SRQR: Chinese Remainder Theorem (April 8, 2021)

> I'm confused about the proof for theorem 4.7. The author proves that $x_0 + (n/d)t$ is not congruent to another $x_0 + (n/d)t$, but then goes on to prove that $x_0 + (n/d)t$ is actually congruent. . . . How does that work?

What's going on is that Burton first proves that all integer solutions are of the form $x = x_0 + (n/d)t$ for some t. Then he shows that solutions of the form $x_0 + (n/d)t$ where t varies between $t = 0$ and $t = d - 1$ are all incongruent.

In the last paragraph, he then proves that, any solution $x = x_0 + (n/d)t$ (where t is *not necessarily* between 0 and $d - 1$) is congruent to one of the solutions where t *is* between 0 and $d - 1$.

I encourage you to re-read the proof with this in mind!

> I'm still confused how finding an "incongruent solution" can be a solution at all? I think the vocabulary is confusing me a little.

This is sort of related to the previous question. First remark: the book says things like "find all incongruent solutions," rather than "find an incongruent solution." When it says "find all incongruent solutions," it's talking about finding *solutions which are incongruent amongst each other*.

For example, let's say I want to solve the congruence

$$2x \equiv 0 \pmod{6}. \tag{0.1}$$

Then $x \equiv 0 \pmod{6}$ is one solution, and $x \equiv 3 \pmod{6}$ is another solution. These two solutions are incongruent between each other (ie, 0 is not congruent to 3 mod 6), so $x \equiv 0 \pmod{6}$ and $x \equiv 3 \pmod{6}$ are two incongruent solutions of equation (0.1).

> In the proof of theorem 4.7, it says, "then any other solution has the form $x = x_0 + (n/d)ty = y_0 + (a/d)t$." However, if we consider a linear congruence as being equivalent to a Diophantine equation, wouldn't it be $y = y_0 - (a/d)t$ instead of $y = y_0 + (a/d)t$?

Yes, if you apply the formula from the theorem in section 2.5 verbatim you will end up with a minus sign. If you like, you can re-write the proof of the Chinese Remainder Theorem using the minus sign. It would probably have been better if Burton had used the minus sign.

The sign doesn't really matter, though. The point is that an integer that can be written in the form $y = y_0 - (a/d)t$ for some integer t if and only if it can *also* be written in the form $y = y_0 + (a/d)t'$ for some integer t' — namely, I just take $t' = -t$.

In example 4.10, I was wondering why it can be written as $x \equiv 0 \pmod 3$, $x \equiv 1 \pmod 4$, $17x \equiv 9 \pmod{23}$? Why does the 17 on the left side disappear?"

The 17 disappears in the first two equations, so let's look at each of those and try to understand why.

The first equation is $17x \equiv 9 \pmod 3$. Notice that $17 equiv 2 \pmod 3$ and $9 \equiv 0 \pmod 3$, so the first equation is equivalent to $2x \equiv 0 \pmod 3$. But notice that $\gcd(2, 3) = 1$, so we can divide both sides of this congruence by 2! More precisely, we can calculate an inverse of 2 mod 3 (which is again 2), and then multiply both sides of the congruence by that inverse to get $4x \equiv 0 \pmod 3$. Since $4 \equiv 1 \pmod 3$, this is equivalent to $x \equiv 0 \pmod 3$.

The second equation is a bit easier $17x \equiv 9 \pmod 4$. This one is easier: notice that $17 \equiv 1 \pmod 4$ and $9 \equiv 1 \pmod 4$, so this is equivalent to $x \equiv 1 \pmod 4$.

Can simultaneous congruence problems with any number of terms be solved? Or is it possible to reach a point where no number could satisfy the constraints?

The Chinese Remainder Theorem effectively guarantees that if you have a system of simultaneous congruences where

(1) each congruence has a solution, and
(2) the moduli of the congruences are pairwise coprime,

then the system has a solution. There's no limit here to the number of congruences as long as both of the above conditions are satisfied.

As soon as you start violating any one of those conditions, though, you can end up with systems that don't have a solution. For example, it's probably clear that if you violate (1), the system won't have a solution — if one of your congruenes doesn't have a solution, surely the system won't have a solution either!

More interesting is if you violate (2). For example, consider the following system:

$$\begin{aligned} 2x &\equiv 1 \pmod 3 \\ x &\equiv 1 \pmod 3 \end{aligned}$$

The first congruence has a solution (namely, $x \equiv 2 \pmod 3$). The second also has a solution (namely, $x \equiv 1 \pmod 3$). But the system has no simultaneous solutions (because a number cannot be simultaneously congruent to 1 mod 3 and 2 mod 3). The issue here is that both my congruences have the same modulus (namely, 3). In particular, I don't have "pairwise coprime" moduli.