Congruences and Modular Arithmetic

- a is **congruent to** b **mod** n means that $n \mid a - b$. Notation: $a = b \pmod{n}$.
- Congruence mod n is an **equivalence relation**. Hence, congruences have many of the same properties as ordinary equations.
- Congruences provide a convenient shorthand for divisibility relations.

Definiton. Let a, b, and m be integers. a is **congruent to** b **mod** m if $m \mid a - b$; that is, if

$$a - b = km \text{ for some integer } k.$$

Write $a = b \pmod{m}$ to mean that a is congruent to b mod m. m is called the **modulus** of the congruence; I will almost always work with positive moduli.

Notice that $a = 0 \pmod{m}$ is equivalent to $m \mid a$. Thus, divisibility is a special case of congruence. In many cases, this means that you can reduce proving results about congruences to results about divisibility that were proved earlier.

Example. $101 = 3 \pmod{2}$ and $2 = 101 \pmod{3}$. □

Proposition. Congruence mod m is an **equivalence relation**:

(a) (**Reflexivity**) $a = a \pmod{m}$ for all a.

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

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

Proof. I'll prove transitivity and leave the proofs of the other two properites to you. Suppose $a = b \pmod{m}$ and $b = c \pmod{m}$. Then there are integers j and k such that

$$a - b = jm, \quad b - c = km.$$

Add the two equations:

$$a - c = (j + k)m.$$

This implies that $a = c \pmod{m}$. □

Example. Consider congruence mod 3. There are 3 **congruence classes**:

$$\{\ldots, -3, 0, 3, 6, \ldots\}, \quad \{\ldots -4, -1, 2, 5, \ldots\}, \quad \{\ldots -5, -2, 1, 4, \ldots\}.$$

Each integer belongs to exactly one of these classes. Two integers in a given class are congruent mod 3. (If you know some group theory, you probably recognize this as constructing $\mathbb{Z}_3$ from $\mathbb{Z}$.)

When you're doing things mod 3, it is if there were only 3 numbers. I'll grab one number from each of the classes to **represent** the classes; for simplicity, I'll use 0, 2, and 1.

Here is an addition table for the classes in terms of these representatives:

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Here's an example: $2 + 1 = 0$, because $2 + 1 = 3$ as integers, and 3's congruence class is represented by 0. This is the table for **addition mod** 3.

I could have chosen different representatives for the classes — say 3, -4, and 4. A choice of representatives, one from each class, is called a **complete system of residues mod** 3. But working mod 3 it's natural to use the numbers 0, 1, and 2 as representatives — and in general, if I'm working mod n, the obvious choice of representatives is the set $\{0, 1, 2, \ldots, n-1\}$. This set is called the **least nonnegative system of residues mod** n, and it is the set of representatives I'll usually use.

(Sometimes I'll get sloppy and call it the **least positive system of residues**, even though it includes 0.) □

Proposition. If $a = b \pmod m$ and $c = d \pmod m$, then

$$a + c = b + d \pmod m \quad \text{and} \quad ac = bd \pmod m.$$

Note: You can use the second property and induction to show that if $a = b \pmod m$, then $a^n = b^n \pmod m$ for all $n \geq 1$.

Proof. Suppose $a = b \pmod m$ and $c = d \pmod m$. Then $m \mid a - b$ and $m \mid c - d$. Therefore,

$$m \mid (a - b) + (c - d) = (a + c) - (b + d), \quad \text{so} \quad a + b = b + d \pmod m.$$

To prove the second congruence, return to the relations $m \mid a - b$ and $m \mid c - d$. By definition of divisibility, there are integers j and k such that

$$a - b = jm \quad \text{and} \quad c - d = km.$$

Thus,

$$a = b + jm \quad \text{and} \quad c = d + km.$$

Multiply these two equations and do some algebra on the right side:

$$ac = (b + jm)(d + km) = bd + bkm + djm + jkm^2 = bd + m(bk + dj + jkm).$$

Hence,

$$ac - bd = m(bk + dj + jkm) \quad \text{and} \quad m \mid ac - bd, \quad \text{so} \quad ac = bd \pmod m. \quad \square$$

Corollary. If $a = b \pmod m$, then

$$a \pm c = b \pm c \pmod m \quad \text{and} \quad ac = bc \pmod m.$$

Proof. Apply the preceding result to the congruences $a = b \pmod m$ and $c = c \pmod m$. □

These results say that congruences behave like equations:

- You can add two congruences.

- You can multiply two congruences.
- You can add a number to both sides of a congruence.
- You can multiply both sides of a congruence by a number.

For instance, you can solve single-variable linear congruences using the same approach that you would use to solve linear equations.

Example. Solve the congruence

$$2x + 11 = 7 \pmod 3.$$

First, reduce all the coefficients mod 3:

$$2x + 2 = 1 \pmod 3.$$

Next, add 1 to both sides, using the fact that $2 + 1 = 0 \pmod 3$:

$$2x = 2 \pmod 3.$$

Finally, multiply both sides by 2, using the fact that $2 \cdot 2 = 4 = 1 \pmod 3$:

$$x = 1 \pmod 3.$$

That is, any number in the set $\{\ldots, -5, -2, 1, 4, \ldots\}$ will solve the original congruence. □

Remark. Notice that I accomplished *division* by 2 (in solving $2x = 2 \pmod 3$ by *multiplying* by 2. The reason this works is that, mod 3, 2 is its own *multiplicative inverse.*

Recall that two numbers x and y are **multiplicative inverses** if $x \cdot y = 1$ and $y \cdot x = 1$. For example, in the rational numbers, $\frac{3}{5}$ and $\frac{5}{3}$ are multiplicative inverses. *Division by a number is defined to be multiplication by its multiplicative inverse.* Thus, division by 3 *means* multiplication by $\frac{1}{3}$.

In the integers, only 1 and -1 have multiplicative inverses. When you perform a "division" in $\mathbb{Z}$ — such as dividing $2x = 6$ by 2 to get $x = 3$ — you are actually factoring and using the Zero Divisor Property:

$$2x = 6, \quad 2x - 6 = 0, \quad 2(x - 3) = 0, \quad x - 3 = 0, \quad x = 3.$$

(I used the Zero Divisor Property in making the third step: Since $2 \neq 0$, $x - 3$ must be 0.)

In doing modular arithmetic, however, many numbers may have multiplicative inverses. In these cases, you can perform division by multiplying by the multiplicative inverse.

Here is a multiplication table mod 3, using the standard residue system $\{0, 1, 2\}$:

$*$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

You can construct similar tables for other moduli. For example, 2 and 3 are multiplicative inverses mod 5, because $2 \cdot 3 = 1 \pmod 5$. So if you want to "divide" by 3 mod 5, you multiply by 2 instead.

This doesn't always work. For example, consider

$$2x = 4 \pmod 6.$$

2 does not have a multiplicative inverse mod 6; that is, there is no k such that $2k = 1 \pmod 6$. You can check by trial that the solutions to the equation above are $x = 2 \pmod 6$ and $x = 5 \pmod 6$ — just look at $2x \pmod 6$ for $x = 0, 1, 2, 3, 4, 5$. □

Proposition. If $ac = bc \pmod m$ and $d = (c, m)$, then

$$a = b \pmod{\frac{m}{d}}.$$

Proof. Write

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

Then

$$(a - b)\frac{c}{d} = k\frac{m}{d}.$$

(Notice that $\frac{c}{d}$ and $\frac{m}{d}$ are integers, since $d \mid c$ and $d \mid m$.) Now $\frac{c}{d}$ divides the right side, but it's relatively prime to $\frac{m}{d}$. Therefore, it must divide k:

$$k = \frac{c}{d}j \text{ for some } j \in \mathbb{Z}.$$

Hence,

$$(a - b)\frac{c}{d} = \frac{c}{d}j \cdot \frac{m}{d},$$

$$a - b = j \cdot \frac{m}{d}.$$

This proves that $a = b \pmod{\frac{m}{d}}$. □

Example. Consider the equation from the last example:

$$2x = 4 \pmod 6.$$

This is

$$(2 \cdot 1)x = (2 \cdot 2) \pmod 6.$$

Apply the last result with $a = 1$, $b = 2$, $c = 2$, and $m = 6$. Now $(2, 6) = 2$, so the result says I can "divide everything by 2":

$$x = 2 \pmod 3.$$

Since the original congruence was mod 6, I have to find the numbers mod 6 which satisfy $x = 3 \pmod 3$. Checking $x = 0, 1, 2, 3, 4, 5$, I find that $x = 2 \pmod 6$ or $x = 5 \pmod 6$. □

Example. In

$$2x = 4 \pmod 7,$$

2 is a common factor of 2 and 4, and $(2, 7) = 1$, so

$$x = 2 \pmod 7.$$

Alternatively, notice that $2 \cdot 4 = 1 \pmod 7$, so if I multiply the equation by 4, I get

$$x = 2 \pmod 7. \quad \square$$

Example. What is the least positive residue of $99^{10} \pmod 7$?

$99 = 1 \pmod 7$, so

$$99^{10} = 1^{10} = 1 \pmod 7 . \quad \square$$

Example. If p is prime, then

$$(x+y)^p = x^p + y^p \pmod p .$$

By the Binomial Theorem,

$$(x+y)^p = \sum_{i=0}^{p} \binom{p}{i} x^i y^{p-i}.$$

A typical coefficient $\binom{p}{i} = \dfrac{p!}{i!\,(p-i)!}$ is divisible by p for $i \neq 0, p$. So going mod p, the only terms that remain are x^p and y^p.

For example

$$(x+y)^2 = x^2 + y^2 \pmod 2 \quad \text{and} \quad (x+y)^3 = x^3 + y^3 \pmod 3 .$$

The result is *not* true if the modulus is not prime. For example,

$$(1+1)^4 = 0 \pmod 4 , \quad \text{but} \quad 1^4 + 1^4 = 2 \pmod 4 . \quad \square$$

Solving Congruences

- A linear congruence $ax = b \pmod{m}$ has solutions if and only if $(a, m) \mid b$.
- You can solve linear congruences by finding modular inverses, by using the Euclidean algorithm, and by turning the congruence into a linear Diophantine equation.

Theorem. Let $d = (a, m)$, and consider the equation

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

(a) If $d \not| b$, there are no solutions.

(b) If $d \mid b$, there are exactly d distinct solutions mod m.

Proof. Observe that

$$ax = b \pmod{m} \quad \Leftrightarrow \quad ax + my = b \quad \text{for some} \quad y.$$

Hence, (a) follows immediately from the corresponding result on linear Diophantine equations. The result on linear Diophantine equations which corresponds to (b) says that there are infinitely many integer solutions

$$x = x_0 + \frac{m}{d}t,$$

where x_0 is a particular solution. I need to show that of these infinitely many solutions, there are exactly d distinct solutions mod m.

Suppose two solutions of this form are congruent mod m:

$$x_0 + \frac{m}{d}t_1 = x_0 + \frac{m}{d}t_2 \pmod{m}.$$

Then

$$\frac{m}{d}t_1 = \frac{m}{d}t_2 \pmod{m}.$$

Now $\frac{m}{d}$ divides both sides, and $\left(\frac{m}{d}, m\right) = \frac{m}{d}$, so I can divide this congruence through by $\frac{m}{d}$ to obtain

$$t_1 = t_2 \pmod{d}.$$

Going the other way, suppose $t_1 = t_2 \pmod{d}$. This means that t_1 and t_2 differ by a multiple of d:

$$t_1 - t_2 = kd.$$

So

$$\frac{m}{d}t_1 - \frac{m}{d}t_2 = \frac{m}{d} \cdot kd = km.$$

This implies that

$$\frac{m}{d}t_1 = \frac{m}{d}t_2 \pmod{m}$$

so

$$x_0 + \frac{m}{d}t_1 = x_0 + \frac{m}{d}t_2 \pmod{m}.$$

Let me summarize what I've just shown. I've proven that two solutions of the above form are equal mod m if and only if their parameter values are equal mod d. That is, if I let t range over a complete system of residues mod d, then $x_0 + \frac{m}{d}t$ ranges over all possible solutions mod m. To be very specific,

$$x_0 + \frac{m}{d}t \pmod{m} \text{ for } t = 0, 1, 2, \ldots, d-1$$

are all the solutions mod m. □

Example. $6x = 7 \pmod 8$. Since $(6, 8) = 2 \not| 7$, there are no solutions. □

Example. $3x = 7 \pmod 4$. Since $(3, 4) = 1 \mid 7$, there will be 1 solutions mod 4. I'll find it in three different ways.

Using linear Diophantine equations.

$$3x = 7 \pmod 4 \text{ implies } 2x + 4y = 7 \text{ for some } y.$$

By inspection $x_0 = 1$, $y_0 = 1$ is a particular solution. $(3, 4) = 1$, so the general solution is

$$x = 1 + 4t, \quad y = 1 - 3t.$$

The y equation is irrelevant. The x equation says

$$x = 1 \pmod 4 .$$

Using the Euclidean algorithm. Since $(3, 4) = 1$, some linear combination of 3 and 4 is equal to 1. In fact,

$$(-1) \cdot 3 + 1 \cdot 4 = 1.$$

This tells me how to juggle the coefficient of x to get $1 \cdot x$:

$$\begin{array}{rrcl} & 4x & = & 0 \pmod 4 \\ - & 3x & = & 7 \pmod 4 \\ \hline & x & = & 1 \pmod 4 \end{array}$$

(I used the fact that $7 = -1 \pmod 4$).

Using inverses mod 4. Here is a multiplication table mod 4:

$*$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

I see that $3 \cdot 3 = 1 \pmod 4$, so I multiply the equation by 3:

$$3x = 7 \pmod 4 , \quad x = 21 = 1 \pmod 4 . \quad \square$$

Theorem. Let $d = (a, b, m)$, and consider the equation

$$ax + by = c \pmod{m}.$$

(a) If $d \not| c$, there are no solutions.

(b) If $d \mid c$, there are exactly md distinct solutions mod m.

I won't give the proof; it follows from the corresponding result on linear Diophantine equations.

Example. Consider the equation

$$2x + 6y = 4 \pmod{10}.$$

$(2, 6, 10) = 2 \mid 4$, so there are $2 \cdot 10 = 20$ solutions mod 10. I'll solve the equation using a reduction trick similar to the one I used to solve two variable linear Diophantine equations.

The given equation is equivalent to

$$2x + 6y + 10z = 4 \text{ for some } z.$$

Set

$$w = \frac{2}{(2,6)}x + \frac{6}{(2,6)}y.$$

Then

$$(2,6)w + 10z = 4, \quad 2w + 10z = 4, \quad w + 5z = 2.$$

$w_0 = -3$, $z_0 = 1$, is a particular solution. The general solution is

$$w = -3 + 5s, \quad z = 1 - s.$$

Substitute for w:

$$\frac{2}{(2,6)}x + \frac{6}{(2,6)}y = -3 + 5s, \quad x + 3y = -3 + 5s.$$

$x_0 = 5s$, $y_0 = -1$, is a particular solution. The general solution is

$$x = 5s + 3t, \quad y = -1 - t.$$

$t = 0, 1, \ldots, 9$ will produce distinct values of y mod 10. Note, however, that s and $s + 2r$ produce $5s$ and $5s + 10r$, which are congruent mod 10. That is, adding a multiple of 2 to a given value of s makes the $5s$ term in x repeat itself mod 10. So I can get all possibilities for x mod 10 by letting $s = 0, 1$.

All together, the distinct solutions mod 10 are

$$x = 5s + 3t, \quad y = -1 - t, \quad \text{where} \quad s = 0, 1 \quad \text{and} \quad t = 0, 1, \ldots, 9. \quad \square$$

The Chinese Remainder Theorem

- The **Chinese Remainder Theorem** gives solutions to systems of congruences with relatively prime moduli.
- The solution to a system of congruences with relatively prime moduli may be produced using a *formula* by computing modular inverses, or using an *iterative procedure* involving successive substitution.

The **Chinese Remainder Theorem** says that certain systems of simultaneous congruences *with different moduli* have solutions. The idea embodied in the theorem was apparently known to Chinese mathematicians a long time ago — hence the name.

I'll begin by collecting some useful lemmas.

Lemma 1. Let m and $a_1, \ldots, a_n$ be positive integers. If m is relatively prime to each of $a_1, \ldots, a_n$, then it is relatively prime to their product $a_1 \cdots a_n$.

Proof. If $(m, a_1 \cdots a_n) \neq 1$, then there is a prime p which divides both m and $a_1 \cdots a_n$. Since $p \mid a_1 \cdots a_n$, p must divide a_i for some i. Now p divides both m and a_i, so $(m, a_i) \neq 1$. This contradiction implies that $(m, a_1 \cdots a_n) = 1$. □

Example. 6 is relatively prime to 25, to 7, and to 11. $25 \cdot 7 \cdot 11 = 1925$, and $(6, 1925) = 1$:

a	q
1925	-
6	320
5	1
1	5

□

I showed earlier that the greatest common divisor (a, b) of a and b is *greatest* in the sense that it is divisible by any common divisor of a and b. The next result is the analogous statement for least common multiples.

Lemma 2. Let m and $a_1, \ldots, a_n$ be positive integers. If m is a multiple of each of $a_1, \ldots, a_n$, then m is a multiple of $[a_1, \ldots, a_n]$.

Proof. By the Division Algorithm, there are unique numbers q and r such that

$$m = q \cdot [a_1, \ldots, a_n] + r, \text{ where } 0 \leq r < [a_1, \ldots, a_n].$$

Now a_i divides both m and $[a_1, \ldots, a_n]$, so a_i divides r. Since this is true for all i, r is a common multiple of the a_i smaller than the *least* common multiple $[a_1, \ldots, a_n]$. This is only possible if $r = 0$. Then $m = q \cdot [a_1, \ldots, a_n]$, i.e. m is a multiple of $[a_1, \ldots, a_n]$. □

Example. 88 is a multiple of 4 and 22. The least common multiple of 4 and 22 is 44, and 88 is also a multiple of 44. □

Lemma 3. Let $a_1, \ldots, a_n$ be positive integers. If $a_1, \ldots, a_n$ are pairwise relatively prime (that is, $(a_i, a_j) = 1$ for $i \neq j$), then

$$[a_1, \ldots, a_n] = a_1 \cdots a_n.$$

Proof. Induct on n. The statement is trivially true for $n = 1$, so I'll start with $n = 2$. The statement for $n = 2$ follows from the equation $xy = [x, y](x, y)$:

$$[a_1, a_2] = \frac{a_1 a_2}{(a_1, a_2)} = \frac{a_1 a_2}{1} = a_1 a_2.$$

Now assume $n > 2$, and assume the result is true for n. I will prove that it holds for $n + 1$.

Claim: $[[a_1, \ldots, a_n], a_{n+1}] = [a_1, \ldots, a_n, a_{n+1}]$.

(Some people take this as an iterative *definition* of $[a_1, \ldots, a_n, a_{n+1}]$.) $[a_1, \ldots, a_n, a_{n+1}]$ is a multiple of each of $a_1, \ldots, a_n$, so by Lemma 2 it's a multiple of $[a_1, \ldots, a_n]$. It's also a multiple of a_{n+1}, so

$$[[a_1, \ldots, a_n], a_{n+1}] \mid [a_1, \ldots, a_n, a_{n+1}].$$

On the other hand, for $i = 1, \ldots, n$,

$$a_i \mid [a_1, \ldots, a_n] \quad \text{and} \quad [a_1, \ldots, a_n] \mid [[a_1, \ldots, a_n], a_{n+1}].$$

Therefore,

$$a_i \mid [[a_1, \ldots, a_n], a_{n+1}].$$

Obviously,

$$a_{n+1} \mid [[a_1, \ldots, a_n], a_{n+1}].$$

Thus, $[[a_1, \ldots, a_n], a_{n+1}]$ is a common multiple of all the a_i's. Since $[a_1, \ldots, a_n, a_{n+1}]$ is the least common multiple, Lemma 2 implies that

$$[a_1, \ldots, a_n, a_{n+1}] \mid [[a_1, \ldots, a_n], a_{n+1}].$$

Since I have two *positive* numbers which divide one another, they're equal:

$$[[a_1, \ldots, a_n], a_{n+1}] = [a_1, \ldots, a_n, a_{n+1}].$$

This proves the claim.
Returning to the proof of the induction step, I have

$$[a_1, \ldots, a_n, a_{n+1}] = [[a_1, \ldots, a_n], a_{n+1}] = [a_1 \cdots a_n, a_{n+1}] = a_1 \cdots a_n a_{n+1}.$$

The second equality follows by the induction hypothesis (the statement for n). The third equality follows from Lemma 1 and the result for $n = 2$. □

Example. 6, 25, and 7 are relatively prime (in pairs). The least common multiple is $[6, 25, 7] = 1050 = 6 \cdot 25 \cdot 7$. □

Theorem. (**The Chinese Remainder Theorem**) Suppose $m_1, \ldots, m_n$ are pairwise relatively prime (that is, $(n_i, m_j) = 1$ for $i \neq j$). Then the system of congruences

$$\begin{aligned} x &= a_1 \pmod{m_1} \\ x &= a_2 \pmod{m_2} \\ &\vdots \\ x &= a_n \pmod{m_n} \end{aligned}$$

has a unique solution mod $m_1 m_2 \cdots m_n$.

Notation.

$$x_1 x_2 \cdots \widehat{x_i} \cdots x_n$$

means the product $x_1 x_2 \cdots x_i \cdots x_n$ with x_i omitted. For example,

$$x_1 x_2 \cdots \widehat{x_4} \cdots x_6 \quad \text{means} \quad x_1 x_2 x_3 x_5 x_6.$$

This is a convenient (and standard) notation for omitting a single variable term in a product of things. □

Proof. Define

$$p_k = m_1 \cdots \widehat{m_k} \cdots m_n.$$

That is, p_k is the product of the m's with m_k omitted. By Lemma 1, $(p_k, m_k) = 1$. Hence, there are numbers s_k, t_k such that

$$s_k p_k + t_k m_k = 1.$$

In terms of congruences,

$$s_k p_k = 1 \pmod{m_k}.$$

Now let

$$x = a_1 p_1 s_1 + a_2 s_2 p_2 + \cdots + a_n p_n s_n.$$

If $j \neq k$, then $m_k \mid p_j$, so mod m_k all the terms but the k-th term die:

$$x = a_k p_k s_k = a_k \cdot 1 = a_k \pmod{m_k}.$$

This proves that x is a solution to the system of congruences (and incidentally, gives a formula for x). Now suppose that x and y are two solutions to the system of congruences.

$$\begin{aligned} x &= a_1 \pmod{m_1} \quad \text{and} \quad y = a_1 \pmod{m_1} \\ x &= a_2 \pmod{m_2} \quad \text{and} \quad y = a_2 \pmod{m_2} \\ &\vdots \\ x &= a_n \pmod{m_n} \quad \text{and} \quad y = a_n \pmod{m_n} \end{aligned}$$

Then

$$x = a_k = y \pmod{m_k} \quad \text{so} \quad x - y = 0 \pmod{m_k} \quad \text{or} \quad m_k \mid x - y.$$

Thus, $x - y$ is a multiple of all the m's, so

$$[m_1, \ldots, m_n] \mid x - y.$$

But the m's are pairwise relatively prime, so by Lemma 3,

$$m_1 \cdots m_n \mid x - y, \text{ i.e. } x = y \pmod{m_1 \cdots m_n}.$$

That is, the solution to the congruences is unique mod $m_1 \cdots m_n$. □

Example. Solve

$$\begin{aligned} x &= 2 \pmod{4} \\ x &= 7 \pmod{9} \end{aligned}.$$

$(4, 9) = 1$, so there is a unique solution mod 36. Following the construction of x in the proof,

$$p_1 = 9, \quad 9 \cdot 1 = 1 \pmod 4, \text{ so take } s_1 = 1$$

$$p_2 = 4, \quad 4 \cdot 7 = 1 \pmod 9, \text{ so take } s_2 = 7$$

Solution:

$$x = a_1 p_1 s_1 + a_2 p_2 s_2 = 18 + 196 = 214 = 34 \pmod{36}. \quad \square$$

Example. Solve

$$\begin{aligned} x &= 3 \pmod 4 \\ x &= 1 \pmod 5 \\ x &= 2 \pmod 3 \end{aligned}.$$

The moduli are pairwise relatively prime, so there is a unique solution mod 60. This time, I'll solve the system using an iterative method.

$$x = 3 \pmod 4, \quad \text{so} \quad x = 3 + 4s.$$

But $x = 1 \pmod 5$, so

$$3 + 4s = 1 \pmod 5, \quad 4s = 3 \pmod 5, \quad 4 \cdot 4s = 4 \cdot 3 \pmod 5, \quad s = 2 \pmod 5, \quad s = 2 + 5t.$$

Hence,

$$x = 3 + 4s = 3 + 4(2 + 5t) = 11 + 20t.$$

Finally, $x = 2 \pmod 3$, so

$$11 + 20t = 2 \pmod 3, \quad 20t = -9 = 0 \pmod 3, \quad 2t = 0 \pmod 3, \quad 2 \cdot 2t = 2 \cdot 2 \pmod 3, \quad t = 0 \pmod 3.$$

Hence, $t = 3u$.
Now put everything back:

$$x = 11 + 20t = 11 + 20(3u) = 11 + 60u, \quad \text{or} \quad x = 11 \pmod{60}. \quad \square$$

You can sometimes solve a system even if the moduli aren't relatively prime; the criteria are similar to those for solving system of linear Diophantine equations. I'll state the result, but omit the proof.

Theorem. Consider the system

$$\begin{aligned} x &= a_1 \pmod{m_1} \\ x &= a_2 \pmod{m_2} \end{aligned}$$

(a) If $(m_1, m_2) \not| a_1 - a_2$, there are no solutions.

(b) If $(m_1, m_2) \mid a_1 - a_2$, there is a unique solution mod $[m_1, m_2]$. $\square$

Note that if $(m_1, m_2) = 1$, case (b) automatically holds, and $[m_1, m_2] = m_1 m_2$ — i.e. I get the Chinese Remainder Theorem for $n = 2$.

Example. Solve

$$\begin{matrix} x = 5 \pmod{12} \\ x = 11 \pmod{18} \end{matrix}.$$

Since $(12, 18) = 6 \mid 11 - 5$, there is a unique solution mod $[12, 18] = 36$. I'll use the iterative method to find the solution.

$$x = 5 \pmod{12}, \quad \text{so} \quad x = 5 + 12s.$$

Since $x = 11 \pmod{18}$,

$$5 + 12s = 11 \pmod{18}, \quad 12s = 6 \pmod{18}.$$

Now I use my rule for "dividing" congruences: 6 divides both 12 and 6, and $(6, 18) = 6$, so I can divide through by 6:

$$2s = 1 \pmod{3}.$$

Multiply by 2, and convert the congruence to an equation:

$$s = 2 \pmod{3}, \quad s = 2 + 3t.$$

Plug back in:

$$x = 5 + 12s = 5 + 12(2 + 3t) = 29 + 36t, \quad x = 29 \pmod{36}. \quad \square$$
