Modular Math and the Chinese Remainder Theorem

by Richard Born
Associate Professor Emeritus
Northern Illinois University
rborn2@niu.edu

Notation

If *N* gives a remainder of *a* when divided by *r*, then we would write this fact mathematically by the equation $N \equiv a \pmod{r}$. We could read this as "N is congruent to a, mod r". Here are some examples related to the video that accompanies this lesson. In the video, Evo discovered that the number the student was thinking of is 27:

- $27 \equiv 1 \pmod{2}$ because 27 divided by 2 gives a remainder of 1.
- $27 \equiv 0 \pmod{3}$ because 27 divided by 3 gives a remainder of 0.
- $27 \equiv 2 \pmod{5}$ because 27 divided by 5 gives remainder a of 2.

In essence, Evo had to solve the following system of modular equations for *x*:

$x \equiv 1 \pmod{2}$
$x \equiv 0 \pmod{3}$
$x \equiv 2 \pmod{5}$

The Chinese remainder theorem provides us with a roadmap for solving a system of modular equations such as the set that Evo had to solve. According the Wikipedia, the Chinese remainder theorem can be stated as follows:

> In number theory, the **Chinese remainder theorem** states that if one knows the remainders of the Euclidean division of an integer *n* by several integers, then one can determine uniquely the **remainder** of the division of *n* by the product of these integers, under the condition that the divisors are pairwise coprime.

That's kind of a mouthful! Our goal is to demystify it so that we can ***use*** the theorem to solve Evo's problem or any problem involving a similar set of modular equations. We are definitely not going to prove the theorem, as it is beyond our current scope of interest!

Step 1 – Make sure that the "divisors are pairwise coprime".

Doing this is equivalent to showing that the greatest common divisor (GCD) of every pair of the divisors is 1. This is not an issue for Evo's problem, as all of the divisors are prime numbers: GCD(2,3) = 1, GCD(3,5) = 1, and the GCD(2,5) = 1.

Step 2 – Determine the Modulus for the Result

The statement of the Chinese remainder theorem says that "one can determine uniquely the **remainder** of the division of *n by the product of these integers*". Therefore, the modulus for the result is the product of the divisors. For Evo's problem, this product is 2•3•5 = 30. This is why the student had to think of a number between 0 and 29. With a modulus of 30, the remainder will be a unique number between 0 and 29. Therefore we can say that:

$$x \equiv Qa + Rb + Sc \pmod{30},$$

where *a*, *b*, and *c* are the remainders from the divisors 2, 3, and 5, respectively.

Step 3 – Determine the Values of Q, R, and S

To find *Q*, form the product 3•5 = 15 of the divisors *except 2* and select the *lowest multiple* of this product that leaves a remainder of 1 on division by 2. Since 15 gives a remainder of 1 when divided by 2, then the lowest multiple of 15 is 15. Therefore, *Q* = 15.

To find *R*, form the product 2•5 = 10 of the divisors *except 3* and select the *lowest multiple* of this product that leaves a remainder of 1 on division by 3. Since 10 gives a remainder of 1 when divided by 3, then the lowest multiple of 10 is 10. Therefore, *R* = 10.

To find *S*, form the product 2•3 = 6 of the divisors *except 5* and select the *lowest multiple* of this product that leaves a remainder of 1 on division by 5. Since 6 gives a remainder of 1 when divided by 5, then the lowest multiple of 6 is 6. Therefore, S = 6.

We conclude that

$$x \equiv 15a + 10b + 6c \pmod{30}$$

where we note again that *a*, *b*, and *c* are the remainders when *x* is divided by 2, 3, and 5, respectively.

Example from Evo's Problem

Suppose the student is thinking of the number *x*. The student specifies that the remainders when divided by 2, 3, and 5 are 1, 2, and 3, respectively. Then $x \equiv 15\bullet1 + 10\bullet2 + 6\bullet3 = 53 \pmod{30} = 23$. Therefore, the student was thinking of the number 23.

YouTube Videos

There are several videos on YouTube that deal with the Chinese remainder theorem, some of which provide more detailed explanations on how to determine the values of Q, R, and S. Just search the web for "Chinese remainder theorem videos".

Exercises

1. In the example Evo problem on the previous page, we discussed how Evo would guess the number 23. Try this out on Evo. Does he get the correct result?

2. Consider the following set of simultaneous modular equations. Do they meet the requirements of the Chinese remainder theorem? Why or why not?

   $x \equiv 2 \pmod 3$
   $x \equiv 3 \pmod 5$
   $x \equiv 5 \pmod 6$

3. Suppose that a set of three simultaneous modular equations involves finding the remainders when a number *x* is divided by by 7, 11, and 13. What is the range for x?

4. In exercise 3, could we design an OzoBlockly program with the stated divisors that makes use of the Chinese remainder theorem? Why or why not?

5. Solve the following set of simultaneous modular equations for *x* using the three steps discussed earlier in this document. Show your work, so it is clear how you solved this modular system of equations. Can an OzoBlockly program be designed for this system using the Chinese remainder theorem? Why or why not?

   $x \equiv 1 \pmod 3$
   $x \equiv 3 \pmod 5$
   $x \equiv 6 \pmod 7$

6. Solve the following set of *four* simultaneous modular equations for *x* using the three steps discussed earlier in this document. Show your work, so it is clear how you solved this modular system of equations. Check your final answer for x and make sure it satisfies all four congruences. If it doesn't, go back and find where you errored.

   $x \equiv 1 \pmod 2$
   $x \equiv 2 \pmod 3$
   $x \equiv 4 \pmod 5$
   $x \equiv 6 \pmod 7$