Section 5. Linear Congruences

Note. In this section, we consider congruence relations of the form $ax \equiv b \pmod{m}$. We give conditions under which solutions do and do not exist and we enumerate the number of solutions.

Definition. A *linear congruence* is a congruence relation of the form $ax \equiv b \pmod{m}$ where $a, b, m \in \mathbb{Z}$ and $m > 0$. A *solution* is an integer x which makes the congruence relation true AND x is a least residue (mod m) (that is, $0 \leq x \leq m-1$).

Note. The congruence relation $ax \equiv b \pmod{m}$ has a solution if the ("unknown") integers x (where $0 \leq x \leq m-1$) and k satisfy $ax = b + km$. But this is a linear Diophantine equation in the unknowns x and k. Theorem 3.1 shows how to solve linear Diophantine equations, so we will apply this here.

Note. If integer r is a solution to $ax \equiv b \pmod{m}$, then there are infinitely many other integers x that also satisfy the equation since for each $x = r + km$ and for all integers k we have: $a(r + km) = ar + km \equiv ar \pmod{m} \equiv b \pmod{m}$.

Exercise 5.1. Construct congruences modulo 12 with no solutions, just one solution, and more than one solution.

Solution. Consider $2x \equiv 1 \pmod{12}$. Since $2x$ is even for all $x \in \mathbb{Z}$, but any number which is 1 (mod 12) is odd, then there are no solutions to this equation.

Consider $x \equiv 1 \pmod{12}$. The unique solution is $x = 1$.

Consider $2x \equiv 2 \pmod{12}$. Then $x = 1$ and $x = 7$ are solutions. □

Note. We want to quantify the number of solutions for a linear congruence. This is accomplished in Theorem 5.1, which is based on the next three lemmas.

Lemma 5.1. If $(a, m) \nmid b$ then $ax \equiv b \pmod{m}$ has no solutions.

Note. With $a = 2$, $b = 1$, and $m = 12$, we see that $(a, m) = (2, 12) = 2$. So $(a, m) = 2 \nmid 1 = b$, and by Lemma 5.1 we see (again) that $2x \equiv 1 \pmod{12}$ has no solution.

Lemma 5.2. If $(a, m) = 1$ then $ax \equiv b \pmod{m}$ has exactly one solution.

Note 5.A. In the proof of Lemma 5.2, we showed that two least residues modulo m are congruent (mod m) then they are equal. We will use the idea again.

Note 5.B. Before we state the result giving the number of solutions to $ax \equiv b$ (mod m), we explain some techniques of solving such equations. We can manipulate the equation until cancellation is a possibility. For example, to solve $4x \equiv 1 \pmod{15}$, can can equivalently consider the equation $4x \equiv 16 \pmod{15}$ which has the unique solution $x = 4$; uniqueness follows from Lemma 5.2. As another example, consider $14x \equiv 27 \pmod{31}$ (which also has a unique solution by Lemma 5.2). First we consider the equivalent equation $14x \equiv 27 + 31 \equiv 58 \pmod{31}$, and we can cancel a factor of 2 to get $7x \equiv 29 \pmod{31}$. We continue adding multiples of 31 until we can cancel the 7: $7x \equiv 29 \equiv 31 \equiv 91 \pmod{31}$. We then have that $x = 13$ as the solution.

Note 5.C. We can use this method to solve linear Diophantine equations $ax+by = c$. This single equation implies the two linear congruences $ax \equiv c \pmod{b}$ and $by \equiv c \pmod{a}$. Solving one equation with the method described in Note 5.B leads to the solution of the original equation.

Example 5.4. Solve (a) $8x \equiv 1 \pmod{15}$, and (b) $9x + 10y = 11$.

Solution. (a) We modify $8x \equiv 1 \pmod{15}$ to $8x \equiv 1 + 15 \equiv 16 \pmod{15}$, and then we can divide out the common factor of 8 to get the solution $x = 2$.

(b) The linear Diophantine equation $9x + 10y = 11$ implies the two linear congruences $9x \equiv 11 \pmod{10}$ and $10y \equiv 11 \pmod{9}$. The second linear congruence can be solved as $10y \equiv 11 \equiv 11 + 9 \equiv 20 \pmod{9}$, and we can cancel a factor of 10 to get $y = 2$ as the solution or, more generally, $y \equiv 2 \pmod{9}$. So we take $y = 2+9t$ where t is an integer. Substituting this into the linear Diophantine equation give $9x + 10(2 + 9t) = 11$ or $9x = 11 - 20 - 90t = -9 - 90t$ or $x = -1 - 10t$ where t is an integer. So all the solutions to the linear Diophantine equation are given by $x = -1 - 10t$ and $y = 2 + 9t$ where $t \in \mathbb{Z}$.

Note. In each of the examples above of the form $ax \equiv b \pmod{m}$, we have the greatest common divisor $(a, m) = 1$. In the event that $(a, m) \neq 1$, we can apply Theorem 4.5. For example, with $6x \equiv 15 \pmod{33}$ we have $(a, m) = (6, 33) = 3$ and by Theorem 4.5 (with $c = 3$) we have $2x \equiv 5 \pmod{11}$. With the method of Note 5.B, we get $2x \equiv 5 \equiv 5+11 \equiv 16 \pmod{11}$ and so $x = 8$ is the solution to this equation. All values of x which satisfy this equation are of the form $x \equiv 8 \pmod{11}$. So the solutions to the original equation (which we take modulo 33) $6x \equiv 15 \pmod{33}$ are $x = 8, 19, 30$. Notice that we get 3 solutions and $(a, m) = 3$. This is not a coincidence, as we now show.

Lemma 5.3. Let $d = (a, m)$. If $d \mid b$ then $ax \equiv b \pmod{m}$ has exactly d solutions.

Note. Lemmas 5.1, 5.2, and 5.3 combine to yield the following result which gives the number of solutions to $ax \equiv b \pmod{m}$ in terms of the greatest common divisor (a, m).

Theorem 5.1. The linear congruence $ax \equiv b \pmod{m}$ has no solutions if $(a, m) \nmid b$. If $(a, m) \mid b$ then there are exactly (a, m) solutions.

Note 5.D. We now turn out attention to the Chinese Remainder Theorem. The first known reference to a problem related to the Chinese Remainder Theorem is in Sun Zi's *Sunzi suanjing* (in English, "Sun Zi's Mathematical Manual"). It is estimated that Sun Zi lived between about 400 and 460, but little is known about him and these dates are debatable. In Problem 26 of Chapter 3, Sun Zi states the following problem:

> "Suppose we have an unknown number of objects. When counted in threes, 2 are left over, when counted in fives, 3 are left over, and when counted in sevens, 2 are left over. How many objects are there?"

(This historical information on Sun Zi is from the MacTutor History of Mathematics Archive biography on Sun Zi, accessed 10/1/2021.) With x as the number of objects, this problem translates into solving the three congruences:

$$x \equiv 1 \pmod{3}, \quad x \equiv 2 \pmod{5}, \quad \text{and} \quad x \equiv 3 \pmod{7}.$$

Note. We now solve Sun Zi's problem. The first congruence $x \equiv 1 \pmod{3}$ implies that $x = 1 + 3k_1$ for some $k_1 \in \mathbb{Z}$. With this in the second congruence, we have $1 + 3k_1 \equiv 2 \pmod{5}$ which implies (by the method of Note 5.B) that $k_2 \equiv 2 \pmod{5}$, or that $k_1 = 2 + 5k_2$ where $k_2 \in \mathbb{Z}$. Then $x = 1 + 3k_1 = 1 + 3(2 + 5k_2) = 7 + 15k_2$ satisfies the first two congruences. This then requires from the third congruence that $x = 5 + 15k_2 \equiv 3 \pmod{7}$, or (reducing modulo 7) $k_2 \equiv 3 \pmod{7}$, or that $k_2 = 3 + 7k_3$ where $k_3 \in \mathbb{Z}$. Then $x = 7 + 15k_2 = 7 + 15(3 + 7k_3) = 52 + 105k_3$ where $k_3 \in \mathbb{Z}$ satisfies all three congruences. That is, $x \equiv 52 \pmod{105}$ satisfies the system of linear congruences. Notice that 105 is the product of 3, 5, and 7 (and these are pairwise relatively prime). The Chinese Remainder Theorem addresses this type of problem.

Theorem 5.2. The Chinese Remainder Theorem.

The system of congruences $x \equiv a_i \pmod{m_i}$ for $i = 1, 2, \ldots, k$, where $(m_i, m_j) = 1$ if $i \neq j$, has a unique solution modulo $m_1 m_2 \cdots m_k$.

Revised: 1/30/2024