Extra Examples

Chinese Remainder Theorem and Solving Systems of Linear Congruencies

Introduction

In this guide, I will go over how to solve systems of linear congruencies using the Chinese Remainder Theorem. Before that however, I give quick examples on how to reduce $a \bmod m$ when $a > m$ and find the modular inverse of $a \bmod m$.

Reducing $a \bmod m$

Sometimes, we have an equation $a \bmod m$ where $a > m$. This can make finding inverses and solving systems of linear congruencies more difficult to work with. In these cases, you should first reduce $a \bmod m$. To do this, we want to find an integer b such that $a \equiv b \bmod m$ where $b < m$.

Confused? Too many variables? How about a specific example!

Let $a = 176$ and $m = 14$, giving us the equation $176 \bmod 14$. Since $176 > 14$, lets try to reduce this to something smaller. The first step is to rewrite 176 in the form:

$$\begin{aligned} a &= mq + r \\ 176 &= 14 * q + r \end{aligned}$$

where q is a quotient and r is the remainder. We can find q and r as follows:

$$\begin{aligned} q &= \left\lfloor \frac{a}{m} \right\rfloor = \left\lfloor \frac{176}{14} \right\rfloor = \lfloor 12.57\ldots \rfloor = 12 \\ r &= a - mq = 176 - 14 * 12 = 176 - 168 = 8 \end{aligned}$$

Tada! Our answer is r. Therefore, $176 \bmod 12 = 8$. So instead of writing $176 \bmod 12$ we can write $8 \bmod 12$ and work with a much smaller number.

How about another example? This time, we want to reduce $4 \bmod 3$. Solving everything we get:

$$\begin{aligned} q &= \left\lfloor \frac{4}{3} \right\rfloor = \lfloor 1.333\ldots \rfloor = 1 \\ r &= 4 - 3 * 1 = 1 \end{aligned}$$

Thus, we can rewrite 4 as $4 = 3 * 1 + 1$. Therefore, $1 \equiv 4 \bmod 3$.

Okay, here is a recap all of the steps. To reduce an equation $a \bmod m$ where $a > m$:

1. Rewrite a as $a = mq + r$ where $q = \lfloor a/m \rfloor$ and $r = a - mq$.
2. This gives us $r = a \bmod m$, or equivalently, $a \equiv r \bmod m$.

Or... just use a calculator :)

Finding Modular Inverses (Examples)

To find the modular inverse of $a \bmod m$, we are looking for an integer s such that $s * a \equiv 1 \bmod m$. (I'm assuming you have already reduced $a \bmod m$ if $a > m$.)

First, find the $\gcd(a, m)$ using the Euclidean Algorithm. This time, I'm going to make sure I match the format in the book. Let $r_0 = m$ and $r_1 = a$. Then your equations should always be in the form:

$$\begin{aligned} r_0 &= r_1 * q_1 + r_2 \\ r_1 &= r_2 * q_2 + r_3 \\ r_2 &= r_3 * q_3 + r_4 \\ &\vdots \\ r_{n-2} &= r_{n-1} * q_{n-1} + r_n \\ r_{n-1} &= r_n * q_n \end{aligned}$$

If $r_n = 1$ then $\gcd(a, m) = 1$ and we can find an inverse. Discard the last equation r_{n-1} to get:

$$\begin{aligned} r_0 &= r_1 * q_1 + r_2 \\ r_1 &= r_2 * q_2 + r_3 \\ r_2 &= r_3 * q_3 + r_4 \\ &\vdots \\ r_{n-2} &= r_{n-1} * q_{n-1} + r_n = r_{n-1} * q_{n-1} + 1 \end{aligned}$$

What you have should match this, except you'll actually have numbers instead of variables everywhere. Put back in every variable r_i except r_n. Then replace r_0 with the variable m and r_1 with the variable a. (We'll go over a numeric example in a moment.)

The next step is to rewrite everything in the form $r_i = \dots$ such that we get:

$$\begin{array}{rcl} a = m * q_1 + r_2 & \longrightarrow & r_2 = a - m * q_1 \\ m = r_2 * q_2 + r_3 & \longrightarrow & r_3 = m - r_2 * q_2 \\ r_2 = r_3 * q_3 + r_4 & \longrightarrow & r_4 = r_2 - r_3 * q_3 \\ \vdots & \vdots & \vdots \\ r_{n-2} = r_{n-1} * q_{n-1} + 1 & \longrightarrow & 1 = r_{n-2} - r_{n-1} * q_{n-1} \end{array}$$

Then, starting with the last equation, backwards substitute until you get something in the form:

$$1 = s * a + t * m$$

Once that happens, we know our modular inverse of $a \bmod m$ is s.

I don't know about you, but all of these variables are making my head hurt. How about a real example!

Let $a = 34$ and $m = 55$. We want to find the modular inverse of 34 mod 55.

Step 1: First we need to use the Euclidean Algorithm to find the $\gcd(34, 55)$. On the left column I'll just show what the variables are, and on the right column will be the actual values:

$$\begin{array}{lclcl}
r_0 = r_1 * q_1 + r_2 & \longrightarrow & 55 = 34 * q_1 + r_2 & \longrightarrow & 55 = 34 * 1 + 21 \\
r_1 = r_2 * q_2 + r_3 & \longrightarrow & 34 = 21 * q_2 + r_3 & \longrightarrow & 34 = 21 * 1 + 13 \\
r_2 = r_3 * q_3 + r_4 & \longrightarrow & 21 = 13 * q_3 + r_4 & \longrightarrow & 21 = 13 * 1 + 8 \\
r_3 = r_4 * q_4 + r_5 & \longrightarrow & 13 = 8 * q_4 + r_5 & \longrightarrow & 13 = 8 * 1 + 5 \\
r_4 = r_5 * q_5 + r_8 & \longrightarrow & 8 = 5 * q_5 + r_6 & \longrightarrow & 8 = 5 * 1 + 3 \\
r_5 = r_6 * q_6 + r_7 & \longrightarrow & 5 = 3 * q_6 + r_7 & \longrightarrow & 5 = 3 * 1 + 2 \\
r_6 = r_7 * q_7 + r_8 & \longrightarrow & 3 = 2 * q_7 + r_8 & \longrightarrow & 3 = 2 * 1 + 1 \\
r_7 = r_8 * q_8 & \longrightarrow & 2 = 1 * q_8 & \longrightarrow & 2 = 1 * 2
\end{array}$$

Wow, I picked a bad pair of numbers. That took forever. Well, now it is time for the next step.

Step 2: Well, we can see our last remainer $r_8 = 1$. This means $\gcd(34, 55) = 1$ and there is an inverse. First, we ditch the last equation r_7 to get:

$$\begin{array}{l}
55 = 34 * 1 + 21 \\
34 = 21 * 1 + 13 \\
21 = 13 * 1 + 8 \\
13 = 8 * 1 + 5 \\
8 = 5 * 1 + 3 \\
5 = 3 * 1 + 2 \\
3 = 2 * 1 + 1
\end{array}$$

Now we reassign the variables. We put back every r_i except for the last $r_n = 1$ (which in this case is r_8), and then replace r_0 with m and r_1 with a:

$$\begin{array}{lclcl}
55 = 34 * 1 + 21 & \longrightarrow & r_0 = r_1 * 1 + r_2 & \longrightarrow & m = a * 1 + r_2 \\
34 = 21 * 1 + 13 & \longrightarrow & r_1 = r_2 * 1 + r_3 & \longrightarrow & a = r_2 * 1 + r_3 \\
21 = 13 * 1 + 8 & \longrightarrow & r_2 = r_3 * 1 + r_4 & \longrightarrow & r_2 = r_3 * 1 + r_4 \\
13 = 8 * 1 + 5 & \longrightarrow & r_3 = r_4 * 1 + r_5 & \longrightarrow & r_3 = r_4 * 1 + r_5 \\
8 = 5 * 1 + 3 & \longrightarrow & r_4 = r_5 * 1 + r_6 & \longrightarrow & r_4 = r_5 * 1 + r_6 \\
5 = 3 * 1 + 2 & \longrightarrow & r_5 = r_6 * 1 + r_7 & \longrightarrow & r_5 = r_6 * 1 + r_7 \\
3 = 2 * 1 + 1 & \longrightarrow & r_6 = r_7 * 1 + 1 & \longrightarrow & r_6 = r_7 * 1 + 1
\end{array}$$

Step 3: Now we rearrange. We rewrite every equation to be in the form $r_i = \ldots$ and get:

$$\begin{array}{rcr}
m = a * 1 + r_2 & \longrightarrow & r_2 = m - a \\
a = r_2 * 1 + r_3 & \longrightarrow & r_3 = a - r_2 \\
r_2 = r_3 * 1 + r_4 & \longrightarrow & r_4 = r_2 - r_3 \\
r_3 = r_4 * 1 + r_5 & \longrightarrow & r_5 = r_3 - r_4 \\
r_4 = r_5 * 1 + r_6 & \longrightarrow & r_6 = r_4 - r_5 \\
r_5 = r_6 * 1 + r_7 & \longrightarrow & r_7 = r_5 - r_6 \\
r_6 = r_7 * 1 + 1 & \longrightarrow & 1 = r_6 - r_7
\end{array}$$

Step 4: Finally, we use backwards substitution and get:

$$\begin{aligned}
1 &= r_6 - r_7 \\
&= r_6 - (r_5 - r_6) && \text{substitute in } r_7 \\
&= 2r_6 - r_5 && \text{simplify} \\
&= 2(r_4 - r_5) - r_5 && \text{substitute in } r_6 \\
&= 2r_4 - 3r_5 && \text{simplify} \\
&= 2r_4 - 3(r_3 - r_4) && \text{substitute in } r_5 \\
&= 5r_4 - 3r_3 && \text{simplify} \\
&= 5(r_2 - r_3) - 3r_3 && \text{substitute in } r_4 \\
&= 5r_2 - 8r_3 && \text{simplify} \\
&= 5r_2 - 8(a - r_2) && \text{substitute in } r_3 \\
&= 13r_2 - 8a && \text{simplify} \\
&= 13(m - a) - 8a && \text{substitute in } r_2 \\
&= 13m - 21a
\end{aligned}$$

Finally, we have the equation in the form we want:

$$1 = -21 * a + 13 * m$$

...almost. We can't have a negative inverse. So time to make it positive:

$$-21 \bmod 55 \equiv -21 + 55 \bmod 55 \equiv 34 \bmod 55$$

Therefore our inverse $s = 34$. If you plug $34 * 34 \bmod 55$ in your calculator, you'll get 1!

Okay, so the steps are:

1. Reduce $a \bmod m$ if necessary.
2. Find the $\gcd(a, m)$ using the Euclidean Algorithm.
3. If $r_n = 1$ we know $\gcd(a, m) = 1$ and there is an inverse.

4. Reassign the variables $r_1, r_2, \ldots, r_{n-1}$ (all remainders except r_n).
5. Reassign the variables r_0 to m and r_1 to a.
6. Rearrange the equations into the form $r_i = r_{i-2} - r_{i-1} * q_{i-1}$.
7. Backwards substitute starting with r_n until we get an equation in the form $1 = s * a + t * m$.
8. If s is negative, add m until it is positive!

After all of these steps, we know the inverse is s. Just remember, reassign, rearrange, and substitute!

Solving Systems of Congruencies Using the Chinese Remainder Theorem

Here are the basic steps. This is meant more for a reference. For more detail, skip to one of the examples.

Given a system of congruencies where $m_1, m_2, \ldots, m_n$ are pairwise relatively prime positive integers:

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

Using the Chinese Remainder Theorem, if we solve the following:

$$\begin{aligned}
m &= \prod_{i=1}^{n} m_i = m_1 m_2 \cdots m_n \\
M_i &= m/m_i \\
M_i s_i &= 1 \bmod m_i \text{ (i.e. } s_i \text{ is the modular inverse of } M_i \bmod m_i \text{)} \\
x &= \sum_{i=1}^{n} a_i M_i s_i = a_1 M_1 s_1 + a_2 M_2 s_2 + \cdots + a_n M_n y_n
\end{aligned}$$

then we know that $x \bmod m$ is the unique solution to our system of congruencies.

Solving Systems of Congruencies: Example 1

Example #19 on page 245. Find all solutions to:

$$\begin{aligned}
x &\equiv 1 \bmod 2 \\
x &\equiv 2 \bmod 3 \\
x &\equiv 3 \bmod 5 \\
x &\equiv 4 \bmod 11
\end{aligned}$$

Before we start, let's be clear on what our variables are:

$a_1 = 1$	$a_2 = 2$	$a_3 = 3$	$a_4 = 4$
$m_1 = 2$	$m_2 = 3$	$m_3 = 5$	$m_4 = 11$

Then, solve for m:

$$m = 2 * 3 * 5 * 11 = 330$$

Next, lets find all the M_i terms:

$$\begin{aligned} M_1 &= m/m_1 \\ &= 330/2 \\ &= 165 \end{aligned} \qquad \begin{aligned} M_2 &= m/m_2 \\ &= 330/3 \\ &= 110 \end{aligned} \qquad \begin{aligned} M_3 &= m/m_3 \\ &= 330/5 \\ &= 66 \end{aligned} \qquad \begin{aligned} M_4 &= m/m_4 \\ &= 330/11 \\ &= 30 \end{aligned}$$

Now the tough part! We need to find the inverses s_1, s_2, s_3, and s_4.

The value s_1 needs to be the modular inverse of $M_1 \bmod m_1$. In this case, we need the inverse of $165 \bmod 2$. Since $165 > 2$ we should reduce this first. We can write $165 = 2 * 82 + 1$ meaning $165 \bmod 2 = 1$. Therefore $165 \bmod 2 \equiv 1 \bmod 2$, and we can alternatively find the inverse of $1 \bmod 2$. This is much easier! We just need a value s_1 such that $1 * s_1 \equiv 1 \bmod 2$. In this case, we can see that $s_1 = 1$ without having to use the Euclidean Algorithm and backwards substitution.

Next, we need s_2 to be the modular inverse of $110 \bmod 3$. If we reduce this we see $110 \bmod 3 \equiv 2 \bmod 3$. Therefore we just need the inverse to $2 \bmod 3$. Again, this is much easier to find. In fact, $s_2 = 2$ but let's work through the algorithm to be sure. (More details on the algorithm is at the end of this document.)

Using the Euclidean Algorithm for the $\gcd(2, 3)$ we get:

$$\begin{aligned} 3 &= 2 * 1 + 1 \\ 2 &= 1 * 2 \end{aligned}$$

Therefore $\gcd(2, 3) = 1$ and we can find the inverse. We drop the last equation, and reassign the variables to get:

$$3 = 2 * 1 + 1 \qquad \longrightarrow \qquad m_2 = a_2 * 1 + 1$$

Rearranged we get:

$$1 = m_2 - a_2$$

From this, we can tell that $s_2 = -1$?? Ew! Negative numbers! Whenever you come across a negative number modulo m_2, keep adding m_2 until the number is positive. Therefore:

$$-1 \bmod 3 \equiv -1 + 3 \bmod 3 \equiv 2 \bmod 3$$

Tada! We have a positive number now, and $s_2 = 2$.

Tired yet? But we have 2 more inverses to find! We need s_3 to be the modular inverse of $66 \bmod 5$. Reduced, we get $66 \bmod 5 \equiv 1 \bmod 5$. Again, we luck out with an easy one to find. The inverse $s_3 = 1$ in this case.

Finally, s_4 must be the modular inverse of $30 \bmod 11$. Reduced, we get $30 \bmod 11 = 8 \bmod 11$. Boo... looks like it is time for our fancy algorithm! (You are excited, I can tell.)

First, find the $\gcd(8, 11)$ using the Euclidean Algorithm:

$$\begin{aligned} 11 &= 8 * 1 + 3 \\ 8 &= 3 * 2 + 2 \\ 3 &= 2 * 1 + 1 \\ 2 &= 1 * 2 \end{aligned}$$

The $\gcd(8, 11) = 1$ so time to find the inverse. Drop the last equation and begin to reassign variables:

$$\begin{array}{rcccc} 11 = 8 * 1 + 3 & \longrightarrow & r_0 = r_1 * 1 + r_2 & \longrightarrow & m_4 = a_4 * 1 + r_2 \\ 8 = 3 * 2 + 2 & \longrightarrow & r_1 = r_2 * 2 + r_3 & \longrightarrow & a_4 = r_2 * 2 + r_3 \\ 3 = 2 * 1 + 1 & \longrightarrow & r_2 = r_3 * 1 + 1 & \longrightarrow & r_2 = r_3 * 1 + 1 \end{array}$$

Next, we rearrange!

$$\begin{array}{rcr} m_4 = a_4 * 1 + r_2 & \longrightarrow & r_2 = m_4 - a_4 \\ a_4 = r_2 * 2 + r_3 & \longrightarrow & r_3 = a_4 - 2r_2 \\ r_2 = r_3 * 1 + 1 & \longrightarrow & 1 = r_2 - r_3 \end{array}$$

And now we use backwards substitution to get:

$$\begin{aligned} 1 &= r_2 - r_3 \\ &= r_2 - (a_4 - 2r_2)r_2 - a_4 + 2r_2 = 3r_2 - a_4 \\ &= 3(m_4 - a_4) - a_4 = 3m_4 - 3a_4 - a_4 \\ &= -4a_4 + 2m_4 \end{aligned}$$

Again, we get a negative inverse which we don't want. So we have to make it positive:

$$-4 \bmod 11 \equiv -4 + 11 \bmod 11 \equiv 7 \bmod 11$$

Therefore our modular inverse $s_4 = 7$. You can double check this in a calculator, and see that $8 * 7 \equiv 1 \bmod 11$.

At this point we have all of our modular inverses:

$$s_1 = 1 \qquad s_2 = 2 \qquad s_3 = 1 \qquad s_4 = 7$$

Finally, we can solve for x:

$$\begin{aligned} x &= \sum_{i=1}^{n} a_i M_i s_i \\ &= a_1 M_1 s_1 + a_2 M_2 s_2 + a_3 M_3 s_3 + a_4 M_4 s_4 \\ &= 1 * 165 * 1 + 2 * 110 * 2 + 3 * 66 * 1 + 4 * 30 * 7 \\ &= 1643 \end{aligned}$$

However, we aren't done yet! This is a solution $\bmod m$. So we need to reduce this to get:

$$x \equiv 1643 \bmod m \equiv 1643 \bmod 330 \equiv 323 \bmod 330$$

WE ARE DONE! The solution to this system of congruencies is $x \equiv 323 \bmod 330$. This means any number in the form $323 + 330k$ where k is a positive integer will work. Just try it out on a calculator!