

Linear Congruence (Page 140)

CprE 310 Fall 2001

I have had several students ask about this and after trying repeatedly to justify what is in the book, I decided to prepare my own viewpoint on this. Here it is.

A linear congruence is defined as solutions to

$$a \cdot x \equiv b \pmod{m}$$

To show what these solutions look like, we can redefine the congruence condition to be

“m divides (ax-b)” which means that

$$\frac{a \cdot x - b}{m} = n \quad n = \dots -4, -3, -2, -1, 0, 1, 2, 3, 4, \dots$$

which has the solutions

$$a \cdot x = (n \cdot m + b) \quad n = \dots -4, -3, -2, -1, 0, 1, 2, 3, 4, \dots$$

#1 One way to solve this would be to simply code the equation

$$x = \frac{1}{a}(n \cdot m + b)$$

and vary n to get the integer values of x. This method seems to be the most computationally simple.

#2 Another solution would be to define a new congruence such that

$$c \equiv b \pmod{m}$$

which has the solutions (m divides c-b)

$$c = n \cdot m + b \quad n = 1, 2, 3, 4, \dots$$

The solutions for the integers x satisfy the condition

$$x = \frac{c}{a}$$

in other words, “a divides c.” This method is next in computational complexity.

#3 Another way to compute the solutions x, is to solve the condition

$$m \cdot \text{Frac}\left\{\frac{ax}{m}\right\} = b$$

Method #3 seems to be the most computationally complex because it takes so many values of x to find the ones that satisfy the equation.

Example 4 (Page 141)

$$a \cdot x = b \pmod{m}$$

$$a=3, b=4, m=7$$

#1 The solutions to

$$x = \frac{1}{3}(n \cdot 7 + 4)$$

$$x = \dots -15, -8, -1, 6, 13, 20, \dots$$

#2 The solutions to $c = 4 \pmod{7}$ are

$$c = n \cdot 7 + 4 \quad n=1, 2, 3, 4, \dots$$

$$c = 11, 18, 25, 32, 39, 46, 53, 60, \dots$$

The whole number solutions to “a divides c” are

$$\frac{18}{3} = 6 \qquad \frac{39}{3} = 13 \qquad \frac{60}{3} = 20$$

so the solutions for x (only illustrating the positive ones) are:

$$x = 6, 13, 20, \dots$$

#3 Using the fractional relationship

$$7 \cdot \text{Frac}\left\{\frac{3x}{7}\right\} = 4$$

gives (positive) solutions

$$x = 6, 13, 20, \dots$$

Problem 2.5-12 in the text.

$$a \cdot x = b \pmod{m}$$

$$a=2, b=7, m=17$$

#1 The solutions to

$$x = \frac{1}{2}(n \cdot 17 + 4)$$

$$x = \dots -39, -22, -5, 12, 29, 46, \dots$$

#2 The solutions to $c = 7 \pmod{17}$ are

$$c = n \cdot 17 + 7 \quad n=1, 2, 3, 4, \dots$$

$$c = \dots -78, -61, -44, -27, -10, 7, 24, 41, 58, 75, 92, \dots$$

The whole number solutions to "a divides c" are

$$\frac{-78}{2} = -39 \quad \frac{-44}{2} = -22 \quad \frac{-10}{2} = -5 \quad \frac{24}{2} = 12 \quad \frac{58}{2} = 29 \quad \frac{92}{2} = 46$$

so the solutions for x are:

$$x = \dots -39, -22, -5, 12, 29, 46, \dots$$

#3 Using the fractional relationship

$$17 \cdot \text{Frac}\left\{\frac{2x}{17}\right\} = 7$$

gives (positive) solutions

$$x = \dots, -5, 12, \dots$$