2-9-2018

Modular Arithmetic

Modular arithmetic is a way of systematically ignoring differences involving a multiple of an integer. If n is an integer, two integers are equal mod n if they differ by a multiple of n; it is as if multiples of n are "set equal to 0".

Definition. Let n, x, and y be integers. x is **congruent to** y **mod** n if $n \mid x - y$. Notation:

$$x = y \pmod{n}.$$

Remarks. $n \mid x - y$ is equivalent to the following statements:

(a) $n \mid y - x$.

(b) $x = y + jn$ for some $j \in \mathbb{Z}$.

(c) $y = x + kn$ for some $k \in \mathbb{Z}$.

I'll often use any of these four statements as the definition of $x = y \pmod{n}$.

A lot of people like to write "$x \cong y \pmod{n}$" instead of "$x = y \pmod{n}$". I don't think there's any harm in using an ordinary equal sign, since the " $(\mathrm{mod}\ n)$" makes the meaning clear. It's also a bit shorter to write.

Example. (**Examples of congruences with numbers**) (a) Demonstrate that $7 = 1 \pmod{6}$ and $57 = -13 \pmod{7}$.

(b) Express "x is even" and "x is odd" in terms of congruences.

(c) What does $x = 0 \pmod{n}$ means in terms of divisibility?

(a)

$$7 = 1 \pmod{6}, \quad \text{since} \quad 6 \mid 7 - 1.$$

$$57 = -13 \pmod{7}, \quad \text{since} \quad 7 \mid 57 - (-13).$$

(b) x is even if and only if $x = 0 \pmod{2}$ and x is odd if and only if $x = 1 \pmod{2}$. □
(c) $x = 0 \pmod{n}$ if and only if $n \mid x$. Thus, congruences provide a convenient notation for dealing with divisibility relations. □

The following proposition says that you can work with modular equations in many of the ways that you work with ordinary equations.

Proposition. Let $n \in \mathbb{Z}$.

(a) If $a = b \pmod{n}$ and $c = d \pmod{n}$, then

$$a + c = b + d \pmod{n}.$$

(b) If $a = b \pmod{n}$ and $c = d \pmod{n}$, then

$$ac = bd \pmod{n}.$$

(c) If $a = b \pmod{n}$, then

$$ac = bc \pmod{n}.$$

Proof. Two ideas for these kinds of proofs:

1. You can often prove statements about congruences by reducing them to statements about divisibility.

2. You can often prove statements about divisibility by reducing them to (ordinary) equations.

(a) Suppose $a = b \pmod{n}$ and $c = d \pmod{n}$.
$a = b \pmod{n}$ means $n \mid a - b$ and $c = d \pmod{n}$ means $n \mid c - d$. By properties of divisibility,

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

Therefore, $a + c = b + d \pmod{n}$.

(b) Suppose $a = b \pmod{n}$ and $c = d \pmod{n}$.
$a = b \pmod{n}$ means $n \mid a - b$, which means $a - b = jn$ for some $j \in \mathbb{Z}$. $c = d \pmod{n}$ means $n \mid c - d$, which means $c - d = kn$ for some $k \in \mathbb{Z}$. Thus, $a = b + jn$, $c = d + kn$, and hence

$$ac = (b + jn)(d + kn) = bd + bkn + djn + jkn^2 = bd + n(bk + dj + jkn).$$

This gives $ac - bd = n(bk + dj + jkn)$, so $n \mid ac - bd$, and hence $ac = bd \pmod{n}$.

(c) Suppose $a = b \pmod{n}$. This means that $n \mid a - b$. By properties of divisibility,

$$n \mid (a - b)c = ac - bc.$$

Therefore, $ac = bc \pmod{n}$. □

Example. (**Solving a congruence**) Solve $3x + 4 = 2x + 8 \pmod{9}$.

In this case, I'll solve the modular equation by adding or subtracting the same thing from both sides.

$$\begin{array}{rrcrcrcl} & 3x & + & 4 & = & 2x & + & 8 \pmod{9} \\ - & & & 4 & = & & & 4 \pmod{9} \\ \hline & 3x & & & = & 2x & + & 4 \pmod{9} \\ - & 2x & & & = & 2x & & \pmod{9} \\ \hline & x & & & = & & & 4 \pmod{9} \end{array}$$

The solution is $x = 4 \pmod{9}$. □

Example. Reduce $497 \cdot 498 \cdot 499 \pmod{500}$ to a number in the range $\{0, 1, \ldots 499\}$, *doing the computation by hand.*

Note that

$$497 = -3 \pmod{500}, \quad 498 = -2 \pmod{500}, \quad 499 = -1 \pmod{500}.$$

So

$$497 \cdot 498 \cdot 499 = (-3)(-2)(-1) = -6 = 494 \pmod{500}. \quad \square$$

The next result says that congruence mod n is an **equivalence relation**.

Proposition.

(a) (Reflexivity) $a = a \pmod{n}$ for all $a \in \mathbb{Z}$.

(b) (Symmetry) Let $a, b \in \mathbb{Z}$. If $a = b \pmod{n}$, then $b = a \pmod{n}$.

(c) (Transitivity) Let $a, b, c \in \mathbb{Z}$. If $a = b \pmod{n}$ and $b = c \pmod{n}$, then $a = c \pmod{n}$.

Proof. (a) If $a \in \mathbb{Z}$, then $n \mid a - a$, so $a = a \pmod{n}$.

(b) If $a = b \pmod{n}$, then $n \mid a - b$, so $n \mid -(a - b) = b - a$. Therefore, $b = a \pmod{n}$.

(c) Suppose $a = b \pmod{n}$ and $b = c \pmod{n}$. $a = b \pmod{n}$ means $n \mid a - b$; $b = c \pmod{n}$ means $n \mid b - c$. Therefore,

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

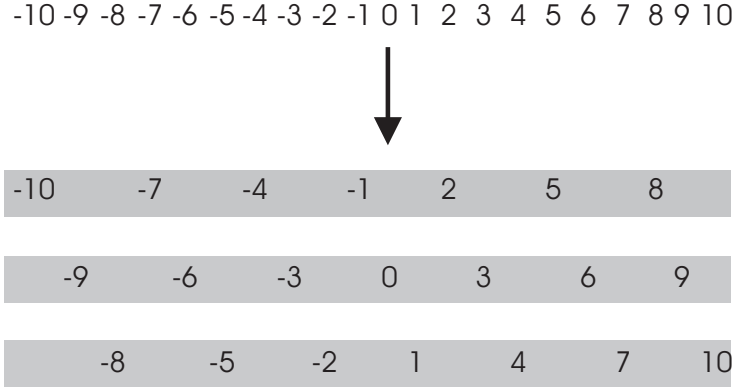
Hence, $a = c \pmod{n}$. □

An equivalence relation on a set gives rise to a **partition** of the set into equivalence classes. In the case of congruence mod n, an equivalence class consists of integers congruent to each other mod n.

Definition. $\mathbb{Z}_n$ (read "Z mod n") is the set of equivalence classes under congruence mod n.

Example. (**Congruence classes mod 3**) Find the equivalence classes of the relation congruence mod 3 on the set of integers.

Relative to the equivalence relation of congruence mod 3 on $\mathbb{Z}$, the integers break up into three *disjoint* sets:



All the elements of a given set are congruent mod 3, and no element in one set is congruent mod 3 to an element of another. The sets divide up the integers like three puzzle pieces.

It's cumbersome to write and use equivalence classes as is, since each equivalence class is a set (infinite, in this case). It's customary to choose a **representative** from each equivalence class and use the representatives to do arithmetic. I'll choose

$$0 \quad \text{from} \quad \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\},$$

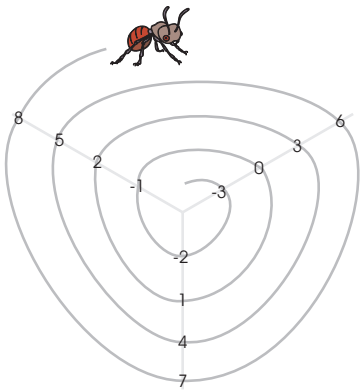
$$1 \quad \text{from} \quad \{\ldots, -8, -5, -2, 1, 4, 7, 10, \ldots\},$$

$$2 \quad \text{from} \quad \{\ldots, -7, -4, -1, 2, 5, 8, 11, \ldots\}.$$

I'll abuse notation and write

$$\mathbb{Z}_3 = \{0, 1, 2\}.$$

$\mathbb{Z}_3$ is called the **cyclic group of order** 3. The "cyclic" nature of $\mathbb{Z}_3$ can be visualized by arranging the integers in a spiral, with each congruence class on a ray.



When you do arithmetic in $\mathbb{Z}_3$, it is as if you count in a circle: 0, 1, 2, then back to 0 again.
You can form other cyclic groups in an analogous way. For example,

$$\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}. \quad \square$$

You can do arithmetic in $\mathbb{Z}_n$ by adding and multiplying as usual, but **reducing the results mod** n.

Example. (**Operation tables for** $\mathbb{Z}_3$) Construct addition and multiplication tables for $\mathbb{Z}_3$.

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

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

For example, as integers $2 + 2 = 4$. I divide 4 by the modulus 3 and get a remainder of 1. Hence, $2 + 2 = 1$.
Likewise, $2 \cdot 2 = 4 = 1$ in $\mathbb{Z}_3$. $\square$

Example. (**Equations in** $\mathbb{Z}_n$) Find $6 \cdot 7$ in $\mathbb{Z}_{11}$, $13 + 19$ in $\mathbb{Z}21$, and -8 in $\mathbb{Z}_{17}$.

$$6 \cdot 7 = 9 \quad \text{in} \quad \mathbb{Z}_{11}.$$
$$13 + 19 = 11 \quad \text{in} \quad \mathbb{Z}_{21}.$$
$$-8 = 9 \quad \text{in} \quad \mathbb{Z}_{17}.$$

-8 means the additive inverse of 8. The last statement is just another way of saying $-8 = 9 \pmod{17}$.
$\square$

Example. (**Using modular arithmetic in a divisibility proof**) Prove that if n is an integer, then $2n^2 + 3n + 2$ is not divisible by 5.

Every integer n is congruent to one of 0, 1, 2, 3, or 4 mod 5. Therefore, I have 5 cases. In each case, I want to show that $2n^2 + 3n + 2$ is not divisible by 5 — or to say it in terms of congruences, I want to show that $2n^2 + 3n + 2 \neq 0 \pmod 5$.

I set $n = 0, 1, 2, 3, 4 \pmod 5$ and "substitute" the value into $2n^2 + 3n + 2$. This substitution is justified by the properties of congruences I discussed above.

For example, if $n = 3 \pmod 5$, then

$$\begin{aligned} n \cdot n &= 3 \cdot 3 \pmod 5 \\ n^2 &= 9 = 4 \pmod 5 \\ 2 \cdot n^2 &= 2 \cdot 4 \pmod 5 \\ 2n^2 &= 8 = 3 \pmod 5 \end{aligned}$$

Likewise, $3n = 3 \cdot 3 = 9 = 4 \pmod 5$. So

$$2n^2 + 3n + 2 = 3 + 4 + 2 = 9 = 4 \pmod 5 .$$

Essentially, I can plug $n = 3$ into $2n^2 + 3n + 2$, then reduce the result mod 5 to one of 0, 1, 2, 3, or 4.

Continuing in this way, I get the following table:

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

In all five cases, $2n^2 + 3n + 2 \neq 0 \pmod 5$. Therefore, $2n^2 + 3n + 2$ is never divisible by 5. □

I showed earlier how to use algebraic operations to solve simple modular equations. How would you solve something like this:

$$6x = 13 \pmod{25}?$$

I'd like to divide both sides by 6, but I only know how to add and multiply. I *can* subtract, but that's because I can add additive inverses. Well, division is multiplication by the multiplicative inverse; what is a multiplicative inverse mod 25?

Definition. Let $a, b \in \mathbb{Z}_n$. a and b are **multiplicative inverses** if $ab = 1 \pmod n$ (or $ab = 1$ in $\mathbb{Z}_n$).

If a is the multiplicative inverse of b, you can write $a = b^{-1}$.

(You don't write "$\frac{1}{b}$" unless you're in a number system like the rational numbers where fractions are in use.)

Example. (**Modular multiplicative inverses**) (a) Prove that 6 and 2 are multiplicative inverses mod 11.

(b) Show that 8 does not have a multiplicative inverse mod 12.

(a) $6 \cdot 2 = 1 \pmod{11}$. □

(b) One tedious way is to take cases:

n	0	1	2	3	4	5
$8n \pmod{12}$	0	8	4	0	8	4
n	6	7	8	9	10	11
$8n \pmod{12}$	0	8	4	0	8	4

No number multiplied by 8 gives 1 mod 12.

I could try all the possibilities because the numbers were small. How would you do this kind of problem if the numbers were larger?

One approach is to simply appeal to the result following this example. However, I can also give a proof by contradiction.

Suppose that 8 has a multiplicative inverse mod 12. Let x be the multiplicative inverse. Then $8x = 1 \pmod{12}$. Multiplying both sides by 3, I get

$$24x = 3 \pmod{12}, \quad \text{or} \quad 0 = 3 \pmod{12}.$$

This is a contradiction, since 0 and 3 do not differ by a multiple of 12. Therefore, 8 does not have a multiplicative inverse mod 12. □

Proposition. $m \in \mathbb{Z}_n$ has a multiplicative inverse if and only if $(m, n) = 1$.

Proof. Suppose $m \in \mathbb{Z}_n$ has a multiplicative inverse, so

$$km = 1 \quad \text{for some} \quad k \in \mathbb{Z}_n.$$

I can regard this as a statement in $\mathbb{Z}$:

$$km = 1 \pmod{n}.$$

This means that km and 1 *differ by* a multiple of n:

$$km - 1 = an \quad \text{for some} \quad a \in \mathbb{Z}.$$

Thus,

$$km - an = 1.$$

This is a linear combination of m and n which gives 1. Therefore, $(m, n) = 1$.

Conversely, suppose $(m, n) = 1$. I may find integers a and b such that

$$am + bn = 1.$$

That is,

$$am = 1 \pmod{n}.$$

Now regarded as an equation in $\mathbb{Z}_n$, this says

$$am = 1 \quad \text{in} \quad \mathbb{Z}_n.$$

That is, m has multiplicative inverse a. □

Example. (**Using the Extended Euclidean algorithm to find modular inverses**) Find the multiplicative inverse of 31 in $\mathbb{Z}_{52}$.

Note that $(31, 52) = 1$. Apply the Extended Euclidean Algorithm:

52	-	5
31	1	3
21	1	2
10	2	1
1	10	0

Thus,

$$1 = 3 \cdot 52 + (-5) \cdot 31.$$

In $\mathbb{Z}_{52}$, $52 = 0$ and $-5 = 47$. The equation says $1 = 47 \cdot 31$. Thus, 47 is the multiplicative inverse of 31 in $\mathbb{Z}_{52}$. □

Theorem. If $(a, n) = 1$, then the following equation has a unique solution:

$$ax = b \quad \text{in} \quad \mathbb{Z}_n.$$

Proof. If $(a, n) = 1$, then a has a multiplicative inverse a^{-1} in $\mathbb{Z}_n$. Thus, $aa^{-1} = 1$ in $\mathbb{Z}_n$.

First, this means that $x = a^{-1}b$ is a solution, since

$$a(a^{-1}b) = (aa^{-1})b = 1 \cdot b = b.$$

Second, if x' is another solution, then $ax' = b$. Multiplying both sides by a^{-1}, I get

$$a^{-1}ax' = a^{-1}b, \quad x' = a^{-1}b.$$

That is, $x' = x$. This means the solution is unique. □

Example. (**Solving modular equations using modular inverses**) Solve

$$13x = 12 \pmod{15}.$$

There is a solution, since $(13, 15) = 1$. I need to find a multiplicative inverse for 13 mod 15.

15	-	7
13	1	6
2	6	1
1	2	0

The Extended Euclidean Algorithm says that

$$(-6)(15) + (7)(13) = 1.$$

Hence, $7 \cdot 13 = 1 \pmod{15}$, i.e. 7 is the multiplicative inverse of 13 mod 15.

Multiply the original equation by 7:

$$7 \cdot 13x = 7 \cdot 12 \pmod{15}, \quad x = 84 = 9 \pmod{15}.$$ □

Proposition. Suppose

$$ac = bc \pmod{n}.$$

Then

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

Proof. I have

$$\begin{aligned} ac &= bc \pmod{n} \\ a\frac{c}{(n,c)} &= b\frac{c}{(n,c)} \pmod{\frac{n}{(n,c)}} \\ a\frac{c}{(n,c)} - b\frac{c}{(n,c)} &= k \cdot \frac{n}{(n,c)} \quad \text{for some} \quad k \in \mathbb{Z} \\ \frac{c}{(n,c)}(a-b) &= k \cdot \frac{n}{(n,c)} \end{aligned}$$

(Note that $(n,c) \mid c$ and $(n,c) \mid n$, so $\dfrac{c}{(n,c)}$ and $\dfrac{n}{(n,c)}$ are actually integers.) Now $\dfrac{n}{(n,c)}$ divides $\dfrac{c}{(n,c)}(a-b)$, but

$$\left(\frac{n}{(n,c)}, \frac{c}{(n,c)}\right) = 1.$$

By Euclid's lemma, $\dfrac{n}{(n,c)} \mid a-b$. Hence,

$$a = b \pmod{\frac{n}{(n,c)}}. \quad \square$$

I can use the preceding result to solve some congruences when I can't immediately use modular inversion.

Example. Solve

$$12x = 30 \pmod{34}.$$

Since $(12, 34) = 2 \neq 1$, 12 doesn't have a multiplicative inverse mod 34. I'll use the preceding result. I "cancel" a factor of 6 from $12x$ and 30, and divide the modulus 34 by $(6, 34) = 2$:

$$\begin{aligned} 12x &= 30 \pmod{34} \\ 6 \cdot 2x &= 6 \cdot 5 \pmod{34} \\ 2x &= 5 \pmod{17} \\ 9 \cdot 2x &= 9 \cdot 5 \pmod{17} \\ x &= 45 = 11 \pmod{17} \end{aligned}$$

Since the original congruence was mod 34, I must find all numbers in $\{0, 1, 2, \ldots 33\}$ which satisfy $x = 11 \pmod{17}$. One is obviously 11. Adding 17, I find that $11 + 17 = 28$ also works. (Adding 17 again takes me out of the set $\{0, 1, 2, \ldots 33\}$.)

The solutions are $x = 11 \pmod{17}$ and $x = 28 \pmod{17}$. $\square$
