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?

- $5 \mid 1$
  - $5 \mid 1$ iff $1 = 5k$
  - $1 \mid 5$ iff $5 = 1k$

- $25 \mid 5$
  - $25 \mid 5$ iff $5 = 25k$
  - $5 \mid 25$ iff $25 = 5k$

- $5 \mid 0$
  - $5 \mid 0$ iff $0 = 5k$
  - $0 \mid 5$ iff $5 = 0k$

- $3 \mid 2$
  - $3 \mid 2$ iff $2 = 3k$
  - $2 \mid 3$ iff $3 = 2k$
## Last class: Division Theorem

### 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: $r \geq 0$ even if $a < 0$.

Not quite the same as $a \% d$. 

**Domain of Discourse**

Integers
Last class: div and mod

\[ x = 7 \cdot (x \text{ div } 7) + (x \text{ mod } 7) \]
# Arithmetic, mod 7

\[(a + b) \mod 7\]

\[(a \times b) \mod 7\]

<table>
<thead>
<tr>
<th>+</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>6</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>6</td>
<td>6</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>\times</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>2</td>
<td>4</td>
<td>6</td>
<td>1</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>3</td>
<td>6</td>
<td>2</td>
<td>5</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>4</td>
<td>1</td>
<td>5</td>
<td>2</td>
<td>6</td>
<td>3</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>5</td>
<td>3</td>
<td>1</td>
<td>6</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>6</td>
<td>0</td>
<td>6</td>
<td>5</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>
New notion of “sameness” or “equivalence” that will help us understand modular arithmetic.

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

There is really a notion of sameness for each \(m > 0\). It may help you to think of \(a \equiv b \pmod{m}\) for a fixed \(m > 0\) as an equivalence \(a \equiv_m b\).

Standard math notation writes the \((\text{mod } m)\) on the right to tell you what notion of sameness \(\equiv\) means.
Modular Arithmetic

**Definition: “a is congruent to b modulo m”**

For \(a, b, m\) with \(m > 0\)

\[a \equiv b \pmod{m} \iff m \mid (a - b)\]

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 \(c \equiv d \pmod{m}\)
Check Your Understanding. What do each of these mean? When are they true?

\[ x \equiv 0 \pmod{2} \]

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

\[ -1 \equiv 19 \pmod{5} \]

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

\[ y \equiv 2 \pmod{7} \]

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.
Modular Arithmetic: A Property

Let \(a, b, m\) be integers with \(m > 0\).
Then, \(a \equiv b \pmod{m}\) if and only if \(a \mod m = b \mod m\).
Modular Arithmetic: A Property

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

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

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

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

$a \equiv b \pmod{m} \iff m \mid (a - b)$
Modular Arithmetic: A Property

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

(\(\Leftarrow\)) Suppose that \(a \mod m = b \mod m\).

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

Then, \(a - b = (mq + (a \mod m)) - (ms + (b \mod m))\)
\[= m(q - s) + (a \mod m - b \mod m)\]
\[= m(q - s) \text{ since } a \mod m = b \mod m\]

Goal: show \(a \equiv b \pmod{m}\), i.e., \(m | (a - b)\).
Modular Arithmetic: A Property

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

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

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

Then, $a - b = (mq + (a \mod m)) - (ms + (b \mod m))$

$= m(q - s) + (a \mod m - b \mod m)$

$= m(q - s)$ since $a \mod m = b \mod m$

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

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

\[(\Rightarrow) \text{ Suppose that } a \equiv b \pmod{m}. \]

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

\textbf{Goal:} show \( a \mod m \equiv b \mod m \)
Modular Arithmetic: A Property

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

$(\Rightarrow)$ 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, $a = b + km$.

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

Goal: show $a \mod m \equiv b \mod m$
Modular Arithmetic: A Property

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

(\( \Rightarrow \)) 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, \( a = b + km \).

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

Combining these, we have \( qm + (a \mod m) = a = b + km \) or equiv., \( b = qm - km + (a \mod m) = (q - k)m + (a \mod m) \). By the Division Theorem, we have \( b \mod m = a \mod m \). \[\square\]

Goal: show \( a \mod m \equiv b \mod m \)
Let \( a, b, m \) be integers with \( m > 0 \). Then, \( a \equiv b \pmod{m} \) if and only if \( a \mod m = b \mod m \).

(\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, \( a = b + km \).

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

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

**Goal:** show \( a \mod m \equiv b \mod m \)
Modular Arithmetic: A Property

Let \( a, b, m \) be integers with \( m > 0 \). Then, \( a \equiv b \pmod{m} \) if and only if \( (a - b) \) is divisible by \( m \).

\((\Rightarrow)\) 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, \( a = b + km \).

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

Combining these, we have \( qm + (a \mod m) = a = b + km \)
or equiv., \( b = qm - km + (a \mod m) = (q - k)m + (a \mod m) \).

By the Division Theorem, we have \( b \mod m = a \mod m \).
The \textbf{mod }$m$\ function vs the $\equiv \left( \text{mod } m \right)$ predicate

• What we have just shown
  – The \textbf{mod }$m$\ function maps any integer $a$ to a remainder $a \mod m \in \{0,1,\ldots,m-1\}$.

  – Imagine grouping together all integers that have the same value of the \textbf{mod }$m$\ function
    That is, the same remainder in $\{0,1,\ldots,m-1\}$.

  – The $\equiv \left( \text{mod } m \right)$ predicate compares integers $a, b$. It is true if and only if the \textbf{mod }$m$\ function has the same value on $a$ and on $b$.
    That is, $a$ and $b$ 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 $a = c$

- 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 “× c” to both sides

These are the facts that allow us to use algebra to solve problems
Let $m$ be a positive integer. If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$.
Modular Arithmetic: Basic Property

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

Suppose that $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$. 
Modular Arithmetic: Basic Property

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

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

Putting these together, we have $a \mod m = c \mod m$, which says that $a \equiv c \pmod{m}$, by the previous property.
Let $m$ be a positive integer. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then $a + c \equiv b + d \pmod{m}$. 
Let $m$ be a positive integer. If \( a \equiv b \pmod{m} \) and \( c \equiv d \pmod{m} \), then \( a + c \equiv b + d \pmod{m} \).

Suppose that \( a \equiv b \pmod{m} \) and \( c \equiv d \pmod{m} \).
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 integers $k, j$.

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

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

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

Modular Arithmetic: Addition Property
Let $m$ be a positive integer.
If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$
then $ac \equiv bd \pmod{m}$.

Suppose that $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. 
Modular Arithmetic: Multiplication Property

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

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 $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$
then $ac \equiv bd \pmod{m}$.

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 $ac = (km + b)(jm + d) = kjm^2 + kmd + bjm + bd$. 

Modular Arithmetic: Multiplication Property

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

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
$ac - bd = m(kjm + kd + bj)$. 
Modular Arithmetic: Multiplication Property

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

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 $ac = (km + b)(jm + d) = k jm^2 + kmd + bjm + bd$. 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 \( a \equiv b \pmod{m} \) and \( b \equiv c \pmod{m} \) then \( a \equiv c \pmod{m} \)

If \( a \equiv b \pmod{m} \) and \( c \equiv d \pmod{m} \) then
\[
\begin{align*}
    a + c & \equiv b + d \pmod{m} \\
    ac & \equiv bd \pmod{m}
\end{align*}
\]

Corollary: If \( a \equiv b \pmod{m} \) then
\[
\begin{align*}
    a + c & \equiv b + c \pmod{m} \\
    ac & \equiv bc \pmod{m}
\end{align*}
\]

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

Let’s start by looking at small examples:

- $0^2 = 0 \equiv 0 \pmod{4}$
- $1^2 = 1 \equiv 1 \pmod{4}$
- $2^2 = 4 \equiv 0 \pmod{4}$
- $3^2 = 9 \equiv 1 \pmod{4}$
- $4^2 = 16 \equiv 0 \pmod{4}$

It looks as though we have:

- If $n$ is even then $n^2 \equiv 0 \pmod{4}$
- If $n$ is odd then $n^2 \equiv 1 \pmod{4}$
Example: Proof by Cases with mod

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

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 $n^2 \equiv 0 \pmod{4}$. 
Example: Proof by Cases with mod

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

Case 1 ($n$ is even): Done.

Case 2 ($n$ is odd):

Suppose $n$ is odd.

Then, $n = 2k + 1$ for some integer $k$.

So, $n^2 = (2k + 1)^2$

So, $n^2 = 4k^2 + 4k + 1$

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.