Sun Tzu's Remainder Theorem

Background

Although still popularly called the Chinese Remainder Theorem, we'll be calling this by a better name as above. The mathematician who came up with the theorem was clearly named Sun Tzu but this is alternatively listed as Sunzi depending on the dialect of Chinese you choose to research within. Be careful with your research as well, as there is a famous military strategist with the same name!

This theorem is concerned with solving not just a single linear congruence but a whole system of them at once. Similar to solving a system of linear equations but without the graphing approach. *smile*

Solving Linear Congruences

Recall from our textbook note that a linear congruence is $ax \equiv b \pmod{m}$ where $a, b, m \in \mathbb{Z}$ and $m > 1$. We are looking for an integer value for the variable x to make the congruence valid. Due to the nature of congruence there will typically be an infinite number of solutions if there is one. They will all be congruent to one another mod m. That is, if $m = 5$ and we find that $x = 3$ is solves the linear congruence we are interested in, x could also be any other value that is congruent to 3 mod 5 such as 8 or -2 or...

To solve such a linear congruence, we can take two approaches at this stage of our math careers. One is to guess and check. Under a particular modulus there will only be so many possibilities, after all. But if $m = 3095$, then it could take a while...

The second method is to use a modular inverse as discussed in the textbook. To use this approach, I remind you, you need to have the following condition is met: a and m must be relatively prime (i.e. $\gcd(a, m) = 1$). Also note that the inverse will be one of an infinite sequence of congruent values like the solution we find. We typically prefer the one between 0 and $m-1$ to others for the final solution statement.

Example 1: Solving a Linear Congruence by Modular Inverse

$3x \equiv 4 \pmod{5}$ can be solved because 3 and 5 are relatively prime to one another (their gcd is 1). We can find the multiplicative inverse, then, of 3 (mod 5) and multiply both sides by this value. Following the extended Euclid's

algorithm we work forward through the sequence of modulo operations:

$$5 = 3 \cdot 1 + 2$$
$$3 = 2 \cdot 1 + 1$$
$$2 = 1 \cdot 2 + 0$$

And we see our gcd is 1 and we can put together the backwards equations which are:

$$1 = 3 - 2 \cdot 1$$
$$2 = 5 - 3 \cdot 1$$

Substituting, for 2 into the first equation, then, we find:

$$\begin{aligned} 1 &= 3 - (5 - 3 \cdot 1) \cdot 1 \\ &= 2 \cdot 3 - 1 \cdot 5 \end{aligned}$$

And thus the inverse of 3 under a mod of 5 is 2. Multiplying both sides of our congruence by 2 we get:

$$\begin{aligned} 2 \cdot 3x &\equiv 2 \cdot 4 \pmod 5 \\ x &\equiv 3 \pmod 5 \end{aligned}$$

So x is 3 or anything congruent to it.

Again, this example might seem simple enough to guess and check, but the only real use of that technique is when the coefficient and modulus are not relatively prime.

Exercises

1. Find the modular inverse of 3 under a modulus of 7. *
2. Find the modular inverse of 10 under a modulus of 13.
3. Find the modular inverse of 4 under a modulus of 6. *
4. Find the modular inverse of 9 under a modulus of 21.

5. Find the modular inverse of 23 under a modulus of 5. $*$

6. Find the modular inverse of 39 under a modulus of 8.

Theorem

So, again, the problem at hand now is to solve more than a single linear congruence simultaneously. We might, for instance, want to solve this system:

$$\begin{aligned} x &\equiv 2 \pmod 3 \\ x &\equiv 3 \pmod 5 \\ x &\equiv 2 \pmod 7 \end{aligned}$$

Here the value chosen for x must satisfy all three conditions set forth by the linear congruences at the same time! Such problems were popular in China at the time of Sun Tzu but were given more lyrically:

> There are certain things whose number is unknown.
> Repeatedly divided by 3, the remainder is 2;
> by 5 the remainder is 3;
> and by 7 the remainder is 2.
> What will be the number?[1]

Sun Tzu's approach can be couched in modern mathematical terms like so:

Theorem 1: Sun Tzu's Remainder Theorem

Let $a_1, a_2, \ldots, a_n, m_1, m_2, \ldots, m_n, x \in \mathbb{Z}$ where all the m_j are pairwise relatively prime and are all greater than 1. Then the system of linear congruences:

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_n \pmod{m_n} \end{aligned}$$

can be solved in the following manner for a unique solution $x \pmod m$ where

[1] Phrasing borrowed from Eric Gossett in Discrete Mathematics with Proof ©2009.

$m = \prod_{j=1}^{n} m_j$ by way of the equation:

$$x = \left(\sum_{j=1}^{n} a_j M_j \tilde{M}_j \right) \mod m$$

Here $M_j = \frac{m}{m_j}$ and $\tilde{M}_j$ is the modular inverse of $M_j \pmod{m_j}$.

So how does this help us? How would we use it to solve the earlier system, for example? Let's see!

Example 2: Sun Tzu System Solution

As a reminder, the system in question was:

$$\begin{aligned} x &\equiv 2 \pmod 3 \\ x &\equiv 3 \pmod 5 \\ x &\equiv 2 \pmod 7 \end{aligned}$$

So we can fill ourselves out a little table to help with the computation. Firstly, $n = 3$ since there are three congruences. Also note that $m = 3 \cdot 5 \cdot 7 = 105$. Then:

$\mathbf{a_j}$	$\mathbf{m_j}$	$\mathbf{M_j}$	$\tilde{\boldsymbol{M}}_{\boldsymbol{j}}$
2	3	35	2
3	5	21	1
2	7	15	1

At least the inverses worked out nicely! (I'll let you practice finding them. Just remember that 1 is always its own inverse under any modulus!)

So now we have:

$$\begin{aligned} x &= \left(\sum_{j=1}^{3} a_j M_j \tilde{M}_j\right) \mod 105 \\ &= (2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1) \mod 105 \\ &= (140 + 63 + 30) \mod 105 \\ &= (35 + 93) \mod 105 && \text{apply modulo early} \\ &= 128 \mod 105 \\ &= 23 \end{aligned}$$

Checking this result, we find that $23 \mod 3 = 2$, $23 \mod 5 = 3$, and $23 \mod 7 = 2$ so it works!

Coefficients That Aren't 1

What happens if the coefficients of the x variable aren't all 1 as demanded implicitly by the theorem? We want to transform the system in such a way that the new form has the same solutions as the original. To do this pre-transformation we will be required to multiply each congruence through by the modular inverse of the coefficient as if we were solving it alone before applying the theorem.

Example 3: Non-1 Coefficients

Let's say we had the system:

$$\begin{aligned} 2x &\equiv 1 \pmod 3 \\ 3x &\equiv 4 \pmod 5 \\ 5x &\equiv 3 \pmod 7 \end{aligned}$$

Here we have coefficients of 2, 3, and 5. We need to remove each by multiplying by the appropriate modular inverse for each congruence. Since 2's inverse under mod 3 is itself, we'll multiply both sides by 2 to get $x \equiv 2 \pmod 3$. Next, we see that 3's inverse under mod 5 is also 2. Multiplying both sides of the congruence by this gives $x \equiv 3 \pmod 5$. (Note how $2 \cdot 4 = 8 = 3 \pmod 5$.) And, finally, we find that the inverse of 5 under mod 7 is 3. So that makes the last congruence $x \equiv 4 \pmod 7$. Thus our new system of congruences — that

should have the same solutions as the first — is:

$$\begin{aligned} x &\equiv 2 \pmod 3 \\ x &\equiv 3 \pmod 5 \\ x &\equiv 2 \pmod 7 \end{aligned}$$

But that was our initial system so we've already solved that. The answer was $x = 23$. Does that work in the newer system as well?

$$\begin{aligned} 2 \cdot 23 = 46 &= 1 \pmod 3 \\ 3 \cdot 23 = 69 &= 4 \pmod 5 \\ 5 \cdot 23 = 115 &= 3 \pmod 7 \end{aligned}$$

Yea! It works!

Exercises

7. Solve the system: $*$

$$\begin{aligned} x &\equiv 4 \pmod 5 \\ x &\equiv 3 \pmod 7 \\ x &\equiv 8 \pmod{13} \end{aligned}$$

8. Solve the system:

$$\begin{aligned} x &\equiv 2 \pmod 3 \\ x &\equiv 3 \pmod 5 \\ x &\equiv 5 \pmod 7 \\ x &\equiv 2 \pmod{11} \end{aligned}$$

9. Solve the system: $*$

$$\begin{aligned} 2x &\equiv 4 \pmod 7 \\ 7x &\equiv 9 \pmod{11} \\ 5x &\equiv 2 \pmod{13} \end{aligned}$$

10. Solve the system:

$$\begin{aligned} 4x &\equiv 3 \pmod 5 \\ 6x &\equiv 2 \pmod 7 \\ 8x &\equiv 3 \pmod{11} \end{aligned}$$

Solutions to Starred Exercises

1. Find the modular inverse of 3 under a modulus of 7.
   We start with Euclid's algorithm for gcd:

$$\begin{aligned} 7 &= 3 \cdot 2 + 1 \\ 3 &= 2 \cdot 1 + 1 \\ 2 &= 1 \cdot 2 + 0 \end{aligned}$$

   Since 1 is the gcd, we can proceed. Then we get our backwards equations by solving for the remainders:

$$\begin{aligned} 1 &= 3 - 2 \cdot 1 \\ 1 &= 7 - 3 \cdot 2 \end{aligned}$$

   Confusingly, we substitute for 1 from the second equation into the 1 on the right side of the first equation! This gives:

$$\begin{aligned} 1 &= 3 - 2 \cdot (7 - 3 \cdot 2) \\ &= -2 \cdot 7 + 5 \cdot 3 \end{aligned}$$

   Thus the inverse of 3 under a modulus of 7 is 5. Checking it, we find that $3 \cdot 5 = 15 = 1 \pmod 7$.

3. Find the modular inverse of 4 under a modulus of 6.
   Here, we find that $\gcd(4, 6) = 2 \neq 1$ and so there is no modular inverse of 4 under a modulus of 6. (I happened to realize this right away, but Euclid's algorithm would have told us it was so, as well:

$$\begin{aligned} 6 &= 4 \cdot 1 + 2 \\ 4 &= 2 \cdot 2 + 0 \end{aligned}$$

   Thus 2 is the gcd of 4 and 6 here as well.)

5. Find the modular inverse of 23 under a modulus of 5.
   This can be done in one of two ways. We can tackle it with 23 and 5 directly or we can find a simpler congruent value for 23 under the modulus of 5 and work with that. Since the congruent value will be the same as 23 under a modulus of 5, it will have the same inverse as well.
   Trying it the first way gives:

$$\begin{aligned} 23 &= 5 \cdot 4 + 3 \\ 5 &= 3 \cdot 1 + 2 \\ 3 &= 2 \cdot 1 + 1 \\ 2 &= 1 \cdot 2 + 0 \end{aligned}$$

   Since 1 is our gcd, we can proceed. Our backwards equations come from solving fot the remainders and are:

$$\begin{aligned} 1 &= 3 - 2 \cdot 1 \\ 2 &= 5 - 3 \cdot 1 \\ 3 &= 23 - 5 \cdot 4 \end{aligned}$$

   We start the next phase by substituting for 2 in the first equation from the second equation:

$$\begin{aligned} 1 &= 3 - (5 - 3 \cdot 1) \cdot 1 \\ &= -1 \cdot 5 + 2 \cdot 3 && \text{now sub for 3 from third equation} \\ &= -1 \cdot 5 + 2 \cdot (23 - 5 \cdot 4) \\ &= 2 \cdot 23 + (-9) \cdot 5 \end{aligned}$$

   Thus the inverse of 23 under mod 5 is 2. Checking this result, we find that $23 \cdot 2 = 46 = 1 \pmod 5$.
   What of the other way? It turns out quite similar. We transform 23 into 3 via the modulo circle and the proceed with Euclid's algorithm between 5 and 3. But isn't this what the first line of the earlier Euclid's calculation did? It found the modulo result of 23 under mod 5 to be 3 via the division algorithm and then proceeded with finding the rest of Euclid's algorithm on 5 and 3! Some people just prefer to work with the 'mod circle' instead of the divisionn algorithm. But they end up the same place, so...

7. Solve the system:

$$\begin{aligned} x &\equiv 4 \pmod 5 \\ x &\equiv 3 \pmod 7 \\ x &\equiv 8 \pmod{13} \end{aligned}$$

We'll begin by calculating $m = 455$ and filling out our handy-dandy table:

$\mathbf{a_j}$	$\mathbf{m_j}$	$\mathbf{M_j}$	$\tilde{\boldsymbol{M}}_{\boldsymbol{j}}$
4	5	91	1
3	7	65	4
8	13	35	3

That last inverse was a doozy! (Well, not by the extended method!) And now we can perform our calculation:

$$\begin{aligned} x &= \left(\sum_{j=1}^{3} a_j M_j \tilde{M}_j\right) \mod 455 \\ &= (4 \cdot 91 \cdot 1 + 3 \cdot 65 \cdot 4 + 8 \cdot 35 \cdot 3) \mod 455 \\ &= (364 + 780 + 840) \mod 455 \\ &= (364 + 325 + 385) \mod 455 && \text{modular addition rule} \\ &= (689 + 385) \mod 455 \\ &= (234 + 385) \mod 455 && \text{modular addition rule} \\ &= 619 \mod 455 \\ &= 164 && \text{modular addition rule} \end{aligned}$$

Checking, we find that $164 \mod 5 = 4$, $164 \mod 7 = 3$, and $164 \mod 13 = 8$. Yippee!

9. Solve the system:

$$\begin{aligned} 2x &\equiv 4 \pmod 7 \\ 7x &\equiv 9 \pmod{11} \\ 5x &\equiv 2 \pmod{13} \end{aligned}$$

First we remove the coefficients of x with some modular inverse magic. 2's inverse for modulus 7 is 4. 7's inverse for modulus 11 is 3. And 5's inverse for modulus 13 is 8. Multiplying through by these, we arrive at a system with a congruent solution:

$$\begin{aligned} x &\equiv 2 \pmod 7 \\ x &\equiv 6 \pmod{11} \\ x &\equiv 3 \pmod{13} \end{aligned}$$

Next we calculate $m = 1001$. Then we fill out our table:

$\mathbf{a_j}$	$\mathbf{m_j}$	$\mathbf{M_j}$	$\tilde{\boldsymbol{M}}_{\boldsymbol{j}}$
2	7	143	5
6	11	91	4
3	13	77	12

Now we can plug and chug:

$$\begin{aligned} x &= \left(\sum_{j=1}^{3} a_j M_j \tilde{M}_j\right) \mod 1001 \\ &= (2 \cdot 143 \cdot 5 + 6 \cdot 91 \cdot 4 + 3 \cdot 77 \cdot 12) \mod 1001 \\ &= (1430 + (1800 + 360 + 24) + (2310 + 462)) \mod 1001 \\ &= (429 + 799 + 384 + 308 + 462) \mod 1001 && \text{modular addition rule} \\ &= (1228 + 384 + 770) \mod 1001 \\ &= (227 + 1154) \mod 1001 && \text{modular addition rule} \\ &= (227 + 153)) \mod 1001 && \text{modular addition rule} \\ &= 380 \mod 1001 \\ &= 380 \end{aligned}$$

Checking this value out, we find that $380 \mod 7 = 2$, $380 \mod 11 = 6$, and $380 \mod 13 = 3$. Awesome!