Linear Congruences

P. Reany

July 4, 2023

Abstract

A linear congruences is an equation in one unknown taken modulo some positive integer.

1 Introduction

Let's look at a generic linear congruence:

$$ax + b \equiv c \pmod{n}. \tag{1}$$

Well, that's a fancy linear congruence. A more typical one would be

$$ax \equiv b \pmod{n}. \tag{2}$$

If a is relatively prime to the modulus n, then x will have a unique answer, for in this case a^{-1} will exists in this number system, yielding.

$$x \equiv a^{-1}b \pmod{n}. \tag{3}$$

2 Problem 1

The following problem I found somewhere in my long intellectual travels: Solve the following linear congruence for x:

$$342x + 448 \equiv 73 \pmod{1003}. \tag{4}$$

The first step is to subtract 448 from both sides, yielding

$$342x \equiv -375 \pmod{1003}, \tag{5}$$

which simplifies to

$$342x \equiv 628 \pmod{1003}. \tag{6}$$

Now, it just so happens that the inverse of 342 modulo 1003 is 349 (and I will prove this soon). Anyway, we have that

$$x \equiv 349 \cdot 628 \pmod{1003}. \tag{7}$$

On multiplying this out and then reducing it mod 1003, we get

$$x \equiv 518 \pmod{1003}\,, \tag{8}$$

Now, to show that $342^{-1} \equiv 349 \pmod{1003}$ we need only apply the Euclidean Algorithm:

$$\begin{aligned} 1003 &= 2 \cdot 342 + 319\,, \\ 342 &= 1 \cdot 319 + 23\,, \\ 319 &= 13 \cdot 23 + 20\,, \\ 23 &= 1 \cdot 20 + 3\,, \\ 20 &= 6 \cdot 3 + 2\,, \\ 3 &= 1 \cdot 2 + 1\,. \end{aligned} \tag{9}$$

Thus, we have shown that 1003 and 342 are relatively prime. Our next task is to solve these for the remainders:

$$\begin{aligned} 1003 - 2 \cdot 342 &= 319\,, \\ 342 - 1 \cdot 319 &= 23\,, \\ 319 - 13 \cdot 23 &= 20\,, \\ 23 - 1 \cdot 20 &= 3\,, \\ 20 - 6 \cdot 3 &= 2\,, \\ 3 - 1 \cdot 2 &= 1\,. \end{aligned} \tag{10}$$

Now, the way this works is that we back-substitute into these equations the remainders in reverse order, until all we have left are multiples of 1003 and 342 on the LHS and unity on the RHS.

$$3 - 1 \cdot [\,20 - 6 \cdot 3\,] = 1\,, \tag{11}$$

which simplifies to

$$7 \cdot 3 - 20 = 1\,. \tag{12}$$

Next,

$$7 \cdot [\,23 - 1 \cdot 20\,] - 20 = 1\,, \tag{13}$$

which simplifies to

$$7 \cdot 23 - 8 \cdot 20 = 1\,. \tag{14}$$

Next,

$$7 \cdot 23 - 8 \cdot [\,319 - 13 \cdot 23\,] = 1\,, \tag{15}$$

which simplifies to

$$111 \cdot 23 - 8 \cdot 319 = 1\,. \tag{16}$$

Next,

$$111 \cdot [\,342 - 1 \cdot 319\,] - 8 \cdot 319 = 1\,, \tag{17}$$

which simplifies to

$$111 \cdot 342 - 119 \cdot 319 = 1\,. \tag{18}$$

Next,

$$111 \cdot 342 - 119 \cdot [\,1003 - 2 \cdot 342\,] = 1\,, \tag{19}$$

which simplifies to

$$349 \cdot 342 - 119 \cdot 1003 = 1\,. \tag{20}$$

Finally, we reduce this last equation modulo 1003, to get

$$349 \cdot 342 \equiv 1 \pmod{1003}\,. \tag{21}$$

And this proves that $342^{-1} \equiv 349 \pmod{1003}$.

3 Problem 2

Simultaneous linear congruences.

If we are given two or more such linear congruences, we need only reduce the coefficients of the x's to unity — if that is possible. Having done that, we can then merely use the techniques typical for the Chinese Remainder Theorem.

Let's get a problem started. Solve the following linear congruences for x:

$$4x \equiv 5 \pmod{7}\,, \tag{22}$$

$$2x \equiv 4 \pmod{5}\,. \tag{23}$$

Well, 4 and 7 are relatively prime, therefore 4 has an inverse mod 7. Since the modulus is small, we can attempt to find the inverse by exhaustive search. The number 2 works because $2 \cdot 4 = 8$ which is congruent to 1 mod 7. For the second equation, 3 works. Thus,

$$x \equiv 10 \pmod{7}\,, \tag{24}$$

$$x \equiv 12 \pmod{5}\,. \tag{25}$$

And these simplify down to

$$x \equiv 3 \pmod{7}\,, \tag{26}$$

$$x \equiv 2 \pmod{5}\,. \tag{27}$$

Another way to state this couple is this: Find x such that when divided by 7 leaves a remainder of 3, and when divided by 5 leaves a remainder of 2.

4 Problem 3

What if, instead of (23), we had

$$2x \equiv 4 \pmod{6}\,? \tag{28}$$

Yes, in this case, 2 is not relatively prime to 6. To see if there is anything more we can do with (28), let's express it without modulo arithmetic as

$$6m + 2x = 4\,, \tag{29}$$

for some integer m. But this equation is equivalent to

$$3m + x = 2\,, \tag{30}$$

which, taken mod 3, becomes

$$x \equiv 2 \pmod 3\,. \tag{31}$$

The upshot of this is that we can arrive at the last equation by dividing (28) through by the number 2.