Chinese Remainder Theorem II

Since these problems are solved most efficiently using the notion of congruence (due to K.F. Gauss), we shall explain and recommend this method.

__Def.__ Let n be a positive integer, $n > 1$. We say that $a \equiv b\,(n)$ [a is congruent to b mod n] if n (evenly) divides $b - a$.

List of important properties

1. If $a = nk + r$ where $0 \le r < n$ then $a \equiv r\,(n)$.
2. If $0 \le r_1 < r_2 < n$, then $r_1 \not\equiv r_2\,(n)$.
3. $a \equiv b(n) \Rightarrow b \equiv a(n)$
4. $a \equiv b(n)$ & $b \equiv c(n) \Rightarrow a \equiv c(n)$.
5. $a \equiv a'(n)$ & $b \equiv b'(n) \Longrightarrow$ $a + b \equiv a' + b'(n)$ & $ab \equiv a'b'(n)$.

(6) If a and n are relatively prime, then there is an integer b such that $ba \equiv 1\ (n)$.

This last property is particularly important for the Chinese Remainder Theorem. It means that we can find integers b and k such that $ba = 1 + nk$. For small numbers one can often see this by quick trial and error methods. For example, if $n = 20$ and $a = 7$, then we know that $3 \cdot 7 = 21$ leaves a remainder of 1 upon division by 20. In all cases one can use the Euclidean algorithm to find b and c such that $1 = ba + cn$, and thus there is a systematic constructive process to find b if educated guessing fails.

Application to CRT problems

Solve
$$x \equiv 13\ (27)$$
$$x \equiv 7\ (16).$$

Method

Step 1. Rewrite $x = 27p + 13$ and insert into the second congruence. We get

$$x = 27p + 13 \equiv 7\ (16)$$
$$27p \equiv 7 - 13 = -6\ (16)$$

But $-6 \equiv 10\ (16)$, so we have

$$27p \equiv 10\ (16)$$

Since $27 \equiv 11\ (16)$, this reduces to

$$11p \equiv 10\ (16)$$

Step 2 Find b such that $11b \equiv 1\ (16)$

Trial + error leads to $11 \cdot 3 = 33 = 1 + 2 \cdot 16$.

What if we didn't see that? Here is how to write $1 = 11b + 16c$

$$16 = 1 \cdot \underset{q_1}{11} + \underset{r_1}{5}$$

$$\underset{q}{11} = 2 \cdot \underset{r_1}{5} + \underline{\underline{1}}$$

Now work backwards (see next page).

$11 = 2 \cdot 5 + 1 =$

$2(16 \cdot 1 - 11 \cdot 1) + 1 =$

$2 \cdot 16 - 2 \cdot 11 + 1$, so

$1 = 1 \cdot 11 + 2 \cdot 11 - 2 \cdot 16 = 3 \cdot 11 - 2 \cdot 16$

what we had guessed!

<u>Step 3</u> Multiply the result of Step 1 by b.

$b = 3$ so $11p \equiv 10\ (16) \rightsquigarrow$

$3 \cdot 11 \cdot p \equiv 30\ (16)$ and hence

$1 \cdot p \equiv 30\ (16)$, so that

$p \equiv 14\ (16)$ and we may write

$p = 16q + 14$. Substitute this into

$x = 27p + 13$, obtaining

$$x = \underbrace{27 \cdot 16}_{432}\, q + \underbrace{27 \cdot 14 + 13}_{391}$$

do the arithmetic (Calculator OK!)

or $x \equiv 391\ (432)$.

<u>CHECK</u> $391 \equiv 13\ (27)$

$391 \equiv 7\ (16)$.

Example with smaller numbers

$$x \equiv 7 \ (8)$$
$$x \equiv 3 \ (9)$$

Step 1 $x = 8p + 7 \equiv 3 \ (9)$,

so $8p \equiv 3 - 7 = -4 \equiv 5 \ (9)$.

Step 2 Find b so $8b \equiv 1 \ (9)$.

Check $b = 8$ works. Also $b \equiv -1$ does,

since $8b \equiv -b \ (9)$.

Step 3 Multiply result in Step 1 by $b \, [= -1]$

and solve: $8p \equiv 5 \ (9) \Rightarrow$

$$p \equiv (-1) \cdot 8 \cdot p \equiv (-1) 5 \equiv 4 \ (9).$$

So $p = 9q + 4$ and

$$x = 8(9q + 4) + 7 =$$
$$72q + 32 + 7 = 72q + 39.$$

$$x \equiv 39 \ (72)$$

CHECK $39 \equiv 7 \ (8)$

$39 \equiv 3 \ (9)$.

Suppose we added $x \equiv 4\,(5)$ to the problem. We take the solution to the first two congruences and pair it with the third congruence. So we have

$$x \equiv 39\ (72)$$

$$x = 72p + 39 \equiv 4\,(5)$$

Simplify: $2p + 4 \equiv 4\,(5)$. $2p \equiv 0\,(5)$

Now find b so $2b \equiv 1\,(5)$. We can take $b = 3$, so we get $p \equiv 3 \cdot 2p \equiv 3 \cdot 0 = 0\,(5)$. So $p = 5q$. Thus our final answer is

$$\cancel{5(72q)+t} \quad 72 \cdot (5q) + 39 = 360q + 39$$

or $x \equiv 39\,(360)$.

CHECK: $x \equiv 39\,(72)$
$x \equiv 4\,(5)$.