Spring 2015
Lecture 10: Functions, Modular arithmetic
[This special lecture was given by a 5-year-old]
a little recap

So far:
- Propositional logic
- Logic to build circuits
- Predicates and quantifiers
- Proof systems and logical inference
- Basic set theory

[optional] Proof review session on Wed @ 6pm in EE 105
empty domains

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 $f$
  
  = all the elements pointed to by something in the domain.
<table>
<thead>
<tr>
<th>( A )</th>
<th>( B )</th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>1</td>
</tr>
<tr>
<td>b</td>
<td>2</td>
</tr>
<tr>
<td>c</td>
<td>3</td>
</tr>
<tr>
<td>d</td>
<td>4</td>
</tr>
<tr>
<td>e</td>
<td>5</td>
</tr>
</tbody>
</table>

Image({a}) = \{1\}
Image({a, e}) = \{1, 5\}
Image({a, b}) = \{1, 2, 3\}
Image(A) = \{1, 2, 3, 4, 5\}
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.
QUIZ!

One-to-one (?)

\( x \mapsto x^2 \)

NO

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

NO

\( x \mapsto e^x \)

NO

\( x \mapsto x^3 \)

YES

Onto (?)

\( x \mapsto x^2 \)

NO only \( y \geq 0 \)

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

NO

\( x \mapsto e^x \)

YES

\( x \mapsto x^3 \)

YES

Domain: Reals
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
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 $b$.”

\[
\begin{align*}
12 &= 6 \times 2, \\
13 &= _{\_} \times 2.
\end{align*}
\]
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 $a = d \cdot q + r$.

$$q = a \div d \quad r = a \mod d$$

Note: $r \geq 0$ even if $a < 0$. Not quite the same as $a \% d$. 
## arithmetic mod 7

9 \times 6 = 7 \left(\text{mod 7}\right)\]

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

\[2 \times 1 = 2 \left(\text{mod 7}\right)\]

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

\[\color{red}5 \times 5 = 25 = 7 \times 3 + 4\]

<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>x</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>2</td>
<td>4</td>
<td>6</td>
<td>1</td>
<td>3</td>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>6</td>
<td>2</td>
<td>5</td>
<td>1</td>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>1</td>
<td>5</td>
<td>2</td>
<td>6</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>3</td>
<td>1</td>
<td>6</td>
<td>4</td>
<td>2</td>
<td>5</td>
</tr>
<tr>
<td>6</td>
<td>6</td>
<td>5</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>6</td>
</tr>
</tbody>
</table>
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 $m$.

\[ 12 \equiv -2 \pmod{7} \]

\[ 12 - (-2) = 14 \]
A $\equiv 0 \pmod{2}$

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

1 $\equiv 0 \pmod{4}$

This statement is false. If we take it mod 1 instead, then the statement is true.

A $\equiv -1 \pmod{17}$

If $A = 17x - 1 = 17x + 16$ 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 $m | (a - b)$

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 $\text{a mod } m = \text{b mod } m$.

Proof: Suppose that $a \text{ mod } m = b \text{ mod } m$.
By the division theorem, $a = mq + (a \text{ mod } m)$ and $b = ms + (b \text{ mod } m)$ for some integers $q, s$.

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

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 $n^2 \equiv 1 \pmod{4}$