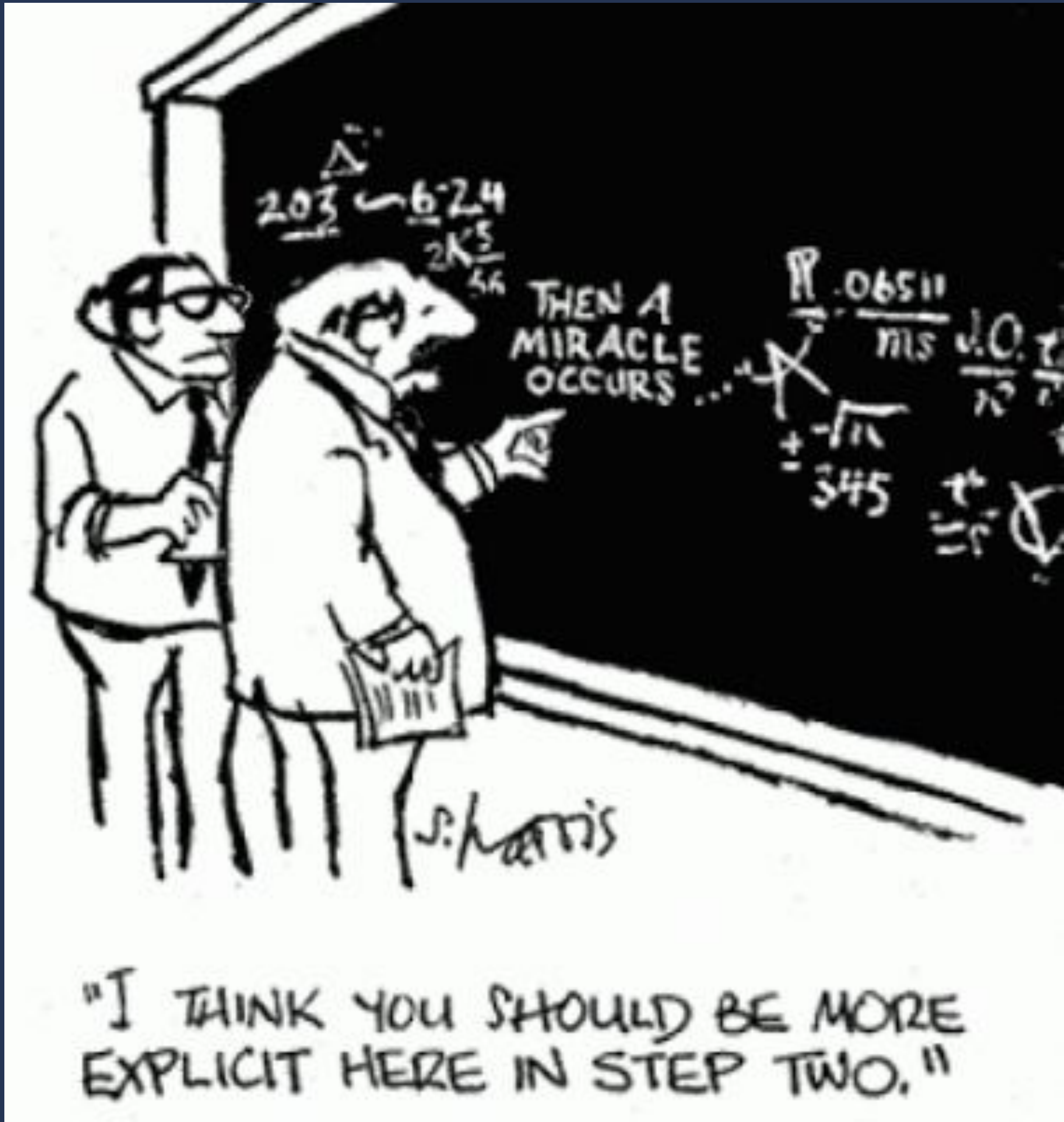
Warning: There will be Math

First

… a bit about proofs



Why would programmers care about proofs?

Why would programmers care about proofs?

- Introduces ways to break problems apart

Why would programmers care about proofs?

- Introduces ways to break problems apart
- Provides tools to perform "If this, then that" analysis

Why would programmers care about proofs?

- Introduces ways to break problems apart
- Provides tools to perform "If this, then that" analysis
- Provides a context for understanding logical systems

Why would programmers care about proofs?

- Introduces ways to break problems apart
- Provides tools to perform "If this, then that" analysis
- Provides a context for understanding logical systems

Why would programmers care about proofs?

- Introduces ways to break problems apart
- Provides tools to perform "If this, then that" analysis
- Provides a context for understanding logical systems

- I have other rants about how we should be teaching logic, number theory, and set theory instead of algebra, trigonometry, and calculus.

In mathematics, a proof is a deductive argument for a mathematical statement.

– **Wikipedia**

In the argument, other previously established statements, such as theorems, can be used.

– **Wikipedia**

Many forms of proofs

- Direct
- Contradiction
- Reducto ad Absurdum
- Existence
- Uniqueness
- Induction

Proof by Contradiction

Start with the opposite of the statement you wish to prove

Use only existing premises

axioms, other proofs

Contradiction

Contradiction

- If you reach an `impossible state`

Contradiction

- If you reach an `impossible state`
- then the opposite statement is `false`

Contradiction

- If you reach an `impossible state`
- then the opposite statement is `false`
- and thus the statement is `true`.

Example

$\sqrt{2}$ is irrational

Definition

Definition

- Rational numbers can be written in form $\dfrac{a}{b}$

Definition

- Rational numbers can be written in form $\dfrac{a}{b}$
- a and b are whole numbers that share no prime factors.

Definition

- Rational numbers can be written in form $\frac{a}{b}$
- a and b are whole numbers that share no prime factors.
- Irrational numbers cannot

Givens

Givens

- Any number written in the form $2n$ must be even

Givens

- Any number written in the form $2n$ must be even
- If n^2 is even then n must be even

Givens

- Any number written in the form $2n$ must be even
- If n^2 is even then n must be even
- If n^2 is even then n^2 must be a multiple of 4

Rational numbers can be written in form $\frac{a}{b}$

Rational numbers can be written in form $\frac{a}{b}$

- a and b are whole numbers that share no prime factors.

Rational numbers can be written in form $\frac{a}{b}$

- a and b are whole numbers that share no prime factors.
- One or both a or b must be odd

Rational numbers can be written in form $\frac{a}{b}$

- a and b are whole numbers that share no prime factors.
- One or both a or b must be odd
- Both a and b cannot be even

Proof by Contradiction

- Assume there is a rational number $\frac{a}{b} = \sqrt{2}$

Deduce information about a

Deduce information about a

- If $\frac{a}{b} = \sqrt{2}$ then

Deduce information about a

- If $\dfrac{a}{b} = \sqrt{2}$ then
- $\dfrac{a^2}{b^2} = 2$

Deduce information about a

- If $\frac{a}{b} = \sqrt{2}$ then
- $\frac{a^2}{b^2} = 2$
- $a^2 = 2b^2$

Deduce information about a

- If $\frac{a}{b} = \sqrt{2}$ then
- $\frac{a^2}{b^2} = 2$
- $a^2 = 2b^2$
- *(given)* Thus a^2 must be even

Deduce information about a

- If $\dfrac{a}{b} = \sqrt{2}$ then
- $\dfrac{a^2}{b^2} = 2$
- $a^2 = 2b^2$
- *(given)* Thus a^2 must be even
- *(given)* Thus a is even

Deduce information about b

Deduce information about b

- $a^2 = 2b^2$ and a is even

Deduce information about b

- $a^2 = 2b^2$ and a is even
- *(given)* Thus a^2 is a multiple of four and can be written as $4n$ where n is odd

Deduce information about b

- $a^2 = 2b^2$ and a is even
- *(given)* Thus a^2 is a multiple of four and can be written as $4n$ where n is odd
- $4n = 2b^2$

Deduce information about b

- $a^2 = 2b^2$ and a is even
- *(given)* Thus a^2 is a multiple of four and can be written as $4n$ where n is odd
- $4n = 2b^2$
- $2n = b^2$

Deduce information about b

- $a^2 = 2b^2$ and a is even
- *(given)* Thus a^2 is a multiple of four and can be written as $4n$ where n is odd
- $4n = 2b^2$
- $2n = b^2$
- *(given)* thus b^2 is even – and *(given)* thus b is even

CONTRADICTION 💣 💥

both a and b cannot be even

- Started with assumption there could be a rational number

- Started with assumption there could be a rational number
- Arrived at contradiction

- Started with assumption there could be a rational number
- Arrived at contradiction
- Thus there is no rational number $\frac{a}{b} = \sqrt{2}$

Induction

- Some statement P is true over some set of numbers (typically the non-negative integers or positive integers)

- Some statement P is true over some set of numbers (typically the non-negative integers or positive integers)
- Show that it is true for smallest number in set (typically 0 or 1)

- Some statement P is true over some set of numbers (typically the non-negative integers or positive integers)
- Show that it is true for smallest number in set (typically 0 or 1)
- Assume is true for n

- Some statement P is true over some set of numbers (typically the non-negative integers or positive integers)
- Show that it is true for smallest number in set (typically 0 or 1)
- Assume is true for n
- Prove that if true for n then true for $n+1$

Sum of the first N positive integers

$$1 + 2 + 3 + 4 + 5 + \ldots + (n-1) + n = \frac{n(n+1)}{2}$$

Show for 1

$$1 = \frac{1(2)}{2} = 1$$

Assume true for k

$$1+2+3+4+5+\ldots+(k-1)+k=\frac{k(k+1)}{2}$$

Prove true for $k+1$

Prove

$$1 + 2 + 3 + 4 + 5 + \ldots + (k-1) + k + (k+1) = \frac{(k+1)((k+1)+1)}{2}$$

Left hand side is

$$(1 + 2 + 3 + 4 + 5 + \ldots + (k - 1) + k) + (k + 1)$$

Left hand side is

$$(1+2+3+4+5+\ldots+(k-1)+k)+(k+1)$$

Reduce to

$$\frac{k(k+1)}{2}+(k+1)$$

$$\frac{k(k+1)}{2} + (k+1)$$

multiply $(k+1)$ by $\frac{2}{2}$

$$\frac{k(k+1)}{2} + (k+1)$$

multiply $(k+1)$ by $\frac{2}{2}$

$$\frac{k(k+1)}{2} + \frac{2(k+1)}{2}$$

$$\frac{k(k+1)}{2} + (k+1)$$

multiply $(k+1)$ by $\frac{2}{2}$

$$\frac{k(k+1)}{2} + \frac{2(k+1)}{2}$$

Common denominator

$$\frac{k(k+1) + 2(k+1)}{2}$$

$$\frac{k(k+1)+2(k+1)}{2}$$

Extract common factor of $(k+1)$

$$\frac{k(k+1)+2(k+1)}{2}$$

Extract common factor of $(k+1)$

$$\frac{(k+1)(k+2)}{2}$$

$$\frac{k(k+1)+2(k+1)}{2}$$

Extract common factor of $(k+1)$

$$\frac{(k+1)(k+2)}{2}$$

$$\frac{(k+1)((k+1)+1)}{2}$$

$$\frac{(k+1)((k+1)+1)}{2}$$

This is the same as our initial right hand side we were trying to prove

Thus: True! 🎉


© RAU

Encounters with Infinity

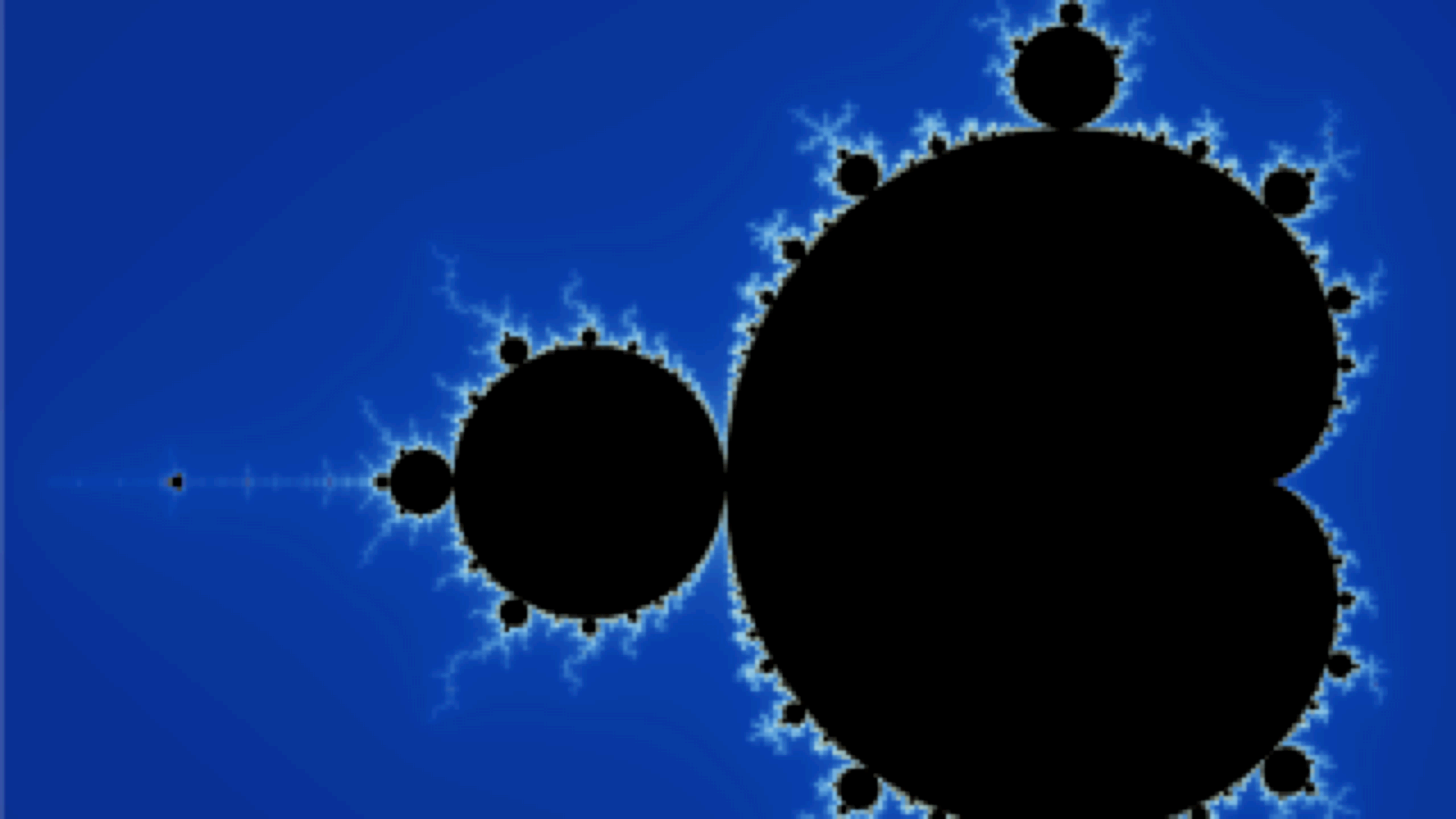
- What is the biggest number?
- How big is outer space?
- Calculus based on the infinitesimal

My love for $Math$

- The life and work of three mathematicians
- Benoit Mandelbrot
- Srinivasa Ramanujan
- Georg Cantor

Fractals

- Computer Recreations - Scientific American
- 1985 article on Mandelbrot fractal
  - https://www.scientificamerican.com/media/inline/blog/File/Dewdney_Mandelbrot.pdf
- Just *had* to program this on my Commodore 128



This complexity comes from the simplest of formula:

$$z \leftarrow z^2 + c$$

Srinivasa Ramanujan

- The Man Who Knew Infinity
- Self taught mathematician
- One of the most amazing mathematicians of the 19th century

$$\frac{1}{\pi} = \frac{2\sqrt{2}}{9801} \sum_{k=0}^{\infty} \frac{(4k)!(1103 + 26390k)}{k!^4 (396^{4k})}$$

- WAT!?!?

Georg Cantor

- 1845 - 1918
- Created Set Theory
- Defined Infinite Sets
- Initial resistance to his work
- Now recognized as fundamental to modern mathematics

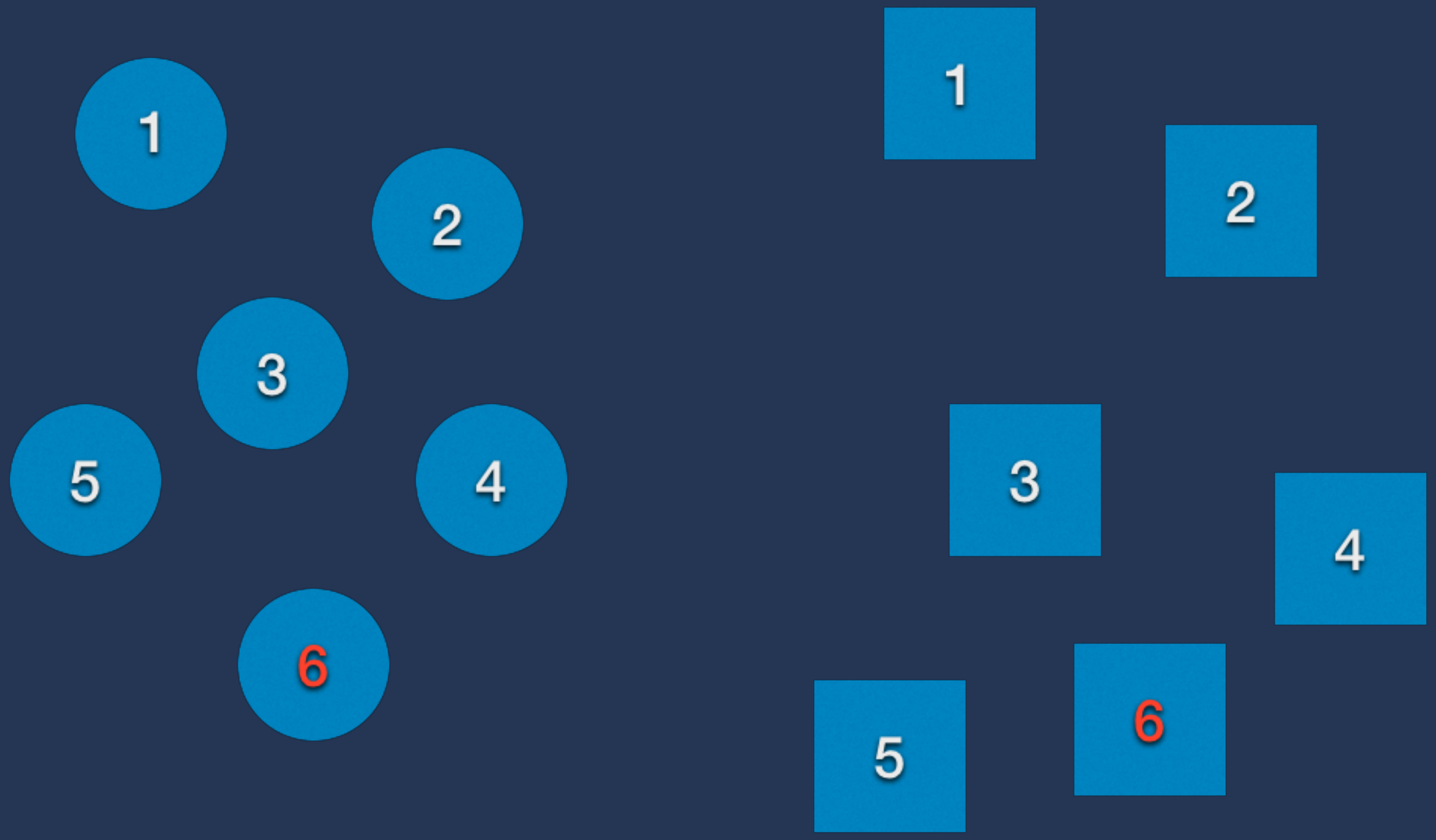
Counting

Cardinality

Are there as many circles as squares?

Are there as many circles as squares?

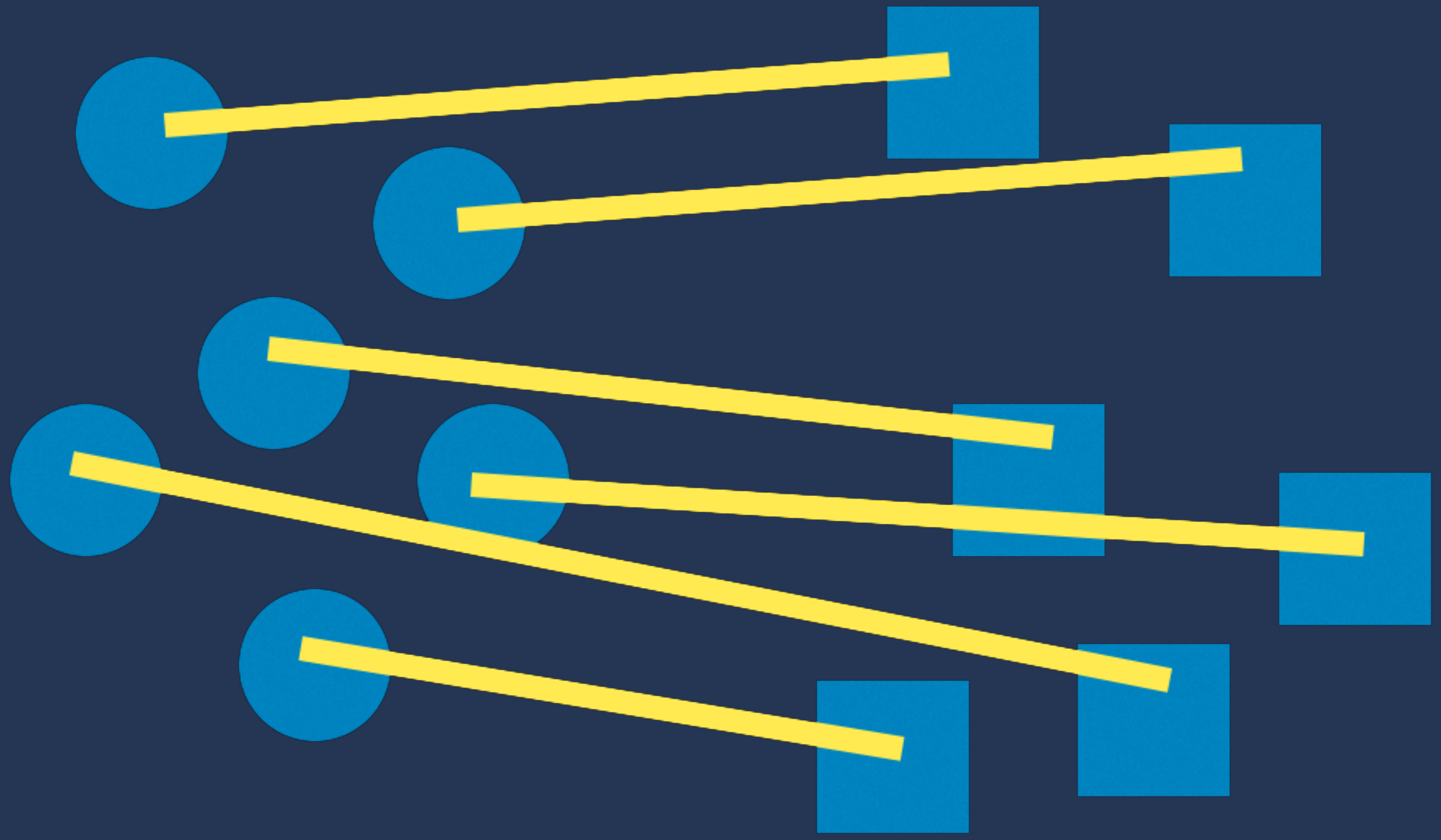
Enumeration



Are there as many circles as squares?

Pairing

We programmers might say map
mathematicians also say this



If a set A is subset of B with B having “left over” elements, B is larger

Does this work for infinite sets?

Which are there more of?

positive integers
or
even integers

Intuition

Intuition

1 2 3 4 5 6 7 8 9 10 11 12 13 14

2 4 6 8 10 12 14

There *must* be *more* positive integers

How could we count?

Not enumeration...

Pairing

... but what pairing?

```
1 2 3 4 5  6   7  8  9 10 11 12 13 14

| | | | |  |   |  |  |  |  |  |  |  |
v v v v v  v   v  v  v  v  v  v  v  v

2 4 5 8 10 12 14 16 18 20 22 24 26 28
```

Cardinality

- For every positive integer we have one even
- For every even we have one positive integer
- Sets are the same count/cardinality

Hilbert's Hotel

Hilbert's Hotel

- Hotel with an infinite number of rooms, all occupied

Hilbert's Hotel

- Hotel with an infinite number of rooms, all occupied
- One guest arrives!

Hilbert's Hotel

- Hotel with an infinite number of rooms, all occupied
- One guest arrives!
- We can make space by moving the guest in room 1 to room 2, 2 to 3, and so on

Hilbert's Hotel

- Hotel with an infinite number of rooms, all occupied
- One guest arrives!
- We can make space by moving the guest in room 1 to room 2, 2 to 3, and so on
- New guest takes room 1

Hilbert's Hotel

Hilbert's Hotel

- Countably infinite number of guests arrives

Hilbert's Hotel

- Countably infinite number of guests arrives
- We can make space by moving the guest in room 1 to room 2, 2 to 4, 3 to 6, and so on

Hilbert's Hotel

- Countably infinite number of guests arrives
- We can make space by moving the guest in room 1 to room 2, 2 to 4, 3 to 6, and so on
- Put new guests in the odd numbered rooms (since we know those are of equal cardinality)

Sets with the same cardinality

- natural numbers $(0, 1, 2, 3, 4, 5, \ldots)$
- square numbers $(0, 1, 4, 9, 16, \ldots)$
- cubed numbers $(0, 1, 8, 27, \ldots)$
- evens
- odds
- primes

Are there “larger” sets?

Real numbers

How do we show there are more reals than natural numbers?

How do we show there are more reals than natural numbers?

- Using a “constructive proof” (and some “proof by contradiction”)

How do we show there are more reals than natural numbers?

- Using a “constructive proof” (and some “proof by contradiction”)
- Building a mathematical object that demonstrates a statement is true.

Assume we can make a mapping from the natural numbers to the reals (here between 0 and 1)

Here is a random example

```
0     .1234567890123456789012345 67…
1     .3333333333333333333333333333…
2     .1415926535897932384626433 83…
3     .9876543210987654321098765 43…
4     .7182818284590452353602874 71…
5     .4242424242424242424242424 24…
6     .1010101010101010101010101 01…
7     .5555555555555555555555555555…
.                    .
.                    .
.                    .
.                    .
.                    .
```

The left column is a countably infinite sequence.

I propose the right side is all the real numbers between 0 and 1

Can we construct a number that disproves this is a complete mapping?

Can we construct a number that disproves this is a complete mapping?

- For the 0th number change the first digit.

Can we construct a number that disproves this is a complete mapping?

- For the 0th number change the first digit.
- For the 1st number change the second digit.

Can we construct a number that disproves this is a complete mapping?

- For the 0th number change the first digit.
- For the 1st number change the second digit.
- For the 2nd number change the third digit.

Can we construct a number that disproves this is a complete mapping?

- For the 0th number change the first digit.
- For the 1st number change the second digit.
- For the 2nd number change the third digit.
- And so on…

Contradiction

Contradiction

- Can’t be the first real number since it differs in the first digit

Contradiction

- Can't be the first real number since it differs in the first digit
- Can't be the second real number since it differs in the second digit

Contradiction

- Can’t be the first real number since it differs in the first digit
- Can’t be the second real number since it differs in the second digit
- Can’t be the third real number since it differs in the third digit

Contradiction

- Can't be the first real number since it differs in the first digit
- Can't be the second real number since it differs in the second digit
- Can't be the third real number since it differs in the third digit
- …

0 .🍕23456789012345678901234567…

1 .3🍕3333333333333333333333333…

2 .14🍕592653589793238462643383…

3 .987🍕54321098765432109876543…

4 .7182🍕1828459045235360287471…

5 .42424🍕424242424242424242424…

6 .101010🍕01010101010101010101…

7 .5555555🍕5555555555555555555…

. .

. .

. .

. .

. .

Cantor’s Diagonal Argument

Cardinality of the Continuum

The cardinality of the set of reals in the range (a, b) - regardless of how “close” a and b are - is the same as the cardinality of all reals.

Are there larger sets?

- Cantor's theorem states that "the cardinality of any set is strictly less than that of its power set"

- Power set: all subsets of elements of the set, including the empty set and the set itself.

Sizes of Infinity

- Natural Numbers
- Real Numbers
- Power set of Reals
    - Set of all functions from R => R
    - All subsets of the real number line
    - “Set of all curves in the plane”

I dare you

I double dog dare you

I triple dog dare you

Oh yeah, well I infinity dog dare you!

•••

Further Reading

- Book: https://www.amazon.com/The-Man-Who-Knew-Infinity/dp/0671750615
- Movie: https://www.amazon.com/Man-Who-Knew-Infinity/dp/B01HRX0T8K
- Books: https://github.com/gstark/kids_math_books

Thank you

... infinity ...