3.3 Linear Congruence Equations

Definition 3.3.1. Let $a_1, a_2, \ldots, a_k, b$ be known integers. An equation of the form

$$a_1x_1 + a_2x_2 + \cdots a_kx_k \equiv b \pmod{n}$$

with unknowns $x_1, x_2, \ldots, x_k$ is called a **linear congruence equation** in k variables.

An example of a linear congruence equation $ax + by + cz \equiv e \pmod{n}$ in the 3 variables x, y, z follows:

Example 1. Consider the linear congruence equation

$$2x + 3y - z \equiv 5 \pmod{11}.$$

Note that $x = 4, y = 3, z = 1$ is a solution to this congruence equation. Furthermore, for any integers i, j, k if $i \equiv 4 \pmod{11}$, $j \equiv 3 \pmod{11}$ and $k \equiv 1 \pmod{11}$, then $x = i, y = j, z = k$ will also be a solution to the above congruence equation.

Definition 3.3.2. Let $n \geq 1$. We shall write $x \equiv a_1, a_2, \ldots, a_k \pmod{n}$ to mean that $x \equiv a_i \pmod{n}$ for some integer a_i in the list $a_1, a_2, \ldots, a_k$.

Example 2. We write $x \equiv 2, 4, 6 \pmod{8}$ to mean either $x \equiv 2 \pmod{8}$ or $x \equiv 4 \pmod{8}$ or $x \equiv 6 \pmod{8}$.

Theorem 3.3.3 (Expand-Collapse Theorem)**.** Let d and k be any positive integers. Then for an integer x the following statements are equivalent:

(1) $x \equiv a \pmod{k}$

(2) $x \equiv a,\ a + k,\ a + 2k, \ldots,\ a + (d-1)k \pmod{dk}$.

Proof. We shall prove that (1) and (2) are equivalent. First we prove that (1) implies (2), and then we will prove that (2) implies (1).

(1) $\Rightarrow$ (2): Assume $x \equiv a \pmod{k}$. Since $x \equiv a \pmod{k}$, there is an integer i such that $(*)$ $x = a + ik$. By the Division Algorithm, we can write $(**)$ $i = qd + r$ for some integers q and r where $0 \leq r < d$. By substituting $(**)$ for i in equation $(*)$ we obtain

$$x = a + ik = a + (qd + r)k = a + q(dk) + rk = a + rk + q(dk)$$

and so, $x = a + rk + q(dk)$ where $0 \leq r < d$. Thus, $x \equiv a + rk \pmod{dk}$ with $0 \leq r < d$. Therefore, $x \equiv a, a + k, a + 2k, \ldots, a + (d-1)k \pmod{dk}$.

(2) $\Rightarrow$ (1): Assume $x \equiv a,\ a + k,\ a + 2k, \ldots,\ a + (d-1)k \pmod{dk}$. Suppose that $x \equiv a + jk \pmod{dk}$ for some $0 \leq j < d$. Then $dk \mid (x - a - jk)$. Thus, $k \mid (x - a - jk)$ and so, $x - a - jk \equiv 0 \pmod{k}$. Hence, $x \equiv a + jk \pmod{k}$. Because $jk \equiv 0 \pmod{k}$, we conclude that $x \equiv a \pmod{k}$. $\square$

Remark 3.3.4. Given the congruence $(\star)$ $x \equiv a_1, a_2, \ldots a_k \pmod{n}$, suppose that (1) $k \mid n$, (2) $a_i - a_{i-1} = d$ for all $1 < i \leq k$, and (3) $d \mid n$. Then $(\star)$ is equivalent to $x \equiv a_1 \pmod{\frac{n}{k}}$.

Example 3. For any integer x, Theorem 3.3.3 asserts that

(i) $x \equiv 2 \pmod{4}$ if and only if $x \equiv 2, 6 \pmod{8}$, where $a = 2,\ d = 2,\ k = 4$;

(ii) $x \equiv 4 \pmod{6}$ if and only if $x \equiv 4, 10, 16 \pmod{18}$, where $a = 4,\ d = 3,\ k = 6$;

(iii) $x \equiv 7 \pmod{8}$ if and only if $x \equiv 7, 15, 23, 31, 39 \pmod{40}$, where $a = 7,\ d = 5,\ k = 8$.

One Linear Congruence Equation in One Variable

In Example 7 of Section 3.2 we solved the congruence equation

$$4x \equiv 6 \pmod{15} \tag{3.10}$$

and derived the solution $x \equiv 9 \pmod{15}$ to equation (3.10). Thus, $4 \cdot 9 \equiv 6 \pmod{15}$. Furthermore, our derivation establishes that any integer x is a solution to (3.10) if and only if $x \equiv 9 \pmod{15}$. Thus, we shall say the solution to equation (3.10) is unique (mod 15).

Consider the congruence equation

$$2x \equiv 4 \pmod{8}. \tag{3.11}$$

After checking the residue system $0, 1, 2, 3, 4, 5, 6, 7$ for solutions to (3.11) we see that $x = 2$ and $x = 6$ are the only solutions in this list. It follows that an integer x is a solution to (3.11) if and only if $x \equiv 2, 6 \pmod{8}$. Thus, we can say that the solution to (3.11) is given by $x \equiv 2, 6 \pmod{8}$. Example 3(i) states that $x \equiv 2, 6 \pmod{8}$ if and only if $x \equiv 2 \pmod{4}$. Thus, an integer x is a solution to (3.11) if and only if $x \equiv 2 \pmod{4}$. We can now say that the solution to (3.11) is unique (mod 4).

Remark. Before we state and prove our next theorem, consider the general congruence equation $(*)$ $ax \equiv b \pmod{n}$ and suppose that x_0 is a solution to this equation. Let $d = (a, n)$. Suppose that an integer x is a solution to $(*)$ if and only if $x \equiv x_0 \pmod{\frac{n}{d}}$. Then, in this case, we shall say that the solution is unique (mod $\frac{n}{d}$).

Theorem 3.3.5. Consider the linear congruence equation

$$ax \equiv b \pmod{n} \tag{3.12}$$

in the unknown x. Let $d = (a, n)$. Then equation (3.12) has solutions if and only if $d \mid b$. Furthermore, if $d \mid b$ then the solution to (3.12) is unique (mod $\frac{n}{d}$). Consequently, if $(a, n) = 1$ then equation (3.12) has a solution and it is unique (mod n).

Proof. Note that a, b, n are fixed integers with $n \geq 1$. Let $d = (a, n)$. The equation $ax \equiv b \pmod{n}$ has a solution for x if and only if there are integers x and y satisfying

$$ax - ny = b. \tag{3.13}$$

Theorem 2.5.1 implies that the Diophantine equation (3.13) has a solution if and only if $d \mid b$. Furthermore, if $d \mid b$, then Theorem 2.5.1 states that there is a solution x_0, y_0 to (3.13) and that every such solution x, y can be put into the form

$$x = x_0 + t\frac{n}{d} \text{ and } y = y_0 + t\frac{a}{d}$$

for some integer t. Hence, every solution x to (3.12) satisfies $x - x_0 = t\frac{n}{d}$ for some integer t. Consequently, every such solution x satisfies $x \equiv x_0 \pmod{\frac{n}{d}}$ and therefore, the solution to (3.12) is unique (mod $\frac{n}{d}$). $\square$

Suppose that you perform a derivation to solve a linear congruence equation of the form $ax \equiv b \pmod{n}$. If you happen to multiply a relevant congruence equation [see Theorem 3.2.3(3)] by a integer c where $(c, n) > 1$, then your final answer *may* obtain some extraneous values that are not solutions to the original congruence equation $ax \equiv b \pmod{n}$. As a very simple example of this phenomena, consider the congruence equation $2x \equiv 3 \pmod{5}$ together with the following derivation:

(1)	$2x \equiv 3 \pmod{5}$	the given congruence equation
(2)	$10x \equiv 15 \pmod{5}$	$5 \times (1)$.

Equation (2) was derived from equation (1). Therefore, every solution to (1) will also be a solution to (2). However, equation (2) holds for every integer x, whereas (1) holds only when $x \equiv 4 \pmod{5}$. Thus, the above derivation has introduced extraneous values that are not solutions to the original congruence equation $2x \equiv 3 \pmod{5}$.

Important Remark. Correct derivations will produce a true solution to a congruence equation. However, derivations can sometimes produce additional values that are not solutions. **After solving a congruence equation, be sure to check your answers.**

In the next example we will solve the congruence equation $7x \equiv 22 \pmod{39}$. A solution to this congruence equation is given on the bottom of page 69 and the top of page 70 of the text. The derivation given in the text introduces a "hidden" factor of 6. Since $(6, 39) = 3$, the solution introduces extraneous values that are not solutions to $7x \equiv 22 \pmod{39}$. We shall give the 'same' derivation as that presented in the text but where the "hidden" factor of 6 is exposed (see line (3) below).

Example 4. Solve the congruence equation $7x \equiv 22 \pmod{39}$.

Solution. Since $(7, 39) = 1$, Theorem 3.3.5 states that the equation $7x \equiv 22 \pmod{39}$ has a solution and that this solution is unique (mod 39). Consider the following derivation:

(1)	$7x \equiv 22 \pmod{39}$	the given congruence equation
(2)	$-39x \equiv 0 \pmod{39}$	a true congruence
(3)	$42x \equiv 132 \pmod{39}$	$6 \times (1)$
(4)	$3x \equiv 132 \pmod{39}$	$(1) + (2)$
(5)	$0 \equiv 117 \pmod{39}$	a true congruence; since $3 \cdot 39 = 117$
(6)	$3x \equiv 15 \pmod{39}$	$(4) - (5)$.
(7)	$x \equiv 5 \pmod{13}$	(6) and Theorem 3.2.7.

Note that $x \equiv 5 \pmod{13}$ is equivalent to $x \equiv 5, 18, 31 \pmod{39}$ by Theorem 3.3.3. Since the solution to $7x \equiv 22 \pmod{39}$ is unique (mod 39), two of these values are not solutions to the original congruence equation $7x \equiv 22 \pmod{39}$. One can check that $x \equiv 31 \pmod{39}$ is the desired solution. Thus, $x \equiv 5, 18 \pmod{39}$ are two values that are not solutions to the original congruence equation.

As a further note, one can solve $7x \equiv 22 \pmod{39}$ by performing a derivation that does not add any extraneous values as follows:

(1)	$7x \equiv 22 \pmod{39}$	the given congruence equation
(2)	$78x \equiv 0 \pmod{39}$	a true congruence; since $2 \cdot 39 = 78$
(3)	$77x \equiv 242 \pmod{39}$	$11 \times (1)$
(4)	$x \equiv -242 \pmod{39}$	$(2) - (3)$
(5)	$0 \equiv 273 \pmod{39}$	a true congruence; since $7 \cdot 39 = 273$
(6)	$x \equiv 31 \pmod{39}$	$(4) + (5)$.

This completes our discussion of Example 4.

A Systematic Method

The proof of Theorem 3.3.5 provides a systematic method, using the Euclidean Algorithm, for deriving a solution for x in the linear congruence equation

$$ax \equiv b \pmod{n}. \tag{3.14}$$

Let $d = (a, n)$ and suppose that $d \mid b$. Let $b = de$ for some integer e. Using the Euclidean Algorithm find integers r and s satisfying $ra + sn = d$. Now we perform the following derivation:

(1)	$ax \equiv b \pmod{n}$	the given congruence equation
(2)	$nx \equiv 0 \pmod{n}$	a true congruence
(3)	$rax \equiv rb \pmod{n}$	$r \times (1)$
(4)	$snx \equiv 0 \pmod{n}$	$s \times (2)$
(5)	$(ra + sn)x \equiv br \pmod{n}$	$(3) + (4)$
(6)	$dx \equiv der \pmod{n}$	because $d = ra + sn$ and $b = de$
(7)	$x \equiv er \left(\bmod\ \dfrac{n}{d}\right)$	by Theorem 3.2.7 if $d > 1$

Let $x_0 = er$. Theorem 3.3.5 states that the solution to (3.14) is unique $(\bmod\ \frac{n}{d})$. It now follows that an integer x is a solution to (3.14) if and only if $x \equiv x_0 \pmod{\frac{n}{d}}$.

Exercises 3.3

Do problems #1–6 on page 76 of text.

EXERCISE NOTES. For Problems 1–6 you must solve these congruence equations by means of derivations as those given in these notes (see Example 4 above, for examples).