Great Theoretical Ideas In Computer Science

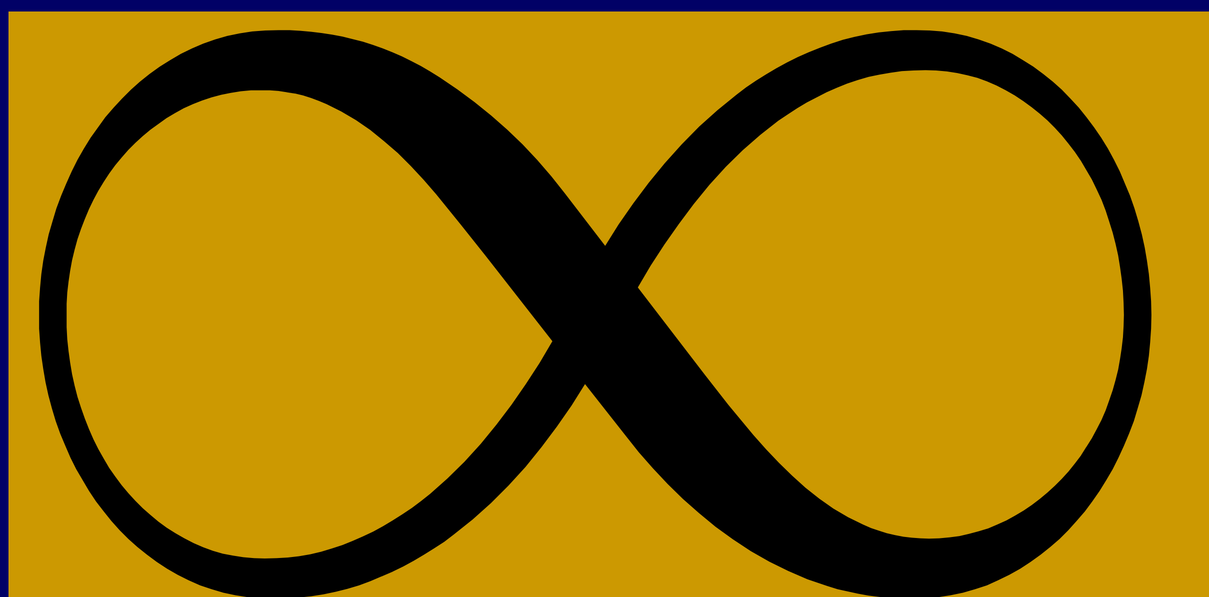
Steven Rudich

CS 15-251 Spring 2004

Lecture 25 Apr 13, 2004

Carnegie Mellon University

Cantor's Legacy: Infinity And Diagonalization



Early ideas from the course

Induction
Numbers
Representation
Finite Counting and probability

A hint of the infinite:

Infinite row of dominoes.
Infinite choice trees, and infinite probability

Infinite RAM Model

Platonic Version: One memory location for each natural number 0, 1, 2, …

Aristotelian Version: Whenever you run out of memory, the computer contacts the factory. A maintenance person is flown by helicopter and attaches 100 Gig of RAM and all programs resume their computations, as if they had never been interrupted.

The Ideal Computer: no bound on amount of memory no bound on amount of time

Ideal Computer is defined as a computer with infinite RAM.

You can run a Java program and never have any overflow, or out of memory errors.

An Ideal Computer Can Be Programmed To Print Out:

π: 3.14159265358979323846264…

2: 2.00000000000000000000000…

e: 2.7182818284559045235336…

1/3: 0.33333333333333333333….

ϕ: 1.6180339887498948482045…

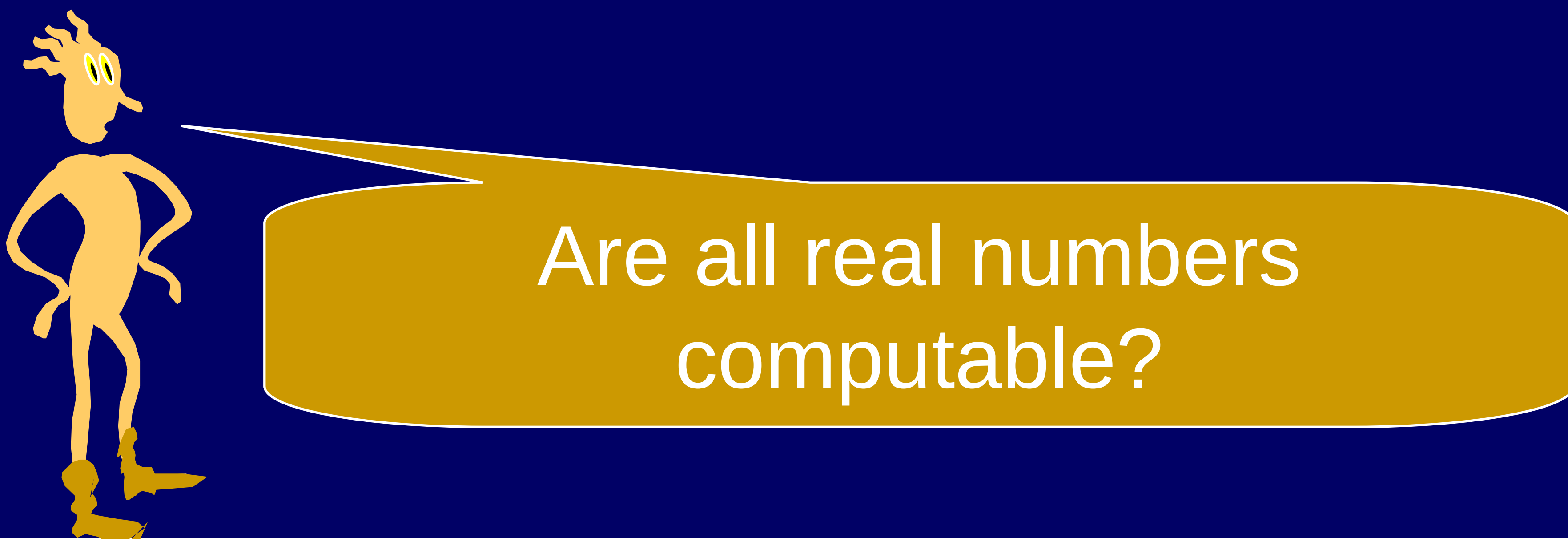
Printing Out An Infinite Sequence..

We say <u>program P prints out the infinite sequence s(0), s(1), s(2), …</u>; if when P is executed on an ideal computer a sequence of symbols appears on the screen such that

- The k^{th} symbol is s(k)
- For every $k \in \mathbb{N}$, P eventually prints the k^{th} symbol. I.e., the delay between symbol k and symbol k+1 is not infinite.

Computable Real Numbers

A real number r is computable if there is a program that prints out the decimal representation of r from left to right. Thus, each digit of r will eventually be printed as part of the output sequence.



Describable Numbers

A real number r is <u>describable</u> if it can be unambiguously denoted by a finite piece of English text.

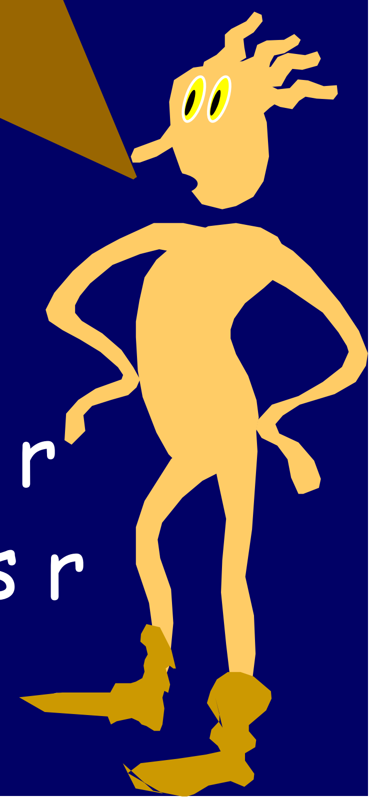
2: "Two."

π: "The area of a circle of radius one."

Is every computable real number, also a describable real number?

Computable r: some program outputs r

Describable r: some sentence denotes r



Theorem: Every computable real is also describable

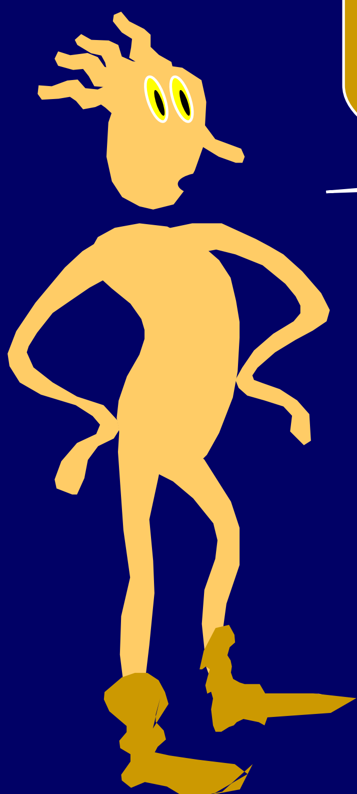
Proof: Let r be a computable real that is output by a program P. The following is an unambiguous denotation:

"The real number output by the following program:" P

MORAL: A computer program can be viewed as a description of its output.

Syntax: The text of the program

Semantics: The real number output by P.



Are all real numbers describable?

To INFINITY ....

and Beyond!

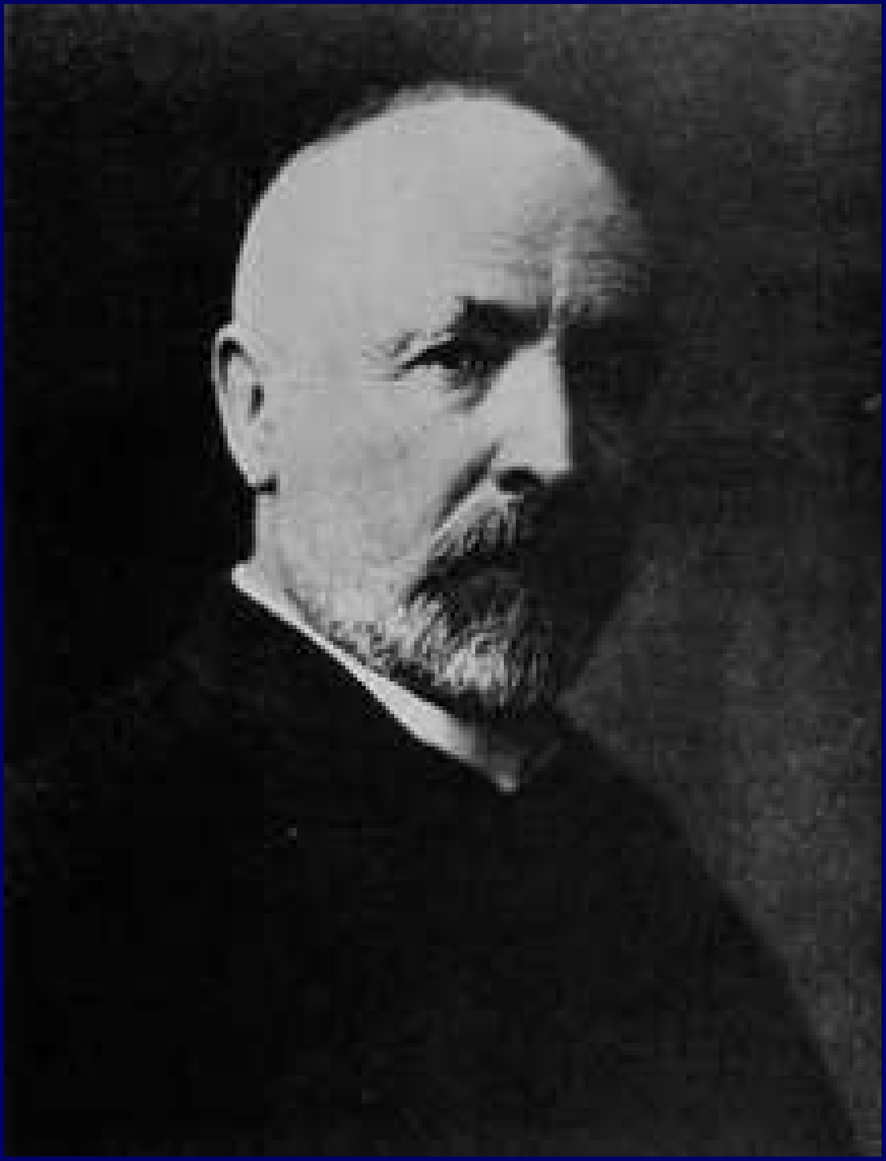
Correspondence Principle

If two finite sets can be placed into 1-1 onto correspondence, then they have the same size.

Correspondence Definition

Two finite sets are defined to have the <u>same size</u> if and only if they can be placed into 1-1 onto correspondence.

Georg Cantor (1845-1918)



Cantor's Definition (1874)

Two sets are defined to have the <u>same size</u> if and only if they can be placed into 1-1 onto correspondence.

Cantor's Definition (1874)

Two sets are defined to have the <u>same cardinality</u> if and only if they can be placed into 1-1 onto correspondence.

Do $\mathbb{N}$ and $\mathbb{E}$ have the same cardinality?

$\mathbb{N}$ = { 0, 1, 2, 3, 4, 5, 6, 7, ... }

$\mathbb{E}$ = The even, natural numbers.

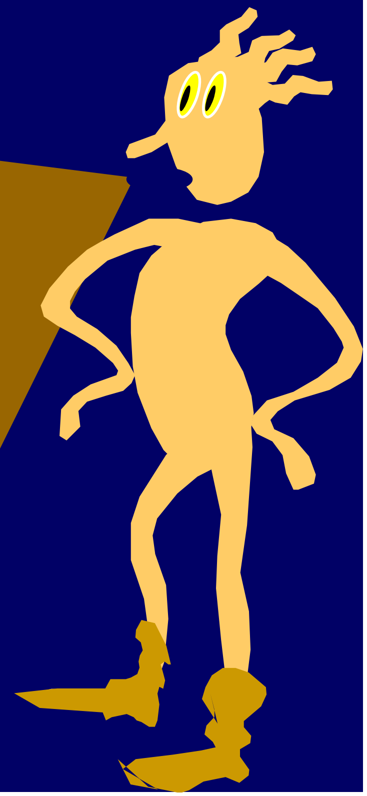
$\mathbb{E}$ and $\mathbb{N}$ do not have the same cardinality! $\mathbb{E}$ is a proper subset of $\mathbb{N}$ with plenty left over.

The attempted correspondence $f(x)=x$ does not take $\mathbb{E}$ *onto* $\mathbb{N}$.

$\mathbb{E}$ and $\mathbb{N}$ do have the same cardinality!

0, 1, 2, 3, 4, 5, ...
0, 2, 4, 6, 8,10, ...

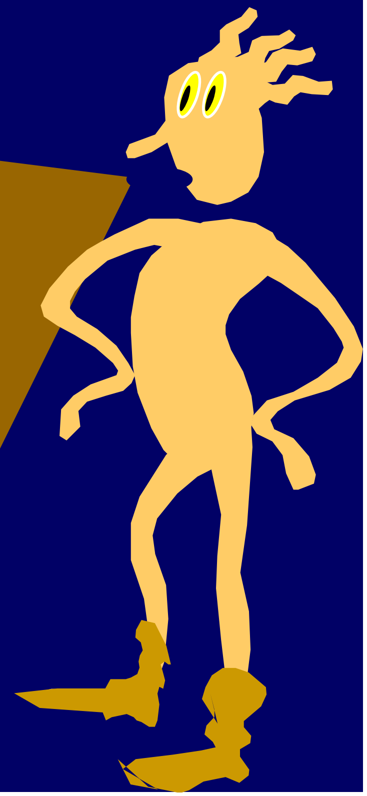
$f(x) = 2x$ is 1-1 onto.



Lesson:

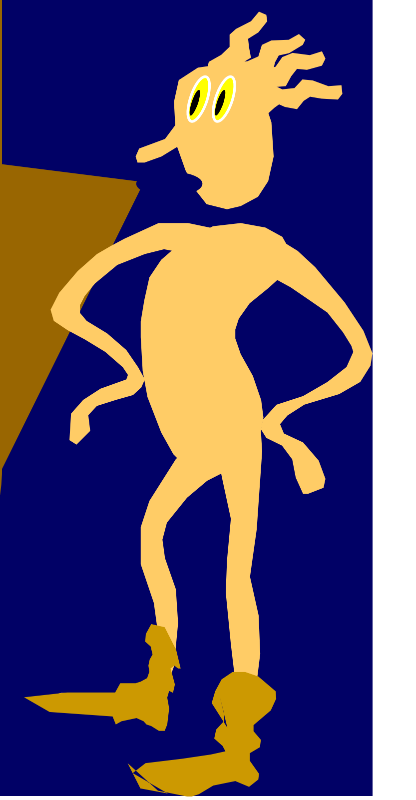
Cantor's definition only requires that *some* 1-1 correspondence between the two sets is onto, not that all 1-1 correspondences are onto.

This distinction never arises when the sets are finite.



If this makes you feel uncomfortable.....

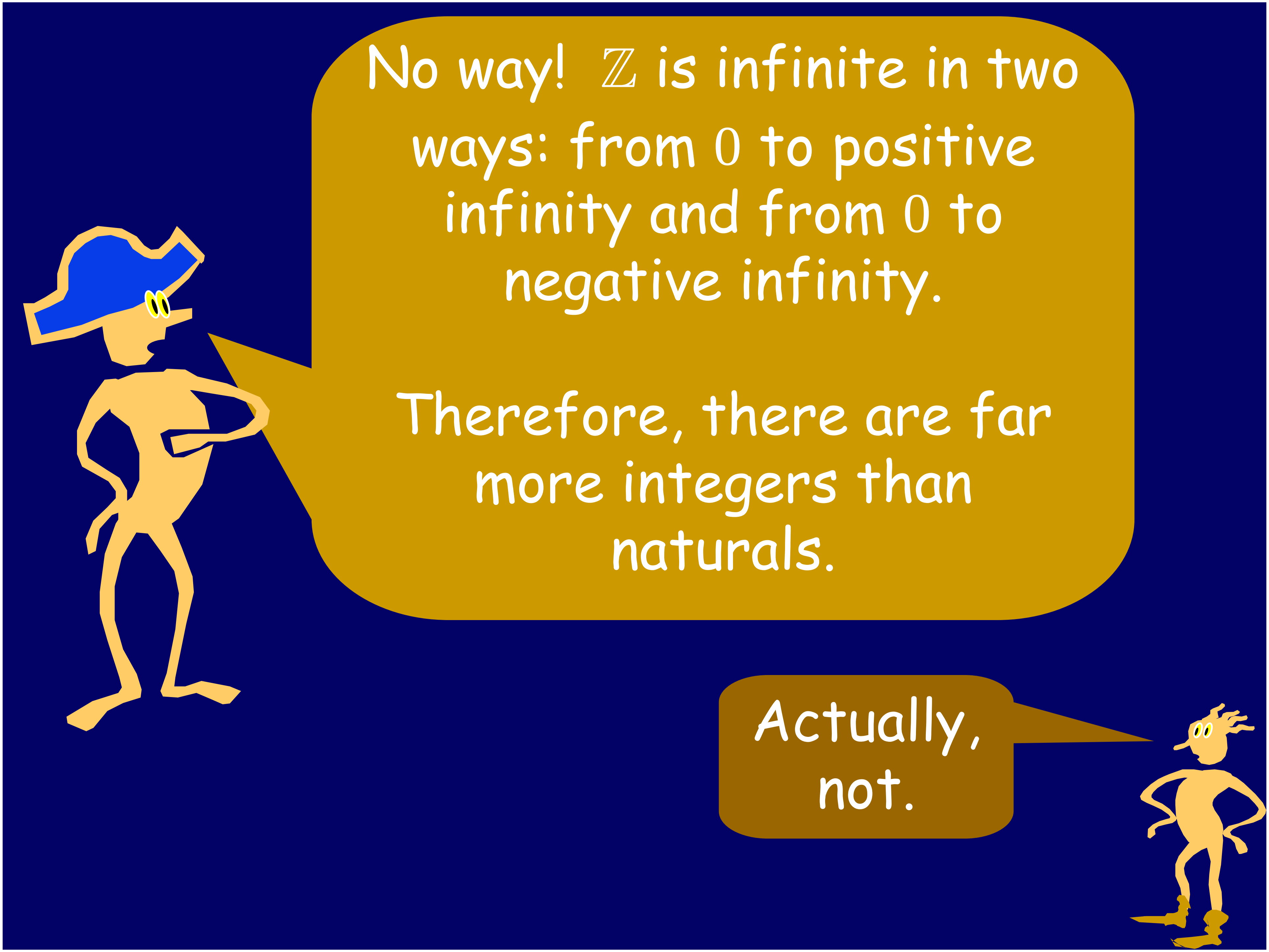
TOUGH! It is the price that you must pay to reason about infinity



Do $\mathbb{N}$ and $\mathbb{Z}$ have the same cardinality?

$\mathbb{N}$ = { 0, 1, 2, 3, 4, 5, 6, 7, ... }

$\mathbb{Z}$ = { ..., -2, -1, 0, 1, 2, 3, ... }

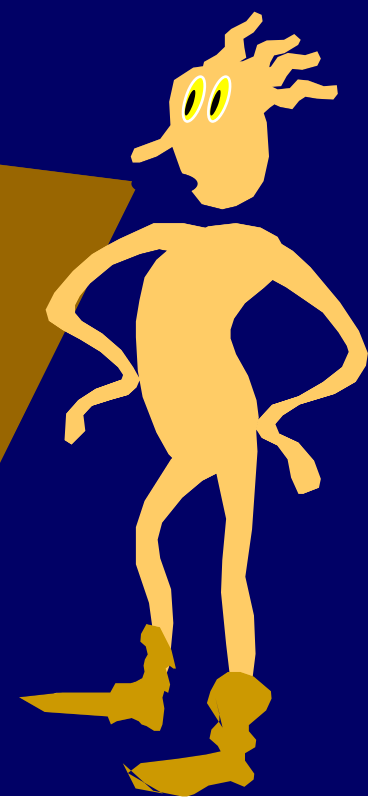

No way! $\mathbb{Z}$ is infinite in two ways: from 0 to positive infinity and from 0 to negative infinity.
Therefore, there are far more integers than naturals.
Actually, not.

$\mathbb{N}$ and $\mathbb{Z}$ do have the same cardinality!

0, 1, 2, 3, 4, 5,   6 …

0, 1, -1, 2, -2, 3, -3, ….

$$f(x) = \begin{cases} \lceil x/2 \rceil & \text{if } x \text{ is odd} \\ -x/2 & \text{if } x \text{ is even} \end{cases}$$



Transitivity Lemma

If f: $A \rightarrow B$ 1-1 onto, and g: $B \rightarrow C$ 1-1 onto
Then h(x) = g(f(x)) is 1-1 onto $A \rightarrow C$

Hence, $\mathbb{N}$, $\mathbb{E}$, and $\mathbb{Z}$ all have the same cardinality.

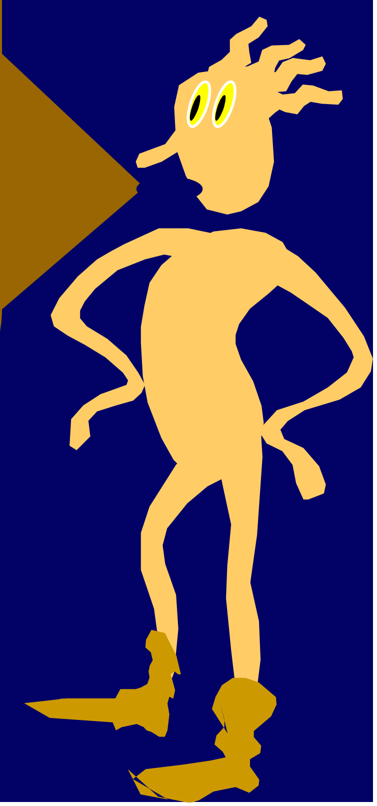
Do $\mathbb{N}$ and $\mathbb{Q}$ have the same cardinality?

$\mathbb{N}$= { 0, 1, 2, 3, 4, 5, 6, 7, ... }

$\mathbb{Q}$ = The Rational Numbers

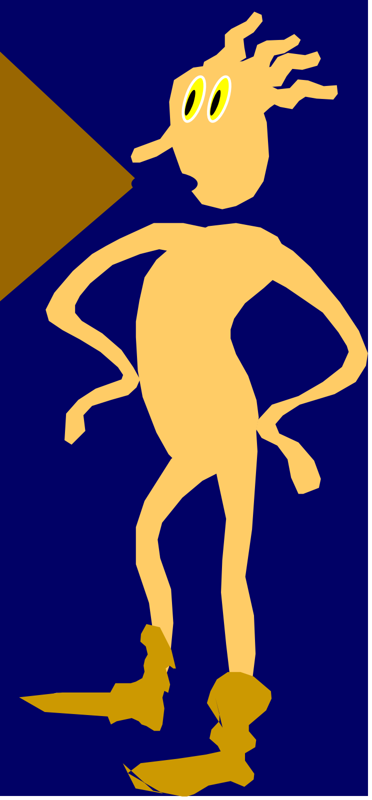
No way!
The rationals are dense: between any two there is a third. You can't list them one by one without leaving out an infinite number of them.

Don't jump to conclusions!
There is a clever way to list the rationals, one at a time, without missing a single one!

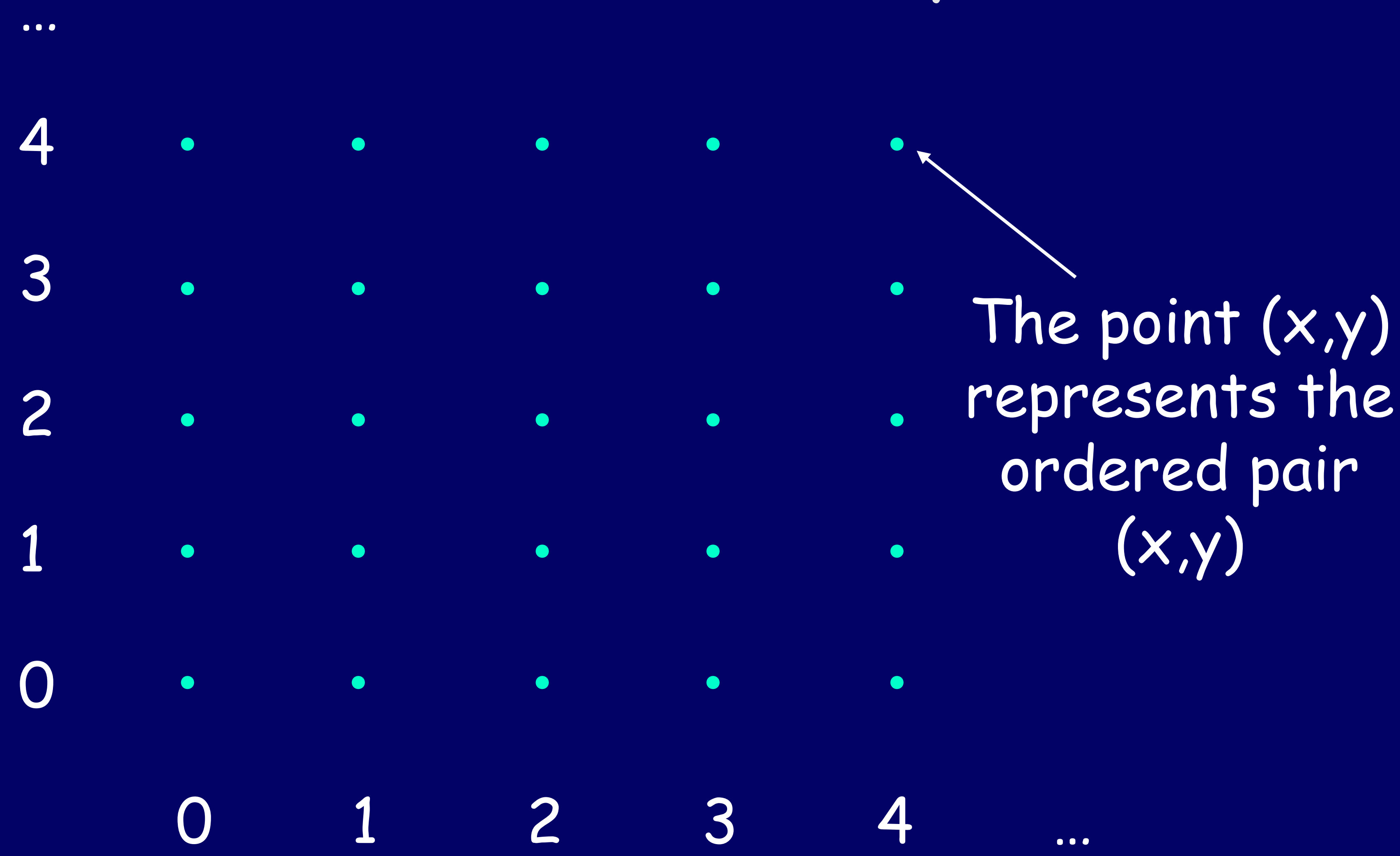


First, let's warm up with another interesting one:

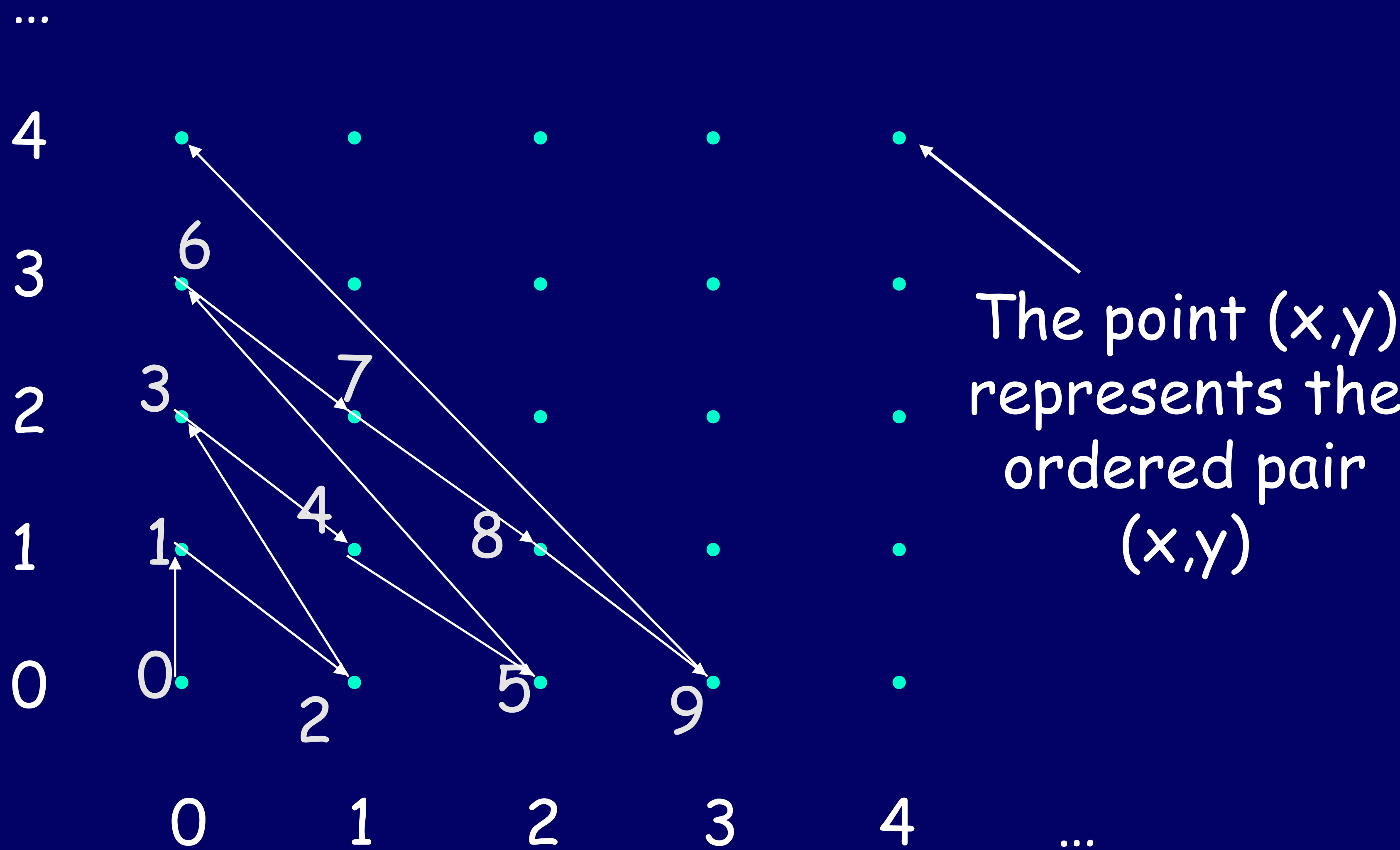
$\mathbb{N}$ can be paired with $\mathbb{N}\times\mathbb{N}$



Theorem: $\mathbb{N}$ and $\mathbb{N}$x$\mathbb{N}$ have the same cardinality



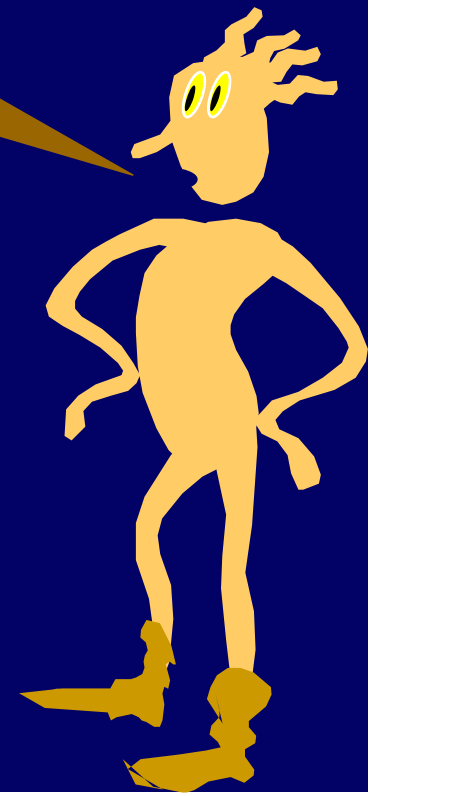
Theorem: $\mathbb{N}$ and $\mathbb{N} \times \mathbb{N}$ have the same cardinality

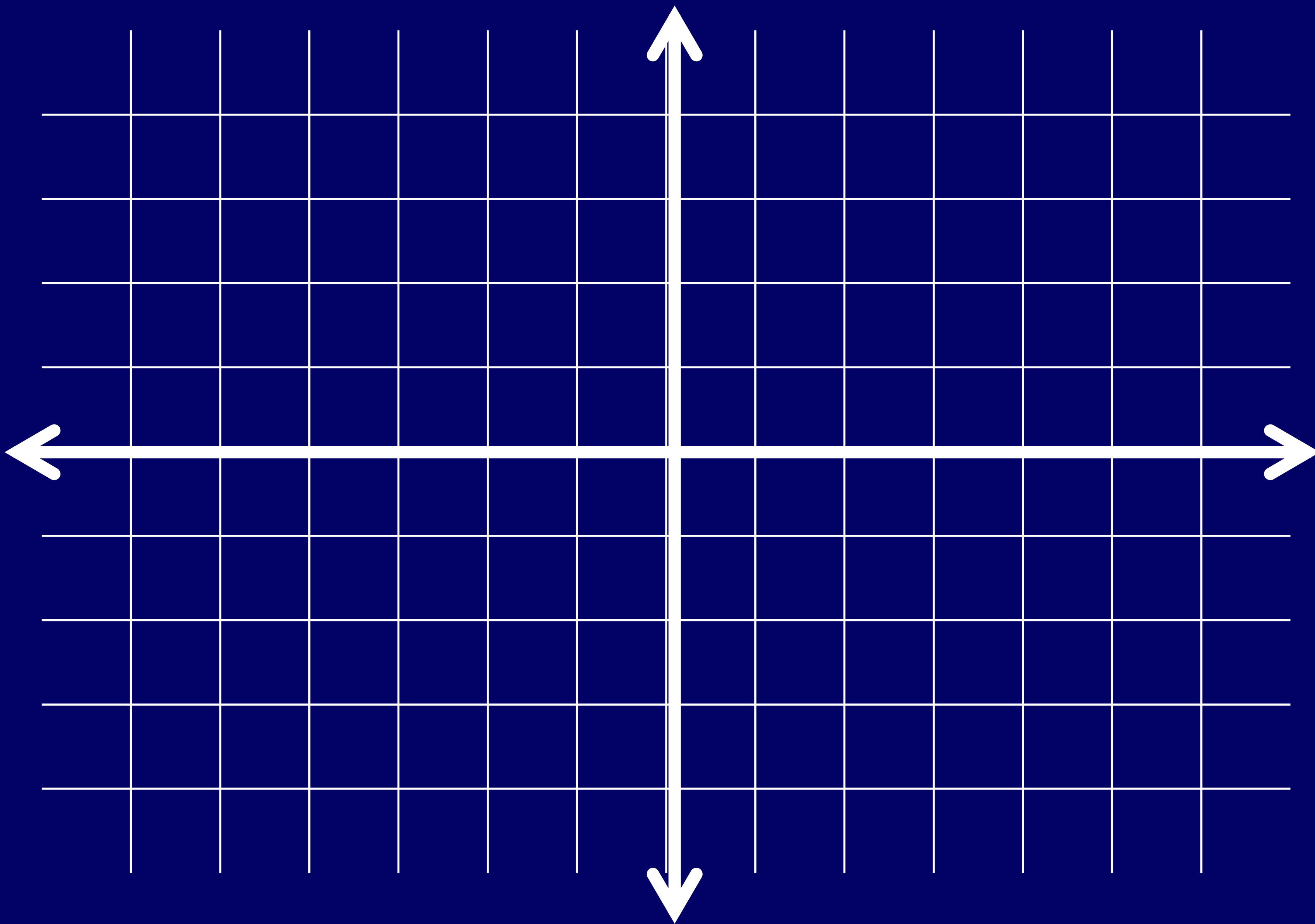


Defining 1,1 onto f: $\mathbb{N} \to \mathbb{N}\times\mathbb{N}$

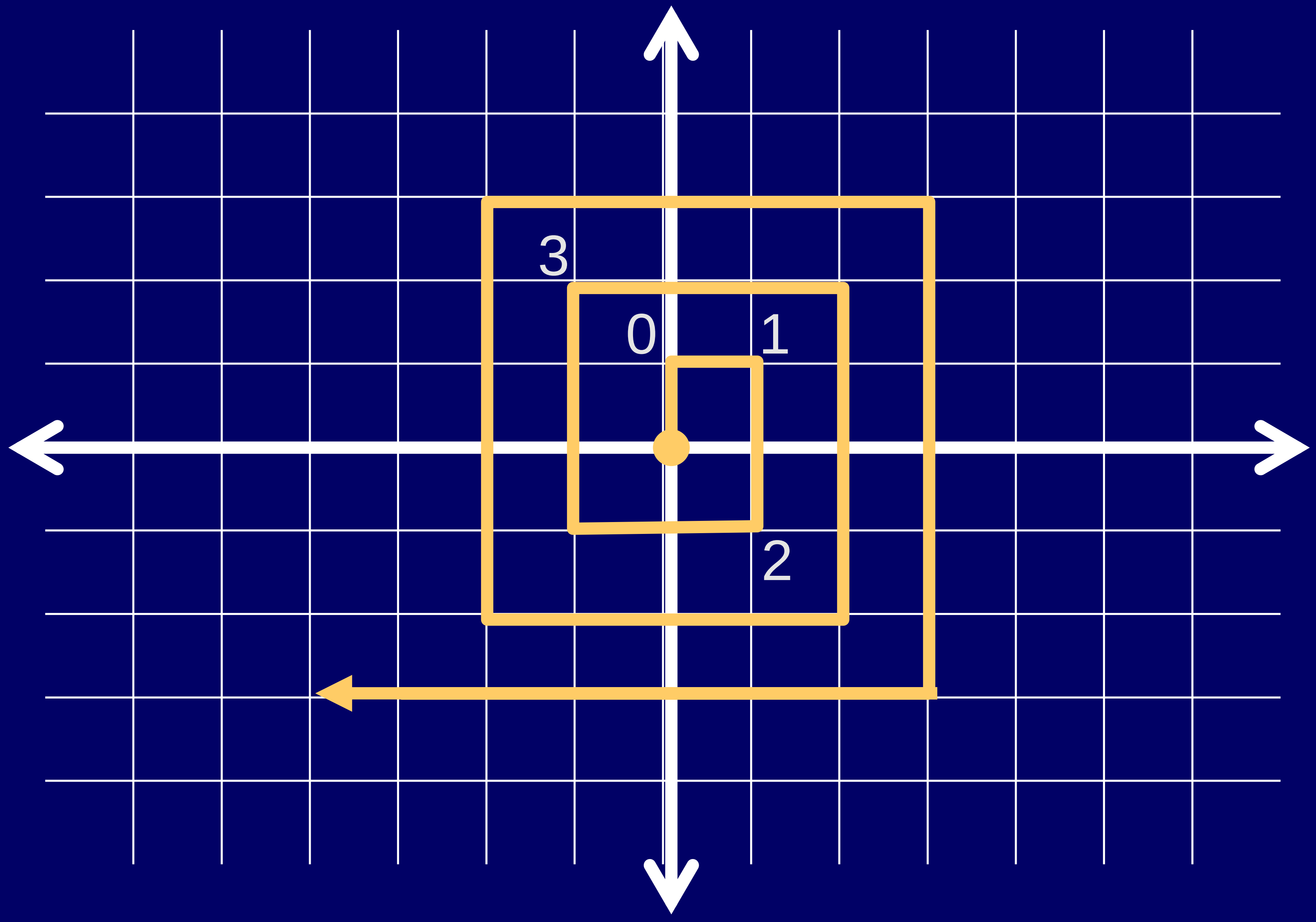
```
k;=0;

For sum = 0 to forever do

{For x = 0 to sum do
      {y := sum-x;
        Let f(k):= The point (x,y);
       k++
       }
}
```

Onto the Rationals!





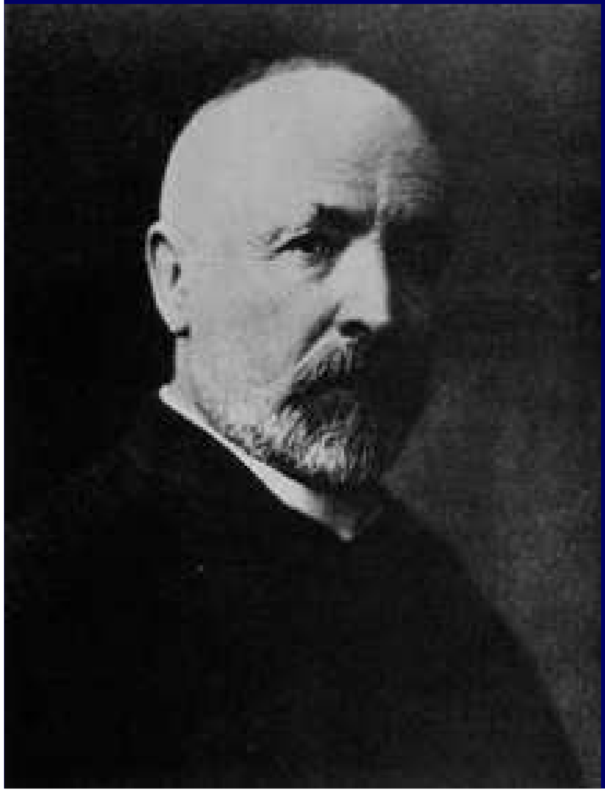
The point at x,y represents x/y



The point at x,y represents x/y

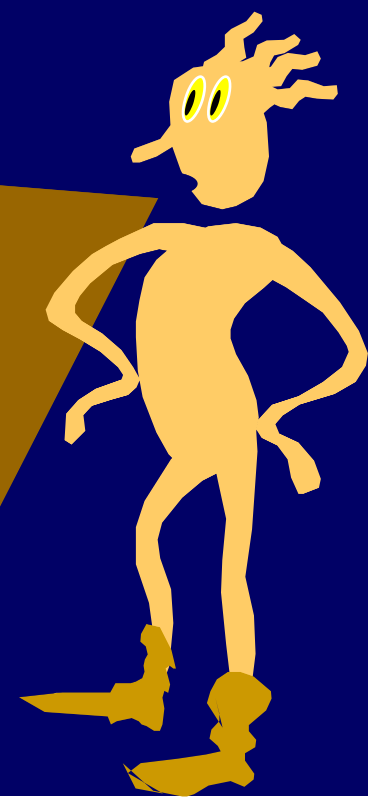
1877 letter to Dedekind:

I see it, but I don't believe it!



We call a set countable if it can be placed into 1-1 onto correspondence with the natural numbers.

So far we know that N, E, Z, and Q are countable.

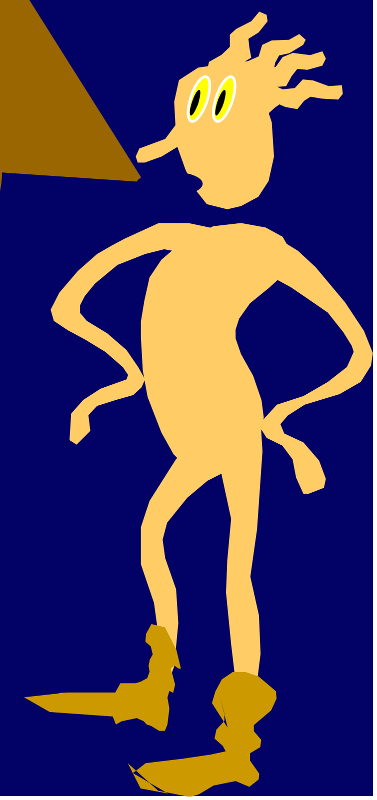


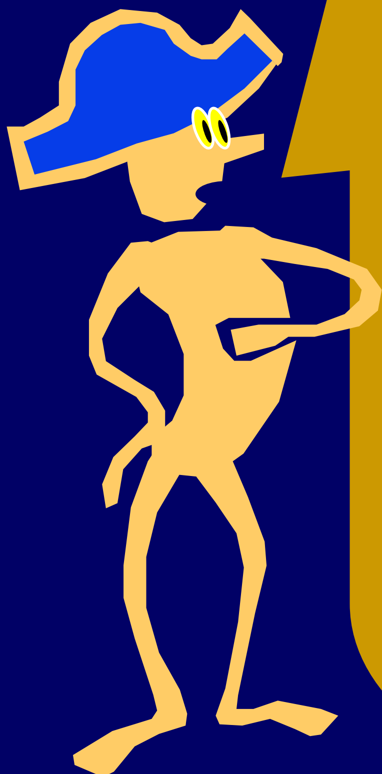
Do $\mathbb{N}$ and $\mathbb{R}$ have the same cardinality?

$\mathbb{N} = \{ 0, 1, 2, 3, 4, 5, 6, 7, \dots \}$

$\mathbb{R}$ = The Real Numbers

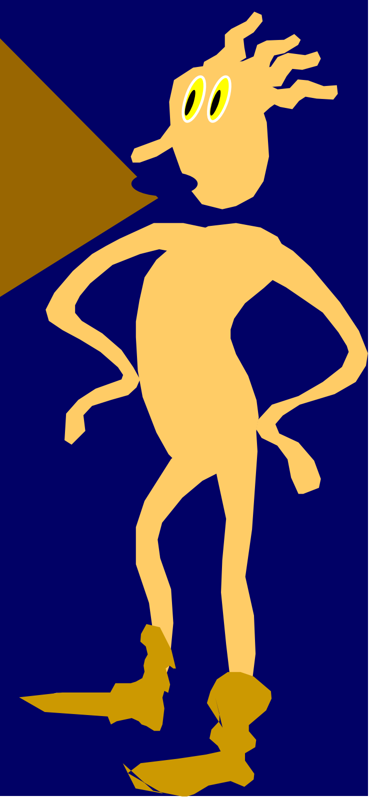
No way!
You will run out of natural numbers long before you match up every real.





Don't jump to conclusions! You can't be sure that there isn't some clever correspondence that you haven't thought of yet.

I am sure!
Cantor proved it.
He invented a very important technique called "DIAGONALIZATION".



Theorem: The set I of reals between 0 and 1 is not countable.

Proof by contradiction:

Suppose I is countable. Let f be the 1-1 onto function from $\mathbb{N}$ to I. Make a list L as follows:

0: decimal expansion of f(0)
1: decimal expansion of f(1)

…

k: decimal expansion of f(k)

…

Theorem: The set I of reals between 0 and 1 is not countable.

Proof by contradiction:

Suppose I is countable. Let f be the 1-1 onto function from $\mathbb{N}$ to I. Make a list L as follows:

0: .3333333333333333333333…

1: .3141592656578395938594982..

…

k: .345322214243555345221123235..

…

L	0	1	2	3	4	…
0						
1						
2						
3						
…						

L	0	1	2	3	4	...
0	d_0					
1		d_1				
2			d_2			
3				d_3		
...					...	

L	0	1	2	3	4
0	d_0				
1		d_1			
2			d_2		
3				d_3	
…					…

$$Confuse_L = .\ C_0 \quad C_1 \quad C_2 \quad C_3 \quad C_4 \quad C_5 \ \ldots$$

L	0	1	2	3	4
0	d_0				
1		d_1			
2			d_2		
3				d_3	
…					…

$$C_k = \begin{cases} 5, & \text{if } d_k = 6 \\ 6, & \text{otherwise} \end{cases}$$

$$\text{Confuse}_L = .\ C_0 \quad C_1 \quad C_2 \quad C_3 \quad C_4 \quad C_5 \ \ldots$$

L	0	1	2	3	4	
0	$c_0 \neq d_0$	c_1	c_2	c_3	c_4	…
1		d_1				
2			d_2			
3				d_3		
…					…	

$$c_k = \begin{cases} 5, & \text{if } d_k = 6 \\ 6, & \text{otherwise} \end{cases}$$

L	0	1	2	3	4	
0	d_0					
1	C_0	$C_1 \neq d_1$	C_2	C_3	C_4	…
2			d_2			
3				d_3		
…					…	

$$C_k = \begin{cases} 5, & \text{if } d_k = 6 \\ 6, & \text{otherwise} \end{cases}$$

L	0	1	2	3	4	
0	d_0					
1		d_1				
2	C_0	C_1	$C_2 \neq d_2$	C_3	C_4	…
3				d_3		
…					…	

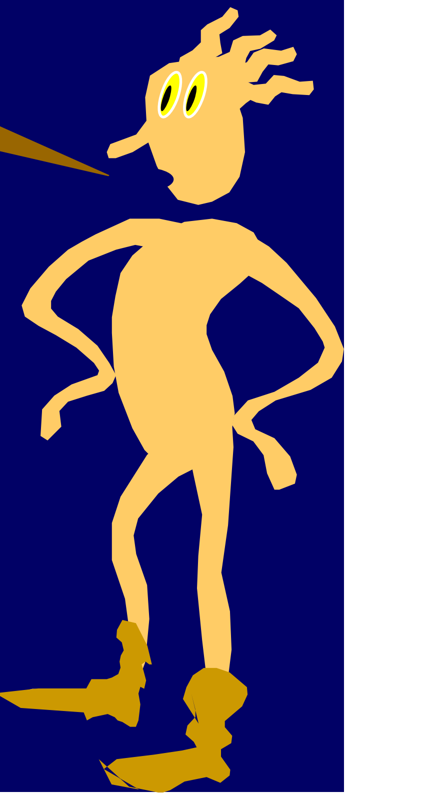
$$C_k = \begin{cases} 5, & \text{if } d_k = 6 \\ 6, & \text{otherwise} \end{cases}$$

L	0	1	2	3	4	
0	d_0					
1		d_1				
2	C_0	C_1	$C_2 \neq d_2$	C_3	C_4	…
3				d_3		
…					…	

$$C_k = \begin{cases} 5, & \text{if } d_k = 6 \\ 6, & \text{otherwise} \end{cases}$$

By design, Confuse_L can't be on the list! Confuse_L differs from the k^{th} element on the list in the k^{th} position. Contradiction of assumption that list is complete.

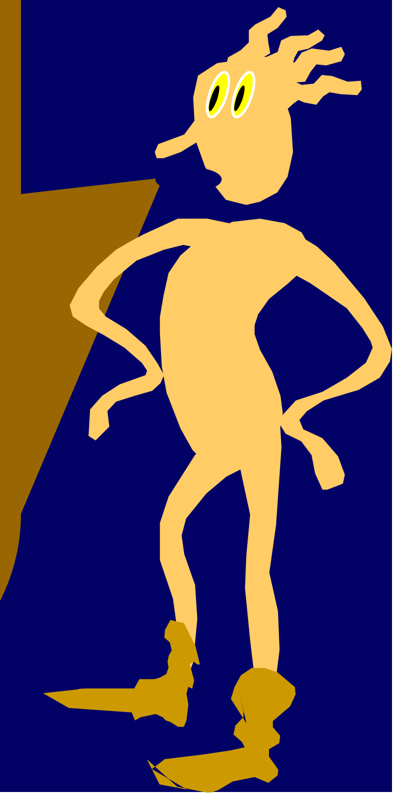
The set of reals is uncountable!



Hold it!

Why can’t the same argument be used to show that $\mathbb{Q}$ is uncountable?

The argument works the same for $\mathbb{Q}$ until the punchline. $\mathrm{CONFUSE}_L$ is not necessarily rational, so there is no contradiction from the fact that it is missing.



Standard Notation

Σ = Any finite alphabet

Example: {a,b,c,d,e,…,z}

Σ^* = All finite strings of symbols from Σ including the empty string ε

Theorem: Every infinite subset S of Σ^* is countable

Proof: Sort S by first by length and then alphabetically. Map the first word to 0, the second to 1, and so on....

Stringing Symbols Together

Σ = The symbols on a standard keyboard

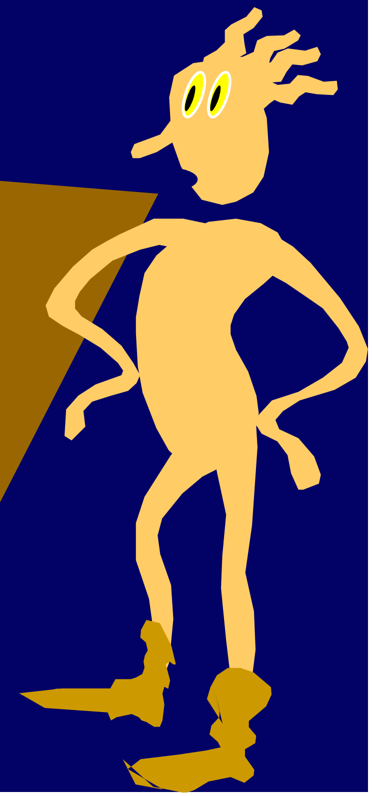
The set of all possible Java programs is a subset of Σ^*

The set of all possible finite pieces of English text is a subset of Σ^*

Thus:

The set of all possible Java programs is countable.

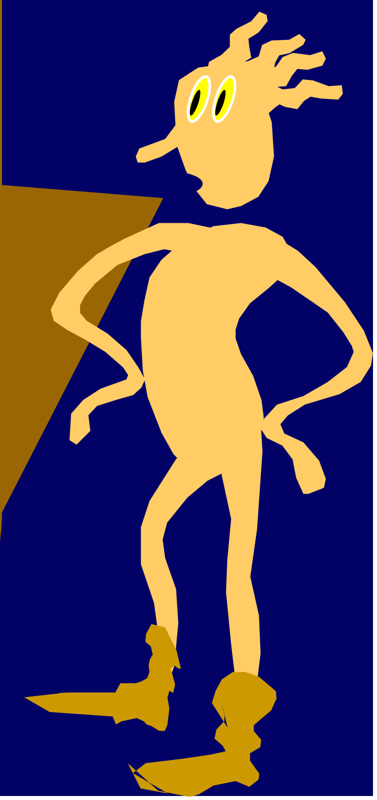
The set of all possible finite length pieces of English text is countable.



There are countably many Java program and uncountably many reals.

HENCE:

MOST REALS ARE NOT COMPUTABLE.



There are countably many descriptions and uncountably many reals.

Hence:

MOST REAL NUMBERS ARE NOT DESCRIBEABLE!


Oh, Bonzo!

Is there a real number that can be described, but not computed?

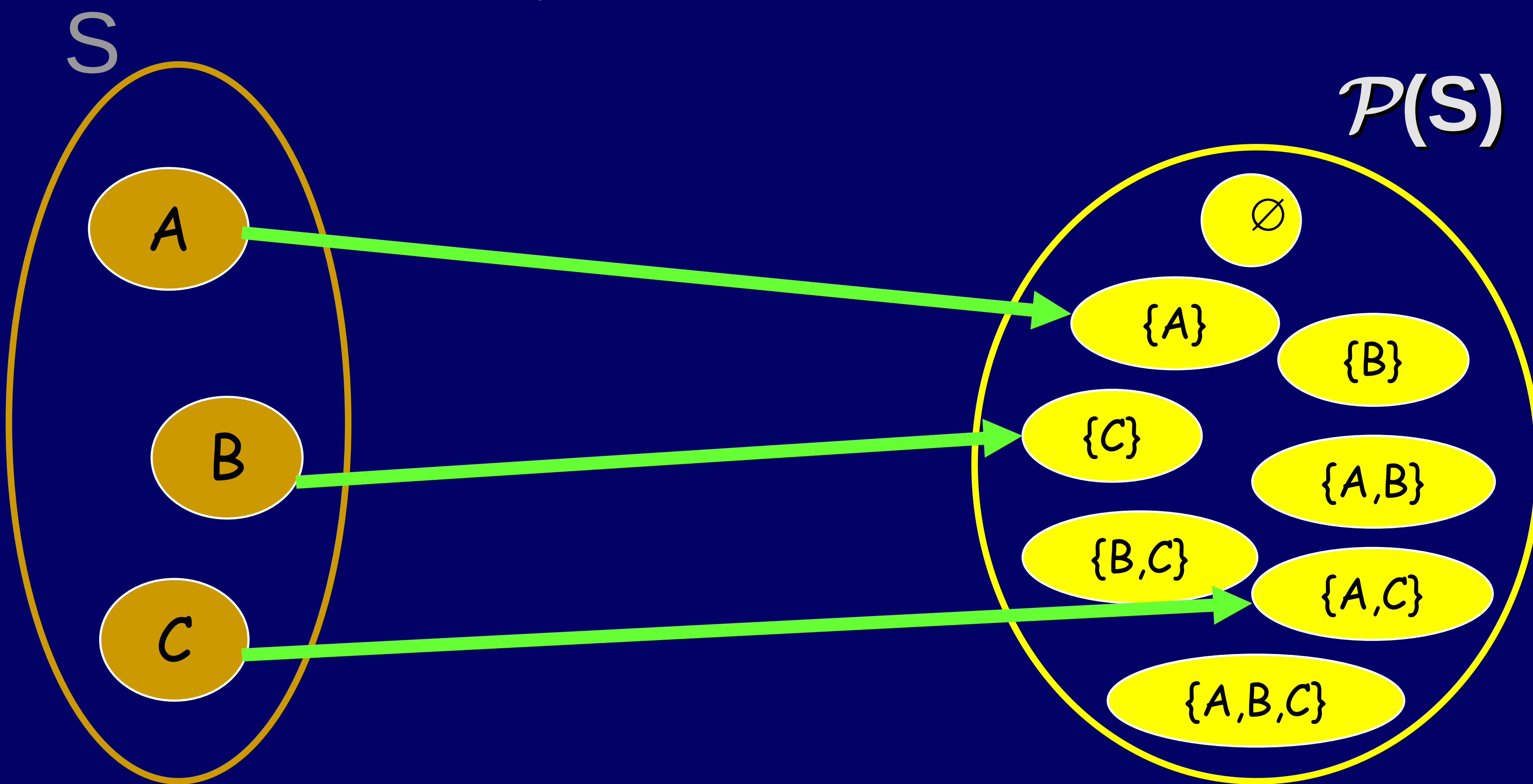
We know there are at least 2 infinities. Are there more?

Power Set

The power set of S is the set of all subsets of S. The power set is denoted $\mathcal{P}(S)$.

Proposition: If S is finite, the power set of S has cardinality $2^{|S|}$

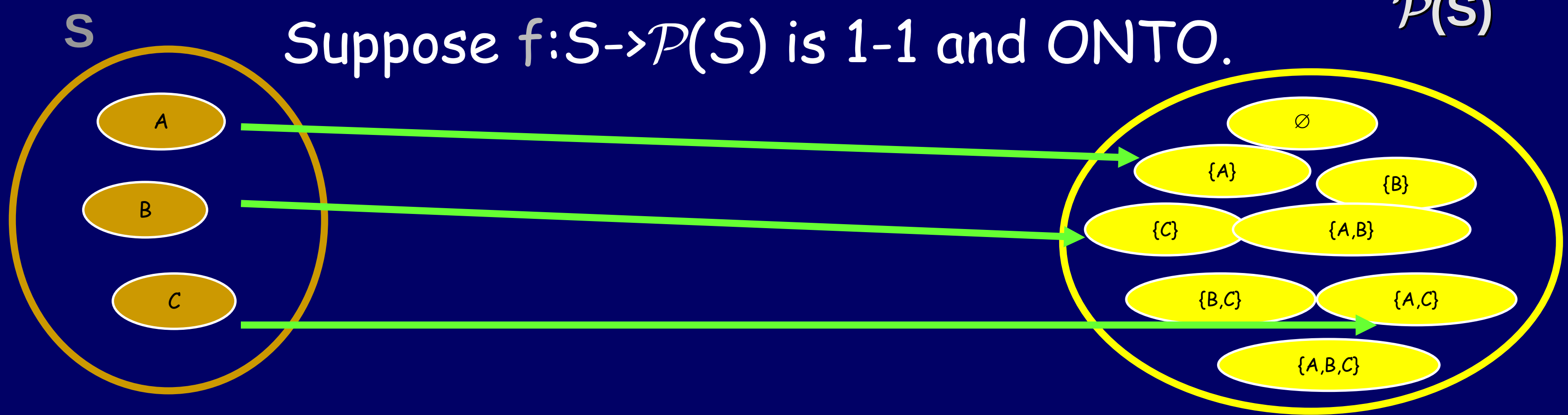
Theorem: S can't be put into 1-1 correspondence with $\mathcal{P}(S)$



Suppose f:S->$\mathcal{P}$(S) is 1-1 and ONTO.

Theorem: S can't be put into 1-1 correspondence with $\mathcal{P}$(S)

Suppose f:S->$\mathcal{P}$(S) is 1-1 and ONTO.



Let CONFUSE = $\{ x \mid x \in S, x \notin f(x) \}$

There is some y such that f(y)=CONFUSE

Is y in CONFUSE?

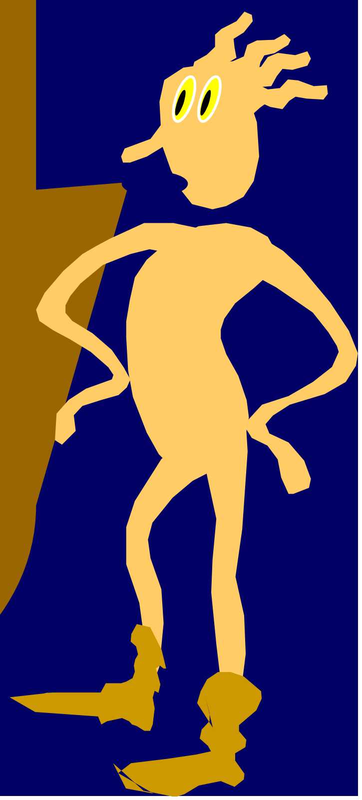
YES: Definition of CONFUSE implies no

NO: Definition of CONFUSE implies yes

This proves that there are at least a countable number of infinities.

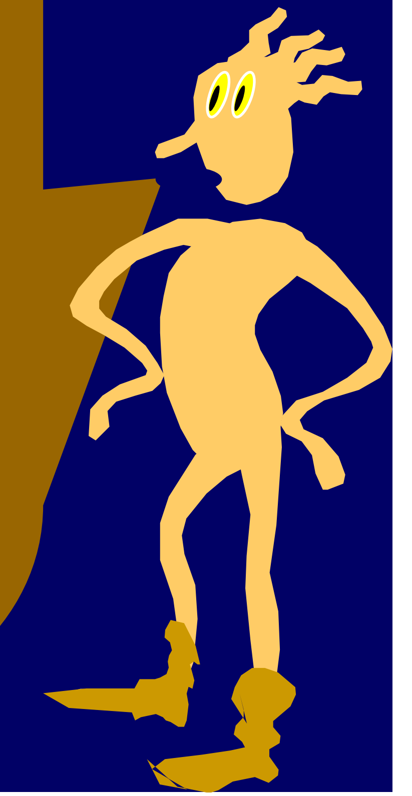
The first infinity is called:

$$\aleph_0$$



$$\aleph_0,\ \aleph_1, \aleph_2, \ldots$$

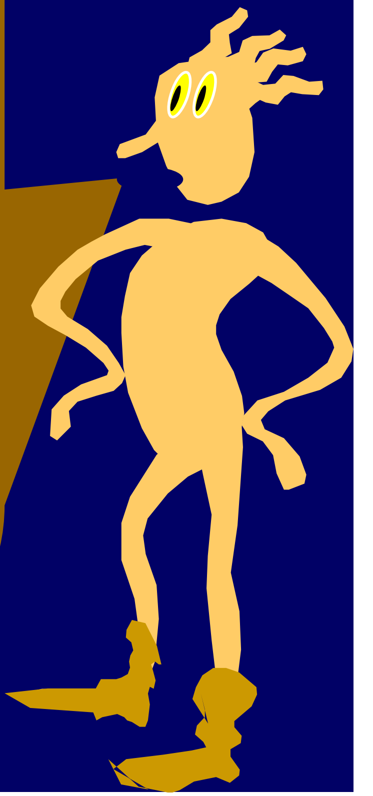
Are there any more infinities?



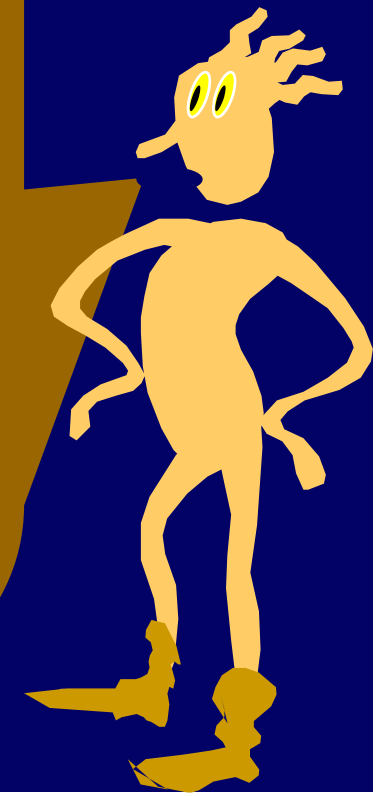
$\aleph_0, \aleph_1, \aleph_2, \ldots$

Let $S = \{\aleph_k \mid k \in \mathbb{N}\}$

$\mathcal{P}(S)$ is provably larger than any of them.

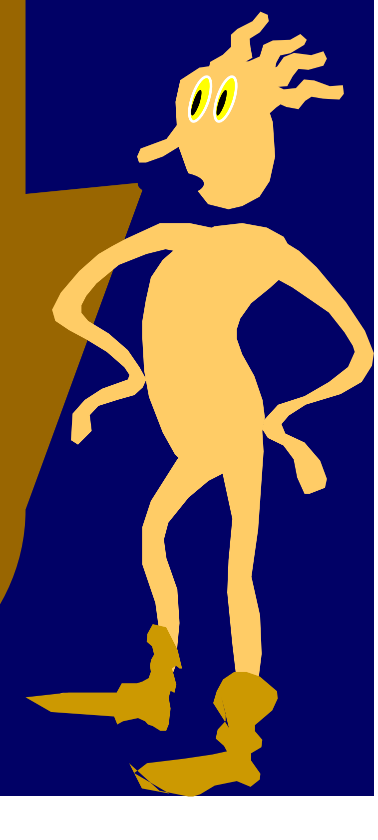


In fact, the same argument can be used to show that no single infinity is big enough to count the number of infinities!

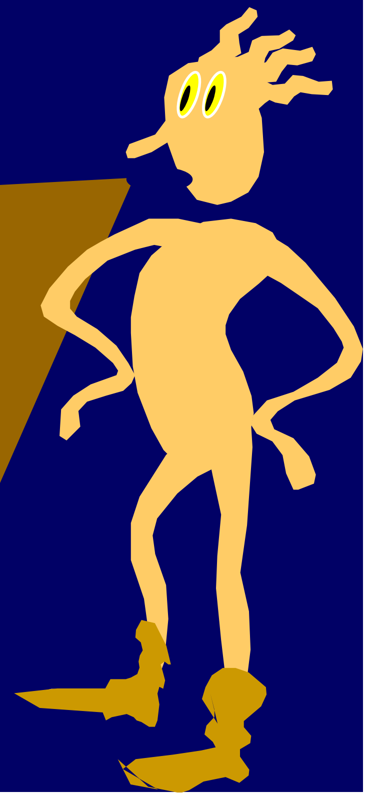


$$\aleph_0,\ \aleph_1, \aleph_2, \ldots$$

Cantor wanted to show that the number of reals was $\aleph_1$



Cantor called his conjecture that $\aleph_1$ was the number of reals the “Continuum Hypothesis.” However, he was unable to prove it. This helped fuel his depression.



The Continuum Hypothesis can't be proved or disproved from the standard axioms of set theory! This has been proved!