

Math Level 2.5 Handouts

Dylan Yu

June 10, 2020

Contents

1	Linear Congruences	2
1.1	Definitions	2
1.2	Examples	2
1.3	Fractions in Modular Arithmetic	3
1.4	Modular Inverses	4
1.5	Problems	6

1 Linear Congruences

1.1 Definitions

A **linear congruence equation** is like an ordinary linear equation, but instead we use **congruences**. For example,

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

Most linear congruences take on the form $ax \equiv b \pmod{m}$. Today we will discuss how to solve them.

1.2 Examples

Example 1.1. What x satisfies

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

Solution. If we plug in 0, it doesn't work. If we plug in 1, it doesn't work. However, if we plug in 2, we get

$$3 \cdot 2 = 6 \equiv 2 \pmod{4}.$$

The next one that works is 6, and the next one is 10, and so on. All of these are in the form $\boxed{2 \pmod{4}}$, so this is our answers. \square

Example 1.2. What x satisfies

$$5x \equiv 7 \pmod{8}?$$

Solution. Let us add 8 to the right hand side, which we can do because 8 is the modulo:

$$5x \equiv 15 \pmod{8}.$$

If we divide by 5, we get

$$x \equiv \boxed{3 \pmod{8}}.$$

\square

Note that **we cannot always divide**. For example, if we had

$$5x \equiv 7 \pmod{8},$$

and divided by 5, we would get

$$x \equiv \frac{7}{5} \pmod{8},$$

which doesn't make much sense. So when do we know when we can divide?

Theorem 1.1 (Modular Division Rule). If

$$ka \equiv kb \pmod{m},$$

and k and m are relatively prime, then

$$a \equiv b \pmod{m}.$$

Example 1.3. What x satisfies

$$6x \equiv 5 \pmod{11}?$$

Solution. If we add 55 to the right hand side, we get

$$6x \equiv 5 + 55 = 60 \pmod{11},$$

and divide by 6, we get

$$x \equiv \boxed{10 \pmod{11}}.$$

□

1.3 Fractions in Modular Arithmetic

Let us go back to the equation

$$x \equiv \frac{7}{5} \pmod{8}.$$

What does $\frac{7}{5}$ actually equal?

Example 1.4. Prove that

$$\frac{7}{5} \equiv 3 \pmod{8}.$$

Solution. If we multiply by 5 on both sides, we get

$$7 \equiv 15 \pmod{8},$$

which is obviously true.

□

So it seems that fractions can become integers in modular arithmetic.

Example 1.5. Find $\frac{14}{3} \pmod{4}$.

Solution. Let $x = \frac{14}{3}$. Then

$$x \equiv \frac{14}{3} \pmod{4},$$

$$3x \equiv 14 \pmod{4},$$

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

If we add 4 to the right hand side, we get

$$3x \equiv 2 + 4 = 6 \pmod{4},$$

and dividing by 3 we get

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

□

The idea here is to **assign a variable to the fraction**. This way, we can easily solve for the fraction.

Example 1.6. Find $\frac{12}{5} \pmod{7}$.

Solution. Let $x = \frac{12}{5}$. Then

$$x \equiv \frac{12}{5} \pmod{7},$$

$$5x \equiv 12 \pmod{7},$$

and subtracting 7 from the right hand side we get

$$5x \equiv 5 \pmod{7},$$

$$x \equiv \boxed{1 \pmod{7}}.$$

□

1.4 Modular Inverses

Let us start with an example:

Example 1.7. If $x \equiv 5 \pmod{6}$, then what is $\frac{1}{x} \pmod{6}$?

Solution. Notice that

$$x \equiv 5 \pmod{6}.$$

This means if we divide both sides by 5x, we get

$$\frac{1}{5} \equiv \frac{1}{x} \pmod{6}.$$

Now we only need to find $\frac{1}{5} \pmod{6}$. If we let $x = \frac{1}{5}$, we get

$$x \equiv \frac{1}{5} \pmod{6},$$

$$5x \equiv 1 \pmod{6},$$

$$5x \equiv 1 - 6 = -5 \pmod{6},$$

$$x \equiv -1 \equiv \boxed{5 \pmod{6}}.$$

□

Let us look at the definition of a modular inverse:

Definition 1.1 (Modular Inverse). A **modular inverse** of an integer b modulo m is an integer b^{-1} such that

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

Example 1.8. Find $5^{-1} \pmod{6}$.

Solution. Notice this is the exact same problem as the last example. However, this time we know that

$$5 \cdot 5^{-1} \equiv 1 \pmod{6}.$$

If $x = 5^{-1}$, then

$$5x \equiv 1 \pmod{6}.$$

If we try values for x , we get $x = \boxed{5 \pmod{6}}$. □

Here is another (**very**) important theorem to keep in mind while solving congruences:

Theorem 1.2 (Congruence Existence Theorem). The congruence $ax \equiv b \pmod{m}$ has **no solutions** when $\gcd(a, m) \nmid b$.

And this one is similar to the one we had before:

Theorem 1.3 (Congruence Property). If $ak \equiv bk \pmod{mk}$ for integers a and b , then $a \equiv b \pmod{m}$.

Using these two, we have this general idea:

1. First, we organize any linear congruence into the form

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

where x is the variable.

2. A linear congruence $ax \equiv b \pmod{m}$ has solutions if and only if $\gcd(a, m) \mid b$.
3. If $\gcd(a, m) \mid b$, then we let $d = \gcd(a, m)$ and rewrite the linear congruence using $a = a_1d$, $b = b_1d$, and $m = m_1d$:

$$a_1dx \equiv b_1d \pmod{m_1d}.$$

This linear congruence has the same solutions as $a_1x \equiv b_1 \pmod{m_1}$.

Let us try an example using this:

Example 1.9. Solve for x in

$$9x + 4 \equiv 10 \pmod{12}.$$

Solution. Let us subtract 4 from both sides to get

$$9x \equiv 6 \pmod{12}.$$

Note that $\gcd(9, 12) = 3$, and $4 \mid 6$. The linear congruence $9x \equiv 6 \pmod{12}$ has solutions then. We can now divide by 3, to get

$$\frac{9}{3}x \equiv \frac{6}{3} \pmod{\frac{12}{3}},$$

which gives us

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

From here we can easily add 4 to right hand side to get $3x \equiv 6 \pmod{4}$, which means

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

□

1.5 Problems

Problem 1.1. Find the inverses of 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 in mod 10.

Problem 1.2. Find all solutions to


$$5x \equiv 1 \pmod{11}.$$


Problem 1.3. What numbers in modulo 15 have inverses?

Problem 1.4. Find all solutions to $48x - 115 \equiv 291 \pmod{13}$.

Problem 1.5. Find all solutions to $56x + 43 \equiv 211 \pmod{96}$.


Problem 1.6. John bought n boxes of cookies containing 11 cookies each. On the way home from the store, John notice 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 .

 **Problem 1.7.** Find all positive integers that leave a remainder of 2 when divided by 5 and a remainder of 6 when divided by 7. How many three-digit positive integers leave a remainder of 2 when divided by 5 and a remainder of 6 when divided by 7?

 **Problem 1.8.** Solve for N in

$$4N \equiv 3 \pmod{7},$$

$$5N \equiv 7 \pmod{8}.$$

 **Problem 1.9.** What can squares be in mod 4?

 **Problem 1.10.** The integer p is a 50-digit prime number. When its square is divided by 120, the remainder is not 1. What is the remainder?