Section 4

Congruences

Week 3

The aim in this section is to introduce new terminology: that of congruence modulo an integer. The concept is not new, but the notation is, as is the way we think about numbers in this context. The language of congruences was invented by **Gauss** (1777 – 1855) and allows us to work with divisibility relationships in much the same way as with equalities.

4.1 Definition and Equivalent Conditions

Let m be an integer with $m > 0$. We say that "a **is congruent to** b **modulo** m", denoted by $a \equiv b \pmod{m}$, if and only if $m|(a-b)$.

For example, $a \equiv b \pmod{2}$ if and only if a and b **have the same parity**, that is, a and b are either both even or both odd. Also, $1 \equiv 4 \equiv 7 \equiv 100 \equiv -2 \equiv -101 \pmod{3}$; $2 \equiv 14 \equiv 146 \equiv -10 \pmod{12}$, etc.

Also, for any multiple km of m, $km \equiv 0 \pmod{m}$ because $m|km$.

Here are some theorems which give necessary and sufficient conditions for integers a and b to be congruent modulo m.

Theorem 4.1 *$a \equiv b \pmod{m}$ if and only if there is an integer k such that $a = b + km$.*

Proof.
We have:

$$\begin{aligned} a \equiv b \pmod{m} \quad & \text{if and only if} \quad m|(a-b) \\ & \text{if and only if} \quad a-b = km \quad \text{for some } k \in \mathbb{Z} \\ & \text{if and only if} \quad a = b + km \quad \text{for some } k \in \mathbb{Z}. \end{aligned}$$

■

Theorem 4.2 *Every integer a is congruent* $\pmod{m}$ *to exactly one of* $0, 1, ..., m-1$.

Proof.
Write $a = km + r$ with $0 \leq r < m$. By the division algorithm this can be done in a unique way. By Theorem 4.1 above, $a \equiv r \pmod{m}$ and the theorem is proved. ■

If $a \equiv r \pmod{m}$, where $r \in \{0, 1, ..., m-1\}$, then we say that r is the **least residue** of a $\pmod{m}$.

Theorem 4.3 $a \equiv b \pmod{m}$ *if and only if a and b leave the same remainder when divided by m.*

Proof. If a and b leave the same remainder r when divided by m, then

$$a = q_1 m + r \quad \text{and} \quad b = q_2 m + r \quad \text{for some } q_1, q_2 \in \mathbb{Z}.$$

Hence

$$a - b = m(q_1 - q_2),$$

i.e. $m|(a-b)$. By the definition of congruence, $a \equiv b \pmod{m}$.
Conversely, suppose $a \equiv b \pmod{m}$. Then $a \equiv b \equiv r \pmod{m}$, where r is a least residue modulo m. By Theorem 4.1,

$$a = q_1 m + r \quad \text{and} \quad b = q_2 m + r \quad \text{for some } q_1, q_2 \in \mathbb{Z}.$$

Since r is a least residue, $0 \leq r < m$ and so r is the remainder when either of a and b is divided by m. ■

We now have three other ways of saying $a \equiv b \pmod{m}$, because the following statements have been proved to be equivalent:

♣ $a \equiv b \pmod{m}$
♣ $m|(a-b)$ (definition)
♣ there exists an integer k such that $a = b + km$
♣ a and b leave the same remainder when divided by m.

4.2 Properties of the Congruence Relation

The next lemma (important because used frequently) is stated without proof – write out the proofs on your own:

Lemma 4.1 *For integers a, b, c, d and $m \geq 1$,*

(a) $a \equiv a \pmod{m}$.

(b) *If* $a \equiv b \pmod{m}$, *then* $b \equiv a \pmod{m}$.

(c) *If* $a \equiv b \pmod{m}$ *and* $b \equiv c \pmod{m}$, *then* $a \equiv c \pmod{m}$.

(d) *If* $a \equiv b \pmod{m}$ *and* $c \equiv d \pmod{m}$, *then* $a + c \equiv b + d \pmod{m}$.

(e) *If* $a \equiv b \pmod{m}$ *and* $c \equiv d \pmod{m}$, *then* $ac \equiv bd \pmod{m}$.

Example: Show that if n is not divisible by 3, then $n^2 \equiv 1 \pmod{3}$.

Solution

If $3 \nmid n$, then $n \equiv 1$ or $2 \pmod{3}$. If $n \equiv 1 \pmod{3}$, then by Lemma 4.1(e),

$$n^2 \equiv 1 \cdot 1 \equiv 1 \pmod{3}.$$

If $n \equiv 2 \pmod{3}$, then similarly

$$n^2 \equiv 2 \cdot 2 \equiv 4 \equiv 1 \pmod{3}.$$

Example: Prove that $39 | (53^{103} + 103^{53})$.

If you try to calculate these numbers on your calculator,
you'll find it a hopeless task! So use your brain instead.

Solution

There are only three integers whose powers are all easy to calculate: $0, 1$ and -1. Thus we somehow have to reduce this expression to those numbers (until we prove some more helpful results, at least). Also, "divide and conquer" – or rather, "factorize and conquer":

Since $39 = 3 \cdot 13$ and $(3, 13) = 1$, $39 | (53^{103} + 103^{53})$ if and only if $3 | (53^{103} + 103^{53})$ and $13 | (53^{103} + 103^{53})$. Now,

$$\begin{aligned} 53 &= 18 \cdot 3 - 1 \equiv (-1) \pmod{3}, \\ 103 &= 34 \cdot 3 + 1 \equiv 1 \pmod{3}, \\ 53 &= 13 \cdot 4 + 1 \equiv 1 \pmod{13}, \\ 103 &= 13 \cdot 8 - 1 \equiv (-1) \pmod{13}. \end{aligned}$$

Hence

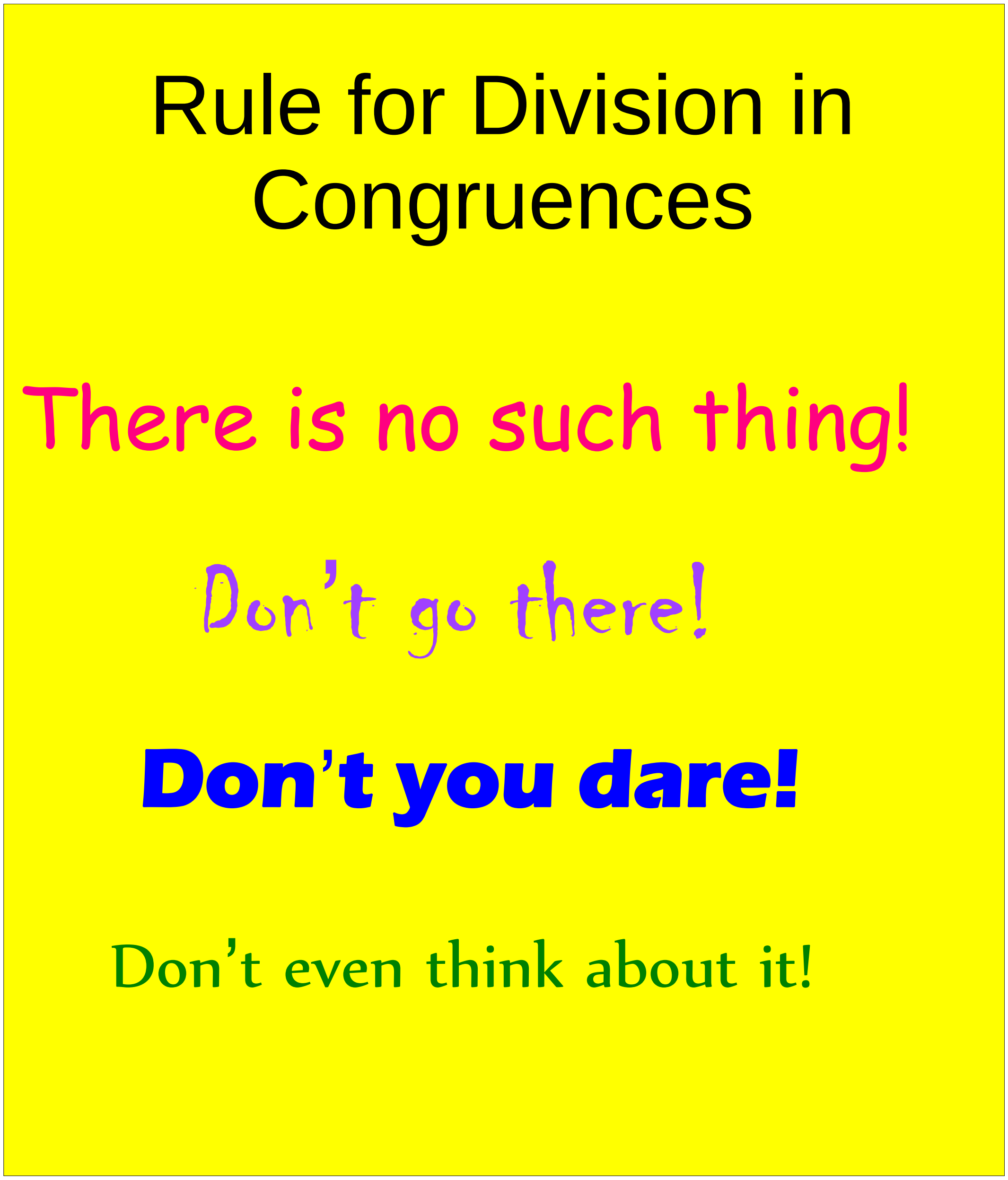
$$53^{103} + 103^{53} \equiv (-1)^{103} + 1^{53} \equiv -1 + 1 \equiv 0 \pmod{3}$$

and

$$53^{103}+103^{53}\equiv 1^{103}+(-1)^{53}\equiv 1-1\equiv 0 \pmod{13},$$

and the result follows.

Warning: Unlike in the case of equality instead of congruence, if $c\neq 0$ and $ac\equiv bc \pmod{m}$, it does not necessarily follow that $a\equiv b \pmod{m}$. For example, $6\equiv 8\equiv 0 \pmod{2}$, but $3\not\equiv 4 \pmod{2}$.



Rule for Division in Congruences

There is no such thing!

Don't go there!

Don't you dare!

Don't even think about it!

What can we do about this?

Theorem 4.4 *If* $ac \equiv bc \pmod{m}$ *and* $\underline{(c, m) = 1}$, *then* $a \equiv b \pmod{m}$.

Proof. From the definition of congruence, $m|(ac-bc)$, i.e. $m|c(a-b)$. But $(c, m) = 1$, hence by Corollary 1.1, $m|(a-b)$ and therefore $a \equiv b \pmod{m}$. ■

What if $(c, m) \neq 1$?

Theorem 4.5 *If* $ac \equiv bc \pmod{m}$ *and* $(c, m) = d$, *then* $a \equiv b \pmod{m/d}$.

This theorem will be used all the time! Remember it!

Proof. Let $c' = c/d$ and $m' = m/d$; by Theorem 1.1, $(m/d, c/d) = (m', c') = 1$. If $ac \equiv bc \pmod{m}$, then $m|(ac - bc)$. Thus

$$ac - bc = km \quad \text{for some } k \in \mathbb{Z}.$$

Dividing both sides of this equation by d we get

$$\begin{aligned} ac/d - bc/d &= km/d, \\ \text{i.e.} \quad ac' - bc' &= km' \end{aligned}$$

and thus $m'|(ac' - bc')$, hence by definition of congruence,

$$ac' \equiv bc' \pmod{m'}.$$

But $(c', m') = 1$ and hence, by Theorem 4.4, $a \equiv b \pmod{m'}$ as required. ■

4.3 Divisibility by 9

Test for divisibility by 9: why does it work?

Theorem 4.6 *Every integer is congruent, modulo* 9, *to the sum of its digits.*

Proof. Suppose the integer n has digital representation

$$\begin{aligned} &d_k d_{k-1} ... d_1 d_0, \\ \text{i.e.}\quad &n = d_k 10^k + d_{k-1} 10^{k-1} + \cdots + d_1 10 + d_0. \end{aligned}$$

But $10 \equiv 1 \pmod 9$ and by Lemma 4.1(e) $10^r \equiv 1^r \equiv 1 \pmod 9$ for any integer r, hence

$$n \equiv d_k + d_{k-1} + \cdots d_1 + d_0 \pmod{9}.$$

■

Example: We can use Theorem 4.6 to check a multiplication without using a calculator – handy in days before such things were known (and used in computer programs today):

Suppose someone says $(365)(127) = 46435$. Then we know he or she is wrong, because

$$(365)(127) \equiv (3 + 6 + 5)(1 + 2 + 7) \equiv (14)(10) \equiv 5 \cdot 1 \equiv 5 \pmod{9}$$

while

$$46435 \equiv 4 + 6 + 4 + 3 + 5 \equiv 22 \equiv 4 \pmod{9}.$$

These two numbers are not congruent modulo 9 and thus not equal.

Example: Find the remainder when 4444^{4444} is divided by 9.

Solution

Apply Theorem 4.6:

$$4444 \equiv 4 + 4 + 4 + 4 \equiv 16 \equiv 7 \equiv -2 \pmod{9}.$$

But we cannot calculate $(-2)^{4444}$, so we use our brains again: $2^3 \equiv 8 \equiv (-1) \pmod{9}$, hence

$$4444^{4444} \equiv (-2)^{4444} \equiv 2^{4444} \equiv 2^{3(1481)+1} \equiv 2(2^3)^{1481} \equiv 2(-1)^{1481} \equiv -2 \equiv 7 \pmod{9};$$

the remainder is 7.

Section 5

Linear Congruences

Linear congruences are essentially the same as linear Diophantine equations, but the new terminology associated with congruences allows us to obtain solutions for the latter.

A **linear congruence** is a congruence of the form

$$ax \equiv b \pmod{m}.$$

(Recall that this is equivalent to $m|(ax-b)$, which means there exists an integer k such that $ax-b=km$.)

- This congruence has a solution if and only if there is an integer x_0 such that $ax_0 \equiv b \pmod{m}$, and thus also an integer y_0 such that $ax_0 = b + my_0$, that is, if and only if the linear Diophantine equation $ax + my = b$ has a solution $x = x_0$, $y = -y_0$.

- Recall that if a linear Diophantine equation has a solution, it has infinitely many. Similarly, if r is a solution to $ax \equiv b \pmod{m}$, then $r + km$ is also a solution for any $k \in \mathbb{Z}$, because
$$a(r+km) \equiv ar + akm \equiv ar \equiv b \pmod{m}.$$

- Note that the difference between any two different integers of the form
$$r + km, \quad k \in \mathbb{Z},$$
is at least m, and the difference between any two consecutive ones (using consecutive values of k) is exactly m. Therefore there is exactly one of them, say s, such that $0 \le s < m$.

- Here is how we find such an s which satisfies the congruence $ax \equiv b \pmod{m}$, if we have an integer r which satisfies the congruence and
$$km \le r < (k+1)m.$$
Subtracting km from this inequality, we get
$$0 \le r - km < m,$$

and we can put

$$s = r - km.$$

5.1 Solutions of Linear Congruences

Here we come to a notational difference between linear Diophantine equations and linear congruences:

- By a **solution** to $ax \equiv b \pmod{m}$ we mean a number r such that $ar \equiv b \pmod{m}$ and r is a least residue $\pmod{m}$, that is, $0 \leq r < m$.

Using this terminology, a linear congruence may have no solution, exactly one solution, or several solutions, but only finitely many since each solution lies between 0 and m.

Examples:

1. The congruence $2x \equiv 1 \pmod{4}$ has no solution, as $2x$ is always even for any integer x, while any integer congruent to $1 \pmod{4}$ is odd.
2. The congruence $5x \equiv 1 \pmod{4}$ has exactly one solution: try each of 0, 1, 2, 3; the only solution is $x \equiv 1 \pmod{4}$.
3. The congruence $2x \equiv 0 \pmod{4}$ has exactly two solutions – check to see that $x \equiv 0, 2 \pmod{4}$ are solutions and $x \equiv 1, 3 \pmod{4}$ are not.

The following results should come as no surprise – we know them from the section on linear Diophantine equations (Section 3).

Lemma 5.1 *If $(a, m) \nmid b$, then $ax \equiv b \pmod{m}$ has no solution.*

Lemma 5.2 *Or, equivalently, if $ax \equiv b \pmod{m}$ has a solution, then $(a, m) | b$.*

Proof. Suppose r is a solution. Then $ar \equiv b \pmod{m}$, hence $m|(ar-b)$, and thus $ar-b = km$ for some $k \in \mathbb{Z}$. Since $(a, m)|a$ and $(a, m)|m$, it follows that $(a, m)|b$. ■

Lemma 5.3 *If $(a, m) = 1$, then $ax \equiv b \pmod{m}$ has exactly one solution.*

Proof. Since $(a, m) = 1$ there exist $r, s \in \mathbb{Z}$ such that $ar + ms = 1$. Multiplying by b yields

$$\begin{aligned} & arb + msb = b, \\ \text{i.e.} \quad & arb - b = (-bs)m \equiv 0 \pmod{m}, \\ \text{i.e.} \quad & a(rb) \equiv b \pmod{m}. \end{aligned}$$

- The least residue of rb modulo m is thus a solution of the congruence.
- We show that this is the only solution. Suppose that both t and q are solutions. Thus

  $$at \equiv b \pmod{m} \text{ and } aq \equiv b \pmod{m}$$

  and therefore

  $$\begin{aligned} at &\equiv aq \pmod{m}, \\ \text{i.e.} \quad t &\equiv q \pmod{m} \qquad \text{since } (a,m)=1. \end{aligned}$$

  ★But t and q are least residues of m, and obviously $t \equiv t \pmod{m}$ while we showed above that $t \equiv q \pmod{m}$. By Theorem 4.2, $t = q$.★ ■

★ The part between the stars proves that if t and q are least residues modulo m and
★ $t \equiv q$ (mod m), then $t = q$. We will use this fact in future without proving it again.

The best way of solving congruences with small moduli is to manipulate the coefficients until cancellation is possible.

Example: Solve the congruence $12x \equiv 20 \pmod{29}$.

Solution

We first simplify; since $(4, 29) = 1$, we get

$$3x \equiv 5 \pmod{29}.$$

The best way to manipulate coefficients is to note that

$$3x \equiv 5 \equiv 5 + (-1)(29) \equiv -24 \pmod{29},$$

hence

$$x \equiv -8 \equiv 21 \pmod{29}.$$

Example: Solve the linear Diophantine equation $9x + 10y = 11$.

Solution

This equation implies two congruences, in the following way: if

$$9x + 10y = 11,$$

then

$$9x = 11 + (-y)10$$

and thus

$$9x \equiv 11 \pmod{10}.$$

Similarly we get

$$10y \equiv 11 \pmod{9}.$$

We can choose any one of these to solve – say the second one. Then

$$10y \equiv y \equiv 11 \equiv 2 \pmod{9},$$

therefore

$$y \equiv 2 \pmod{9}.$$

But this means that

$$y = 9t + 2,$$

where t is any integer. Substitute in the original equation:

$$\begin{aligned} & & 9x + 10(9t+2) &= 11, \\ \text{i.e.} & & 9x &= -9 - 90t \\ \text{i.e.} & & x &= -1 - 10t. \end{aligned}$$

Thus we have all the solutions of the Diophantine equation:

$$\left.\begin{array}{l} x = -1 - 10t \\ y = 2 + 9t, \end{array}\right\}, \; t \in \mathbb{Z}.$$

What happens if $(a, m) \neq 1$?

Lemma 5.4 *If $(a, m) = d$ and $d|b$, then*

$$ax \equiv b \pmod{m} \tag{5.1}$$

has exactly d solutions.

Proof. Cancel the common factor. This gives the congruence

$$(a/d)x \equiv b/d \pmod{m/d} \tag{5.2}$$

which has exactly one solution by Lemma 5.3. Say $x = r$ is a solution of (5.2). Then

$$0 \leq r < m/d \quad \text{(definition of a solution).} \tag{5.3}$$

- Then r is a solution of (5.1) because

$$\begin{aligned}(a/d)r \equiv b/d \pmod{m/d} &\Rightarrow (a/d)r = b/d + k(m/d) \text{ for some } k \in \mathbb{Z}\\ &\Rightarrow ar = b + km \text{ for some } k \in \mathbb{Z}\\ &\Rightarrow ar \equiv b \pmod{m}.\end{aligned}$$

Let s be an arbitrary integer that satisfies (5.1). Then $ar \equiv as \equiv b \pmod{m}$ and since $(a, m) = d$, this reduces to

$$\begin{aligned} &s \equiv r \pmod{m/d},\\ \text{i.e.}\quad &s = r + k(m/d) \quad \text{for some } k \in \mathbb{Z}.\end{aligned}$$

Putting $k = 0, 1, ..., d - 1$, we get d different values of s.

- We show that these numbers are least residues modulo m:

The smallest possible s so obtained is obtained when $k = 0$, i.e. $s = r$, and the largest when $k = d - 1$, i.e. $s = r + (d - 1)m/d$. From this and (5.3) we get

$$0 \leq r \leq r + k(m/d) \leq r + (d - 1)m/d < m/d + (d - 1)m/d = m,$$

that is,

$$0 \leq r + k(m/d) < m.$$

Thus these d numbers are also solutions of (5.1). ■

Example: How many solutions does the congruence $12x \equiv 4 \pmod{20}$ have? Find them.

Solution

Since $(12, 20) = 4 = d$ and $4|4$, there are four solutions. Simplifying, we get

$$\begin{aligned} &3x \equiv 1 \equiv 6 \pmod{5},\\ \text{i.e.}\quad &x \equiv 2 \pmod{5}.\end{aligned}$$

Thus $x \equiv 2 + 5k$, where $k = 0, 1, 2, 3 = d - 1$, are all the solutions, i.e.

$$x \equiv 2,\ 7,\ 12,\ 17 \pmod{20}.$$

Lemmas 5.1 – 5.4 are summarized as follows.

Theorem 5.1 *The congruence* $ax \equiv b \pmod{m}$ *has no solutions if* $(a, m) \nmid b$. *If* $(a, m)|b$, *then it has exactly* (a, m) *solutions.*

5.2 The Chinese Remainder Theorem

Another type of problem: A system of congruences with different moduli. Find an integer x such that $2x \equiv 1 \pmod{5}$, $3x \equiv 2 \pmod{7}$, $4x \equiv 3 \pmod{11}$.

Can we solve this system of congruences?

The following theorem tells us when we can do it: any system of linear congruences with different moduli has a unique solution, modulo the product of the moduli, if the moduli are pairwise relatively prime. The proof is not required for exam purposes but the theorem will be used over and over again – so remember it! It is called the *Chinese Remainder Theorem* because its original form appeared in a third-century AD book *The Mathematical Classic of Sun Zi* by the Chinese mathematician Sun Tzu.

Theorem 5.2 (The Chinese Remainder Theorem) *The system of congruences*

$$x \equiv a_i \pmod{m_i}, \quad i = 1, 2, ..., k,$$

where $(m_i, m_j) = 1$ *if* $i \neq j$, *has a unique solution modulo* $m_1 m_2 ... m_k$.

We illustrate the method of the proof with the following example.

Example: Solve the system $2x \equiv 1 \pmod{5}$, $3x \equiv 2 \pmod{7}$, $4x \equiv 3 \pmod{11}$.

Solution

We want to find a solution which is a least residue modulo $5 \cdot 7 \cdot 11 = 385$.

- **Begin with the first congruence and solve it.**

If $2x \equiv 1 \equiv 6 \pmod{5}$, then $x \equiv 3 \pmod{5}$, thus $x = 5r + 3$ for some integer r, and we have written x in terms of r.

- **Substitute into the second congruence and solve it.** Thus

$$\begin{aligned} & 3(5r+3) \equiv 2 \pmod{7}, \\ \text{i.e.} \quad & 15r \equiv -7 \equiv 0 \pmod{7}, \\ \text{i.e.} \quad & r \equiv 0 \pmod{7}. \end{aligned}$$

Then $r = 7s$ for some integer s, and so (write x in terms of s) $x = 35s + 3$.

- **Substitute into the third congruence and solve it.** Thus

$$\begin{aligned} 4(35s+3) &\equiv 4(2s+3) \pmod{11} \\ &\equiv 8s+1 \equiv 3 \pmod{11}, \\ \text{i.e.} \qquad 8s &\equiv 2 \equiv 13 \equiv 24 \pmod{11}, \\ \text{i.e.} \qquad s &\equiv 3 \pmod{11}. \end{aligned}$$

Hence $s = 11t + 3$ for some integer t, and therefore (write x in terms of t)

$$x = 35(11t+3) + 3 = 385t + 108 \equiv 108 \pmod{385}.$$

The solution is $x = 108$.

Theorem 5.3 (General Chinese Remainder Theorem) *A system of linear congruences*

$$x \equiv a_i \pmod{m_i}, \quad i = 1, 2, ..., k,$$

has solutions if and only if for every pair of congruences $x \equiv a_i \pmod{m_i}$, $x \equiv a_j \pmod{m_j}$ in the system,

$$a_i \equiv a_j \pmod{(m_i, m_j)}.$$

If solutions exist, they are of the form

$$x \equiv b \pmod{\operatorname{lcm}(m_1, m_2, ..., m_k)}$$

for some integer b.