2-16-2019

Modular Arithmetic

Definiton. Let a, b, and m be integers. $a = b \pmod{m}$ (read "a equals b mod m" or a is congruent to b mod m) if any of the following equivalent conditions hold:

(a) $m \mid a - b$.

(b) $m \mid b - a$.

(c) $a = b + jm$ (or $a - b = jm$) for some $j \in \mathbb{Z}$.

(d) $b = a + km$ (or $b - a = km$) for some $k \in \mathbb{Z}$.

m is called the **modulus** of the congruence. I will almost always work with positive moduli.

Note that $a = 0 \pmod{m}$ if and only if $m \mid a$. Thus, modular arithmetic gives you another way of dealing with divisibility relations. Another way of saying this is: Mod m any multiple of m is 0.

Remark. Many people prefer to write "$a \equiv b \pmod{m}$". Since equality mod m is an equivalence relation, since "=" is a little less writing than "$\equiv$", and since there isn't much risk of confusion, I'll write "=".

Example.

(a) Reduce $101 \pmod{3}$ to a number in the range $\{0, 1, 2\}$.

(b) Reduce $-101 \pmod{3}$ to a number in the range $\{0, 1, 2\}$.

(a) $101 = 2 \pmod{3}$, because $3 \mid 101 - 2 = 99$.

(b) $-101 = 1 \pmod{3}$, because $3 \mid -101 - 1 = -102$. □

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 by way of example. 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 $a = c \pmod{m}$. □

Theorem. Suppose $a = b \pmod{m}$ and $c = d \pmod{m}$. Then:

(a) $a + c = b + d \pmod{m}$.

(b) $ac = bd \pmod{m}$.

Note that you can use the second property and induction to show that if $a = b \pmod{m}$, then

$$a^n = b^n \pmod{m} \quad \text{for all} \quad n \geq 1.$$

Proof. Suppose $a = b \pmod{m}$ and $c = d \pmod{m}$.

(a) $m \mid a - b$ and $m \mid c - d$, so by properties of divisibility,

$$m \mid (a - b) + (c - d) = (a + c) - (b + d).$$

This implies that $a + c = b + d \pmod{m}$.

(b) $m \mid a - b$ and $m \mid c - d$ imply that there are integers j and k such that

$$a = b + mj \quad \text{and} \quad c = d + mk.$$

Multiplying these two equations, I obtain

$$\begin{aligned} ac &= (b + mj)(d + mk) \\ ac &= bd + m(dj + bk + mjk) \\ ac - bd &= m(dj + bk + mjk) \end{aligned}$$

Hence, $m \mid ac - bd$, so $ac = bd \pmod{m}$. □

Corollary. Suppose $a = b \pmod{m}$. Then:

(a) $a \pm c = b \pm c \pmod{m}$.

(b) $ac = bc \pmod{m}$.

Proof. Apply the theorem to the equations $a = b \pmod{m}$ and $c = c \pmod{m}$. □

Assume that the modulus m is a positive integer. By the Division Algorithm, every integer n can be written as

$$n = qm + r \quad \text{where} \quad 0 \leq r < m.$$

Reducing this equation mod m, I have $qm = 0 \pmod{m}$, so

$$n = r \pmod{m}.$$

Since $0 \leq r < m$, I have $r \in \{0, 1, \ldots m - 1\}$. In other words, mod m every integer can be reduced to a number in $\{0, 1, \ldots m - 1\}$. This set is called the **standard residue system mod** m, and answers to modular arithmetic problems will usually be simplified to a number in this range.

Example. (a) What are the equivalence classes under the relation of congruence mod 3?

(b) Construct an addition table for addition mod 3.

(a) 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 $\mathbb{Z}$.)

(b) 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, but I would have gotten an equivalent table. The simplest thing is to use the numbers $\{0, 1, 2\}$ from the standard residue system mod 3. □

Example. (**Reducing an expression mod n**) Reduce $100^5 \pmod 7$ to an element in the standard residue system $\{0, 1, \ldots, 6\}$.

$100 = 2 \pmod 7$, so

$$100^5 = 2^5 = 32 = 4 \pmod 7 . \quad \square$$

Example. Simplify $994 \cdot 996 \cdot 997 \cdot 998 \pmod{1000}$ to a number in the range $\{0, 1, \ldots 999\}$.

Rather than deal with large "positive" numbers, I'll convert them to small "negative" numbers:

$$994 = -6 \pmod{1000}, \quad 996 = -4 \pmod{1000}, \quad 997 = -3 \pmod{1000}, \quad 998 = -2 \pmod{1000}.$$

So

$$994 \cdot 996 \cdot 997 \cdot 998 = (-6)(-4)(-3)(-2) = 144 \pmod{1000} . \quad \square$$

Example. (**A modular binomial theorem**) Prove that 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,

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

Example. Prove that if $x \in \mathbb{Z}$, then $4x^2 + x + 3$ is not divisible by 5.

The phrase "not divisible by 5" leads one to think of doing things mod 5.
Every integer is equal to one of 0, 1, 2, 3, or 4 mod 5. Make a table:

$x \pmod 5$	0	1	2	3	4
$4x^2 + x + 3 \pmod 5$	3	3	1	2	1

From the table, $4x^2 + x + 3 \neq 0 \pmod 5$ for all $x \in \mathbb{Z}$, so $5 \nmid 4x^2 + x + 3$ for all $x \in \mathbb{Z}$. □

Example. Give a counterexample to show that $a = b \pmod n$ does not imply that $x^a = x^b \pmod n$, for $a, b, n, x \in \mathbb{Z}$.

For instance, $7 = 4 \pmod 3$, but $2^7 \neq 2^4 \pmod 3$ (since $128 \neq 16 \pmod 3$). □

Example. Solve the congruence

$$6x + 1 = 2(x + 2) \pmod 7 .$$

The modular arithmetic properties allow me to solve this equation the way I would solve a linear equation, up to a point. I multiply out the left side, then get the x's on one side:

$$\begin{aligned} 6x + 1 &= 2(x + 2) \pmod 7 \\ 6x + 1 &= 2x + 4 \pmod 7 \\ 4x &= 3 \pmod 7 \end{aligned}$$

If this were an equation over the real numbers, you could divide both sides by 4 — equivalently, multiply both sides by $\frac{1}{4}$.

What would "$\frac{1}{4}$" mean mod 7? This is the multiplicative inverse of 4, which we write as 4^{-1} (in modular arithmetic you don't use fraction notation). This means: What number multiplied by 4 gives 1 mod 7?

Since there are only 7 numbers mod 7, I can do this by trial and error, multiplying 4 by 0, 1, ... until I get 1. I find that

$$2 \cdot 4 = 8 = 1 \pmod 7 .$$

So for this modular equation, I multiply both sides by 2:

$$\begin{aligned} 2 \cdot 4x &= 2 \cdot 3 \pmod 7 \\ 8x &= 6 \pmod 7 \\ x &= 6 \pmod 7 \end{aligned}$$ □

You can see that finding multiplicative inverses mod n can be useful in solving congruences. Sometimes they can be found by more refined trial and error than simply trying all the numbers mod n.

Since multiples of n equal 0 mod n,

$$1 = 1 + n = 1 + 2n = 1 + 3n = \cdots \pmod n .$$

I can sometimes use this to find inverses mod n.

Example.

(a) Use trial and error to find $5^{-1} \pmod 7$.

(b) Use trial and error to find $45^{-1} \pmod{89}$.

(c) Prove that 25 does not have a multiplicative inverse mod 30.

(a) I take multiples of 7 and add 1, stopping when I get a number which is divisible by 5:

$$7 + 1 = 8, \quad \text{but} \quad 5 \not| 8.$$

$$14 + 1 = 15. \quad \text{and} \quad 5 \mid 15.$$

Since $3 \cdot 5 = 15$, I have $5^{-1} = 3 \pmod 7$. □

(b) I take multiples of 89 and add 1, stopping when I get a number which is divisible by 45:

$$89 + 1 = 90, \quad \text{and} \quad 45 \mid 90.$$

Since $2 \cdot 45 = 90$, I have $45^{-1} = 2 \pmod{90}$. □

(c) Suppose that $25x = 1 \pmod{30}$ (so $x = 25^{-1} \pmod{30}$). Then

$$\begin{aligned} 25x &= 1 \pmod{30} \\ 6 \cdot 25x &= 6 \cdot 1 \pmod{30} \\ 150x &= 6 \pmod{30} \\ 0 &= 6 \pmod{30} \end{aligned}$$

This contradiction shows that there is no such x, so 25 does not have a multiplicative inverse mod 30. □

The previous method still has its limitations, as you can see by trying to use it to find $47^{-1} \pmod{61}$. And as you saw, some elements don't have multiplicative inverses mod n. The following theorem says which elements have multiplicative inverses, and how to find them if they exist.

Theorem. m has a multiplicative inverse mod n if and only if $(m, n) = 1$.

Proof. Suppose m has a multiplicative inverse mod n. This means that $am = 1 \pmod n$ for some a. Then

$$am + bn = 1 \quad \text{for some} \quad b \in \mathbb{Z}.$$

Hence, $(m, n) = 1$.
Conversely, if $(m, n) = 1$, then

$$am + bn = 1 \quad \text{for some} \quad a, b \in \mathbb{Z}.$$

Reducing mod n, I get $am = 1 \pmod n$, which means that m has a multiplicative inverse mod n. □

As the proof shows, you can find $a^{-1} \pmod n$ by applying the Extended Euclidean algorithm to a and n.

Example. (**Finding elements which have multiplicative inverses**) Which elements of $\{0, 1, 2, \ldots, 11\}$ have multiplicative inverses mod 12?

The numbers in $\{0, 1, 2, \ldots, 11\}$ which are relatively prime to 12 and 1, 5, 7, and 11. Hence, 1, 5, 7, and 11 have multiplicative inverses mod 12. □

Example. Find $47^{-1} \pmod{61}$.

Apply the Extended Euclidean Algorithm to 61 and 47:

61	-	13
47	1	10
14	3	3
5	2	1
4	1	1
1	4	0

Write the linear combination, then reduce mod 61:

$$(-10) \cdot 61 + 13 \cdot 47 = 1$$
$$13 \cdot 47 = 1 \pmod{61}$$

Hence, $47^{-1} = 13 \pmod{61}$. □

Proposition. If $ac = bc \pmod{m}$, then

$$a = b \left(\mod \frac{m}{(c,m)}\right).$$

Proof. Write

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

Then

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

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

$$k = \frac{c}{(c,m)}j \quad \text{for some} \quad j \in \mathbb{Z}.$$

Hence,

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

Therefore, $a = b \left(\mod \frac{m}{(c,m)}\right)$. □

Notice that you "divide the equality" by c, but you divide the modulus by (c,m).

Example. (**Solving a congruence with cancellation**) Solve

$$12x = 30 \pmod{38}.$$

$$12x = 30 \pmod{38}$$
$$6 \cdot 2x = 6 \cdot 5 \pmod{38}$$

By the previous result, if I "cancel" the factors of 6, I must divide the modulus by $(6, 38) = 2$. This makes the modulus 19:

$$6 \cdot 2x = 6 \cdot 5 \pmod{38}$$
$$2x = 5 \pmod{19}$$

Now $(2, 19) = 1$, so I can solve this congruence by multiplying by $2^{-1} \pmod{19}$. Noting that $2 \cdot 10 = 10 = 1 \pmod{19}$, I see that I need to multiply by 10:

$$10 \cdot 2x = 10 \cdot 5 \pmod{19}$$
$$20x = 50 \pmod{19}$$
$$x = 12 \pmod{19}$$

(If you didn't see that $2^{-1} = 10 \pmod{19}$ by trial, you'd use the Extended Euclidean algorithm as before.)

The original congruence was mod 38, so I want all solutions in the range $\{0, 1, \ldots 37$. I have one: $x = 12$. To get others, I add multiples of 19 until I exceed 37. Thus, $x = 12 + 19 = 31$ is the other solution.

All together, the solutions are $x = 12 \pmod{38}$ and $x = 31 \pmod{38}$. □

Example. (**A congruence with no solutions**) Show that the following congruence has no solutions:

$$4x = 5 \pmod{14}.$$

Suppose that x is a solution. Multiply the equation by 7:

$$4x = 5 \pmod{14}$$
$$7 \cdot 4x = 7 \cdot 5 \pmod{14}$$
$$28x = 35 \pmod{14}$$
$$0 = 7 \pmod{14}$$

This contradiction shows that the equation has no solutions. □

These examples show that linear congruences may have solutions or may be unsolvable. We can understand better what is happening by relating them to linear Diophantine equations.