiv 2(\text{mod } 3)$$
$$x \equiv 2(\text{mod } 5)$$
$$x \equiv 2(\text{mod } 7)$$

Solution : First, the cheap answer. Notice that $x = 2$ works by inspection. But that's no fun. The Chinese remainder theorem says that a solution of these equations exists. The proof of the Chinese remainder theorem says that the solution will look like

$$x = 2(5)(7)(\overline{5}_3)(\overline{7}_3) + 2(3)(7)(\overline{3}_5)(\overline{7}_5) + 2(3)(5)(\overline{3}_7)(\overline{5}_7)$$

where the notation $\overline{k}_m$ means the inverse of k modulo m. Notice that the book actually writes the solution as

$$x = 2(35)(\overline{35}_3) + 2(21)(\overline{21}_5) + 2(15)(\overline{15}_7).$$

In either case we need to find some inverses. But finding the inverses of 5 and 7 modulo 3 can be done a little easier than finding the inverse of 35 modulo 3. Okay, maybe not so much easier in that case, but I'll bet it will be easier to find the inverses of 3 and 5 modulo 7 instead of the inverse of 15 modulo 7. No, actually not really. Shucks... My point is, you can do this either way since $(\overline{3}_7)(\overline{5}_7) = \overline{15}_7$. Anyhoo,

$$\begin{aligned} x &= 2(5)(7)(\overline{5}_3)(\overline{7}_3) + 2(3)(7)(\overline{3}_5)(\overline{7}_5) + 2(3)(5)(\overline{3}_7)(\overline{5}_7) \\ &= 2(5)(7)(2)(1) + 2(3)(7)(2)(3) + 2(3)(5)(5)(3) \\ &= 140 + 252 + 450 \\ &= 842 \\ &\equiv 2(\text{mod } (3)(5)(7)). \end{aligned}$$

To see that you get the same thing,

$$\begin{aligned} x &= 2(35)(\overline{35}_3) + 2(21)(\overline{21}_5) + 2(15)(\overline{15}_7) \\ &= 2(35)(2) + 2(21)(1) + 2(15)(1) \\ &= 140 + 42 + 30 \\ &= 212 \\ &\equiv 2(\text{mod } (3)(5)(7)). \end{aligned}$$

(2) Find a solution to the following system of linear congruences.

$$x \equiv 2 (\text{mod } 3)$$
$$x \equiv 3 (\text{mod } 5)$$
$$x \equiv 6 (\text{mod } 8)$$
$$x \equiv 1 (\text{mod } 11)$$

Solution : Again we will use the proof of the Chinese Remainder Theorem which asserts that since the numbers 3, 5, 8, and 11 are pairwise relatively prime, the solution will be,

$$\begin{aligned} x = {} & 2(5)(8)(11)(\overline{5}_3)(\overline{8}_3)(\overline{11}_3) + 3(3)(8)(11)(\overline{3}_5)(\overline{8}_5)(\overline{11}_5) + \\ & 6(3)(5)(11)(\overline{3}_8)(\overline{5}_8)(\overline{11}_8) + 1(3)(5)(8)(\overline{3}_{11})(\overline{5}_{11})(\overline{8}_{11}) \end{aligned}$$

$$\begin{aligned} = {} & 2(5)(8)(11)(2)(2)(2) + 3(3)(8)(11)(2)(2)(1) + \\ & 6(3)(5)(11)(3)(5)(3) + 1(3)(5)(8)(4)(9)(7) \end{aligned}$$

$$= 7040 + 3168 + 44550 + 30240$$

$$= 84998$$

$$\equiv 518 (\text{mod } (3)(5)(8)(11))$$

(3) Find a solution to the following system of linear congruences.

$$2x \equiv 2 (\text{mod } 3)$$
$$3x \equiv 2 (\text{mod } 5)$$
$$4x \equiv 2 (\text{mod } 7)$$

Solution : We actually did this in class. To use the Chinese Remainder Theorem we need to only have x's on the left side of all of the congruences. So, we will need to find the inverse of 2 modulo 3, the inverse of 3 modulo 5, and the inverse of 4 modulo 7. Mercifully, we know that this can be done since each of those pairs are relatively prime. Indeed, $\overline{2}_3 = 2$, $\overline{3}_5 = 2$, and $\overline{4}_7 = 2$. So, we can rewrite this system of congruences as

$$2 \cdot 2x \equiv 2 \cdot 2 (\text{mod } 3)$$
$$2 \cdot 3x \equiv 2 \cdot 2 (\text{mod } 5)$$
$$2 \cdot 4x \equiv 2 \cdot 2 (\text{mod } 7).$$

It will then become,

$$x \equiv 1 (\text{mod } 3)$$
$$x \equiv 4 (\text{mod } 5)$$
$$x \equiv 4 (\text{mod } 7).$$

The solution guaranteed by the Chinese Remainder Theorem is,

$$\begin{aligned} x &= 1(5)(7)(\overline{5}_3)(\overline{7}_3) + 4(3)(7)(\overline{3}_5)(\overline{7}_5) + 4(3)(5)(\overline{3}_7)(\overline{5}_7) \\ &= (1)(5)(7)(2)(1) + 4(3)(7)(2)(3) + 4(3)(5)(5)(3) \\ &= 70 + 504 + 900 \\ &= 1474 \\ &\equiv 4 (\text{mod } (3)(5)(7)). \end{aligned}$$