Linear Congruences

A congruence of the form

$$ax \equiv b \pmod{m} \tag{1}$$

where x is an unknown integer, is called a linear congruence in one variable.

THEOREM 1: Let a, b, and m be integers with $m > 0$ and $(a, m) = d$. If $d \nmid b$, then (1) has no solutions. If $d \mid b$, then (1) has exactly d incongruent solutions modulo m.

COROLLARY: If a and m are relatively prime integers with $m > 0$ and b is an integer, then the linear congruence $ax \equiv b \pmod{m}$ has a unique solution modulo m:

$$x \equiv bs \pmod{m} \tag{2}$$

where s is such number that

$$as \equiv 1 \pmod{m} \tag{3}$$

Proof: We show that (2) is the solution of (1). In fact, if we multiply (2) by a and (3) by b (we can do that by Theorem 4 from Section 4.1), we get

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

and

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

which imply (1) by Theorem 2 from Section 4.1. Finally, note that there are no other solutions by the Theorem above. ■

DEFINITION: Given an integer a with $(a, m) = 1$, an integer solution x of $ax \equiv 1 \pmod{m}$ is called an **inverse** of a modulo m.

EXAMPLE: Find all solutions of the congruence

$$2x \equiv 1 \pmod{3}$$

Solution: We first note that $(2, 3) = 1$. Therefore we can apply the Corollary above. Since $s = 2$ is a particular solution of $2s \equiv 1 \pmod{3}$, we get

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

EXAMPLE: Find all solutions of the congruence

$$3x \equiv 4 \pmod{8}$$

Solution: We first note that $(3, 8) = 1$. Therefore we can apply the Corollary above. Since $s = 3$ is a particular solution of $3s \equiv 1 \pmod{8}$, we get

$$x \equiv bs \equiv 4 \cdot 3 \equiv 12 \equiv 4 \pmod{8}$$

EXAMPLE: Find all solutions of the following congruence

$$2x \equiv 5 \pmod{7}$$

Solution: We first note that $(2, 7) = 1$. Therefore we can apply the Corollary above. Since $s = 4$ is a particular solution of $2s \equiv 1 \pmod{7}$, we get

$$x \equiv bs \equiv 5 \cdot 4 \equiv 6 \pmod{7}$$

EXAMPLE: Find all solutions of the congruence

$$9x + 23 \equiv 28 \pmod{25}$$

Solution: By Theorem 4 from Section 4.1, we can rewrite this congruence as

$$9x \equiv 5 \pmod{25}$$

Note that $(9, 25) = 1$. Therefore we can apply the Corollary above. Since $s = 14$ is a particular solution of $9s \equiv 1 \pmod{25}$, we get

$$x \equiv bs \equiv 5 \cdot 14 \equiv 70 \equiv 20 \pmod{25}$$

REMARK: A particular solution s of the congruence $9s \equiv 1 \pmod{25}$ can be found either by guessing or the extended Euclidean algorithm or by the following method:

First we rewrite $25/9$ as

$$\frac{25}{9} = 2 + \frac{7}{9} = 2 + \frac{1}{9/7} = 2 + \frac{1}{1 + \frac{2}{7}} = 2 + \frac{1}{1 + \frac{1}{7/2}} = 2 + \frac{1}{1 + \frac{1}{3 + \frac{1}{2}}}$$

Then we replace $1/2$ by 0:

$$2 + \frac{1}{1 + \frac{1}{3 + 0}} = 2 + \frac{1}{1 + \frac{1}{3}} = 2 + \frac{1}{4/3} = 2 + \frac{3}{4} = \frac{11}{4}$$

One can check that $s = -11$ is a particular solution of the congruence $9s \equiv 1 \pmod{25}$. We also note that $-11 \equiv 14 \pmod{25}$.

EXAMPLE: Find all solutions of the congruence

$$541x \equiv 23 \pmod{121}$$

Solution: Note that $(541, 121) = 1$. Therefore we can apply the Corollary above. Since $s = 17$ is a particular solution of $541x \equiv 1 \pmod{121}$, we get

$$x \equiv bs \equiv 23 \cdot 17 \equiv 391 \equiv 28 \pmod{121}$$

REMARK: A particular solution s of the congruence $541x \equiv 1 \pmod{121}$ can be found either by guessing or by the extended Euclidean algorithm or by the following method:

First we rewrite 541/121 as

$$\frac{541}{121} = 4 + \frac{57}{121} = 4 + \frac{1}{121/57} = 4 + \frac{1}{2 + \frac{7}{57}} = 4 + \frac{1}{2 + \frac{1}{57/7}} = 4 + \frac{1}{2 + \frac{1}{8 + \frac{1}{7}}}$$

Then we replace 1/7 by 0:

$$4 + \frac{1}{2 + \frac{1}{8 + 0}} = 4 + \frac{1}{2 + \frac{1}{8}} = 4 + \frac{1}{17/8} = 4 + \frac{8}{17} = \frac{76}{17}$$

One can check that $s = 17$ is a particular solution of the congruence $541s \equiv 1 \pmod{121}$.

EXAMPLE: Find all solutions of the following congruence

$$2x \equiv 5 \pmod{8}$$

Solution: Since

$$(2, 8) = 2$$

we can't apply the Corollary above. Instead, we note that $2x \equiv 5 \pmod{8}$ is equivalent to $2x - 8y = 5$, which is impossible, since the left-hand side is divisible by 2, whereas the right-hand side is not. So, this equation has no solutions.

EXAMPLE: Find all solutions of the congruence

$$8x \equiv 7 \pmod{18}$$

Solution: Since

$$(8, 18) = 2$$

we can't apply the Corollary above. Instead, we note that $8x \equiv 7 \pmod{18}$ is equivalent to $8x - 18y = 7$, which is impossible, since the left-hand side is divisible by 2, whereas the right-hand side is not. So, this equation has no solutions.

EXAMPLE: Find all solutions of the following congruence

$$4x \equiv 2 \pmod{6}$$

Solution 1: Since

$$(4, 6) = 2$$

we can't apply the Corollary above. However, by Theorem 7 from Section 4.1 we can rewrite $4x \equiv 2 \pmod{6}$ as

$$2x \equiv 1 \pmod{3}$$

by canceling out 2. Note that $(2, 3) = 1$, therefore we can apply the Corollary above to the new congruence. Since $s = 2$ is a particular solution of $2s \equiv 1 \pmod{3}$, we get

$$x \equiv bs \equiv 1 \cdot 2 \equiv 2 \pmod{3}$$

Solution 2: By the Theorem above, the congruence $4x \equiv 2 \pmod 6$ has exactly two incongruent solutions modulo 6, since $(4, 6) = 2$. We find these solutions by first finding a particular solution and then adding the appropriate multiples of

$$\frac{m}{(a, m)} = \frac{6}{(2, 6)} = \frac{6}{2} = 3$$

To find a particular solution of the congruence $4x \equiv 2 \pmod 6$, we first find a particular solution of the linear Diophantine equation $4x - 6y = 2$ either by guessing or using the Euclidean algorithm (Theorem 2 from Section 3.4). We have $x_0 = -1,\ y_0 = -1$. A complete set of two incongruent solutions modulo 6 is given by

$$x \equiv x_0 = -1 \equiv 5 \pmod 6$$

and

$$x \equiv x_0 + 3 = -1 + 3 = 2 \pmod 6$$

REMARK: Note that these two solutions modulo 6 can be combined into just one solution modulo 3.

EXAMPLE: Find all solutions of the congruence

$$6x \equiv 3 \pmod{15}$$

Solution: Since

$$(6, 15) = 3$$

we can't apply the Corollary above. However, since $(3, 15) = 3$, by Theorem 7 from Section 4.1 we can rewrite $6x \equiv 3 \pmod{15}$ as

$$2x \equiv 1 \pmod 5$$

by canceling out 3. Note that $(2, 5) = 1$, therefore we can apply the Corollary above to the new equation. Since $s = 3$ is a particular solution of $2s \equiv 1 \pmod 5$, we get

$$x \equiv bs \equiv 1 \cdot 3 \equiv 3 \pmod 5$$

Solution 2: By the Theorem above, the congruence $6x \equiv 3 \pmod{15}$ has exactly three incongruent solutions modulo 15, since $(3, 15) = 3$. We find these solutions by first finding a particular solution and then adding the appropriate multiples of

$$\frac{m}{(a, m)} = \frac{15}{(6, 15)} = \frac{15}{3} = 5$$

To find a particular solution of the congruence $6x \equiv 3 \pmod{15}$, we first find a particular solution of the linear Diophantine equation $6x - 15y = 3$ either by guessing or using the Euclidean algorithm (Theorem 2 from Section 3.4). We have $x_0 = -2,\ y_0 = -1$. A complete set of three incongruent solutions modulo 15 is given by

$$x \equiv x_0 = -2 \equiv 13 \pmod{15}$$

$$x \equiv x_0 + 5 = -2 + 5 = 3 \pmod{15}$$

$$x \equiv x_0 + 5 \cdot 2 = -2 + 10 = 8 \pmod{15}$$

REMARK: Note that these three solutions modulo 15 can be combined into just one solution modulo 5.

EXAMPLE: Find all solutions of the congruence

$$9x \equiv 12 \pmod{15}$$

Solution: Since

$$(9, 15) = 3$$

we can't apply the Corollary above. However, since $(12, 15) = 3$, by Theorem 7 from Section 4.1 we can rewrite $9x \equiv 12 \pmod{15}$ as

$$3x \equiv 4 \pmod{5}$$

by canceling out 3. Note that $(3, 5) = 1$, therefore we can apply the Corollary above to the new equation. Since $s = 2$ is a particular solution of $3s \equiv 1 \pmod{5}$, we get

$$x \equiv bs \equiv 4 \cdot 2 = 8 \equiv 3 \pmod{5}$$

Solution 2: By the Theorem above, the congruence $9x \equiv 12 \pmod{15}$ has exactly three incongruent solutions modulo 15, since $(9, 15) = 3$. We find these solutions by first finding a particular solution and then adding the appropriate multiples of

$$\frac{m}{(a, m)} = \frac{15}{(9, 15)} = \frac{15}{3} = 5$$

To find a particular solution of the congruence $9x \equiv 12 \pmod{15}$, we first find a particular solution of the linear Diophantine equation $9x - 15y = 12$ either by guessing or using the the extended Euclidean algorithm (Theorem 2 from Section 3.4) or by the following method:

First we rewrite 15/9 as

$$\frac{15}{9} = \frac{5}{3} = 1 + \frac{2}{3} = 1 + \frac{1}{3/2} = 1 + \frac{1}{1 + \frac{1}{2}}$$

Then we replace 1/2 by 0:

$$1 + \frac{1}{1 + 0} = 1 + \frac{1}{1} = 3 = \frac{3}{1}$$

We have $x_0 = 3,\ y_0 = -1$. A complete set of three incongruent solutions modulo 15 is given by

$$x \equiv x_0 = 3 \pmod{15}$$

$$x \equiv x_0 + 5 = 3 + 5 = 8 \pmod{15}$$

$$x \equiv x_0 + 5 \cdot 2 = 3 + 10 = 13 \pmod{15}$$

REMARK: Note that these three solutions modulo 15 can be combined into just one solution modulo 5.

THEOREM 2: Let p be prime. The positive integer a is its own inverse modulo p if and only if

$$a \equiv 1 \pmod{p} \quad \text{or} \quad a \equiv -1 \pmod{p}$$

Proof: If $a \equiv 1 \pmod{p}$ or $a \equiv -1 \pmod{p}$, then $a^2 \equiv 1 \pmod{p}$ by Theorem 5 from Section 4.1.

Conversely, if a is its own inverse modulo p, then

$$a^2 \equiv 1 \pmod{p}$$

Hence, $p \mid (a^2 - 1)$. Because $a^2 - 1 = (a - 1)(a + 1)$, this implies that $p \mid (a - 1)$ or $p \mid (a + 1)$ by Theorem 2 from Section 3.5. Therefore, $a \equiv 1 \pmod{p}$ or $a \equiv -1 \pmod{p}$. ■