Lecture 11: Modular Arithmetic and Applications
Last Class: Divisibility

Definition: “b divides a”

For \(a, b\) with \(b \neq 0\):
\[b \mid a \iff \exists q \ (a = qb)\]

Check Your Understanding. Which of the following are true?

- \(5 \mid 1\)  iff \(1 = 5k\)
- \(25 \mid 5\)  iff \(5 = 25k\)
- \(5 \mid 0\)  iff \(0 = 5k\)
- \(3 \mid 2\)  iff \(2 = 3k\)
- \(1 \mid 5\)  iff \(5 = 1k\)
- \(5 \mid 25\) iff \(25 = 5k\)
- \(0 \mid 5\)  iff \(5 = 0k\)
- \(2 \mid 3\)  iff \(3 = 2k\)
Recall: Elementary School Division

For $a, b$ with $b > 0$, we can divide $b$ into $a$.

If $b \mid a$, then, by definition, we have $a = qb$ for some $q$. The number $q$ is called the quotient.

Dividing both sides by $b$, we can write this as

$$\frac{a}{b} = q$$

(We want to stick to integers, though, so we’ll write $a = qb$.)
For $a, b$ with $b > 0$, we can divide $b$ into $a$.

If $b \nmid a$, then we end up with a remainder $r$ with $0 < r < b$.

Now, instead of

\[
\frac{a}{b} = q
\]

we have

\[
\frac{a}{b} = q + \frac{r}{b}
\]

Multiplying both sides by $b$ gives us

\[
a = qb + r
\]

(A bit nicer since it has no fractions.)
Recall: Elementary School Division

For $a, b$ with $b > 0$, we can divide $b$ into $a$.

If $b \mid a$, then we have $a = qb$ for some $q$.
If $b \nmid a$, then we have $a = qb + r$ for some $q, r$ with $0 < r < b$.

In general, we have $a = qb + r$ for some $q, r$ with $0 \leq r < b$, where $r = 0$ iff $b \mid a$. 
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
\( q = a \ \text{div} \ b \)
and non-negative remainder
\( r = a \ \text{mod} \ b \).

Note: \( r \geq 0 \) even if \( a < 0 \).
Not quite the same as \( a \ % \ d \).
div and mod

\[ x = 7 \cdot (x \text{ div } 7) + (x \text{ mod } 7) \]
Ordinary arithmetic

$2 + 3 = 5$
Arithmetic on a Clock

\[ 2 + 3 = 5 \]

\[ 23 = 3 \cdot 7 + 2 \]

If \( a = 7q + r \), then \( r \) \((= a \mod b)\) is where you stop after taking \( a \) steps on the clock.
### Arithmetic, mod 7

- **(a + b) mod 7**
- **(a × 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>×</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>
Modular Arithmetic

Definition: “a is congruent to b modulo m”

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

\[ a \equiv_m b \iff m \mid (a - b) \]

New notion of “sameness” that will help us understand modular arithmetic
Modular Arithmetic

Definition: “a is congruent to b modulo m”

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

$$a \equiv_m b \iff m \mid (a - b)$$

The standard math notation is

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

A chain of equivalences is written

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

Many students find this confusing, so we will use $\equiv_m$ instead.
Modular Arithmetic

Definition: “a is congruent to b modulo m”

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

\[ a \equiv_m b \iff m \mid (a - b) \]

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

\( x \equiv_2 0 \)

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

\( -1 \equiv_5 19 \)

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

\( y \equiv_7 2 \)

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, $a \equiv_m b$ if and only if $a \mod m = b \mod m$. 
Modular Arithmetic: A Property

Let $a, b, m$ be integers with $m > 0$. Then, $a \equiv_m b$ if and only if $a \mod m = b \mod m$.

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 $a \equiv_m b$, i.e., $m \mid (a - b)$. 
Modular Arithmetic: A Property

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

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

Goal: show \( a \equiv_m b \), i.e., \( m \mid (a - b) \).
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 $a \equiv_m b$. 

Let $a, b, m$ be integers with $m > 0$.
Then, $a \equiv_m b$ if and only if $a \mod m = b \mod m$. 

Modular Arithmetic: A Property
Modular Arithmetic: A Property

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

Suppose that \( a \equiv_m b \).

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

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

Suppose that \( a \equiv_m b \).

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 \( 0 \leq (a \mod m) < m \).
Modular Arithmetic: A Property

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

Suppose that \( a \equiv_m b \).

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 \textit{mod} $m$ function vs the $\equiv_m$ predicate

- What we have just shown
  - The \textit{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 \textit{mod} $m$ function
    That is, the same remainder in $\{0,1,\ldots,m-1\}$.

  - The $\equiv_m$ predicate compares integers $a,b$. It is true if and only if the \textit{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 “$\times c$” to both sides

These are the facts that allow us to use algebra to solve problems
Let $m$ be a positive integer. If $a \equiv_m b$ and $b \equiv_m c$, then $a \equiv_m c$. 
Let $m$ be a positive integer. If $a \equiv_m b$ and $b \equiv_m c$, then $a \equiv_m c$.

Suppose that $a \equiv_m b$ and $b \equiv_m c$. 
Modular Arithmetic: Basic Property

Let $m$ be a positive integer.
If $a \equiv_m b$ and $b \equiv_m c$, then $a \equiv_m c$.

Suppose that $a \equiv_m b$ and $b \equiv_m c$. 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 $a \equiv_m c$, by the previous property.