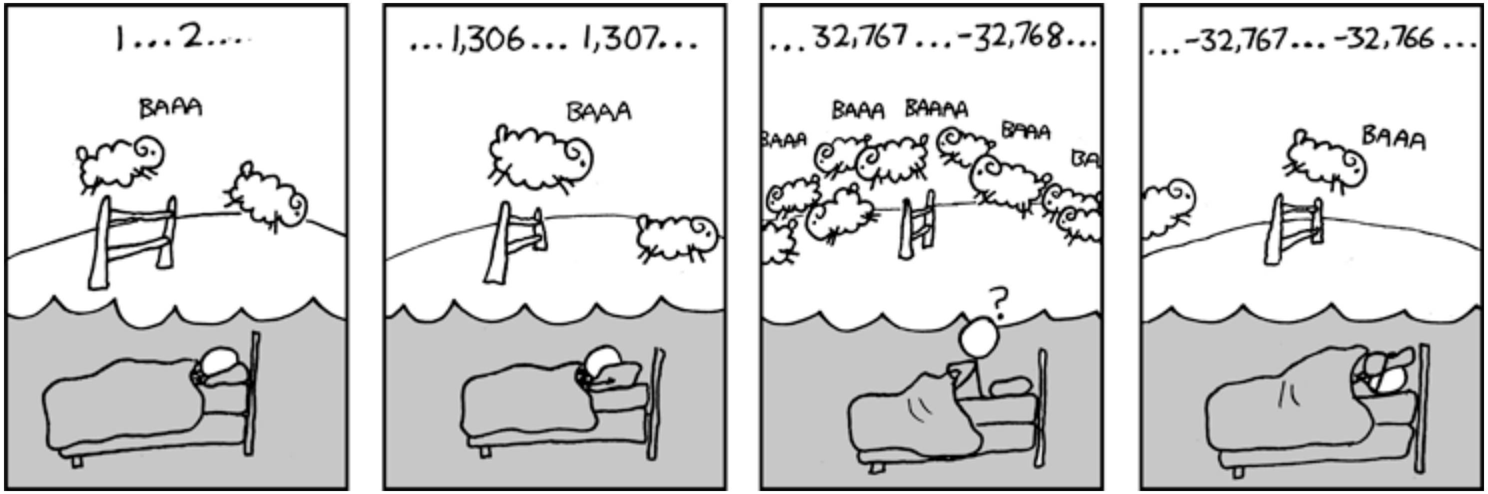
CSE 311: Foundations of Computing

Lecture 10: Modular Arithmetic



Last Class: Divisibility

Definition: "b divides a"

For a, b with $b \neq 0$:

$$b \mid a \leftrightarrow \exists q \ \ (a = qb)$$

Check Your Understanding. Which of the following are true?

5 | 1	25 | 5	5 | 0	3 | 2
5 | 1 iff 1 = 5k	25 | 5 iff 5 = 25k	5 | 0 iff 0 = 5k	3 | 2 iff 2 = 3k
1 | 5	5 | 25	0 | 5	2 | 3
1 | 5 iff 5 = 1k	5 | 25 iff 25 = 5k	0 | 5 iff 5 = 0k	2 | 3 iff 3 = 2k

Last class: Division Theorem

Domain of Discourse
Integers

Division Theorem

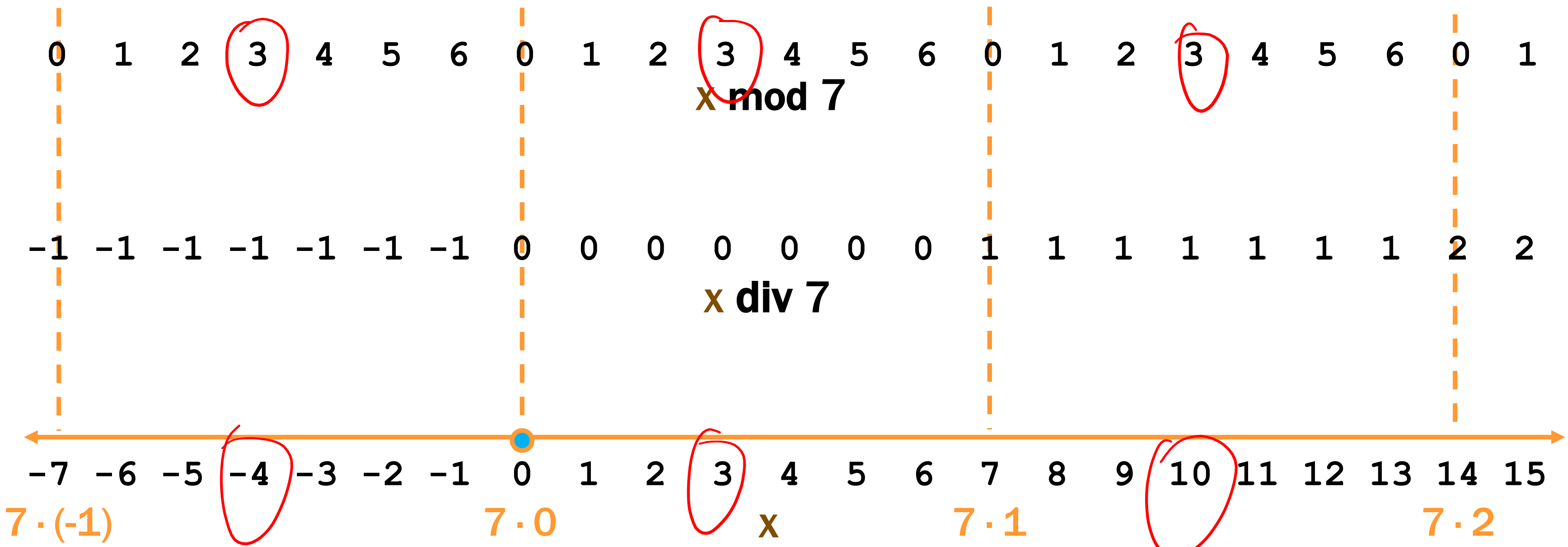
For a, b with $b > 0$
there exist *unique* integers q, r with $0 \leq r < b$
such that $a = qb + r$.

To put it another way, if we divide b into a, we get a unique quotient q = a **div** b
and non-negative remainder r = a **mod** b

Note: r ≥ 0 even if a < 0.
Not quite the same as `a % d`.

Last class: div and mod $x \equiv 3 \pmod{7}$

$$\boxed{x = 7 \cdot (x \text{ div } 7) + (x \text{ mod } 7)}$$



Arithmetic, mod 7

(14 + 1) mod 7
(0 + 1) mod 7

(a + b) mod 7

(a × b) mod 7

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

x	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Modular Arithmetic

Domain of Discourse
Integers

$(14+1)\ m7$

$(0+1)\ m7$

Definition: "a is congruent to b modulo m"

For a, b, m with $m > 0$

$$a \equiv b \pmod{m} \leftrightarrow m \mid (a - b)$$

New notion of "sameness" or "equivalence" that will help us understand modular arithmetic.

$14 \equiv 0 \pmod 7$

This is a predicate (T/F values) on integers a, b, m. It does not produce numbers as output.

$8 \equiv 1 \pmod 7$

There is really a notion of sameness for each $m > 0$.
It may help you to think of $\boldsymbol{a \equiv b} \pmod{m}$ for a fixed $m > 0$ as an equivalence $\boxed{\boldsymbol{a} \equiv_m \boldsymbol{b}}$.
Standard math notation writes the $(\mathrm{mod}\ m)$ on the right to tell you what notion of sameness $\equiv$ means.

Modular Arithmetic

Domain of Discourse
Integers

Definition: "a is congruent to b modulo m"

For a, b, m with $m > 0$

$$a \equiv b \pmod{m} \leftrightarrow m \mid (a - b)$$

A chain of equivalences is written

$$a \equiv b \equiv c \equiv d \pmod{m}$$

This means $a \equiv b \pmod{m}$
and $b \equiv c \pmod{m}$
and $c \equiv d \pmod{m}$

Modular Arithmetic

Domain of Discourse
Integers

Definition: "a is congruent to b modulo m"

For a, b, m with $m > 0$

$$a \equiv b \pmod{m} \leftrightarrow m \mid (a - b)$$

Check Your Understanding. What do each of these mean? When are they true?

x ≡ 0 (mod 2)

This statement is the same as saying "x is even"; so, any x that is even (including negative even numbers) will work.

x is even

-1 ≡ 19 (mod 5)

$-1 - 19 = -20$

This statement is true. 19 - (-1) = 20 which is divisible by 5

true

$5 \mid 20$? ✓

y ≡ 2 (mod 7)

This statement is true for y in { ..., -12, -5, 2, 9, 16, ...}. In other words, all y of the form 2+7k for k an integer.

y has remainder 2 when divided by 7

Modular Arithmetic: A Property

$a \equiv b \pmod{m} \leftrightarrow m \mid (a - b)$

Let $\boldsymbol{a, b, m}$ be integers with $\boldsymbol{m > 0}$.
Then, $\boldsymbol{a \equiv b} \pmod{\boldsymbol{m}}$ if and only if $\boldsymbol{a \bmod m = b \bmod m}$.

Modular Arithmetic: A Property

$a \equiv b \pmod{m} \leftrightarrow m \mid (a - b)$

Let $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{m}$ be integers with $\boldsymbol{m} > \mathbf{0}$.
Then, $\boldsymbol{a} \equiv \boldsymbol{b} \pmod{\boldsymbol{m}}$ if and only if $\boldsymbol{a} \mathbin{\mathbf{mod}} \boldsymbol{m} = \boldsymbol{b} \mathbin{\mathbf{mod}} \boldsymbol{m}$.

($\Leftarrow$) Suppose that $a \bmod m = b \bmod m$.

By the division theorem, $a = mq + (a \bmod m)$ and
$b = ms + (b \bmod m)$ for some integers q,s.

Goal: show $a \equiv b \pmod{m}$, i.e., $m \mid (a - b)$.

Modular Arithmetic: A Property

$a \equiv b \pmod{m} \leftrightarrow m \mid (a-b)$

Let $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{m}$ be integers with $\boldsymbol{m} > \boldsymbol{0}$.
Then, $\boldsymbol{a} \equiv \boldsymbol{b} \pmod{\boldsymbol{m}}$ if and only if $\boldsymbol{a} \bmod \boldsymbol{m} = \boldsymbol{b} \bmod \boldsymbol{m}$.

($\Leftarrow$) Suppose that $a \bmod m = b \bmod m$.

By the division theorem, $a = mq + (a \bmod m)$ and
$b = ms + (b \bmod m)$ for some integers q, s.

Then, $a - b = (mq + (a \bmod m)) - (ms + (b \bmod m))$
$= m(q-s) + (a \bmod m - b \bmod m)$
$= m(q-s)$ since $a \bmod m = b \bmod m$

Goal: show $a \equiv b \pmod{m}$, i.e., $m \mid (a-b)$.

Modular Arithmetic: A Property

$a \equiv b \pmod{m} \leftrightarrow m \mid (a-b)$

Let $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{m}$ be integers with $\boldsymbol{m > 0}$.
Then, $\boldsymbol{a} \equiv \boldsymbol{b}\ (\mathrm{mod}\ \boldsymbol{m})$ if and only if $\boldsymbol{a}\ \mathbf{mod}\ \boldsymbol{m} = \boldsymbol{b}\ \mathbf{mod}\ \boldsymbol{m}$.

($\Leftarrow$) Suppose that $a \bmod m = b \bmod m$.

By the division theorem, $a = mq + (a \bmod m)$ and
$b = ms + (b \bmod m)$ for some integers q,s.

Then, $a - b = (mq + (a \bmod m)) - (ms + (b \bmod m))$
$= m(q - s) + (a \bmod m - b \bmod m)$
$= m(q - s)$ since $a \bmod m = b \bmod m$

Therefore, $m \mid (a - b)$ and so $a \equiv b \pmod{m}$.

Goal: show $a \equiv b \pmod{m}$, i.e., $m \mid (a - b)$.

(Halfway there)

Modular Arithmetic: A Property

$a \equiv b \pmod{m} \leftrightarrow m \mid (a - b)$

Let $\boldsymbol{a, b, m}$ be integers with $\boldsymbol{m > 0}$.
Then, $\boldsymbol{a \equiv b \pmod{m}}$ if and only if $\boldsymbol{a \bmod m = b \bmod m}$.

($\Rightarrow$) Suppose that $a \equiv b \pmod{m}$.

Then, $m \mid (a - b)$ by definition of congruence.
So, $a - b = km$ for some integer k by definition of divides.
Therefore, $a = b + km$.

Goal: show $a \bmod m \equiv b \bmod m$

Modular Arithmetic: A Property

$a \equiv b \pmod{m} \leftrightarrow m \mid (a - b)$

Let $\boldsymbol{a, b, m}$ be integers with $\boldsymbol{m > 0}$.
Then, $\boldsymbol{a \equiv b} \pmod{\boldsymbol{m}}$ if and only if $\boldsymbol{a \bmod m = b \bmod m}$.

(⇒) Suppose that $a \equiv b \pmod{m}$.

Then, $m \mid (a - b)$ by definition of congruence.
So, $a - b = km$ for some integer k by definition of divides.
Therefore, $a = b + km$.

By the Division Theorem, we have $a = qm + (a \bmod m)$,
where $0 \leq (a \bmod m) < m$.

Goal: show $a \bmod m \equiv b \bmod m$

Modular Arithmetic: A Property

$a \equiv b \pmod{m} \leftrightarrow m \mid (a - b)$

Let $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{m}$ be integers with $\boldsymbol{m} > \boldsymbol{0}$.
Then, $\boldsymbol{a} \equiv \boldsymbol{b} \pmod{\boldsymbol{m}}$ if and only if $\boldsymbol{a} \bmod \boldsymbol{m} = \boldsymbol{b} \bmod \boldsymbol{m}$.

(⇒) Suppose that $a \equiv b \pmod{m}$.

Then, $m \mid (a - b)$ by definition of congruence.
So, $a - b = km$ for some integer k by definition of divides.
Therefore, $a = b + km$.

By the Division Theorem, we have $a = qm + (a \bmod m)$, where $0 \leq (a \bmod m) < m$.

Combining these, we have $qm + (a \bmod m) = a = b + km$
or equiv., $b = qm - km + (a \bmod m) = (q - k)m + (a \bmod m)$.
By the Division Theorem, we have $b \bmod m = a \bmod m$. ■

Goal: show $a \bmod m \equiv b \bmod m$

Modular Arithmetic: A Property

$a \equiv b \pmod{m} \leftrightarrow m \mid (a - b)$

Let $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{m}$ be integers with $\boldsymbol{m} > \boldsymbol{0}$.
Then, $\boldsymbol{a} \equiv \boldsymbol{b} \pmod{\boldsymbol{m}}$ if and only if $\boldsymbol{a} \bmod \boldsymbol{m} = \boldsymbol{b} \bmod \boldsymbol{m}$.

(⇒) Suppose that $a \equiv b \pmod{m}$.

Then, $m \mid (a - b)$ by definition of congruence.
So, $a - b = km$ for some integer k by definition of divides.
Therefore, $a = b + km$.

By the Division Theorem, we have $a = qm + (a \bmod m)$,
where $0 \leq (a \bmod m) < m$.

Combining these, we have $qm + (a \bmod m) = a = b + km$
or equiv., $b = qm - km + (a \bmod m) = (q - k)m + (a \bmod m)$.
By the Division Theorem, we have $b \bmod m = a \bmod m$. ∎

Goal: show $a \bmod m \equiv b \bmod m$

Modular Arithmetic: A Property

Let a, b, m be integers with $m >$
Then, $a \equiv b \pmod{m}$ if and only

In future, we will usually go directly between these without discussing "divides" every time.

($\Rightarrow$) Suppose that $a \equiv b \pmod{m}$.

Then, $m \mid (a - b)$ by definition of congruence.
So, $a - b = km$ for some integer k by definition of divides.
Therefore, $a = b + km$.

By the Division Theorem, we have $a = qm + (a \bmod m)$,
where $0 \leq (a \bmod m) < m$.

Combining these, we have $qm + (a \bmod m) = a = b + km$
or equiv., $b = qm - km + (a \bmod m) = (q - k)m + (a \bmod m)$.
By the Division Theorem, we have $b \bmod m = a \bmod m$. $\blacksquare$

The $\mathbf{mod}\ \boldsymbol{m}$ function vs the $\equiv \pmod{\boldsymbol{m}}$ predicate

- What we have just shown
  - The $\mathbf{mod}\ \boldsymbol{m}$ function maps any integer $\boldsymbol{a}$ to a remainder $\boldsymbol{a}\ \mathbf{mod}\ \boldsymbol{m} \in \{0,1,..,\boldsymbol{m}-1\}$.
  - Imagine grouping together all integers that have the same value of the $\mathbf{mod}\ \boldsymbol{m}$ function

    That is, the same remainder in $\{0,1,..,\boldsymbol{m}-1\}$.
  - The $\equiv \pmod{\boldsymbol{m}}$ predicate compares integers $\boldsymbol{a}, \boldsymbol{b}$. It is true if and only if the $\mathbf{mod}\ \boldsymbol{m}$ function has the same value on $\boldsymbol{a}$ and on $\boldsymbol{b}$.

    That is, $\boldsymbol{a}$ and $\boldsymbol{b}$ are in the same group.

Recall: Familiar Properties of "="

- If $a = b$ and $b = c$, then $a = c$.
  - i.e., if $a = b = c$, then $a = c$

$$\begin{array}{rl} & a = b \\ + & c = d \\ \hline & a+c = b+d \end{array}$$

- If $a = b$ and $c = d$, then $a + c = b + d$.
  - in particular, since $c = c$ is true, we can "$+\ c$" to both sides
- If $a = b$ and $c = d$, then $ac = bd$.
  - in particular, since $c = c$ is true, we can "$\times c$" to both sides

These are the facts that allow us to use algebra to solve problems

Modular Arithmetic: Basic Property

Let m be a positive integer.
If $\boldsymbol{a} \equiv \boldsymbol{b} \pmod{m}$ and $\boldsymbol{b} \equiv \boldsymbol{c} \pmod{m}$,
then $\boldsymbol{a} \equiv \boldsymbol{c} \pmod{m}$.

Modular Arithmetic: Basic Property

Let m be a positive integer.
If $\boldsymbol{a} \equiv \boldsymbol{b} \pmod{m}$ and $\boldsymbol{b} \equiv \boldsymbol{c} \pmod{m}$,
then $\boldsymbol{a} \equiv \boldsymbol{c} \pmod{m}$.

Suppose that $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$.

Modular Arithmetic: Basic Property

Let m be a positive integer.
If $\boldsymbol{a} \equiv \boldsymbol{b} \pmod{m}$ and $\boldsymbol{b} \equiv \boldsymbol{c} \pmod{m}$,
then $\boldsymbol{a} \equiv \boldsymbol{c} \pmod{m}$.

Suppose that $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$.
Then, by the previous property, we have
$a \bmod m = b \bmod m$ and $b \bmod m = c \bmod m$.

Putting these together, we have $a \bmod m = c \bmod m$, which says that $a \equiv c \pmod{m}$, by the previous property.

∎

Modular Arithmetic: Addition Property

Let m be a positive integer.
If $\boldsymbol{a} \equiv \boldsymbol{b} \pmod{m}$ and $\boldsymbol{c} \equiv \boldsymbol{d} \pmod{m}$
then $\boldsymbol{a} + \boldsymbol{c} \equiv \boldsymbol{b} + \boldsymbol{d} \pmod{m}$.

Modular Arithmetic: Addition Property

Let m be a positive integer.
If $\boldsymbol{a} \equiv \boldsymbol{b} \pmod{m}$ and $\boldsymbol{c} \equiv \boldsymbol{d} \pmod{m}$
then $\boldsymbol{a} + \boldsymbol{c} \equiv \boldsymbol{b} + \boldsymbol{d} \pmod{m}$.

Suppose that $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$.

Modular Arithmetic: Addition Property

Let m be a positive integer.
If $\boldsymbol{a} \equiv \boldsymbol{b} \pmod{m}$ and $\boldsymbol{c} \equiv \boldsymbol{d} \pmod{m}$
then $\boldsymbol{a} + \boldsymbol{c} \equiv \boldsymbol{b} + \boldsymbol{d} \pmod{m}$.

Suppose that that $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$.
Unrolling the definitions, we can see that $a - b = km$ and $c - d = jm$ for some integers k, j.

$(a-b)+(c-d)$
$= km + jm$

Adding the equations together gives us
$(a + c) - (b + d) = m(k + j)$.

By the definition of congruence, we have $a + c \equiv b + d \pmod{m}$.

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

■

Modular Arithmetic: Multiplication Property

Let m be a positive integer.
If $\boldsymbol{a} \equiv \boldsymbol{b} \pmod{m}$ and $\boldsymbol{c} \equiv \boldsymbol{d} \pmod{m}$
then $\boldsymbol{ac} \equiv \boldsymbol{bd} \pmod{m}$.

Suppose that $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$.

Modular Arithmetic: Multiplication Property

Let m be a positive integer.
If $\boldsymbol{a} \equiv \boldsymbol{b} \pmod{m}$ and $\boldsymbol{c} \equiv \boldsymbol{d} \pmod{m}$
then $\boldsymbol{ac} \equiv \boldsymbol{bd} \pmod{m}$.

Suppose that $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$.
Unrolling the definitions, we can see that $a - b = km$ and $c - d = jm$ for some integer k, j or equivalently, $a = km + b$ and $c = jm + d$.

Modular Arithmetic: Multiplication Property

Let m be a positive integer.
If $\boldsymbol{a} \equiv \boldsymbol{b} \pmod{m}$ and $\boldsymbol{c} \equiv \boldsymbol{d} \pmod{m}$
then $\boldsymbol{ac} \equiv \boldsymbol{bd} \pmod{m}$.

$m \mid ac - bd$

Suppose that $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$.
Unrolling the definitions, we can see that $a - b = km$ and $c - d = jm$ for some integer k, j or equivalently, $a = km + b$ and $c = jm + d$.

Multiplying both together gives us $ac = (km + b)(jm + d) = kjm^2 + kmd + bjm + bd$.

Modular Arithmetic: Multiplication Property

Let m be a positive integer.
If $\boldsymbol{a} \equiv \boldsymbol{b} \pmod{m}$ and $\boldsymbol{c} \equiv \boldsymbol{d} \pmod{m}$
then $\boldsymbol{ac} \equiv \boldsymbol{bd} \pmod{m}$.

Suppose that $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$.
Unrolling the definitions, we can see that $a - b = km$ and $c - d = jm$ for some integer k, j or equivalently, $a = km + b$ and $c = jm + d$.

Multiplying both together gives us $ac = (km + b)(jm + d) = kjm^2 + kmd + bjm + bd$. Re-arranging, this becomes $ac - bd = m(\underline{kjm + kd + bj})$.

Modular Arithmetic: Multiplication Property

Let m be a positive integer.
If $\boldsymbol{a} \equiv \boldsymbol{b} \pmod{m}$ and $\boldsymbol{c} \equiv \boldsymbol{d} \pmod{m}$
then $\boldsymbol{ac} \equiv \boldsymbol{bd} \pmod{m}$.

Suppose that $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$.
Unrolling the definitions, we can see that $a - b = km$ and $c - d = jm$ for some integer k, j or equivalently, $a = km + b$ and $c = jm + d$.

Multiplying both together gives us $ac = (km + b)(jm + d) = kjm^2 + kmd + bjm + bd$. Re-arranging, this becomes $ac - bd = m(kjm + kd + bj)$.

This says $ac \equiv bd \pmod{m}$ by the definition of congruence. ■

Modular Arithmetic: Properties

If $\boldsymbol{a} \equiv \boldsymbol{b} \pmod{m}$ and $\boldsymbol{b} \equiv \boldsymbol{c} \pmod{m}$ then $\boldsymbol{a} \equiv \boldsymbol{c} \pmod{m}$

If $\boldsymbol{a} \equiv \boldsymbol{b} \pmod{m}$ and $\boldsymbol{c} \equiv \boldsymbol{d} \pmod{m}$ then

$$\boldsymbol{a} + \boldsymbol{c} \equiv \boldsymbol{b} + \boldsymbol{d} \pmod{m} \text{ and}$$
$$\boldsymbol{ac} \equiv \boldsymbol{bd} \pmod{m}$$

Corollary: If $\boldsymbol{a} \equiv \boldsymbol{b} \pmod{m}$ then

$$\boldsymbol{a} + \boldsymbol{c} \equiv \boldsymbol{b} + \boldsymbol{c} \pmod{m} \text{ and}$$
$$\boldsymbol{ac} \equiv \boldsymbol{bc} \pmod{m}$$

These allow us to solve problems in modular arithmetic, e.g.

- **add/subtract numbers from both sides of equations**
- **multiply numbers on both sides of equations.**
- **use chains of equivalences**

$$x+1=5 \longrightarrow x=4$$

$$x+1 \equiv 5 \pmod 7$$

$$x \equiv 4 \pmod 7$$

Example: Proof by Cases with mod

Let $\boldsymbol{n}$ be an integer. Prove that $\boldsymbol{n^2 \equiv 0}$ (mod 4) or $\boldsymbol{n^2 \equiv 1}$ (mod 4).

Let's start by looking at small examples:

$\mathbf{0^2 = 0 \equiv 0}$ (mod 4)
$\mathbf{1^2 = 1 \equiv 1}$ (mod 4)
$\mathbf{2^2 = 4 \equiv 0}$ (mod 4)
$\mathbf{3^2 = 9 \equiv 1}$ (mod 4)
$\mathbf{4^2 = 16 \equiv 0}$ (mod 4)
$5^2 = 25 \equiv 1$ (mod 4)

It looks as though we have:

If $\boldsymbol{n}$ is even then $\boldsymbol{n^2 \equiv 0}$ (mod 4)
If $\boldsymbol{n}$ is odd then $\boldsymbol{n^2 \equiv 1}$ (mod 4)

Example: Proof by Cases with mod

Let $\boldsymbol{n}$ be an integer. Prove that $\boldsymbol{n^2 \equiv 0} \pmod 4$ or $\boldsymbol{n^2 \equiv 1} \pmod 4$.

Case 1 (n is even):

Suppose n is even.
Then, $n = 2k$ for some integer k.
So, $n^2 = (2k)^2 = 4k^2 = 4k^2 + 0$.
So, by the definition of congruence,
we have $n^2 \equiv 0 \pmod 4$.

$4 \mid n^2 - 0$ $\quad$ $4 \mid n^2$

Example: Proof by Cases with mod

Let $\boldsymbol{n}$ be an integer. Prove that $\boldsymbol{n^2 \equiv 0} \pmod 4$ or $\boldsymbol{n^2 \equiv 1} \pmod 4$.

Case 1 (n is even): Done.

Case 2 (n is odd):

Suppose n is odd.
Then, $n = 2k + 1$ for some integer k.
So, $n^2 = (2k + 1)^2$
$= 4k^2 + 4k + 1$
$= 4(k^2 + k) + 1$.
So, by definition of congruence,
we have $n^2 \equiv 1 \pmod 4$.

Result follows by proof by cases since n is either even or odd