

$$\equiv \times \boxed{?} \equiv \pmod{\equiv}$$

It's not that I'm so smart, it's just that I stay with problems longer. – Albert Einstein

CHAPTER 14

Linear Congruences

14.1 Introduction

A **linear congruence equation** is a lot like an ordinary linear equation. Here is an example:

$$3x \equiv 2 \pmod{4}.$$

Definition: A **linear congruence equation** is a congruence that involves a variable raised only to the first power.

For the rest of this chapter, we simply refer to **linear congruence equations** as **linear congruences**. In general, for integers a and b , a modulus m , and a single variable x , a linear congruence can be expressed in the form

$$ax \equiv b \pmod{m},$$

though expressing a linear congruence in this form sometimes requires simplification as we will see.

Here are a few examples of linear congruences with their solutions:

$3x \equiv 2 \pmod{4}$	is satisfied by	$x \equiv 2 \pmod{4}$
$5y \equiv 7 \pmod{8}$	is satisfied by	$y \equiv 3 \pmod{8}$
$6x \equiv 5 \pmod{11}$	is satisfied by	$x \equiv 10 \pmod{11}$

There are also linear congruences with no solutions, such as

$$2x \equiv 1 \pmod{4}.$$

This chapter explores both how to determine when linear congruences have solutions and how to find any solutions they have.

CHAPTER 14. LINEAR CONGRUENCES

14.2 Modular Inverses and Simple Linear Congruences

Problems

Problem 14.1: Find all values of x that satisfy each of the following linear congruences.

- (a) $x - 3 \equiv 0 \pmod{4}$
- (b) $x - 2 \equiv 0 \pmod{4}$
- (c) $x - 1 \equiv 0 \pmod{4}$
- (d) $x + 1 \equiv 0 \pmod{4}$
- (e) $x + 2 \equiv 0 \pmod{4}$
- (f) $x + 3 \equiv 0 \pmod{4}$

Problem 14.2:

- (a) Find the smallest positive multiple of 4 that is 1 more than a multiple of 5.
- (b) Find all solutions to $4n \equiv 1 \pmod{5}$.

Problem 14.3: For each of the following linear congruences, find all solutions or show that there are none.

- | | |
|-----------------------------|-----------------------------|
| (a) $2x \equiv 1 \pmod{10}$ | (e) $6x \equiv 1 \pmod{10}$ |
| (b) $3x \equiv 1 \pmod{10}$ | (f) $7x \equiv 1 \pmod{10}$ |
| (c) $4x \equiv 1 \pmod{10}$ | (g) $8x \equiv 1 \pmod{10}$ |
| (d) $5x \equiv 1 \pmod{10}$ | (h) $9x \equiv 1 \pmod{10}$ |

Problem 14.4: In this problem we examine when an integer b cannot have an inverse modulo m .

- (a) Show that $\gcd(b, m)$ is a divisor of $bx - tm$ for any integers x and t .
- (b) Show that if there is some x such that $bx \equiv 1 \pmod{m}$, then $\gcd(b, m) \mid 1$.
- (c) Conclude that b^{-1} modulo m does not exist when $\gcd(b, m) > 1$.

Problem 14.5: Let r be a module-60 residue such that $\gcd(r, 60) = 1$.

- (a) Show that if $rx \equiv ry \pmod{60}$ for integers x and y , then x and y are members of the same modulo-60 residue class.
- (b) Show that when r is multiplied by each of the modulo-60 residues, no two of the products are congruent modulo 60.
- (c) Show that r has *exactly one* inverse modulo 60.

Problem 14.6: John bought n boxes of cookies containing 11 cookies each. On the way home from the store, John noticed that if he ate just one cookie, the total number of cookies remaining would be a multiple of 23. What is the smallest possible value of n ?

Extra! *Nothing endures but change.* – Heraclitus



14.2. MODULAR INVERSES AND SIMPLE LINEAR CONGRUENCES

Problem 14.1: Solve each of the following linear congruences.

- | | |
|-------------------------------|-------------------------------|
| (a) $x - 3 \equiv 0 \pmod{4}$ | (d) $x + 1 \equiv 0 \pmod{4}$ |
| (b) $x - 2 \equiv 0 \pmod{4}$ | (e) $x + 2 \equiv 0 \pmod{4}$ |
| (c) $x - 1 \equiv 0 \pmod{4}$ | (f) $x + 3 \equiv 0 \pmod{4}$ |

Solution for Problem 14.1: We could solve each linear congruence by plugging in all possible modulo-4 residues to find out which, if any, of them work. However, we know that we can add or subtract any integer to both sides of a congruence to produce another valid congruence. Adding 3 to both sides of the first congruence, we get


$$x \equiv 3 \pmod{4},$$

which describes all possible solutions for x : $\dots, -5, -1, 3, 7, \dots$

We add to or subtract from each side of each congruence in order to isolate the variable:

$$\begin{array}{ll} x - 2 \equiv 0 \pmod{4} & \Rightarrow x \equiv 2 \pmod{4} \\ x - 1 \equiv 0 \pmod{4} & \Rightarrow x \equiv 1 \pmod{4} \\ x + 1 \equiv 0 \pmod{4} & \Rightarrow x \equiv 3 \pmod{4} \\ x + 2 \equiv 0 \pmod{4} & \Rightarrow x \equiv 2 \pmod{4} \\ x + 3 \equiv 0 \pmod{4} & \Rightarrow x \equiv 1 \pmod{4} \end{array}$$

So, we have solutions to each of the simple linear congruences. \square

Concept:  In much the same way that we solve ordinary algebraic linear equations, we solve simple linear congruences by manipulating both sides of the congruence until the variable is isolated.

Unfortunately, not all of the same methods we use to solve algebraic equations are available in modular arithmetic. We need to develop other methods for solving more complicated linear congruences.

Problem 14.2: Find all solutions to $4n \equiv 1 \pmod{5}$.

Solution for Problem 14.2:

Bogus Solution: First, we find a multiple of 4 that is congruent to 1 (mod 5):



$$4n \equiv 1 \equiv 6 \equiv 11 \equiv 16 \pmod{5}.$$

Dividing both sides of $4n \equiv 16 \pmod{5}$ by 4, we get $n \equiv 4 \pmod{5}$.

Extra! *I have learned throughout my life as a composer chiefly through my mistakes and pursuits of false assumptions, not by my exposure to founts of wisdom and knowledge. – Igor Stravinsky*

CHAPTER 14. LINEAR CONGRUENCES

While the answer in the bogus solution is correct, the method is not. Division is not a valid operation in modular arithmetic. However, matching 1 with a congruent multiple of 4 was a good start! We note that

$$4 \cdot 4 \equiv 1 \pmod{5}.$$

We can use this fact to solve our original linear congruence. Multiplying both sides of $4n \equiv 1 \pmod{5}$ by 4 we get

$$16n \equiv 4 \pmod{5}.$$

But $16 \equiv 1 \pmod{5}$, so the left-hand side is $16n \equiv 1n \equiv n \pmod{5}$. Finally, our congruence becomes $n \equiv 4 \pmod{5}$, which are the solutions to the congruence $4n \equiv 1 \pmod{5}$. \square

WARNING!! Division is not defined in modular arithmetic!



Here's an example where division fails to find all the solutions to a linear congruence:

$$3x \equiv 3 \pmod{6}$$

Dividing both sides of this linear congruence by 3, we get $x \equiv 1 \pmod{6}$. While these solutions satisfy the original linear congruence, so do $x \equiv 3 \pmod{6}$ and $x \equiv 5 \pmod{6}$.

Without the operation of division available to us, we used multiplication to solve Problem 14.2. We multiplied 4 by a number we found (which happened also to be 4) to get 1 (mod 5). In other words, we multiplied 4 by its inverse modulo 5 in order to isolate the variable n .

Definition: A **modular inverse** of an integer b modulo m is an integer b^{-1} such that

$$b \cdot b^{-1} \equiv 1 \pmod{m}.$$

More simply, we refer to b^{-1} as an **inverse**.

For instance, using the modulo-5 multiplication table at right, we find inverses of some modulo-5 residues:

$$1^{-1} \equiv 1 \pmod{5}$$

$$2^{-1} \equiv 3 \pmod{5}$$

$$3^{-1} \equiv 2 \pmod{5}$$

$$4^{-1} \equiv 4 \pmod{5}$$

	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Note that 1 is its own inverse with any modulus because $1 \cdot 1 \equiv 1 \pmod{m}$. Also, $0 \cdot x \equiv 0 \pmod{m}$, so 0 never has an inverse with any modulus.

Extra! *The sorcery and charm of imagination, and the power it gives to the individual to transform his world into a new world of order and delight, makes it one of the most treasured of all human capacities. – Frank Barron*

14.2. MODULAR INVERSES AND SIMPLE LINEAR CONGRUENCES

Problem 14.3: Find the inverses of all modulo-10 residues that have inverses.

Solution for Problem 14.3: We write out an entire modulo-10 multiplication table to be sure we find all the inverses of modulo-10 residues (and thus all integers modulo 10):

	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9
2	0	2	4	6	8	0	2	4	6	8
3	0	3	6	9	2	5	8	1	4	7
4	0	4	8	2	6	0	4	8	2	6
5	0	5	0	5	0	5	0	5	0	5
6	0	6	2	8	4	0	6	2	8	4
7	0	7	4	1	8	5	2	9	6	3
8	0	8	6	4	2	0	8	6	4	2
9	0	9	8	7	6	5	4	3	2	1

From the modulo-10 multiplication table, we find that

$$1^{-1} \equiv 1 \pmod{10}$$

$$3^{-1} \equiv 7 \pmod{10}$$

$$7^{-1} \equiv 3 \pmod{10}$$

$$9^{-1} \equiv 9 \pmod{10}$$

and that there is no inverse modulo 10 for 0, 2, 4, 5, 6, or 8.

□

Problem 14.4: Prove that b^{-1} modulo m does not exist when $\gcd(b, m) > 1$.

Solution for Problem 14.4: When b^{-1} exists, it's the solution to the linear congruence

$$bx \equiv 1 \pmod{m}.$$

This means that for some value of x ,

$$bx - tm = 1,$$

for some integer t . Now, let $d = \gcd(b, m)$. Thus, $d \mid bx$ and $d \mid tm$. Since a divisor of two integers is a divisor of their difference,

$$d \mid (bx - tm).$$

But we know that $bx - tm = 1$, so $d \mid 1$. Hence $d = 1$. Thus, when b^{-1} exists, the GCD of b and m is 1. So, when $\gcd(b, m) > 1$, b^{-1} does not exist. □

Important: If $\gcd(b, m) > 1$, then b does not have an inverse modulo m .



In Problem 14.3, we found that each modulo-10 residue that is relatively prime to 10 has an inverse. In fact, every modulo-10 residue appears as a product in each row and column (of the modulo-10 multiplication table) started with a multiplicand that is relatively prime to 10.

Problem 14.5: Let r be a modulo-60 residue such that $\gcd(r, 60) = 1$. Show that r has an inverse modulo 60.

Solution for Problem 14.5: Let x and y be integers such that $rx \equiv ry \pmod{60}$. Thus,

$$rx - ry = r(x - y) = 60t$$

CHAPTER 14. LINEAR CONGRUENCES

for some integer t . This means that $60 \mid r(x - y)$. But, since $\gcd(r, 60) = 1$, we know that $60 \mid (x - y)$. Thus, $x \equiv y \pmod{60}$. This means that when $x \not\equiv y \pmod{60}$, we have $rx \not\equiv ry \pmod{60}$. So, when we multiply r by each of the modulo-60 residues, none of the products are equivalent modulo 60 to each other. This means that each product is equivalent to a different modulo-60 residue, one of which is 1. Thus, *exactly one* of the modulo-60 residues is an inverse modulo 60 of r . \square

Notice that in Problem 14.5, nothing in our solution depended specifically on the number 60. We can just as easily replace 60 with any modulus m and our solution shows that when r and m are relatively prime, r^{-1} modulo m exists. Combining this with the fact that residues not relatively prime with m don't have inverses modulo m , we summarize our work:

Important: For a given modulus m , a residue r has a single modulo- m residue that is an inverse of r modulo m if and only if $\gcd(m, r) = 1$. Otherwise, r has no inverse modulo m .

Note that when the modulus m is prime, every residue other than 0 is relatively prime to the modulus, thus every nonzero residue has an inverse modulo m .

Problem 14.6: John bought n boxes of cookies containing 11 cookies each. On the way home from the store, John noticed that if he ate just one cookie, the total number of cookies remaining would be a multiple of 23. What is the smallest possible value of n ?

Solution for Problem 14.6: John bought $11n$ cookies where $11n \equiv 1 \pmod{23}$. Our goal is to find the smallest positive integer n that satisfies the congruence. Our answer will be the inverse of 11 modulo 23.

Solution 1: We add multiples of 23 to 1 until we reach an integer that is a multiple of 11:

$$1 \equiv 24 \equiv 47 \equiv 70 \equiv 93 \equiv 116 \equiv 139 \equiv 162 \equiv 185 \equiv 208 \equiv 231 \pmod{23}.$$

Since $11 \cdot 21 = 231 \equiv 1 \pmod{23}$, 21 is the inverse of 11 modulo 23.

Solution 2: While looking for an integer n such that $11n \equiv 1 \pmod{23}$, we find that

$$11 \cdot 2 \equiv -1 \pmod{23}.$$

Multiplying both sides of the congruence by -1 and organizing, we get

$$11 \cdot (-2) \equiv 1 \pmod{23}.$$

Since $-2 \equiv 21 \pmod{23}$, we have $11 \cdot 21 \equiv 1 \pmod{23}$. So 21 is the inverse of 11 modulo 23. \square

Exercises

14.2.1 Find all solutions to each of the following linear congruences.

- | | |
|-----------------------------------|---------------------------------|
| (a) $x - 5 \equiv 2 \pmod{3}$ | (c) $5x \equiv 1 \pmod{11}$ |
| (b) $x + 223 \equiv 114 \pmod{8}$ | (d) $2x + 17 \equiv 0 \pmod{9}$ |

14.2.2 Find the inverses modulo 11 for the residues 1-10 inclusive.

14.2.3 Which modulo-15 residues have inverses?

14.2.4★ Prove that an integer cannot have more than one inverse for a given modulus.