

11. Systems of linear congruences

Example Find all integers x which satisfy the congruences $x \equiv 3 \pmod{5}$ and $x \equiv 5 \pmod{8}$..

Solution

An integer x which satisfies $x \equiv 3 \pmod{5}$ has the form $x = 3 + 5u$, $u \in \mathbf{Z}$.

This x also satisfies $x \equiv 5 \pmod{8}$ is and only if

$$3 + 5u \equiv 5 \pmod{8}$$

i.e. $5u \equiv 2 \pmod{8}$ subtracting 3 from each side

i.e. $5u \equiv 10 \pmod{8}$ as $2 \equiv 10 \pmod{8}$

i.e. $u \equiv 2 \pmod{8}$ as $\gcd(5,8) = 1$

Thus, $u = 2 + 8t$, $t \in \mathbf{Z}$, and then

$$x = 3 + 5u = 3 + 5(2+8t), t \in \mathbf{Z},$$

i.e. $x = 13 + 40t$, $t \in \mathbf{Z}$.

Note that the solution can be expressed as $x \equiv 13 \pmod{40}$.

Note We have a solution expressed in terms of a congruence whose modulus, 40, is the product of the original moduli, 3 and 5.

Example Show that there are *no* integers satisfying both $x \equiv 5 \pmod{8}$ and also $x \equiv 3 \pmod{4}$.

Solution An integer x which satisfies $x \equiv 5 \pmod{8}$ has the form $x = 5+8u$, $u \in \mathbf{Z}$.

Then $x = 1 + 4(1+2u)$, so that $x \equiv 1 \pmod{4}$.

But then we *cannot* have $x \equiv 3 \pmod{4}$, so there are *no* solutions to both.

Definition Positive integers m,n are *coprime* if $\gcd(m,n) = 1$.

Note The outcomes in these examples are quite different. The key is that, in the first case, the moduli, 3 and 5, are coprime. In the second, the moduli are 8 and 4 which are *not* coprime.

Our aim is to solve a system of an arbitrary number of congruences, but it is useful to start with just two.

Lemma Suppose that a, A, m, M are integers, with m, M positive and coprime. Then the congruences $x \equiv a \pmod{m}$ and $x \equiv A \pmod{M}$ have a common solution which is unique modulo mM .

Proof

Each solution of $x \equiv a \pmod{m}$ has the form $x = a + mu, u \in \mathbf{Z}$.

This also satisfies $x \equiv A \pmod{M}$ if and only if

$$a + mu \equiv A \pmod{M}$$

i.e. $mu \equiv A - a \pmod{M}$ (*)

Now, as m, M are coprime, $\gcd(m, M) = 1$, so the congruence (*) has a solution which is unique modulo M . If $u = U$ is a solution, then the general solution is

$$u = U + Mt, t \in \mathbf{Z},$$

Then $x = a + mu = a + m(U + Mt)$

i.e. $x = (a + mU) + mMt, t \in \mathbf{Z}$.

Thus the solution is unique modulo mM .

Definition

Positive integers m_1, \dots, m_n are pairwise coprime, if, whenever $i \neq j$, $\gcd(m_i, m_j) = 1$.

The Chinese Remainder Theorem

Suppose that positive integers m_1, \dots, m_n are pairwise coprime, and that a_1, \dots, a_n are any integers. Then the system

$$x \equiv a_1 \pmod{m_1}, \quad \dots, \quad x \equiv a_n \pmod{m_n}$$

has a solution which is unique modulo the product $m_1 \dots m_n$

Proof We give a proof by induction on n , the number of congruences.

Suppose that the result is true for any system of $n-1$ congruences. Then the system $x \equiv a_1 \pmod{m_1}, \dots, x \equiv a_{n-1} \pmod{m_{n-1}}$ has a solution X which is unique modulo $M = m_1 \dots m_{n-1}$

Thus, the first $n-1$ congruences are equivalent to the congruence $x \equiv X \pmod{M}$.

It follows that the original system of n congruences can be replaced by the *two* congruences

$$x \equiv X \pmod{M}, \quad x \equiv a_n \pmod{m_n}.$$

We tackle these using the Lemma, but first we must check that the conditions of the Lemma are fulfilled, i.e. that M and m_n are coprime.

Let us suppose that this is false, i.e. that $\gcd(M, m_n) > 1$.

Then there is a *prime* p with $p \mid M$ and $p \mid m_n$

As p is prime, and $p \mid M = m_1 \dots m_{n-1}$, $p \mid m$ for some i .

But then $p \mid m_i$ and $p \mid m_n$, so $\gcd(m_i, m_n) > 1$, contradicting the hypothesis that $m_1 \dots m_n$ are pairwise coprime.

Hence $\gcd(M, m_n) = 1$.

Now the Lemma applies, so the system $x \equiv X \pmod{M}$, $x \equiv a_n \pmod{m_n}$ has a solution which is unique modulo $Mm_n = m_1 \dots m_n$.

But this is equivalent to the original system, so this has a solution which is unique modulo the given product.

Note that the proof not only establishes the truth of the theorem, but also gives a technique which allows us to *find* solutions.

Example Solve the system of congruences

$$x \equiv 3 \pmod{4}, \quad x \equiv 2 \pmod{7}, \quad x \equiv 1 \pmod{9}.$$

Solution

Note that the moduli 4, 7, 9 are pairwise coprime, so the Chinese remainder Theorem applies.

The congruence $x \equiv 1 \pmod{9}$ has solutions $x = 1+9u, u \in \mathbf{Z}$.

This also satisfies $x \equiv 2 \pmod{7}$ if and only if

$$x = 1+9u \equiv 2 \pmod{7}$$

i.e. $9u \equiv 2-1 = 1 \pmod{7}$

i.e. $2u \equiv 1 \pmod{7}$ as $9 \equiv 2 \pmod{7}$

i.e. $2u \equiv 8 \pmod{7}$ as $2 \equiv 8 \pmod{7}$

i.e. $u \equiv 4 \pmod{7}$ as $\gcd(2,7) = 1$

i.e. $u = 4+7v, v \in \mathbf{Z}$.

Thus, the solutions of the second and third congruences have the form

$$x = 1+9u = 1+9(4+7v) = 37 + 63v, v \in \mathbf{Z}.$$

This also satisfies the first congruence if and only if

$$x = 37+63v \equiv 3 \pmod{4}$$

i.e. $63v \equiv 3-37 \equiv -34 \pmod{4}$

i.e. $3v \equiv 2 \pmod{4}$ as $63 \equiv 3$ and $-34 \equiv 2 \pmod{4}$

i.e. $3v \equiv 6 \pmod{4}$ as $2 \equiv 6 \pmod{4}$

i.e. $v \equiv 2 \pmod{4}$ as $\gcd(3,4) = 1$.

Thus, $v = 2+4t, t \in \mathbf{Z}$, so that,

$$x = 37+63v$$

i.e. $x = 37+63(2+4t)$

i.e. $x = 163+252t, t \in \mathbf{Z}$.

This is the general solution. It may also be written $x \equiv 163 \pmod{252}$

Notes

- (1) In the solution of this example, we began with the *largest* modulus, and added further congruences in *descending* order of moduli. This is usually more efficient than working in *ascending* order.
- (2) the Lemma and the Theorem apply to systems of congruences, each of the form $x \equiv a \pmod{m}$. If we have a system including linear congruences of the more general form $Ax \equiv B \pmod{m}$, we must first bring such a congruence into the simpler form $x \equiv a \pmod{m}$.

Example Solve the system of congruences

$$3x \equiv 1 \pmod{4}, \quad x \equiv 2 \pmod{7}, \quad x \equiv 1 \pmod{9}.$$

Solution

The first congruence is not of standard form, so we begin by finding its solution.

Note that $3x \equiv 1 \pmod{4}$ is equivalent to $3x \equiv 9 \pmod{4}$, as $9 \equiv 1 \pmod{4}$.

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

Using this to replace the first congruence, we get the system

$$x \equiv 3 \pmod{4}, \quad x \equiv 2 \pmod{7}, \quad x \equiv 1 \pmod{9}.$$

This is the system we solved in the previous example, so we must get exactly the same solution, $x \equiv 163 \pmod{252}$.

The technique is efficient, and it can sometimes pay to use it in unexpected problems.

Example Find the general solution of the congruence $85x \equiv 31 \pmod{168}$.

Solution Note that $168 = 3 \cdot 7 \cdot 8$, and 3, 7, 8 are pairwise coprime, so that the given congruence is equivalent to the system

$$85x \equiv 31 \pmod{3}, 85x \equiv 31 \pmod{7}, 85x \equiv 31 \pmod{8}$$

In each congruence, we can reduce the coefficients relative to the modulus :

$$x \equiv 1 \pmod{3}, x \equiv 3 \pmod{7}, 5x \equiv 7 \pmod{8}$$

The third of these is not yet in standard form. As $7 \equiv 15 \pmod{8}$ may rewrite it as $5x \equiv 15 \pmod{8}$, so that $x \equiv 3 \pmod{8}$.

We now have the system

$$x \equiv 1 \pmod{3}, x \equiv 3 \pmod{7}, x \equiv 3 \pmod{8}$$

The third gives $x = 3 + 8u$, $u \in \mathbf{Z}$, This satisfies the second if and only if

$$x = 3 + 8u \equiv 3 \pmod{7}$$

i.e. $8u \equiv 0 \pmod{7}$

i.e. $u \equiv 0 \pmod{7}$, as $8 \equiv 1 \pmod{7}$

Thus, $u = 7v$, $v \in \mathbf{Z}$, so that $x = 3 + 8u = 3 + 56v$, $v \in \mathbf{Z}$.

This satisfies the first congruence if and only if

$$x = 3 + 56v \equiv 1 \pmod{3}$$

i.e. $56v \equiv 1 - 3 \equiv -2 \pmod{3}$

i.e. $2v \equiv 4 \pmod{3}$ as $56 \equiv 2$, and $-2 \equiv 4 \pmod{3}$

i.e. $v \equiv 2 \pmod{3}$

Thus $v = 2t$, $t \in \mathbf{Z}$, so that $x = 3 + 56v = 3 + 56(2 + 3t) = 115 + 168t$.

Thus, the solution of the given congruence is $x \equiv 115 \pmod{168}$.

Note In solving the system of congruences, we could have saved some time. We had the congruences $x \equiv 3 \pmod{7}$, and $x \equiv 3 \pmod{8}$. These have the obvious solution $x = 3$. Then, by the Lemma, the general solution is $x \equiv 3 \pmod{56}$ since we know that the solution is unique modulo $7 \cdot 8 = 56$.

Alternative solution

The congruence $85x \equiv 31 \pmod{168}$ is equivalent to the diophantine equation

$$85x + 168y = 31.$$

We can solve this using the Euclidean Algorithm as in earlier sections.

$$\begin{aligned} 168 &= 1 \cdot 85 + 83 \\ 85 &= 1 \cdot 83 + 2 \\ 83 &= 41 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0 \end{aligned}$$

Backtracking :

$$\begin{aligned} 1 &= 83 - 41 \cdot 2 \\ &= 83 - 41 \cdot (85 - 83) \\ &= 42 \cdot 83 - 41 \cdot 85 \\ &= 42 \cdot (168 - 85) - 41 \cdot 85 \\ &= 42 \cdot 168 - 83 \cdot 85 \end{aligned}$$

Multiplying through by 31,

$$\begin{aligned} 31 &= (31 \cdot 42) \cdot 168 - (31 \cdot 83) \cdot 85 \\ &= 1302 \cdot 168 - 2573 \cdot 85 \end{aligned}$$

This gives us a solution $x = -2573$, $y = 1302$, and hence the general solution

$$x = -2573 + 168t, y = 1302 - 85t, t \in \mathbf{Z}$$

To see that this is the same as the earlier solution, we can check that -2573 is congruent to 115 modulo 168 . This follows as $115 = -2573 + 16 \cdot 168$.