Power set of a set A = set of all subsets of A

$$\boxed{\mathcal{P}(A) = \{\, B : B \subseteq A \,\}}$$

$|A| = 10$

$|\mathcal{P}(A)| = 2^{10}$

$A = \{1, \ldots, 10\}$

$B \in \mathcal{P}(A)$

e.g. $\text{Days} = \{M, W, F\}$

$$\begin{aligned}\mathcal{P}(\text{Days}) = \{\, & \varnothing, \\ & \{M\}, \{W\}, \{F\}, \\ & \{M, W\}, \{W, F\}, \{M, F\}, \\ & \{M, W, F\} \;\}\end{aligned}$$

e.g. $\mathcal{P}(\varnothing) = \{\varnothing\}$

$|\varnothing| = 0$

$2^0 = 1$

Fall 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

Question: If the domain of discourse is empty and P is a predicate, what is the truth value of:

$\exists x\, P(x)$ F

$\forall x\, P(x)$ T

(a_1, b_0), (a_2, b_1), (a_3, b_0)

$B = \{b_0, b_1, b_2, b_3\}$

A **function** from A to B:

- Every element of A is assigned to exactly one element of B.
- We write $f : A \to B$.
- "Image of X under f" = "$f(X)$"

$X \subset A$

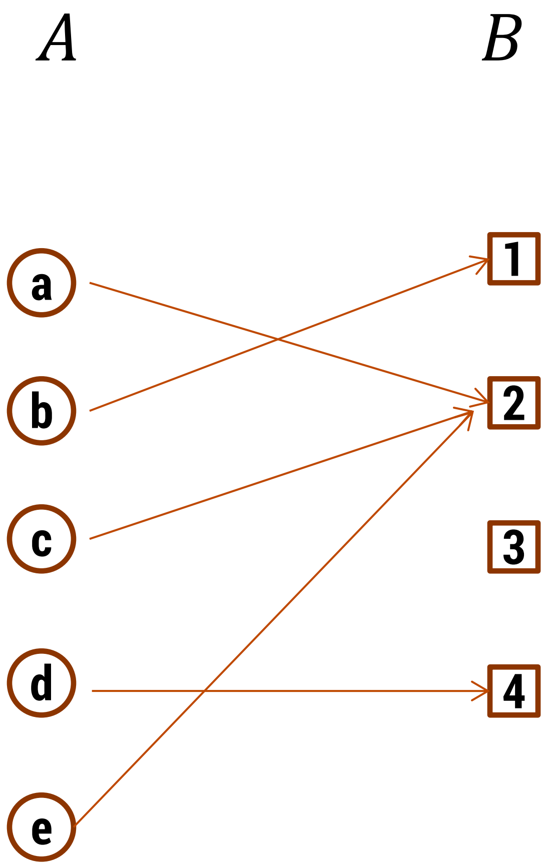
$= \{x : \exists y\, (y \in X \wedge x = f(y))\}$

$f(\{a_1, a_2\}) = \{b_0, b_1\}$

$f(\{a_1, a_3\}) = \{b_0\}$

- **Domain** of f is A
- **Codomain** of f is B
- **Image** of f = Image of domain under f = $f(A)$

  = all the elements pointed to by something in the domain.

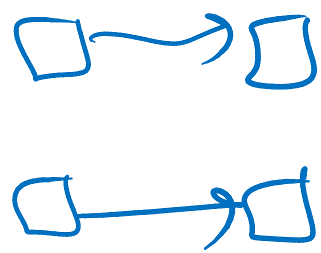


Image({a}) = $\{2\}$
Image({a, e}) = $\{2\}$
Image({a, b}) = $\{1, 2\} = \{2, 1\}$
Image(A) = $\{1, 2, 4\}$

injections and surjections

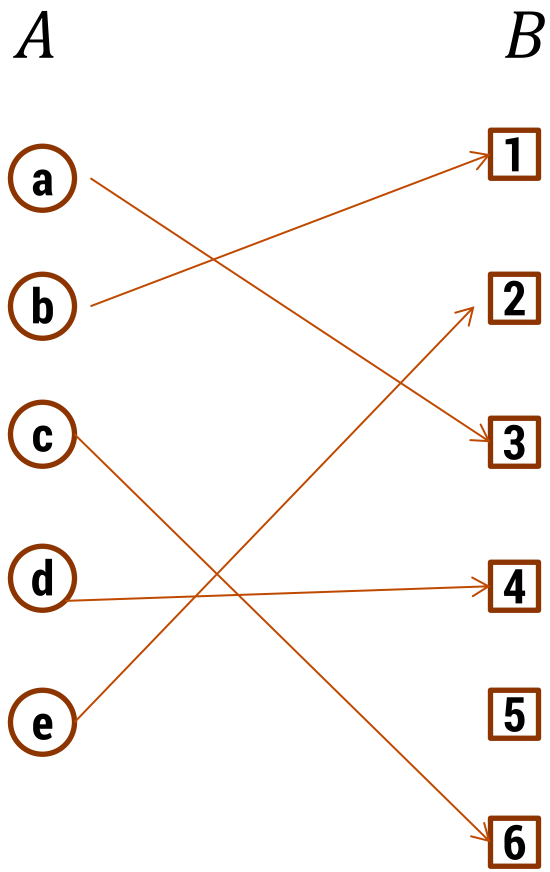
A **function** $f : A \to B$ is **one-to-one** (or, **injective**) if every output corresponds to at most one input, i.e. $f(x) = f(x') \Rightarrow x = x'$ for all $x, x' \in A$.

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 $f(x) = y$.



if onto $\to |A| \geq |B|$

is this function one-to-one? is it onto?



one to one ✓

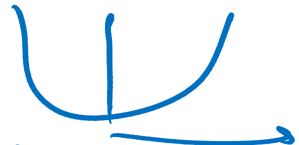
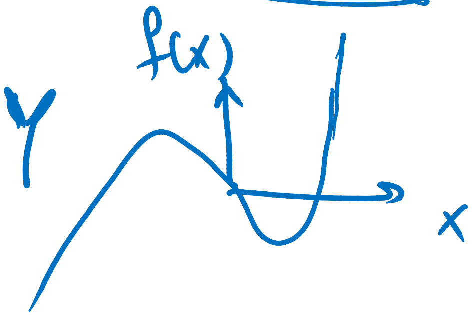
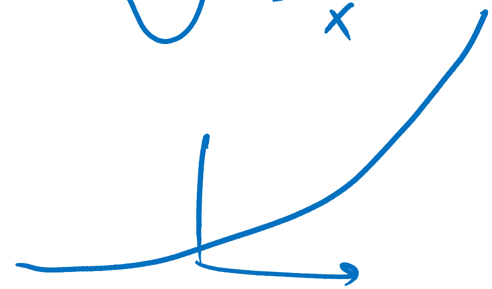
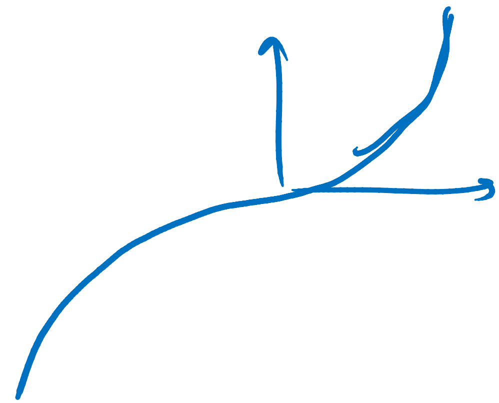
It is one-to-one, because nothing

onto ✗

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 (?)		Onto (?)	
$x \mapsto x^2$	N	$-2, 2$	N	
$x \mapsto x^3 - x$	N	$0, 1, -1$	Y	
$x \mapsto e^x$	Y		N	
$x \mapsto x^3$	Y		Y	

Domain: Reals

Co-domain : Real

a harder quiz

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

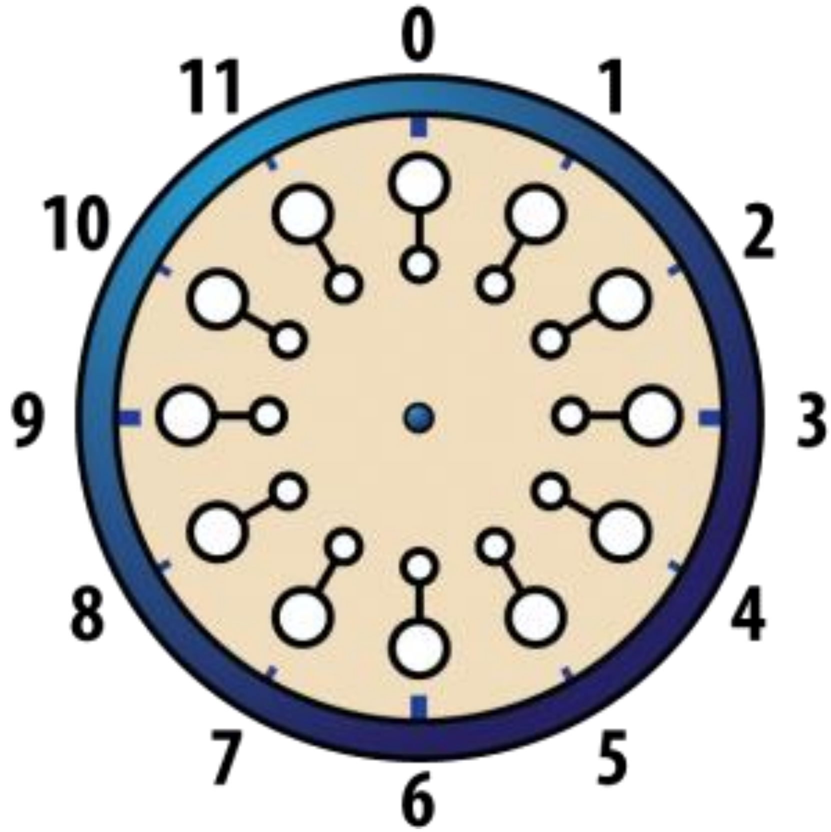
thanks, java

```
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.”
        );
    }
}
```

```
 ----jGRASP exec: java Test
I will be alive for at least -186619904 seconds.

 ----jGRASP: operation complete.
```

Arithmetic over a finite domain: Math with wrap around



Integers a, b, with a ≠ 0. We say that a **divides** b iff there is an integer k such that b = k a. The notation a | b denotes "a divides b."

$10 \mid 15$ ✗

$4 \mid 20$ ✓

$3 \mid -12$ ✓ $\quad -12 = 3 \cdot -4$

Let a be an integer and d a positive integer. Then there are *unique* integers q and r, with $0 \le r < d$, such that $a = d\,q + r$.

$q = a$ **div** d $\qquad$ $r = a$ **mod** d

$a = 10 \quad d = 3$

$q = 3 \quad r = 1$

$a = -11 \quad d = 3$

$q = -4 \quad r = +1$

$-11 = 3 \cdot -4 + 1$

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

$$a +_7 b = (a + b) \bmod 7$$

$$a \times_7 b = (a \times b) \bmod 7$$

$5 \times_7 5 = 4$

$25 \bmod 7 = 4$

+	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 congruence

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 ≡ b (mod m) to indicate that a is congruent to b modulo m.

$10 \equiv 2 \mod 7$ No

$10 \equiv 3 \mod 7$

$10 \equiv -4 \mod 7$

$12 \equiv 20 \mod 8$

–

modular arithmetic: examples

$A \equiv 0 \pmod{2}$

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 $A = 17x - 1 = 17(x-1) + 16$ for an integer x, then it works.

Note that $(m - 1) \bmod m$

$$= ((m \bmod m) + (-1 \bmod m)) \bmod m$$
$$= (0 + -1) \bmod m$$
$$= -1 \bmod m$$

modular arithmetic can haz sense

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

modular arithmetic can haz sense

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

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
$a \bmod m = (b+km) \bmod m = b \bmod m$

modular arithmetic can haz sense

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

modular arithmetic can haz sense

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)) − (mr + (b mod m))
= m(q − r) + (a mod m − b mod m)
= m(q − r) since a mod m = b mod m

Therefore m | (a-b) and so $a \equiv b \pmod{m}$

consistency of addition

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

consistency of multiplication

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

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

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

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