CHINESE REMAINDER THEOREM

E. L. Lady

The Chinese Remainder Theorem involves a situation like the following: we are asked to find an integer x which gives a remainder of 4 when divided by 5, a remainder of 7 when divided by 8, and a remainder of 3 when divided by 9.

In other words, we want x to satisfy the following congruences.

$$x \equiv 4 \pmod 5$$

$$x \equiv 7 \pmod 8$$

$$x \equiv 3 \pmod 9.$$

There can be any number of moduluses (here 5, 8, and 9), but no two of them should have any factor in common. Otherwise the existence of a solution cannot be guaranteed.

The method for solving this set of three simultaneous congruences is to reduce it to three separate problems whose answers may be added together to get a solution to the original problem.

To understand this, think about why

$$144 + 135 + 120$$

will be a solution to the simultaneous congruences.

To start with, an easy calculation shows that 144 gives a reminder of 4 when divided by 5. On the other hand, 135 and 120 are multiples of 5, so adding them doesn't change this reminder. Thus

$$144 + 135 + 120 \equiv 144 \equiv 4 \pmod 5.$$

Now consider the second term in the sum. Long division shows that 135 gives a reminder of 7 when divided by 8. On the other hand, 144 and 120 are multiples of 8, so adding them on doesn't change this reminder. I.e.

$$144 + 135 + 120 \equiv 135 \equiv 7 \pmod 8.$$

Finally, notice that the last term in the sum is 120, and 120 gives a reminder of 3 when divided by 9. But 144 and 135 are multiples of 9, so adding them in doesn't affect this remainder. Thus

$$144 + 135 + 120 \equiv 120 \equiv 3 \pmod 9.$$

Therefore 399, which is the sum of 144, 135, and 120, satisfies all three of the congruences. (Skeptics can check this by long division.)

Other solutions can be found by adding or subtracting multiples of 360. This will not effect any of the three congruences since $360 = 5 \times 8 \times 9$. For instance, $399 - 360 = 39$ is a also a solution.

Having now seen why 399 is a valid solution, we can also partly see the process by which it was created. We found it as the sum of three numbers.

> The first number, 144, gives the right remainder when divided by 5 and is also a multiple of 8 and of 9.
>
> The second number, 135, is a multiple of 5 and of 9 and gives the correct remainder when divided by 8.
>
> The third number, 120, is congruent to 3 module 9 and is a multiple of both 5 and 8.

So where did we get these three numbers?

To start with, taking the last two of the three moduli 5, 8, and 9, compute $8 \times 9 = 72$. We look for a multiple of 72 which satisfies the first congruence, i. e. is congruent to 4 modulo 5. In fact, twice 72 is 144, and $144 \equiv 4 \pmod 5$. So 144 is the first summand we want.

Next notice that 5×9 is 45. We look for a multiple of 45 which satisfies the second congruence, i. e. is congruent to 7 modulo 8. We find (by trial and error) that

$$1 \times 45 = 45 \equiv 5 \pmod 8$$
$$2 \times 45 = 90 \equiv 2 \pmod 8$$
$$3 \times 45 = 135 \equiv 7 \pmod 8.$$

Thus 135 is the second summand required.

Finally, we look for a multiple of 40 which is congruent to 3 module 9. We can check that

$$40 \equiv 4 \pmod 9$$
$$80 \equiv 8 \pmod 8$$
$$120 \equiv 3 \pmod 9.$$

Now the required answer is the sum $144 + 135 + 120$, namely 399.

Consider another example. Look for a number x satisfying the following congruences.

$$x \equiv 1 \pmod 2$$
$$x \equiv 2 \pmod 3$$
$$x \equiv 3 \pmod 5$$
$$x \equiv 1 \pmod 7.$$

We start by noticing that $3 \times 5 \times 7 = 105$. So we look for a multiple of 105 which is congruent to 1 modulo 2 (i. e. an odd multiple of 105). We can choose 105 itself, since it is odd.

Now consider the congruence modulo 3. The other three moduli are 2, 5, and 7, and $2 \times 5 \times 7 = 70$. So we look for a multiple of 70 which is congruent to 2 modulo 3. By exploiting the advantage of congruence arithmetic, we can do this fairly efficiently, once we see by long division that $70 \equiv 1 \pmod 3$. This immediately yield

$$2 \times 70 \equiv 2 \times 1 \equiv 2 \pmod 3,$$

so that for the second number we can choose $140 = 2 \times 70$.

Now consider the congruence modulo 5. Since the other three moduli are 2, 3, and 7, and $2 \times 3 \times 7 = 42$, we look for a multiple of 42 which is congruent to 3 modulo 5. Long division shows that $42 \equiv 2 \pmod 5$. Thus

$$2 \times 42 \equiv 2 \times 2 \equiv 4 \pmod 5$$
$$3 \times 42 \equiv 3 \times 2 = 6 \equiv 1 \pmod 5$$
$$4 \times 42 \equiv 4 \times 2 = 8 \equiv 3 \pmod 5$$

So for the third number we use $168 = 4 \times 42$.

Finally, to make things work modulo 7, we consider multiples of $2 \times 3 \times 5 = 30$. We want a multiple of 30 which is congruent to 1 modulo 7. Since $30 \equiv 2 \pmod 7$, we get

$$2 \times 30 \equiv 2 \times 2 = 4 \pmod 7$$
$$3 \times 30 \equiv 3 \times 2 = 6 \pmod 7$$
$$4 \times 30 \equiv 4 \times 2 = 8 \equiv 1 \pmod 7$$

Thus for the third number we use $120 = 4 \times 30$.

Adding the four numbers we've found together, we get a solution of

$$105 + 140 + 168 + 120 = 533.$$

Skeptics can check by long division that

$$533 \equiv 1 \pmod 2$$
$$533 \equiv 2 \pmod 3$$
$$533 \equiv 3 \pmod 5$$
$$533 \equiv 1 \pmod 7.$$

Since $2 \times 3 \times 5 \times 7 = 210$, adding or subtracting multiples of 210 will not affect this result. Thus $113 = 533 - 2 \cdot 210$ is also a solution.

One solution to a system of congruences

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$
$$\dots$$
$$x \equiv a_n \pmod{m_n}$$

with the m_i mutually prime to each other can be found by adding together n numbers. The i^{th} of these numbers should be congruent to a_i modulo m_i and it should be a multiple of all the other moduli m_k.

In the examples given above, finding these n different numbers seemed to involve a certain amount of trial and error, and one might wonder whether this would always be successful.

For instance, in one of the above calculuations we wanted a multiple of 42 which is congruent to 3 modulo 5. Although we did actually find such a number, it seemed that this might have actually been a matter of luck. In fact, though, the existence of such a number was guaranteed by the fact that 42 and 5 are relatively prime. Any number theory student should be aware of the following fact.

If a and m are relatively prime, then the congruence $az \equiv b \pmod m$ is always solvable for z, no matter what b is.

To see why this has to be true, consider, for instance, the first 5 multiples of 42 and reduce modulo 5. The arithmetic can be simplified by using the fact that $42 \equiv 2 \pmod 5$.

$$0 \times 42 \equiv 0 \pmod 5$$

$$1 \times 42 \equiv 2 \pmod 5$$

$$2 \times 42 \equiv 2 \times 2 = 4 \pmod 5$$

$$3 \times 42 \equiv 3 \times 2 \equiv 1 \pmod 5$$

$$4 \times 42 \equiv 4 \times 2 \equiv 3 \pmod 5$$

Notice that one the right hand side, every number from 0 to 4 occurs, showing that a congruence $42z \equiv b \pmod 5$ can always be solved, no matter what b is. (As a practical matter, we may as well assume that b is between 0 and 4.)

This is not a coincidence, but is a consequence of the fact that 42 has no factor in common with 5. If any of the five numbers from 0 to 4 had been missing on the right-hand side of the five congruences listed, then at least one right-hand side would have to be repeated. But, given the fact that 42 has no factors in common with 5, this would not be possible. For instance, if we had, by error, computed $4 \times 42 \equiv 2 \pmod 5$, then since also $1 \times 42 \equiv 2 \pmod 5$, it would follow that $3 \times 42 = 4 \times 42 - 1 \times 42$ would be a multiple of 5. But this is not possible, since neither 3 nor 42 has any prime factors in common with 5 (which is a prime number, of course).

To use a less obvious example, we can see that there must be some multiple of 24 which is congruent to 7 modulo 35, even though it would take some work to actually find this multiple. This is because if we were to list the first 35 multiples of 24 (0, 24, 48, 72, 96, ...) and reduce modulo 35 (yielding 0, 24, 13, 2, 26, ...), there could not be any repetitions. This is because if $24x \equiv 24y \pmod{35}$ where x and y were different numbers between 0 and 34, then $24(x - y)$ would be a multiple of 35. But 24 is neither a multiple of 5 nor of 7, so this would force $x - y$ to be a multiple of 35. But since x and y were different numbers between 0 and 34, there's no way this could be true.

Consequently no number between 0 and 34 could be omitted, showing that every possible congruence $24z \equiv b \pmod{35}$ is solvable.