3.2 Solving linear congruences.

Solving equations of the form $ax \equiv b \,(\mathrm{mod}\, m)$, where x is an unknown integer.

Example (i) Find **an** integer x for which $56x \equiv 1 \bmod 93$.

Solution We have already solved this in the previous Chapter. Starting with $a = 93$ and $b = 56$ we used Euclid's Algorithm to show that

$$93 \times (-3) + 56 \times 5 = 1$$

Modulo 93 this gives $56 \times 5 \equiv 1 \bmod 93$. Hence $x = 5$ is a solution.

■

We can attempt to solve all such linear congruences by using Euclid's Algorithm.

Example (ii) Find **all** integers x for which $5x \equiv 12 \bmod 19$.

Solution If x **is** an integer solution, then $5x = 12 + 19t$ for some $t \in \mathbb{Z}$, or $5x - 19t = 12$. Such pairs (x, t) can be found by Euclid's Algorithm. Since $\gcd(5, 19) = 1$ which divides 12, this method **will** give solutions. Start with

$$\begin{aligned} 19 &= 3 \times 5 + 4 \\ 5 &= 1 \times 4 + 1, \end{aligned}$$

Work back to get

$$\begin{aligned} 1 &= 5 - 1 \times 4 \\ &= 5 - 1 \times (19 - 3 \times 5) \\ \text{Thus} \qquad 1 &= 4 \times 5 - 1 \times 19. \end{aligned}$$

Multiply by 12 to get

$$5 \times 48 - 19 \times 12 = 12, \tag{1}$$

so **a** solution to $5x - 19t = 12$ is $(x_0, t_0) = (48, 12)$.

Looking at (1) modulo 19 all multiples of 19 disappear and we get $5 \times 48 \equiv 12 \bmod 19$. Hence a *particular* answer to $5x \equiv 12 \bmod 19$ is $x = 48$.

For the *general* solution a method is to start with the trivial

$$5 \times 19 - 19 \times 5 = 0.$$

Then multiplying by ℓ, so

$$5 \times 19\ell - 19 \times 5\ell = 0$$

for all $\ell \in \mathbb{Z}$. Add this to (1) to get

$$5(48 + 19\ell) - 19\,(12 + 5\ell) = 12$$

for any $\ell \in \mathbb{Z}$. Thus all solutions to $5x \equiv 12 \bmod 19$ are given by $x = 48 + 19\ell$, $\ell \in \mathbb{Z}$, which is the same as $x \equiv 48 \bmod 19$, itself the same as $x \equiv 10 \bmod 19$. ■

Example (iii) Solve $4043x \equiv 25 \bmod 166361$.

Solution We have seen this in the previous Chapter. For **if** this congruence has a solution then

$$166361 \times (-\ell) + 4043x = 25$$

for some integers x and ℓ. Yet since $\gcd(166361, 4043) = 13$ and $13 \nmid 25$, this Diophantine equation has **no** integer solution. Contradiction. Hence the congruence has no integer solutions. ■

Example (iv) Find all solutions in integers x to $15x \equiv 12 \bmod 57$.

Solution To solve $15x \equiv 12 \bmod 57$ we will solve $15x = 12 + 57t$, i.e. $15x - 57t = 12$ for $x, t \in \mathbb{Z}$. Start from

$$\begin{aligned} 57 &= 3 \times 15 + 12 \\ 15 &= 1 \times 12 + 3 \\ 12 &= 4 \times 3 + 0 \end{aligned}$$

to see that $\gcd(57, 15) = 3$. Since $3|12$ the equation $15x - 57t = 12$ and thus the congruence will have solutions. Working back we see that

$$\begin{aligned} 3 &= 15 - 1 \times 12 \\ &= 15 - (57 - 3 \times 15)\,. \end{aligned}$$

Thus $57 \times (-1) + 15 \times 4 = 3$. Multiply by 4 to get

$$57 \times (-4) + 15 \times 16 = 12. \tag{2}$$

So $(x_0, t_0) = (16, 4)$ is a particular solution of $15x - 57t = 12$. Looking at (2) modulo 57 we see that $15 \times 16 = 12 \bmod 67$ so **a** solution of $15x \equiv 12 \bmod 57$ is $x_0 = 16$.

If (x_0, t_0) is a particular solution and $x, t)$ is a general solution, then

$$\begin{aligned} 15x_0 - 57t_0 &= 12 \\ 15x - 57t &= 12. \end{aligned}$$

Subtract to get

$$15\,(x_0 - x) - 57\,(t_0 - t) = 0, \tag{3}$$

or $15\,(x_0 - x) = 57\,(t_0 - t)$. Though we have $15|LHS \Rightarrow 15|57\,(t_0 - t)$, we cannot deduce that $15|\,(t_0 - t)$ since $\gcd(15, 57) \neq 1$. Instead divide all terms in (3) by $\gcd(15, 57) = 3$ to get

$$5\,(x_0 - x) = 19\,(t_0 - t)\,. \tag{4}$$

This time

$$\begin{aligned} 5|LHS &\Rightarrow 5|19\,(t_0 - t) \\ &\Rightarrow 5|\,(t_0 - t)\,, \text{ since } \gcd(5, 19) = 1, \end{aligned}$$

in which case $t_0 - t = 5\ell$ for some $\ell \in \mathbb{Z}$. Substitute back into (4) to get $5\,(x_0 - x) = 19 \times 5\ell$ or $x_0 - x = 19\ell$. Thus the general solution to (2) is

$$(x, t) = (x_0 - 19\ell, t_0 - 5\ell) = (16 - 19\ell, 4 - 5\ell)$$

for $\ell \in \mathbb{Z}$.

So all the solutions to $15x \equiv 12 \bmod 57$ are given by $16 - 19\ell, \ell \in \mathbb{Z}$. This could be written as $x \equiv 16 \bmod 19$. But it is more usual to express the answer in the same modulus as the question.

Varying ℓ $(= ..., -2, -1, 0, -1, -2, -3, ...)$ we find solutions $... - 22$, -3, 16, 35, 54, 73, ... But $-3 \equiv 54 \bmod 57$ and $73 \equiv 16 \bmod 57$, and so before and after 16, 35 and 54 we are not getting new solutions, mod 57. On the other hand 16, 35 and 54 are **not** congruent (i.e. they are *incongruent*) mod 57. So we give the solutions to $15x \equiv 12 \bmod 57$ as

$$x \equiv 16,\ 35 \text{ or } 54 \bmod 57.$$

$\blacksquare$

Note that the number of incongruent solutions here equals 3, which is the same as $\gcd(57, 19)$. This is not a coincidence, as can be seen in the following.

Theorem The congruence $ax \equiv c \pmod{m}$ is soluble in integers if, and only if, $\gcd(a, m)\,|c$. The number of incongruent solutions modulo m is $\gcd(a, m)$.

Proof The ideas for this proof can be found around p.244 in PJE and are not given here.

Alternative ways to solve *some* linear congruences.

Example Solve $5x \equiv 6 \bmod 19$.

Solution TRICK Note that we can change any coefficients by adding multiples of 19, as in

$$6 \equiv 5x \equiv (5 + 19)\, x \equiv 24x \bmod 19.$$

Now both 6 and 24 are divisible by 6, which is coprime to 19. Thus by the Theorem (ii) above we deduce that $4x \equiv 1 \bmod 19$. In turn

$$4x \equiv 1 \equiv 1 + 19 \equiv 20 \bmod 19.$$

Both 4 and 20 are divisible by 4 which is coprime to 19 and so we can use Theorem (ii) again to deduce $x \equiv 5 \bmod 19$. ∎

Definition If a' is a solution of the congruence $ax \equiv 1 \pmod{m}$ then a' is called the ***(multiplicative) inverse*** of a modulo m and we say that a is ***invertible.***

Note The congruence $ax \equiv 1 \pmod{m}$ has solutions if, and only if, $\gcd(a, m) | 1$, i.e. $\gcd(a, m) = 1$. Thus a has an inverse modulo m iff a and m are coprime.

Example Above we solved $56x \equiv 1 \bmod 93$, finding $x = 5$. Hence 5 is the inverse of 56 modulo 93.

If we can find the multiplicative inverse to $a \bmod m$ we can then solve $ax \equiv b \bmod m$ by multiplying both sides by a' to get $x \equiv (a'a)\, x \equiv a'b \bmod m$.

Example Solve $56x \equiv 23 \bmod 93$.

Solution Multiply both sides of the equation by the inverse of $53 \bmod 93$, i.e. 5, to get $280x \equiv 115 \bmod 93$, i.e. $x \equiv 115 \equiv 22 \bmod 93$. ∎

The advantage of finding the inverse is that once found we can solve each of $56x \equiv b \bmod 93$, for **any** $b \in \mathbb{Z}$.

And of course, if 5 is the inverse of $56 \bmod 93$ then 56 is the inverse of $5 \bmod 93$. Hence

Example Solve $5x \equiv 23 \bmod 93$.

Solution Multiply both sides of the equation by the inverse of $5 \bmod 93$, i.e. 56, to get $280x \equiv 1288 \bmod 93$, that is,. $x \equiv 1288 \equiv 79 \bmod 93$. ∎

Advice, use these techniques of either adding multiples of the modulus to the coefficients or finding inverses to solve congruences *if it doesn't take you too long to do.* If in doubt, use Euclid's Algorithm to solve $ax \equiv b \bmod m$.