

10. Linear congruences.

Given integers a, b, m with $m \geq 1$, “solve the congruence $ax \equiv b \pmod{m}$ ” means “find *all* integers x which satisfy the congruence”.

If there are solutions, then we can express the answer as $x \equiv c \pmod{M}$ or, equivalently, as $x = c + Mt, t \in \mathbf{Z}$. The integer M will emerge from the calculation. It is always a *divisor* of m .

Example Solve the congruence $3x \equiv 4 \pmod{5}$.

Solution $3x \equiv 4 \pmod{5} \Leftrightarrow 3x \equiv 9 \pmod{5}$ as $4 \equiv 9 \pmod{5}$
 $\Leftrightarrow x \equiv 3 \pmod{5}$ as $\gcd(5,3) = 1$
 - see section 9

Thus, the solution is $x \equiv 3 \pmod{5}$.

The solution could also be expressed as $x = 3 + 5t, t \in \mathbf{Z}$.

Note. The first line of the solution requires some explanation. Since we are working modulo 5, we can replace the integer 4 by any integer congruent to 4 modulo 5. We chose 9 since that is divisible by 3, the coefficient of x in the given congruence. This then allows us to use the cancellation technique we met in the previous section.

Example Solve the congruence $6x \equiv 9 \pmod{15}$.

Solution $6x \equiv 9 \pmod{15} \Leftrightarrow 2x \equiv 3 \pmod{5}$ as $\gcd(15,6) = 3$
 - see section 9
 $\Leftrightarrow 2x \equiv 8 \pmod{5}$ as $3 \equiv 8 \pmod{5}$
 $\Leftrightarrow x \equiv 4 \pmod{5}$ as $\gcd(5,2) = 1$.

Thus, the solution is $x \equiv 4 \pmod{5}$.

The solution could also be expressed as $x = 4 + 5t, t \in \mathbf{Z}$.

Here, the original modulus was 15. Our answer involved a congruence modulo 5. We could observe that the solutions are $\dots -6, -1, 4, 9, 14, 19, \dots$. These are obtained by taking integer values of t in the alternative form $x = 4 + 5t, t \in \mathbf{Z}$. Then we can observe that the solution may be expressed as

$$x \equiv 4, 9 \text{ or } 14 \pmod{15}.$$

This form uses congruences with the *same modulus*, 15, as the original problem.

Theorem 1 Let a, b, m be integers with m positive, and let $d = \gcd(a, m)$.

Then the congruence $ax \equiv b \pmod{m}$ has integer solutions if and only if $d \mid b$.

When $d \mid b$, the solution is unique modulo the integer $M = m/d$.

Proof

A solution of $ax \equiv b \pmod{m}$ is an integer x such that $ax - b = mu$, for some $u \in \mathbf{Z}$.

For any such solution, we get a solution $x = x, y = -u$ of the equation

$$ax + my = b.$$

The problem of finding solutions of this diophantine equation is discussed in Theorem 6.1 (Theorem 1 of Section 6). There we learned that

there are solutions if and only if $d \mid b$ (as $d = \gcd(a, m)$),

We also learned that, when solutions *do* exist, i.e. when $d \mid b$, then the *general solution* is given by

$$x = x' + (m/d)t, \quad y = y' - (a/d)t, \quad t \in \mathbf{Z}.$$

where x', y' is *any* solution of the equation.

Note that m/d and a/d are integers as $d = \gcd(a, m)$. Also, $m/d = M$, by definition.

In this case, the values of x are given by $x = x' + Mt, t \in \mathbf{Z}$, or, equivalently, by the congruence $x \equiv x' \pmod{M}$. The values of y are of no interest in this context.

The values of x are as in the statement of the theorem.

Note. Just as in the second example above, we can express the solution in terms of congruences modulo m . To see this, we note that the first few solutions can be obtained by putting $t = 0, 1, 2, \dots, d-1$. This gives

$$x', \quad x'+M, \quad x'+2M, \quad x'+3M, \quad \dots, \quad x'+(d-1)M$$

The next solution is $x'+dM$, but this is congruent to x' modulo $m = Md$.

Thus the solutions are given by

$$x \equiv x', \quad x'+M, \quad x'+2M, \quad x'+3M, \quad \dots, \quad \text{or } x'+(d-1)M \pmod{m}$$

Thus, we have $d = \gcd(a, m)$ solutions which are *different modulo m*.

Example Solve the congruence $9x \equiv 5 \pmod{12}$.

Solution

Here, $\gcd(9,12) = 3$. In the notation of Theorem 1, $a = 9$, $m = 12$.

Now 3 does *not* divide 5, so there are *no* solutions.

Our main tactic in solving $ax \equiv b \pmod{m}$ when we know that a solution exists is to replace b by $b+m$, $b+2m$, ... until we reach a multiple of a . The replacements give equivalent congruences since each of these replacements is congruent to b modulo m . We then use the cancellation theory of Section 9.

Example Solve the congruence $3x \equiv 1 \pmod{4}$.

Solution

Here, $\gcd(3,4) = 1$, so we *do* have solutions.

As we are working modulo 4, we can replace the 1 on the right by 5 or 9 or...

As 9 is a multiple of 3, and $\gcd(3,4) = 1$, we cancel the 3 to get $x \equiv 3 \pmod{4}$.

In the congruence $ax \equiv b \pmod{m}$, we can get an equivalent congruence by replacing a by any $a' \equiv a \pmod{m}$, and b by any $b' \equiv b \pmod{m}$. This may well simplify the problem.

Example Solve the congruence $19x \equiv 142 \pmod{4}$.

Solution

Observe that $19 \equiv 3 \pmod{4}$, and $142 \equiv 2 \pmod{4}$.

Thus, the given congruence is equivalent to $3x \equiv 2 \pmod{4}$.

We note that this is equivalent to $3x \equiv 6 \pmod{4}$ as $2 \equiv 6 \pmod{4}$.

Now $\gcd(3,4) = 1$, so we can cancel the 3 to get $x \equiv 2 \pmod{4}$.

Note. If we had applied our standard tactic, we would have replaced 142 by 146, by 150, ..., until we reached a multiple of 19. If we try this, we find that we need to add 4s until we reach 190. This takes 12 steps. The solution we have given is much more efficient.

Moral.

In tackling the congruence $ax \equiv b \pmod{m}$, we should begin by

- (1) checking that solution exist – see Theorem 1, then
- (2) replacing a and b by their remainders on division by d . These are integers in the range $0, \dots, m-1$.

When $d = 1$, we get a useful special case of Theorem 1, which we state as the

Corollary If $\gcd(a,m) = 1$, then the congruence $ax \equiv b \pmod{m}$ has a solution, and this is unique modulo m .

Proof

In the notation of the theorem, we have $d = \gcd(a,m) = 1$.

Then, for any b , we have $d \mid b$.

Thus by the theorem, the congruence has solutions.

Also, the solution is unique modulo $m/d = m$ as we have $d = 1$.

The cases where $\gcd(a,m) = 1$ and $b = 1$ are particularly interesting. The corollary tells us that $ax \equiv 1 \pmod{m}$ has a solution which is unique modulo m .

Definition

Suppose that $\gcd(a,m) = 1$. A solution of the congruence $ax \equiv 1 \pmod{m}$ is called an *inverse of a modulo m*.

From the Corollary, if a' is an inverse of a modulo m , then the set of inverses has the form $\{x : x \equiv a' \pmod{m}\}$.

Example Suppose that $\gcd(a,m) = 1$. If a' is an inverse of a modulo m then the solution of the congruence $ax \equiv b \pmod{m}$ is $x \equiv a'b \pmod{m}$.

Solution

From our theory, we know that, as $\gcd(a,m) = 1$, the congruence $ax \equiv b \pmod{m}$ has solution $x \equiv c \pmod{m}$ for some integer c .

As a' is an inverse of a modulo m , $a'a \equiv 1 \pmod{m}$, so also $aa' \equiv 1 \pmod{m}$

We now check that $x = a'b$ is a solution. For this value of x ,

$$ax = a(a'b) = (aa')b \equiv 1 \cdot b \equiv b \pmod{m}.$$

Example Find the inverses of 1, 2, 3, 4, 5, 6 modulo 5.

Solution For a small modulus, such as 7, it is probably easiest to solve the congruences by trial and error. For each congruence in turn, we try $x = 1, 2, 3, 4, 5, 6$ to see which works. We get

x	1	2	3	4	5	6
inverse of x modulo 7	1	4	5	2	3	6

Theorem 2 – Wilson’s Theorem For a prime p , $(p-1)! + 1 \equiv 0 \pmod{p}$.

The proof is rather difficult. However, the *ideas* behind the proof are simple, and are clearly illustrated by a *numerical* example.

We consider the prime 7. Theorem 2 states that $6!+1 \equiv 0 \pmod{7}$

Now $6! = 1.2.3.4.5.6$. We can arrange the factors in *any* order. We choose to put

$6! = 1.(2.4).(3.5).6$.

From the preceding example, we know that 2.4 and 3.5 are each 1 modulo 7. So

$6! \equiv 1.1.1.6 \equiv 6 \pmod{7}$, and hence

$6!+1 \equiv 6+1 \equiv 7 \equiv 0 \pmod{7}$, as required.

In the general case, the factors of $(p-1)!$ are the integers 1, 2, ..., $p-1$.

Other than 1 and $p-1$, the factors fall into pairs (x,y) with $xy \equiv 1 \pmod{p}$.

Thus, $(p-1)!$ Can be arranged as 1...product of pairs x,y as above... $p-1$.

Then $(p-1)! \equiv p-1 \pmod{p}$, so $(p-1)!+1 \equiv p \equiv 0 \pmod{p}$, as required.

Example Show that 23 is the smallest proper factor of $22!+1$.

Solution Let d be an integer in the range $2, \dots, 22$.

Then d occurs as a factor in $22!$, so that $d \mid 22!$

But then d does *not* divide $22!+1$ (the remainder on division by d is 1)

Now 23 is prime, so Wilson’s Theorem says $23 \mid (22!+1)$

In other words, 23 *does* divide $22!+1$, so is the *smallest* proper divisor.

The converse of Wilson’s Theorem is also true.

Converse of Wilson’s Theorem If $(n-1)!+1 \equiv 0 \pmod{n}$, then n is prime.

Proof Suppose it is false – there is a *composite* n with $(n-1)!+1 = nt, t \in \mathbf{Z}$.

As n is composite, it has a proper divisor d , so $1 < d < n$ and $d \mid n$.

Then $d \mid (n-1)!$, so $(n-1)!+1 \equiv 1 \pmod{d}$, and $d \mid n$, so $nt \equiv 0 \pmod{d}$.

But $(n-1)!+1 = nt$, so we have a contradiction.

Thus, the converse *must* be true.