Solving Systems of Linear Congruences

DeVon Herr

July 2018

0 Preface

This document presumes you know the basics of modular arithmetic. Namely, you should know how to take the modulus of a number, and how to use modular arithmetic to make math questions easier.

0.1 Notation

$$\gcd(a, b, c, ...z)$$

Means the greatest common divisor/factor between all the numbers inside the argument/parentheses.

A set of numbers $\{a,\ b,\ c,\ ...\ z\}$ is said to be co-prime if the two numbers share no common factors, that is, $\gcd(a, b) = 1$.

A linear congruence is an equality described using the modulus function under some base.

$$a \equiv b \pmod{n}$$

0.2 Linear Congruences are Arithmetic Sequences

Consider the linear congruence $a \equiv b \pmod{n}$. All solutions to the linear congruence should then be of form $a \equiv kn + b$ where k is an arbitrary integer.

The proof is as follows. If $a \equiv b \pmod{n}$, then by inspection, b is a solution to the linear congruence. Since adding the base should make no difference to the remainder, what happens if we add n to our first solution?

$$b + n \pmod{n} \equiv b \pmod{n} + n \pmod{n}$$

(Here, we are taking the modulus of each term, which is allowed.)

$$b \pmod{n} + n \pmod{n} \equiv b \pmod{n} + 0$$

(Any number perfectly divides itself with no remainder. Therefore, the remainder of any number when divided by itself is zero.)

$$b \pmod{\text{n}} + 0 = b \pmod{\text{n}}$$

Aha! Another solution. $b + n$, too, solves the linear congruence. We can repeat the process by adding n again to get that $b+n+n = b+2n$ is a solution, or again so that $b + n + n + n = b + 3n$ is a solution, and so forth. Essentially, any integer that can be written as $b + kn$ or $kn + b$ where k is any integer we please, is a solution to the linear congruence.

Now consider the set of all solutions:

$$\{..., b - 3n,\ b - 2n,\ b - n,\ b,\ b + n,\ b + 2n,\ b + 3n, ...\}$$

This forms an arithmetic progression/sequence, as to go "up" or "down" one term requires the addition (or subtraction) of a constant n.

0.3 Simplifying Linear Congruences by Division

Just as how $2x = 4$ can be further simplified to $x = 2$, a similar albeit slightly different process can be applied to linear congruences. In particular, one has to consider the gcd of the common factor.

If $ac = bc \pmod{\text{n}}$, and $\gcd c, m = 1$, then this can be simplified to $a = b \pmod{\text{n}}$. This is because multiplying by an integer that is co-prime with the modulus does not make a difference.

However, multiplying by a integer that has a factor in common with the modulus *does* make a difference. Consider $27 \equiv 45 \equiv 69 \pmod{12}$. This is veritably true, as $27 \equiv 3 \pmod{12}$ and $69 \equiv 3 \pmod{12}$. However, dividing the two by their common factor does not produce a valid result.

$$\begin{aligned} \frac{45}{3} &\stackrel{?}{\equiv} \frac{69}{3} \pmod{12} \\ 15 &\stackrel{?}{\equiv} 23 \pmod{12} \\ 3 &\not\equiv 11 \pmod{12} \end{aligned} \tag{1}$$

In particular, there is an issue as 3 and the base, 12, have a factor in common (it doesn't have to be that 3 is a factor, just the two share a factor). **To remedy this, one then divides the modulus itself by this common factor.** In the example, it then becomes the following.

$$\begin{aligned} \frac{45}{3} &\stackrel{?}{\equiv} \frac{69}{3} \pmod{\frac{12}{\gcd(12,3)}} \\ 15 &\stackrel{?}{\equiv} 23 \pmod{\frac{12}{3}} \\ 15 &\stackrel{?}{\equiv} 23 \pmod{4} \\ 3 &\stackrel{\checkmark}{\equiv} 3 \pmod{4} \end{aligned} \tag{2}$$

More succinctly, given the following generic linear congruence:

$$\begin{aligned} ab &\equiv ac \pmod{n} \\ b &\equiv c \pmod{\frac{n}{\gcd(n,a)}} \end{aligned} \tag{3}$$

0.4 Simplifying Linear Congruences by Arithmetic

Sometimes the linear congruence will not "give up" to just division. This is sometimes necessary when one side of the linear congruence has a variable term with a coefficient. Consider the following example.

$$3x = 5 \pmod{7}$$

We want to solve for x, and to do so we need to isolate the variable term. However, diving by 3 reduces the right hand side to a fraction, which can't realistically be worked with. What now? We want to make the right hand side equal to a multiple of 3 so we can divide it, but how?

Remember, in mathematics, the dark arts are always some form of adding 0 or multiplying by 1. In this case, since we want to *change* the number's multiplicative properties, we will try adding 0. In particular, we can add 7 to both sides of the equation. It shouldn't change anything, since $7 \equiv 0 \pmod{7}$.

$$\begin{aligned} 3x + 7 &\equiv 5 + 7 \pmod{7} \\ 3x &\equiv 12 \pmod{7} \\ \frac{3x}{3} &\equiv \frac{12}{3} \pmod{\frac{7}{\gcd(7,3)}} \\ x &\equiv 4 \pmod{\frac{7}{1}} \\ x &\equiv 4 \pmod{7} \end{aligned} \tag{4}$$

0.4.1 When the Base is Really Large

If the base gets really big, both computing and checking if a given number works takes an annoying amount of time. What we are looking for is known as a modular multiplicative inverse, which can be solved in numerous ways.

Given the following linear congruence:

$$ax \equiv b \pmod{n}$$

Take the first number (in this case, a), and keep subtracting until it is a multiple of n. Then use the subtrahend (the number you used to subtract) and multiply both sides.

1 Introduction

A system of linear congruences is exactly as it sounds. Instead of an integer having one linear congruence, it will have multiple. Instead of the following,

$$a = b \text{ (mod n)}$$

It will be something more of the following.

$$x \equiv \begin{cases} b_1 \pmod{n_1} \\ b_2 \pmod{n_2} \\ b_3 \pmod{n_3} \\ \cdot \\ \cdot \\ \cdot \\ b_k \pmod{n_k} \end{cases}$$

2 Basics of Existence

Certain systems of linear congruences may not have any solutions. These arise when at least two linear congruences "disagree." Consider the straightforward example below.

$$a \equiv \begin{cases} 0 \pmod 2 \\ 1 \pmod 2 \end{cases}$$

This is a contradiction. No integer can simultaneously have no remainder *and* a remainder of one when divided by two. More colloquially, no number is simultaneously even *and* odd. Therefore there are no solutions to this linear congruence.

By something known as the Chinese Remainder Theorem, **if all of the bases are co-prime, a solution is guaranteed**, and one can skip the methods outlined in section 3, which revolve around checking if a solution exists. If they are not co-prime, then one has to take measures to discern if solutions exist, outlined in section 3.

3 "Reduce" the Linear Congruences

The first step is to simplify all the linear congruences. This is often not necessary, but it may be necessary in some systems.

3.1 "Factor" the Linear Congruences

The second step in solving a system of linear congruences is to check if a solution can or cannot exist. Again, this may not be necessary as well.

Although the **Basics of Existence** is sufficient for obvious contradictions by inspection, sometimes the contradiction is more subtle.

For example, take the following linear congruence.

$$x \equiv 1 \pmod{15}$$

Verbally, the statement is "x, when divided by the number 15, leaves a remainder of 1." Since 15 is a multiple of 3, then it is *also* true that x should be one greater than a multiple of three. The same can be said for five as well. Thus the following deduction holds.

$$x \equiv 1 \pmod{15} \Rightarrow x \equiv \begin{cases} 1 \pmod{3} \\ 1 \pmod{5} \end{cases}$$

The "factoring" of sorts can be done to any factor of the modulus but, generally speaking, **one should factor to as many perfect prime powers and stop**. In the case of a number such as $2^3 \cdot 3^2$, one should "factor" it into the modulus of 2^3 and 3^2, and no further.

3.2 Check for Compatibility

Find all linear congruences that have bases that share a common factor. Then, check if the remainders are congruent when divided by the greatest common factor. Given the following example:

$$x \equiv \begin{cases} 1 \pmod{86} \\ 94 \pmod{182} \end{cases}$$

One would then have to check if the following holds.

$$\begin{aligned} 1 &\stackrel{?}{\equiv} 94 \pmod{\gcd(86, 182)} \\ 1 &\stackrel{?}{\equiv} 94 \pmod{2} \\ 1 &\not\equiv 0 \pmod{2} \end{aligned} \tag{5}$$

Aha! A contradiction. **Therefore the statements can not have a solution**. On the other hand, if the statements were compatible, it is safe. Repeat until all linear congruences that share a common factor in their base are checked. **If all are compatible, a solution exists**.

3.3 Remove "Redundant" Linear Congruences

Once all of the linear congruences are "reduced" and "factored," there may be obvious overlap. Consider the following example.

$$x \equiv \begin{cases} 1 \pmod{2} \\ 1 \pmod{4} \end{cases}$$

In this case, the second linear congruence contains more information; all numbers that leave a remainder of one when divided by four will also leave a remainder of one when divided by two. This is because multiples of four are also multiples of two.

$$x \equiv 1 \pmod 4 \Rightarrow x \equiv 1 \pmod 2$$

The same cannot be said the other way around; a number that leaves a remainder of one when divided by two is not guaranteed to have a remainder of one when divided by four.

$$x \equiv 1 \pmod 2 \not\Rightarrow x \equiv 1 \pmod 4$$

For this reason, the $x \equiv 1 \pmod 4$ statement is, in a sense, stronger than $x \equiv 1 \pmod 2$. For this reason, one can remove the "weaker" linear congruence and leave only the "stronger" one.

4 Find the "Cycle Number"

Formally, this is called the least common multiple or LCM, but no matter. Take the least common multiple of all of the bases to get the cycle number. That is, given the following system:

$$x \equiv \begin{cases} b_1 \pmod{n_1} \\ b_2 \pmod{n_2} \\ b_3 \pmod{n_3} \\ \cdot \\ \cdot \\ \cdot \\ b_k \pmod{n_k} \end{cases}$$

The cycle number is LCM$(n_1 \cdot n_2 \cdot n_3 \cdot ... \cdot n_k)$.

If you have successfully "reduced" the linear congruences such that the bases are only the "strongest" prime powers, it follows from prime properties that you can simply multiply them together.

The use of the cycle number is that given a solution to the system of linear congruences, **one can add/subtract the cycle number to get another solution**. If one views the solutions as an arithmetic sequence, the cycle number is equivalent to the common difference between terms in the sequence.

This number can also be used to verify solutions done the analytic way.

5 Method 1: Smart Bashing

Okay! We can finally start solving them! Let's say we have the following system.

$$x \equiv \begin{cases} 2 \pmod 3 \\ 2 \pmod 4 \\ 1 \pmod 5 \end{cases}$$

By inspection, all bases are co-prime so, by the Chinese Remainder Theorem, a solution is guaranteed.

The cycle number is given by the least common multiple of the bases, which turns out to be $3 \cdot 4 \cdot 5 = 60$ as they are co-prime. We then need to see what numbers under 60 can solve the system. If it works, we can then add or subtract 60 at will to find all solutions.

The trick is to take the statement with the largest base, and list out all numbers that work for it. By inspection (or algebra), the statement:

$$1 \pmod 5$$

Is equivalent to the following arithmetic sequence.

$$a_k = 1 + 5k$$

Listing all terms of the sequence under 60 gives the following set.

$$\{1,\ 6,\ 11,\ 16,\ 21,\ 26,\ 31,\ 36,\ 41,\ 46,\ 51,\ 56\}$$

Go through each integer and see if it solves the other linear congruences until a solution is found. The solution is 26, as the following linear congruences hold.

Thus, all solutions will be of form $x = 26 + 60k$ where k is an integer, or alternatively $x \equiv 26 \pmod{60}$.

6 Method 2: The Analytic Approach

This is better for people that like their work being composed of algebra instead of lists. This is also the ideal way if bases begin to be incredibly large. Consider the following example.

$$x \equiv \begin{cases} 3 \pmod 7 \\ 7 \pmod{12} \\ 4 \pmod{17} \end{cases}$$

Since the three bases are co-prime, by the Chinese Remainder Theorem, there exists a solution to the system.

Solve the first linear congruence. The solution to the first is some integer of form:

$$x = 3 + 7k$$

For arbitrary integer k.

Since our desired number x is also congruent to the second statement, equate the solution of the first linear congruence to the second linear congruence, and simplify.

$$\begin{aligned} 3 + 7k &\equiv 7 \pmod{12} \\ 7k &\equiv 4 \pmod{12} \\ 7k + 2 \cdot 12 &\equiv 4 + 2 \cdot 12 \pmod{12} \\ 7k &\equiv 28 \pmod{12} \\ \frac{7k}{7} &\equiv \frac{28}{7} \pmod{\frac{12}{\gcd(12, 7)}} \\ k &\equiv 4 \pmod{\frac{12}{1}} \\ k &\equiv 4 \pmod{12} \end{aligned} \tag{6}$$

The solutions to the final statement are integers of form:

$$k = 12l + 4$$

For arbitrary integer l.

It's important that you keep your variables clear and to not have overlap on your variable names.

Substituting this back into our original equation involving k gives the following:

$$\begin{aligned} x &= 3 + 7k \\ x &= 3 + 7(12l + 4) \\ x &= 3 + 84l + 28 \\ x &= 31 + 84l \end{aligned} \tag{7}$$

Then the process is repeated again with the third linear congruence. Since the numbers are becoming large, we will calculate the modular multiplicative inverse. We do this by observing the following:

$$\frac{84 - 16}{17} = 7 \in \mathbb{Z}$$

Thus 16 is the modular multiplicative inverse of 84 in base 17.

$$\begin{aligned} 31 + 84l &= 4 \pmod{17} \\ 84l &= -27 \pmod{17} \\ 16l &= 7 \pmod{17} \\ 16 \cdot 16l &= 16 \cdot 7 \pmod{17} \\ 256l &= 112 \pmod{17} \\ l &= 10 \pmod{17} \end{aligned} \tag{8}$$

The solutions to the final statement are of form:

$$l = 17m + 10$$

For arbitrary integer m.
Substitute into our second equation.

$$\begin{aligned} x &= 31 + 84l \\ x &= 31 + 84(17m + 10) \\ x &= 31 + 1428m + 840 \\ x &= 871 + 1428m \end{aligned} \tag{9}$$

And we are done.

7 Addendum: The Smallest Solution

If the question asks for the smallest solution, let $x = 0$.

8 Practice Problems

1. $$x \equiv \begin{cases} 1 \pmod 6 \\ 17 \pmod{39} \\ 69 \pmod{42069} \end{cases}$$

2. $$x \equiv \begin{cases} 8 \pmod{12} \\ 6 \pmod 9 \end{cases}$$

3. $$x \equiv \begin{cases} 8 \pmod{12} \\ 6 \pmod{13} \end{cases}$$

4. "There are certain things whose number is unknown. If we count them by threes, we have two left over; by fives, we have three left over; and by sevens, two are left over. How many things are there?"