

## 9.1 Linear Congruence

We are all familiar with linear equations like

$$ax + b = 0$$

We are going to talk about a different kind of linear “equation” known as linear congruence. They are of the form

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

Let’s consider some linear congruence. First, we look at  $3x \equiv 1 \pmod{6}$ . If we try everything from 0 to 5, it is easy to notice that this does not have a solution.

How about  $2x \equiv 4 \pmod{6}$ . We have one solution  $\{2, 8, 14, \dots\}$  and another solution  $\{5, 11, 17, \dots\}$ . In total, we have two solutions. Further, these two solution sets are incongruent because elements from one set is not congruent to those from the other set modulo 6.

$2x \equiv 5 \pmod{6}$  does not have a solution. But  $3x \equiv 1 \pmod{5}$  have the solution  $\{2, 7, 12, \dots\}$ .

The two examples that do not have a solution are  $3x \equiv 1 \pmod{6}$  and  $2x \equiv 5 \pmod{6}$ . The ones that do have solutions are  $2x \equiv 4 \pmod{6}$  and  $3x \equiv 1 \pmod{5}$ . From these examples, we make the observation that one thing in common among the linear congruences that do not have a solution is that the GCD of  $a$  and  $m$  does not divide  $b$ . In particular, we have that  $\gcd(3, 6) \nmid 1$  and  $\gcd(2, 6) \nmid 5$ . On the other hand,  $\gcd(2, 6) \mid 4$  and  $\gcd(3, 5) \mid 1$ .

We can generalize this into the following theorem:

**Theorem 9.1.** Let  $ax \equiv b \pmod{m}$  be a linear congruence in one variable and let  $d = \gcd(a, m)$ . If  $d \nmid b$ , then the linear congruence has no solution in  $\mathbb{Z}$ . If  $d \mid b$ , then the linear congruence has exactly  $d$  incongruent solutions modulo  $m$  in  $\mathbb{Z}$ .

The proof can be broken into two parts:

- (1) Showing that if  $d \nmid b$ , then the linear congruence has no solution. This can be proved using the contrapositive of the original statement (namely, if the linear congruence has solution, then  $d \mid b$ );
- (2) Showing that if  $d \mid b$ , then the linear congruence has a solution,  $x_0$ . And given a solution  $x_0$ , we can construct infinitely many solutions of a given form and that among those infinitely many solutions, we have  $d$  incongruent solutions. More specifically, it suffices to show the following:
  - a. Show that a solution  $x_0$  exists.
  - b. Given a solution  $x_0$ , show that  $ax \equiv b \pmod{m}$  has infinitely many solutions in  $\mathbb{Z}$  of a given form.
  - c. Given a solution  $x_0$ , show that every solution has the form in (b).
  - d. Show that there are  $d$  incongruent solutions.

**Proof.** We begin the proof by proving Part (1) by its contrapositive.

Assume that  $ax \equiv b \pmod{m}$  has a solution. By definition of congruence,  $m \mid ax - b$ . By definition of divisibility,  $m \mid ax - b$  iff there exists some  $y \in \mathbb{Z}$  such that  $my = ax - b$ . This, in turn, is true iff  $ax - my = b$  has a solution. Since  $d$  is the gcd of  $a$  and  $m$ ,  $d \mid a$  and  $d \mid m$ . By Proposition 2.2, it follows that  $d \mid ax - my$ . Since  $b = ax - my$  iff  $ax \equiv b \pmod{m}$  has a solution,  $d \mid b$  if the original linear congruence has a solution.

Now we proceed to prove Part (2)a. Assume  $d \mid b$ . Since  $d$  is the gcd of  $a$  and  $m$ , by Proposition 4.2, there exists  $r, s \in \mathbb{Z}$  such that

$$d = ar + ms$$

Further,  $d \mid b$  implies  $b = de$  for some  $e \in \mathbb{Z}$ . So, by substitution

$$b = de = (ar + ms)e = a(re) + m(se)$$

which clearly suggests a solution with  $x = re$  and  $y = -se$  that solves  $ax - my = b$  (and thus solves  $ax \equiv b \pmod{m}$ ).

For Part (2)b, let  $x_0$  be an arbitrary solution for the linear congruence  $ax \equiv b \pmod{m}$ . Let  $n \in \mathbb{Z}$  and we consider

$$x = x_0 + \left(\frac{m}{d}\right)n$$

Since  $d \mid m$ ,  $\frac{m}{d}$  is an integer, so it follows that  $x$  is also an integer. Furthermore, we observe that

$$\begin{aligned} a\left(x_0 + \left(\frac{m}{d}\right)n\right) &= ax_0 + a\left(\frac{m}{d}\right)n \\ &= ax_0 + \left(\frac{a}{d}\right)mn \\ &\equiv ax_0 \pmod{m} \\ &\equiv b \pmod{m} \end{aligned}$$

Since for every solution  $x$ ,  $ax \equiv b \pmod{m}$  but also  $b \equiv a(x_0 + (\frac{m}{d})n) \pmod{m}$ , for all  $n \in \mathbb{Z}$ ,

$$x_0 + \left(\frac{m}{d}\right)n$$

is also a solution to  $ax \equiv b \pmod{m}$ . ■