

## CHAPTER II: CONGRUENCES

### Section 1: Linear Congruences

After discussing primes and divisibility, the next natural topic is the theory of congruences. Introduced by Carl Friedrich Gauss in 1801, congruences are a convenient way to describe divisibility. They also provide us a powerful tool in fields of mathematics such as theory of equations, algebraic number theory, and cryptography.

**Definition 2.1.1** Let  $a$  and  $b$  be integers. We say  $a$  *is congruent to  $b$  modulo  $m$*  if  $m \mid (b - a)$ . (Recall that this notation means “ $m$  divides  $b - a$ ”.) This is denoted by  $a \equiv b \pmod{m}$ . The integer  $m$  is called the *modulus*.

**Example 2.1.2** Since 5 divides the difference of 31 and 1, we have that  $31 \equiv 1 \pmod{5}$ .

If we divide an integer  $a$  by a modulus  $m$ , we get a quotient and a remainder (by the Division Algorithm). In symbols,

$$a = mq + r \quad (\text{for } 0 \leq r < m)$$

Clearly, the difference  $a - r$  is a multiple of the modulus  $m$ , so  $a \equiv r \pmod{m}$ . Therefore, every integer is congruent modulo  $m$  to some integer between 0 and  $m - 1$  (inclusive).

Congruences with the same modulus have many of the same properties as equations. For example,

$$\begin{aligned} \text{if } a \equiv b \pmod{m} \text{ and } c \equiv d \pmod{m}, \text{ then} \\ a \pm c \equiv b \pm d \pmod{m}, \text{ and} \\ ac \equiv bd \pmod{m}. \end{aligned}$$

So we can add, subtract, and multiply congruences with the same modulus. It is not always possible to divide like congruences however. Notice that  $12 \cdot 2 \equiv 9 \cdot 2 \pmod{6}$  and  $2 \equiv 2 \pmod{6}$  but 12 is not congruent to 9 (mod 6). We shall soon see when you can “cancel out” common factors.

**Linear congruences** are congruences with unknowns to the first power. Their general form is  $ax \equiv b \pmod{m}$ . By the above discussion, many of these can be solved in much the same way that linear equations can be solved.

**Example 2.1.3** Solve  $x + 6 \equiv 2 \pmod{15}$ .

Subtracting 6 from both sides yields  $x \equiv -4 \pmod{15}$ . This is the same as  $x \equiv 11 \pmod{15}$  since  $-4$  and 11 are the same modulo 15 (their difference is divisibly by 15).

**Example 2.1.4** Solve  $4x \equiv 3 \pmod{19}$ .

Since we do not have division, we must get creative. Multiplying both sides by 5 yields  $20x \equiv 15 \pmod{19}$  which is the same as  $x \equiv 15 \pmod{19}$  since 20 is congruent to 1 modulo 19.

Notice that when solving a congruence modulo  $m$ , we are looking for the integer(s) between 0 and  $m-1$  inclusive that satisfy the given congruence. So another technique we could use, albeit not very efficiently, is to substitute each possible value into the congruence and check.

**Example 2.1.5** Solve  $x^2 + 3x \equiv 3 \pmod{5}$ .

By substituting the  $x$ -values 0,1,2,3, and 4 we see that  $x \equiv 3 \pmod{5}$  and  $x \equiv 4 \pmod{5}$  are the two solutions.

Of course there are congruences that have no solutions. For example, if the congruence  $4x \equiv 91 \pmod{130}$  had a solution, 130 would have to divide  $4x-91$ . But  $4x-91$  is always odd, therefore it cannot be divisible by an even number. Before getting to the general theory of solving linear congruences, let's do another example.

**Example 2.1.6** Solve  $12x \equiv 8 \pmod{20}$ .

To solve this, we are looking for a value of  $x$  such that 20 divides  $12x-8$ . In other words, we are looking for an  $x$ -value such that  $12x-8=20y$  for some  $y$ . This can be rewritten as  $12x-20y=8$ . This is an example of a class of equations called Diophantine equations after the third century Greek mathematician Diophantus. Simply by checking every value from 0 to 19, we see that one answer is  $x \equiv 4 \pmod{20}$ . In fact, there are four solutions, 4, 9, 14, and 19. What we seek is a general method.

Consider the linear congruence  $ax \equiv b \pmod{m}$ , and let  $d = \gcd(a, m)$ . In Section 1.2 we saw that we could write  $d$  as a linear combination of  $a$  and  $m$  (Theorem 1.2.3). In fact, in the proof of that theorem, we saw that *every* linear combination of  $a$  and  $m$  is a multiple of  $d$ . We'll use that fact now. As we saw in the last example, solving the linear congruence  $ax \equiv b \pmod{m}$  is equivalent to solving  $ax-b=my$  which is equivalent to solving the Diophantine equation  $ax-my=b$ . (Since  $x, y$  are integers, we could just as easily write  $ax+my=b$ .) As we just noted, this will only be possible if  $b$  is a multiple of  $d$ . So we have the following theorem.

**Theorem 2.1.7 (Linear Congruence Theorem)** Let  $a$ ,  $b$ , and  $m$  be integers with  $m \geq 1$  and let  $d = \gcd(a, m)$ . The linear congruence  $ax \equiv b \pmod{m}$  has solutions if and only if  $d \mid b$ .

In fact, we can say even more than this theorem tells us. If  $d \mid b$ , we will have  $d$  distinct solutions to the linear congruence  $ax \equiv b \pmod{m}$ . To find them, first solve the Diophantine equation  $ax + my = d$  for  $x$  and  $y$ . The first solution to the related congruence is then  $\frac{bx}{d}$ . The remaining solutions can be determined by adding multiples of  $\frac{m}{d}$  (and reducing modulo  $m$  when necessary). Let's see this in action.

**Example 2.1.8** Solve  $6x \equiv 3 \pmod{15}$

The  $\gcd(6,15) = 3$ , which divides 3 so there are solutions, in fact there are exactly three distinct (i.e. incongruent) solutions. To find the first, we need to solve  $6x + 15y = 3$  for  $x$  and  $y$ . Using the Euclidean algorithm we see that

$$\begin{aligned} 15 &= 6 \cdot 2 + 3 \\ 6 &= 3 \cdot 2 \end{aligned}$$

This confirms that  $\gcd(6,15) = 3$  but it also helps us find  $x$  and  $y$  from the Diophantine equation. Clearly,  $6 \cdot (-2) + 15 \cdot (1) = 3$ , so  $x = -2$  and  $y = 1$ . The first solution is therefore  $x = \frac{3(-2)}{3} = -2 \equiv 13 \pmod{15}$ . By repeatedly adding  $\frac{15}{3} = 5$  (and reducing when necessary) we find the other solutions of  $x \equiv 18 \equiv 3 \pmod{15}$  and  $x \equiv 8 \pmod{15}$ .

**Example 2.1.9** Solve  $4x \equiv 41 \pmod{111}$ .

Since 4 and 111 are relatively prime,  $\gcd(4,111) = 1$ . This implies that we have a unique solution. To find it, we must solve the Diophantine equation  $4x + 111y = 1$ . Again using the Euclidean algorithm,

$$\begin{aligned} 111 &= 4 \cdot 27 + 3 \\ 4 &= 3 \cdot 1 + 1 \\ 3 &= 1 \cdot 3 \end{aligned}$$

Working in reverse, we get that  $1 = 4 \cdot (28) + 111 \cdot (-1)$ . So the first (and only) solution is  $x \equiv \frac{41 \cdot 28}{1} = 1148 \equiv 38 \pmod{111}$ .

**Exercise 2.1.10** Solve  $10x \equiv 30 \pmod{150}$ .

**Exercise 2.1.11** Solve  $6x \equiv 9 \pmod{33}$ .

**Exercise 2.1.12** Solve  $12x \equiv 4 \pmod{1000}$ .

**Exercise 2.1.13** Solve  $31x \equiv 409 \pmod{2311}$ .