An integer $p \geq 2$ is called prime if 1 and p are the only positive divisors of p.

More on Sets and Proofs: ex: 7, 11, 23,

Theorem: (Euclid) The set of prime numbers is infinite.

Proof: Suppose that the set of prime numbers is finite. Let $p_1, p_2, \ldots, p_k$ be all the elements in the set of prime numbers.

Consider the number $(p_1 \cdot p_2 \cdot \ldots \cdot p_k) + 1 = p$. Notice that p_i is not a divisor of p for any $1 \leq i \leq k$. Also note that $p > p_i$ for any $1 \leq i \leq k$. Then p is a prime. (Check why) But $p > p_i$, so p is not in the list $p_1, \ldots, p_k$.

This is a contradiction to $p_1, \ldots, p_k$ being the set of all prime numbers.

ex: 3, 5, 7, 11

$p = 3 \cdot 5 \cdot 7 \cdot 11 + 1$

What really are sets anyway?

Does it make sense for a set to contain itself?

Say a set A is defined as $A = \{1, 2, A\}$.

Then, $A = \{1, 2, \{1, 2, A\}\}$.

$\vdots$ $A = \{1, 2, \{1, 2, \{1, 2, A\}\}\}$

$\vdots$

So we may consider to define a "set" of all sets that don't contain themselves as an element.

$$\boxed{S = \{A | A \text{ is a set } \wedge A \notin A\}}$$

Does S contain itself?

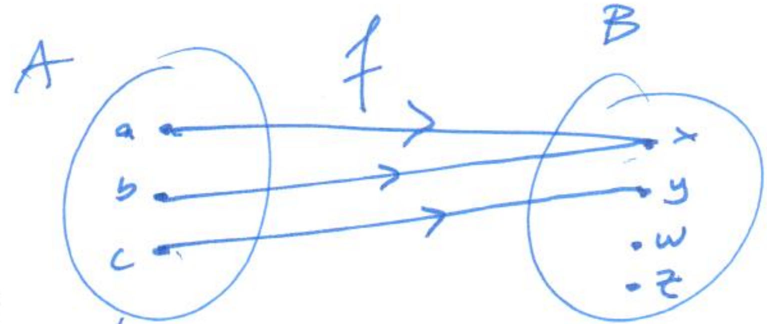
This is known as **Bertrand Russell's Paradox** (1901).

Puzzle: In a certain town there is a male barber who shaves all those men, and only those men, who do not shave themselves. Does the barber shave himself?

[Also see Alan Turing's "Halting Problem".]

the image of a is x

$f(a) = x$
$f(b) = x$
$f(c) = y$



f is a function

Functions

Image of A is $\{x, y\}$

Defns: A **function** f from a set A to a set B is a rule that assigns each element of A to exactly one element in B. We write $f : A \to B$.

A is called the **domain** of f, B is called the **codomain** of f.

For an element $a \in A$, $f(a)$ is the **image of a**. (Note that $f(a) \in B$.)

The subset of B that contains all elements that are images of some $a \in A$ is called the **image of A**. Formally, the image of A is $\{f(a) : a \in A\}$. Similarly we can define the image of a subset S of A. The image of $S \subseteq A$ is $\{f(a) : a \in S\}$.

The **preimage** $f^{-1}(b)$ of an element $b \in B$ is defined as $f^{-1}(b) = \{a \in A : f(a) = b\}$.

Example:

the preimage is a set

preimage of $x = \{a, b\}$

$f^{-1}(x) = \{a, b\}$

$f^{-1}(w) = \emptyset$

$f^{-1}(y) = \{c\}$

f is 1-1: $f(x) = f(y) \to x = y$

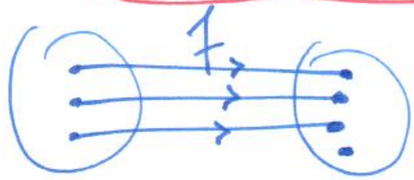
negation:

$\neg(f(x) = f(y) \to x = y)$

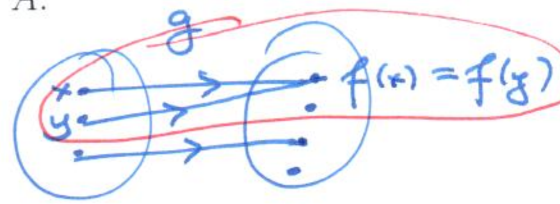
$\neg(\neg(f(x) = f(y)) \vee x = y)$

$f(x) = f(y) \wedge x \neq y$

Defns: A function $f : A \to B$ is **one-to-one** (also called an **injection**) if $f(x) = f(y) \to x = y$ for all $x, y \in A$.

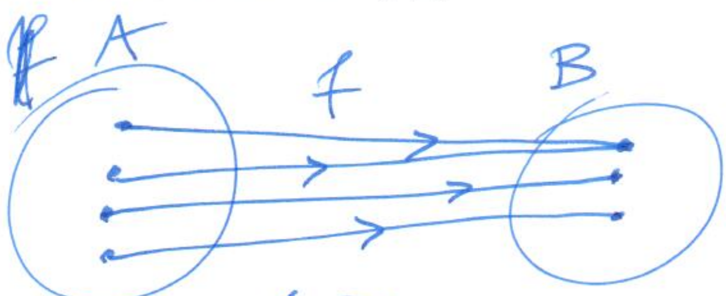


f is one-to-one (injective)

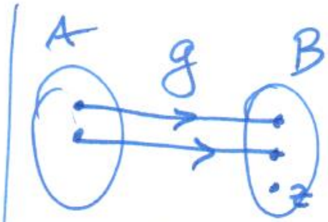


g is not one-to-one

A function $f : A \to B$ is **onto** (also called a **surjection**) if for each $b \in B$ there exists $a \in A$ such that $f(a) = b$.

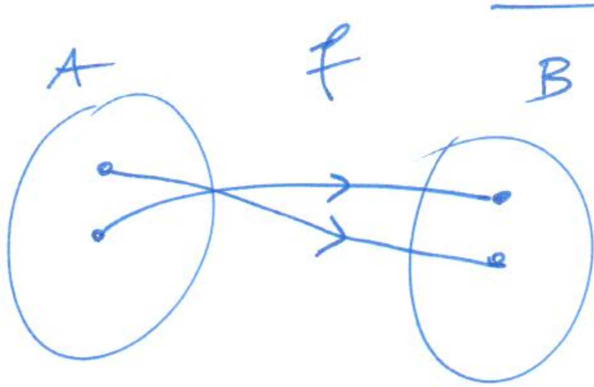


f is onto

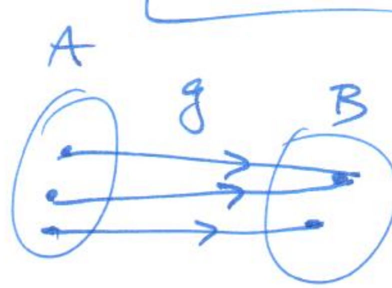


g is not onto because z is not the image of any element in A

A function $f : A \to B$ is a **bijection** (also called a **one-to-one correspondence**) if it is one-to-one and onto.



f is a bijection (1-1-correspondence)



g is not a bijection because it is not 1-1. (g is onto)