**Power set** of a set \( A \) = set of all subsets of \( A \)

\[
\mathcal{P}(A) = \{ B : B \subseteq A \}
\]

e.g. Days = \( \{M, W, F\} \)

\[
\mathcal{P}(\text{Days}) = \{ \emptyset, \{M\}, \{W\}, \{F\}, \{M, W\}, \{W, F\}, \{M, F\}, \{M, W, F\} \}
\]

e.g. \( \mathcal{P}(\emptyset) = \{ \emptyset \} \neq \emptyset \)

\( \emptyset \subseteq \emptyset \)
\[ \{ \mathcal{P}(A) \} \subseteq \mathcal{P}(\mathcal{P}(A)) \]

\[ \mathcal{P}(A) \subseteq \mathcal{P}(\mathcal{P}(A)) \]

false

\[ |A| = k \]

If \(|A| \leq n\), what is \(|\mathcal{P}(A)|\)?

\[ |\mathcal{P}(A)| = 2^k \]

size of \(|A \times A \times A \times A|\)?

\[ |\mathcal{P}(\mathcal{P}(A))| = 2^{(2^k)} \]

\[ |\mathcal{P}(\mathcal{P}(A))| = 2^{(2^n)} \]

\[ A = \{1\} \]

\[ \mathcal{P}(A) = \{\phi, \{1\}\} \]

\[ \mathcal{P}(\mathcal{P}(A)) = \{\phi, \{\phi\}, \{\{1\}\}, \{\phi, \{1\}\}\} \]

\[ B \subseteq B \]

Since \( B \subseteq B \), \( B \in \mathcal{P}(B) \)

\[ B = \mathcal{P}(A) \]

\[ |A \times A| = n^2 \]
Fall 2015
Lecture 10: Functions, Modular arithmetic
So far:
- Propositional logic
- Logic to build circuits
- Predicates and quantifiers
- Proof systems and logical inference
- Basic set theory
Question: If the domain of discourse is empty and $P$ is a predicate, what is the truth value of:

$$\exists x \ P(x)$$

$$\forall x \ P(x)$$
A function from $A$ to $B$:

- Every element of $A$ is assigned to exactly one element of $B$.
- We write $f : A \rightarrow B$.
- “Image of $X$ under $f$” = "$f(X)$”
  \[= \{ x : \exists y \ (y \in X \land x = f(y)) \}\]

- **Domain of $f$ is** $A$
- **Codomain of $f$ is** $B$
- **Image of $f$** = Image of domain under $f$
  \[= \text{all the elements pointed to by something in the domain.}\]
A function $f : A \to B$ is one-to-one (or, injective) if every output corresponds to at most one input, i.e. $f(x) = f(x') \Rightarrow x = x'$ for all $x, x' \in A$.

A function $f : A \to B$ is onto (or, surjective) if every output gets hit, i.e. for every $y \in B$, there exists $x \in A$ such that $f(x) = y$. 
is this function one-to-one? is it onto?

It is one-to-one, because nothing in B is pointed to by multiple elements of A.

It is not onto, because 5 is not pointed to by anything.
One-to-one (?)

- $x \mapsto x^2$
  - $-2 \mapsto 4$ \( \times \)
  - $2 \mapsto 4$ \( \times \)

- $x \mapsto x^3 - x$
  - $1 \mapsto 0$ \( \times \)
  - $0 \mapsto 0$ \( \times \)

- $x \mapsto e^x$
  - \( \checkmark \)
  - \( \times \)

- $x \mapsto x^3$
  - \( \checkmark \)

Onto (?)

- $x \mapsto |x|^{1/3} \sin(x)$
  - \( \checkmark \)
Dear HBO, this is a slide about digital watermarking.


“number theory” (and applications to computing)

• How whole numbers work
  [fascinating, deep, weird area of mathematics that no one understands, but the basics are easy and really useful]

• Many significant applications
  – Cryptography [this is how SSL works]
  – Hashing
  – Security
  – Error-correcting codes [this is how your bluray player works]

• Important tool set
public class Test {
    final static int SEC_IN_YEAR = 364*24*60*60;
    public static void main(String args[]) {
        System.out.println(
            "I will be alive for at least "+
            SEC_IN_YEAR * 101 + " seconds."
        );
    }
}
Arithmetic over a finite domain: Math with wrap around

$2 - 4 \equiv 10 \pmod{12}$

+8

+5
Integers $a, b$, with $a \neq 0$. We say that $a$ divides $b$ iff there is an integer $k$ such that $b = k \cdot a$. The notation $a \mid b$ denotes “$a$ divides $b$.”

$3 \mid 15 \quad 1 \nmid 15$

$15 \nmid 17$

$a \mid b$

$3 \mid 0$ ?

$0 = 0.3$

$b = k \cdot a$
Let $a$ be an integer and $d$ a positive integer. Then there are unique integers $q$ and $r$, with $0 \leq r < d$, such that $a = d \times q + r$.

\[
q = a \div d \quad r = a \mod d
\]

\[
a = 15 \\
\div 4 = q \\
a = -13 \\
\div 4 = q
\]

\[
a = 3 \\
\mod 3 = r \\
a = -4 \\
\mod 3 = r
\]

Note: $r \geq 0$ even if $a < 0$. Not quite the same as $a \% d$. 

**arithmetic mod 7**

\[ a +_7 b = (a + b) \text{ mod } 7 \]
\[ a \times_7 b = (a \times b) \text{ mod } 7 \]

<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>

-2 \quad -1
Let $a$ and $b$ be integers, and $m$ be a positive integer. We say $a$ is **congruent** to $b$ **modulo** $m$ if $m$ divides $a - b$. We use the notation $a \equiv b \pmod{m}$ to indicate that $a$ is congruent to $b$ modulo $m$. 

\[ a \equiv b \pmod{m} \iff m \mid a - b \]
A ≡ 0 (mod 2)
This statement is the same as saying “A is even”; so, any
A that is even (including negative even numbers) will work.

1 ≡ 0 (mod 4)
This statement is false. If we take it mod 1 instead, then the
statement is true.

A ≡ -1 (mod 17)
If A = 17x − 1 = 17(x-1) + 16 for an integer x, then it works.
Note that (m − 1) mod m
= ((m mod m) + (-1 mod m)) mod m
= (0 + -1) mod m
= -1 mod m
Theorem: Let $a$ and $b$ be integers, and let $m$ be a positive integer. Then $a \equiv b \pmod{m}$ if and only if $a \mod m = b \mod m$.

Proof: Suppose that $a \equiv b \pmod{m}$.

By definition: $a \equiv b \pmod{m}$ implies $m \mid (a - b)$

which by definition implies that $a - b = km$ for some integer $k$.

Therefore $a = b + km$.

Taking both sides modulo $m$ we get

$$a \mod m = (b+km) \mod m = b \mod m$$
Theorem: Let $a$ and $b$ be integers, and let $m$ be a positive integer. Then $a \equiv b \pmod{m}$ if and only if $a \mod m = b \mod m$.

Proof: 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 $q, s$.

$$a - b = (mq + (a \mod m)) - (ms + (b \mod m))$$
$$= m(q - r) + (a \mod m - b \mod m)$$
$$= m(q - r) \text{ since } a \mod m = b \mod m$$

Therefore $m \mid (a-b)$ and so $a \equiv b \pmod{m}$.
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 $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. Unrolling definitions gives us some $k$ such that $a - b = km$, and some $j$ such that $c - d = jm$.

Adding the equations together gives us $(a + c) - (b + d) = m(k + j)$. Now, re-applying the definition of mod gives us $a + c \equiv b + d \pmod{m}$. 
Let $m$ be a positive integer. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $ac \equiv bd \pmod{m}$.

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

Unrolling definitions gives us some $k$ such that $a - b = km$, and some $j$ such that $c - d = jm$.

Then, $a = km + b$ and $c = jm + d$.

Multiplying both together gives us

\[ ac = (km + b)(jm + d) = k jm^2 + kmd + jmb + bd \]

Rearranging gives us $ac - bd = m(kjm + kd + jb)$.

Using the definition of mod gives us $ac \equiv bd \pmod{m}$. 
Let $n$ be an integer.
Prove that $n^2 \equiv 0 \pmod{4}$ or $n^2 \equiv 1 \pmod{4}$