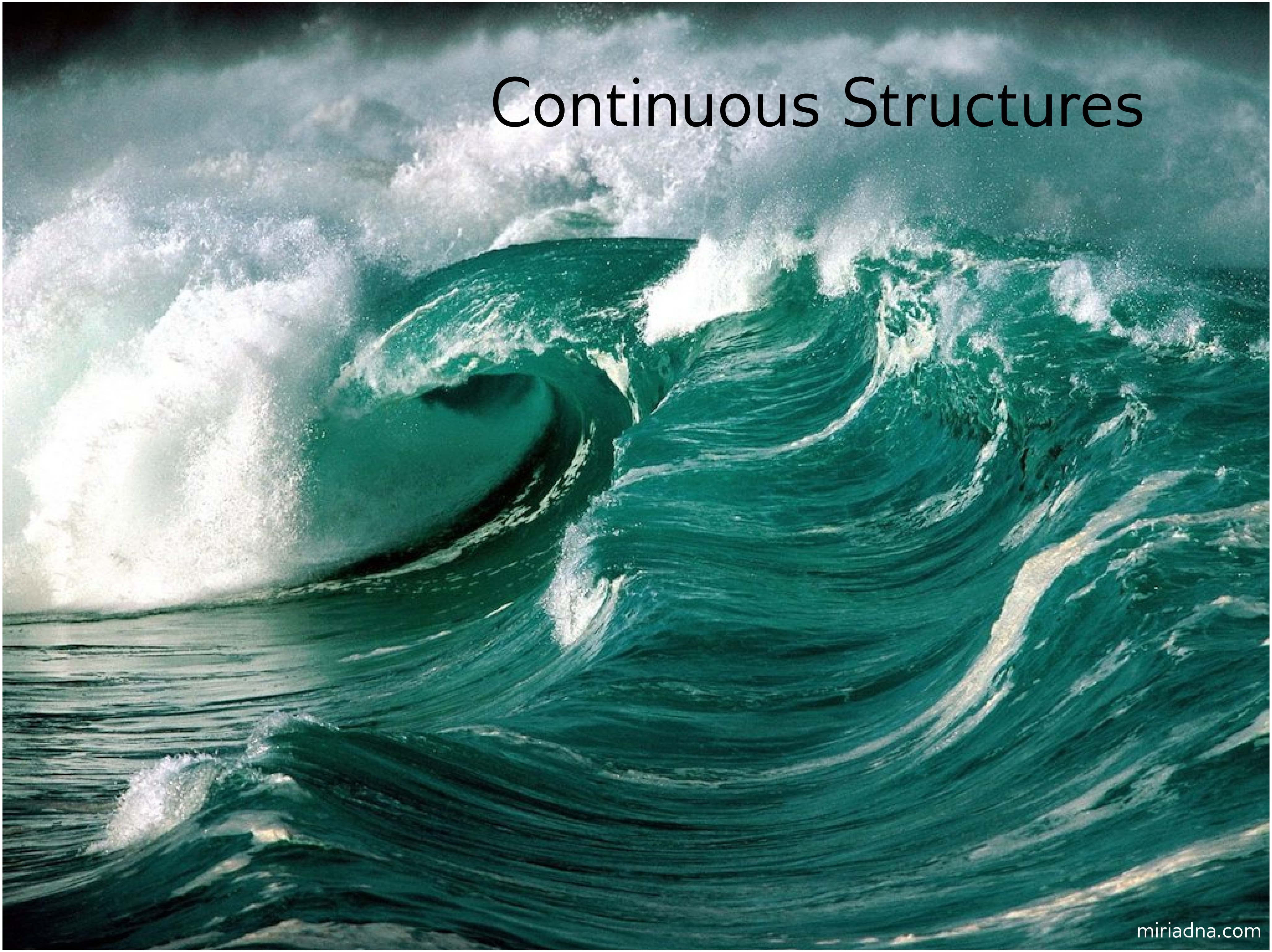
CS 2800: Discrete Structures

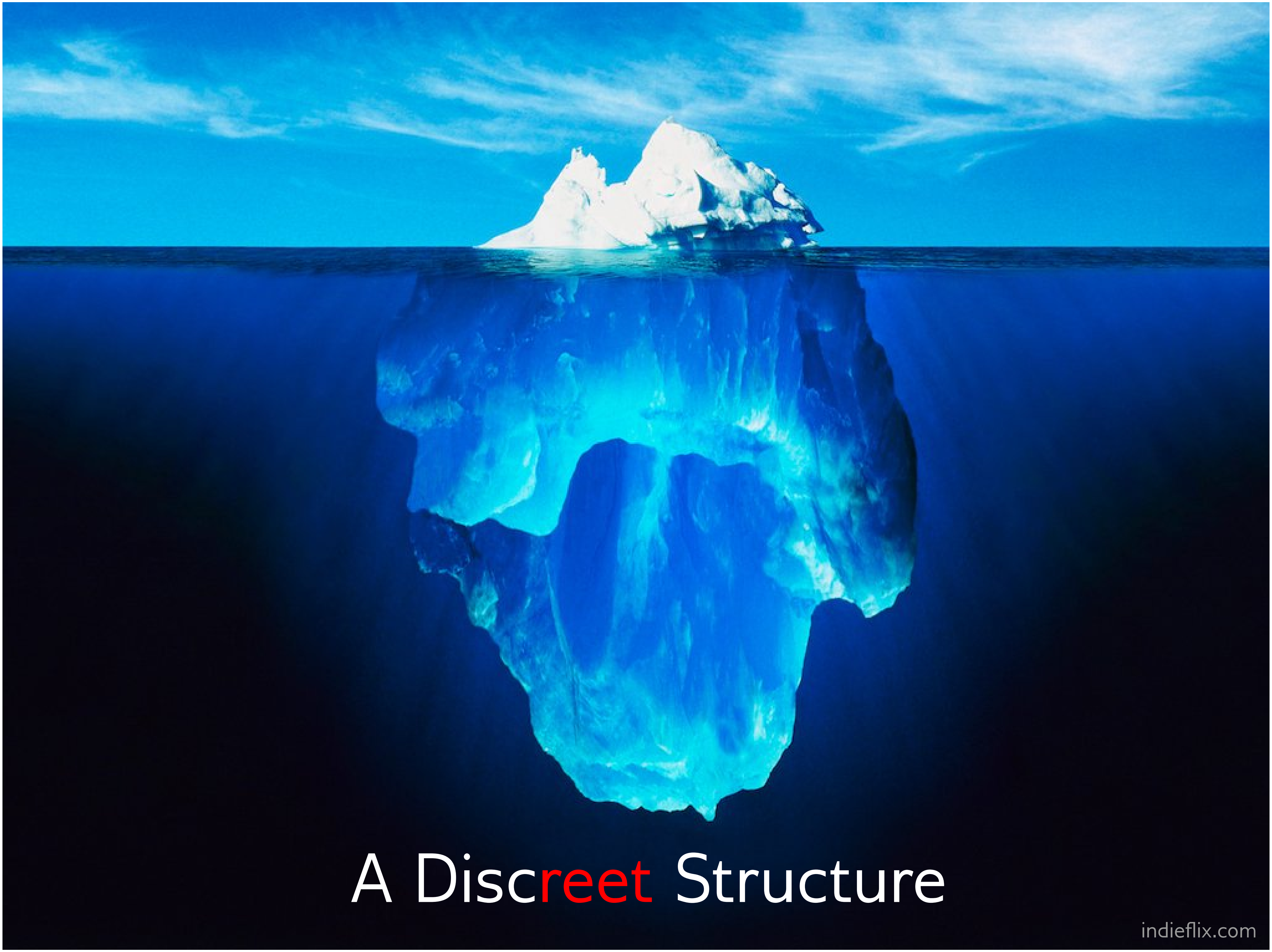
Fall 2016

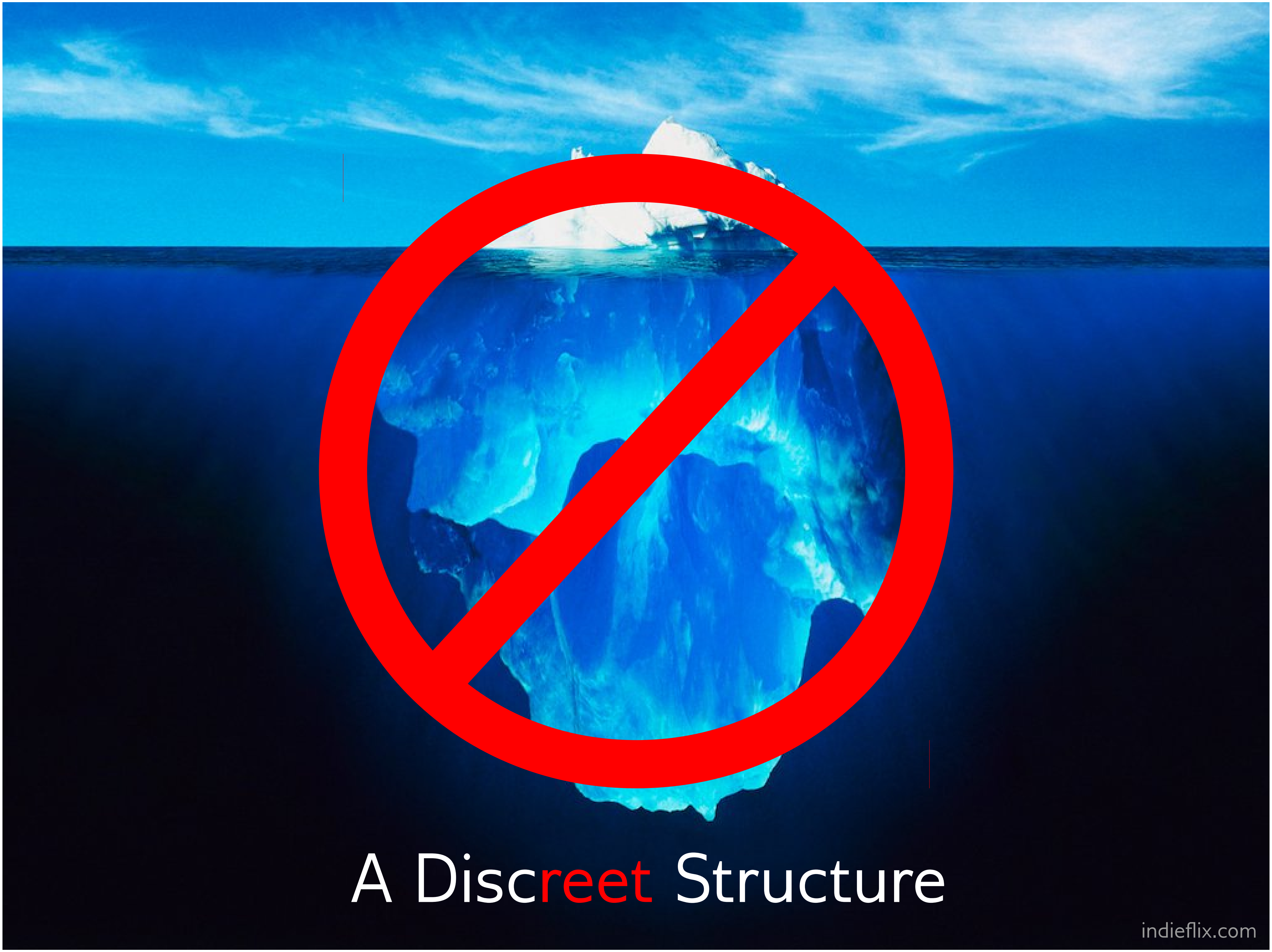
Mike George
Joe Halpern

Slides largely taken from Sid Chaudhuri, with thanks.

Discrete Structures


Continuous Structures
miriadna.com


A Discreet Structure
indieflix.com

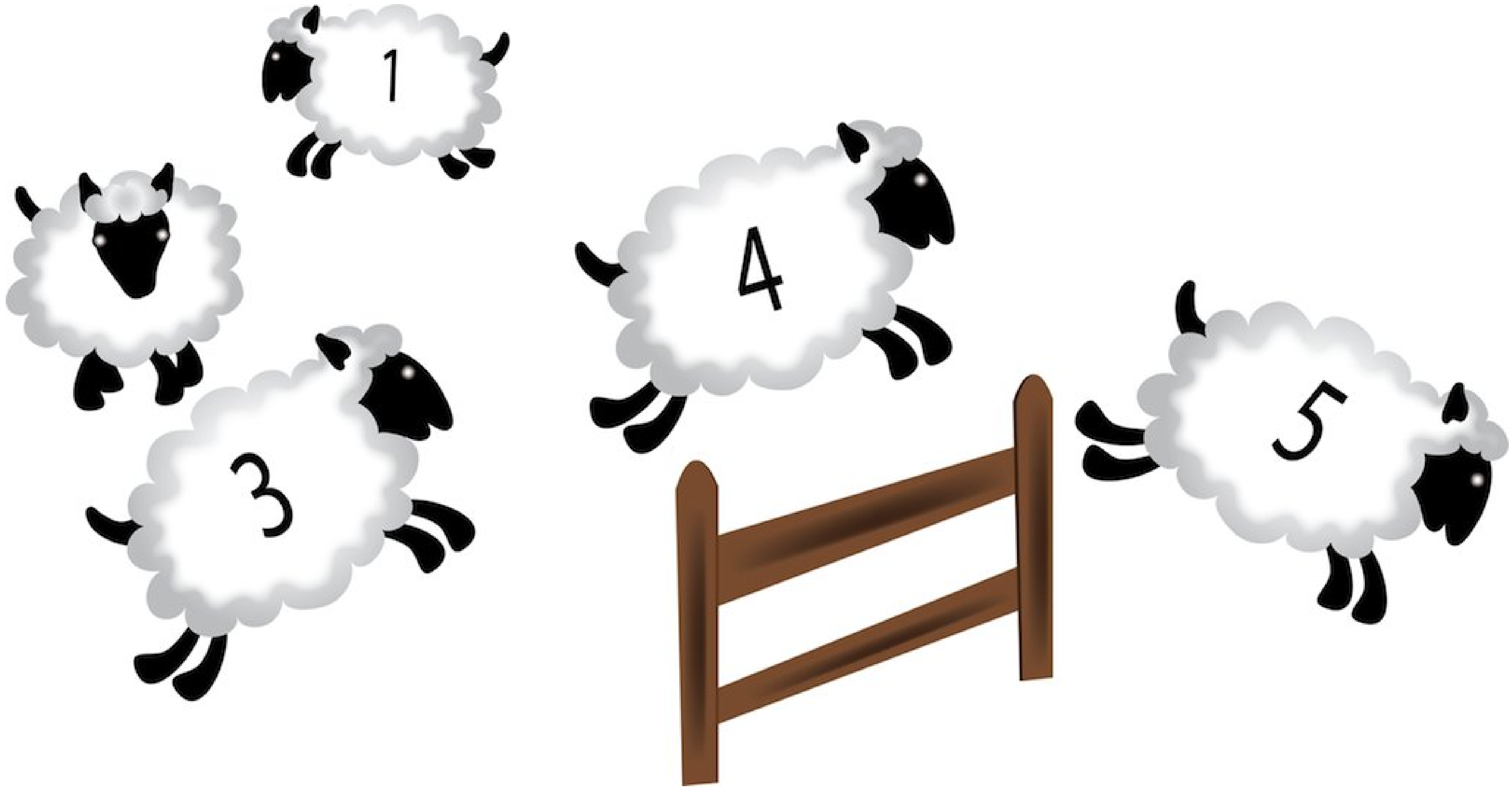


A Discreet Structure
indieflix.com

- discrete: individually separate and distinct
- discreet
  - careful and circumspect in one's speech or actions, especially in order to avoid causing offense or to gain an advantage.
  - intentionally unobtrusive.

Things we can count with the integers

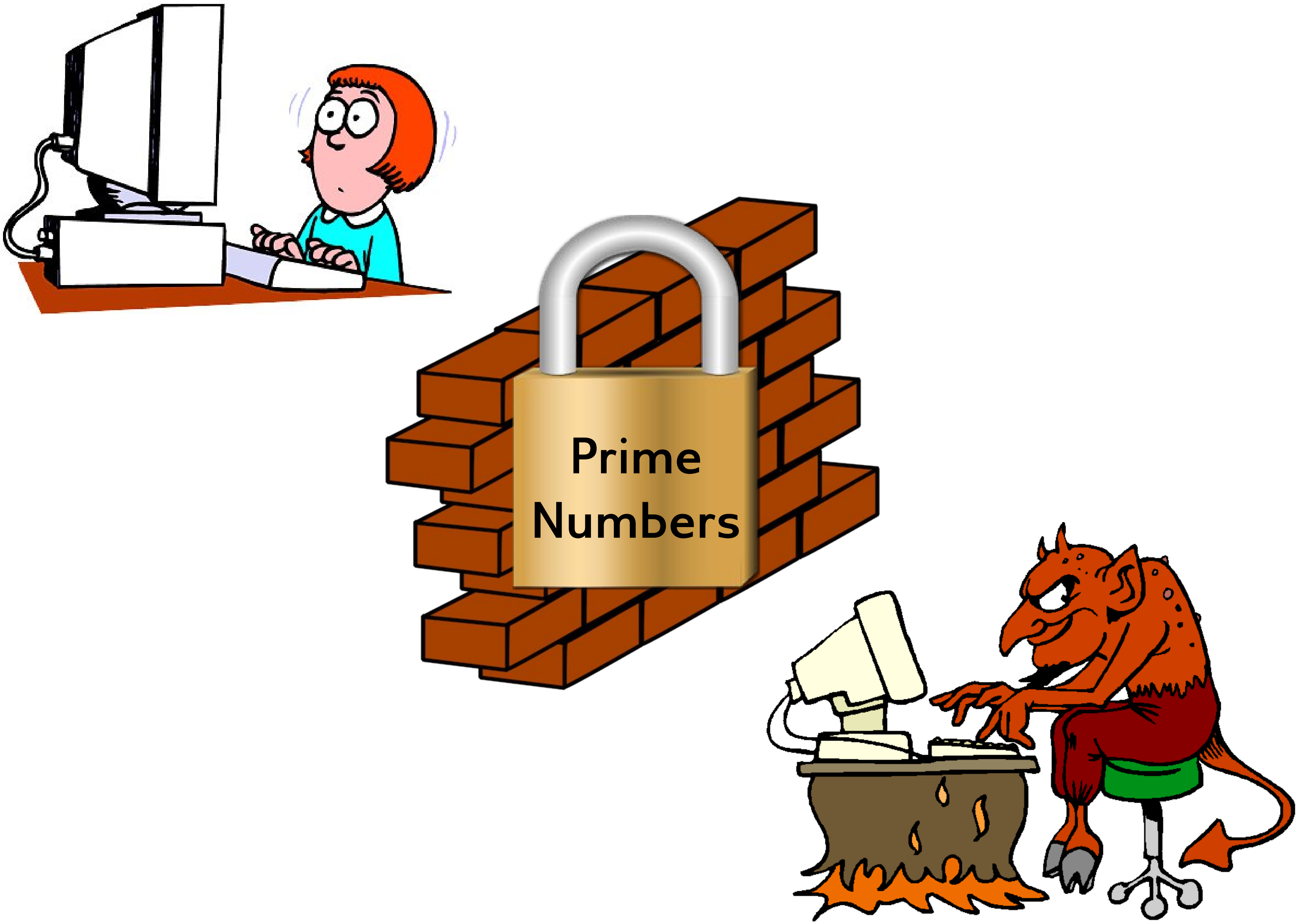
Things we can count with the integers



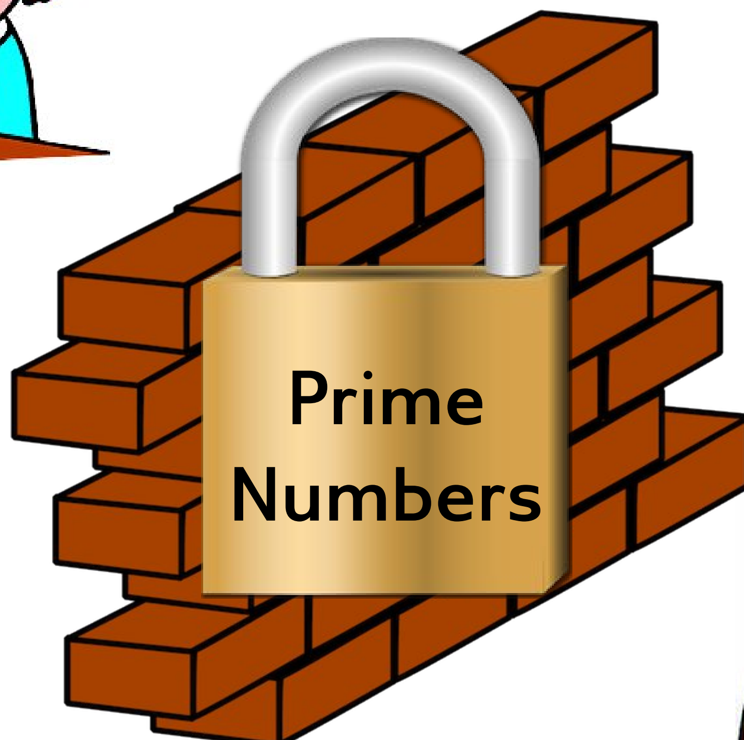
Prime Numbers

A number with exactly two divisors:
1 and **itself**

2, 3, 5, 7, 11, 13, 17...



eldhughes.com, pleasureinlearning.com



NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

How many prime numbers exist?

How many prime numbers exist?

1,000?

How many prime numbers exist?

1,000?

1,000,000?

How many prime numbers exist?

1,000?
1,000,000?
An infinite number?

How many prime numbers exist?

1,000?

1,000,000?

An infinite number

Euclid's Proof of Infinitude of Primes

(~300BC)

Euclid's Proof of Infinitude of Primes

- Suppose there is a finite number of primes

Euclid's Proof of Infinitude of Primes

- Suppose there is a finite number of primes
- Then there is a largest prime, p

Euclid's Proof of Infinitude of Primes

- Suppose there is a finite number of primes
- Then there is a largest prime, p
- Consider $n = (1 \times 2 \times 3 \times ... \times p) + 1$

Euclid's Proof of Infinitude of Primes

- Suppose there is a finite number of primes
- Then there is a largest prime, p
- Consider $n = (1 \times 2 \times 3 \times \ldots \times p) + 1$
- n cannot be prime (p is the largest)

Euclid's Proof of Infinitude of Primes

- Suppose there is a finite number of primes
- Then there is a largest prime, p
- Consider $n = (1 \times 2 \times 3 \times \ldots \times p) + 1$
- n cannot be prime (p is the largest)
- Therefore it has a (prime) divisor $< n$

Euclid's Proof of Infinitude of Primes

- Suppose there is a finite number of primes
- Then there is a largest prime, p
- Consider $n = (1 \times 2 \times 3 \times \ldots \times p) + 1$
- n cannot be prime (p is the largest)
- Therefore it has a (prime) divisor $< n$
- But no number from 2 to p divides n

Euclid's Proof of Infinitude of Primes

- Suppose there is a finite number of primes
- Then there is a largest prime, p
- Consider $n = (1 \times 2 \times 3 \times \ldots \times p) + 1$
- n cannot be prime (p is the largest)
- Therefore it has a (prime) divisor $< n$
- But no number from 2 to p divides n
- So n has a prime divisor greater than p

Euclid's Proof of Infinitude of Primes

- Suppose there is a finite number of primes
- Then there is a **largest prime, p**
- Consider $n = (1 \times 2 \times 3 \times \ldots \times p) + 1$
- n cannot be prime (p is the largest)
- Therefore it has a (prime) divisor $< n$
- But no number from 2 to p divides n
- So n has a **prime divisor greater than p**

Contradiction!!!

Discrete Structures

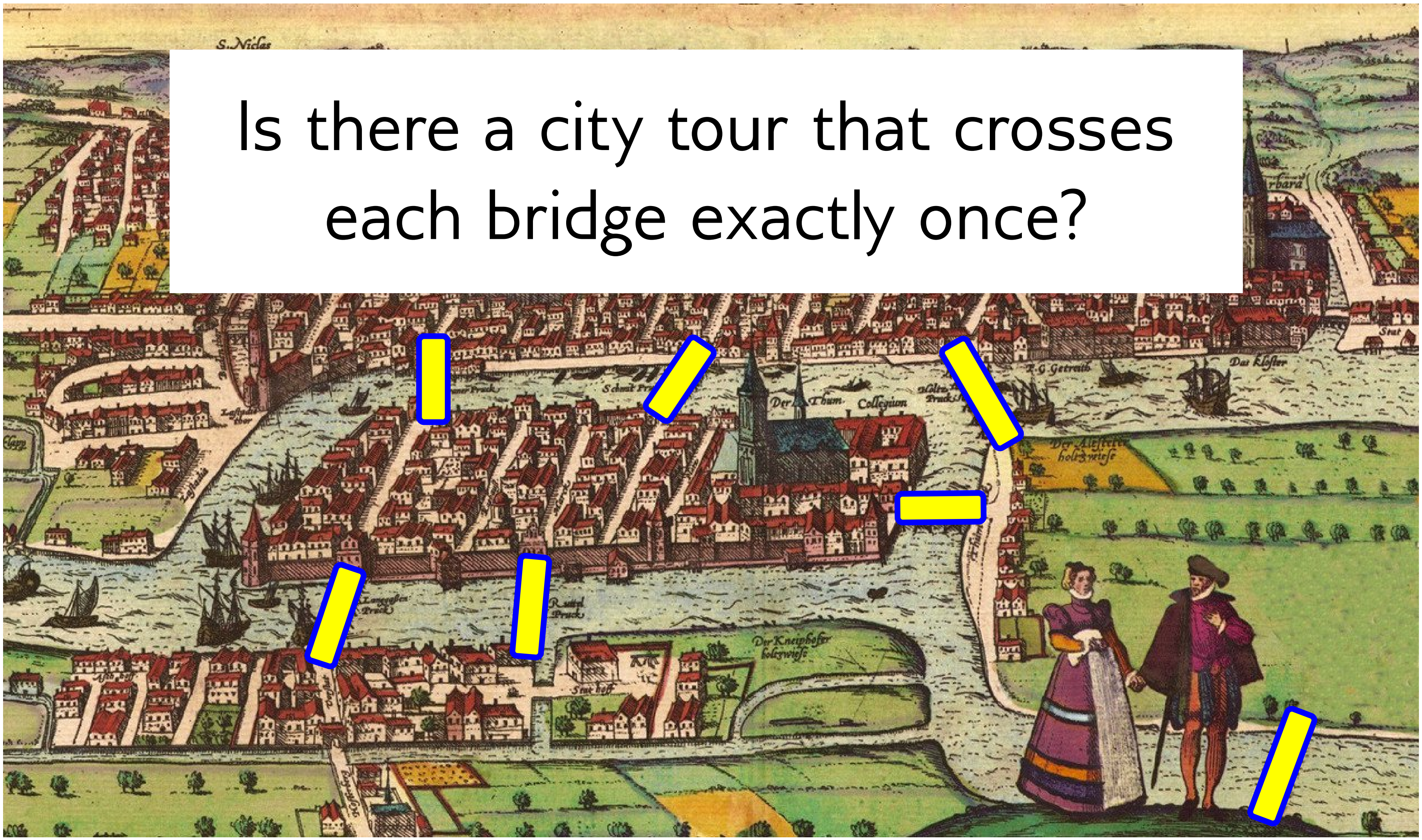
- Number theory
- Proof systems
- Sets, functions, relations
- Counting and probability

Bridges of Königsberg

Braun & Hogenberg, "Civitates Orbis Terrarum", Cologne 1585. Photoshopped to clean up right side and add 7th bridge.

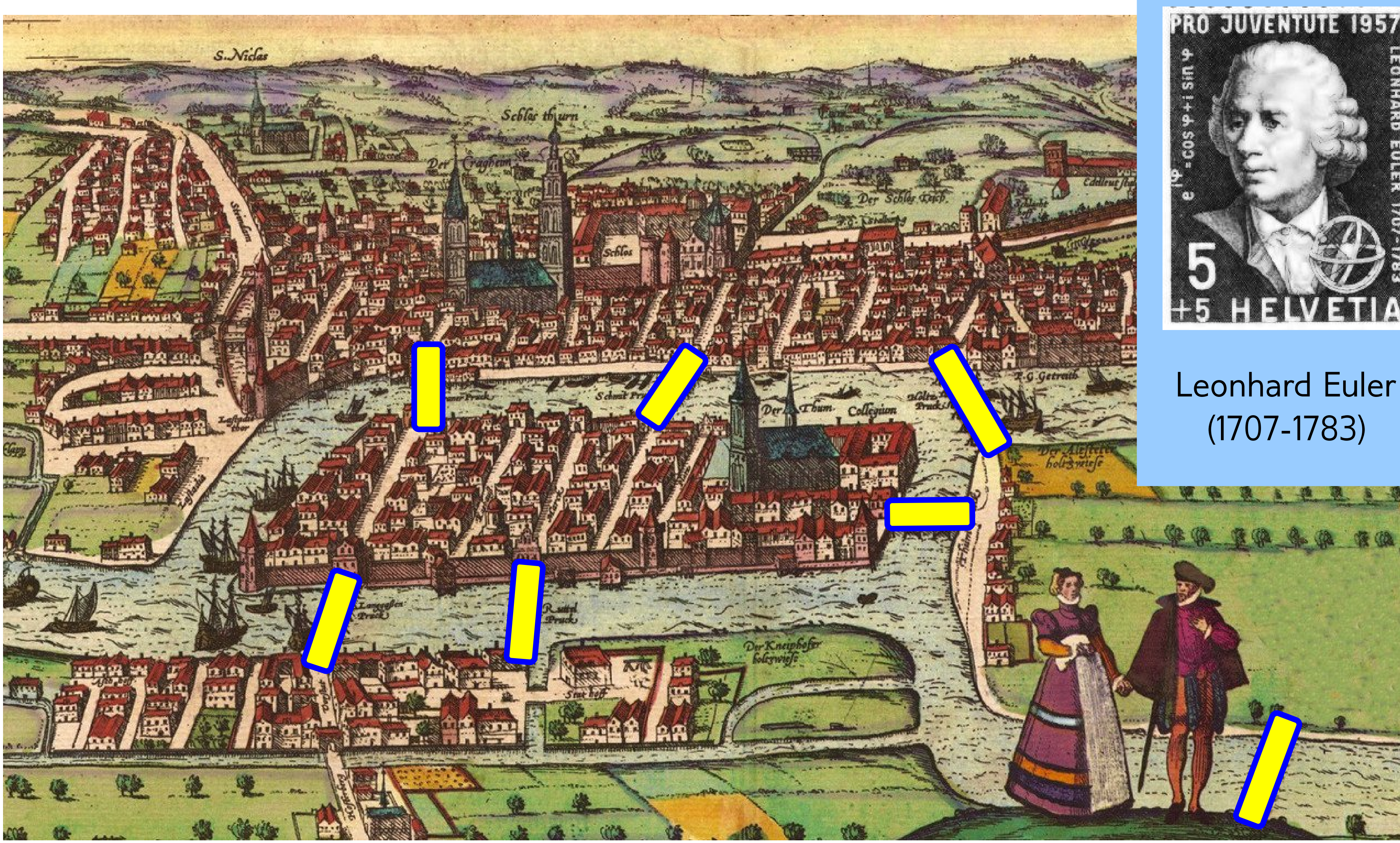
Bridges of Königsberg

Is there a city tour that crosses each bridge exactly once?



Braun & Hogenberg, “Civitates Orbis Terrarum”, Cologne 1585. Photoshopped to clean up right side and add 7th bridge.

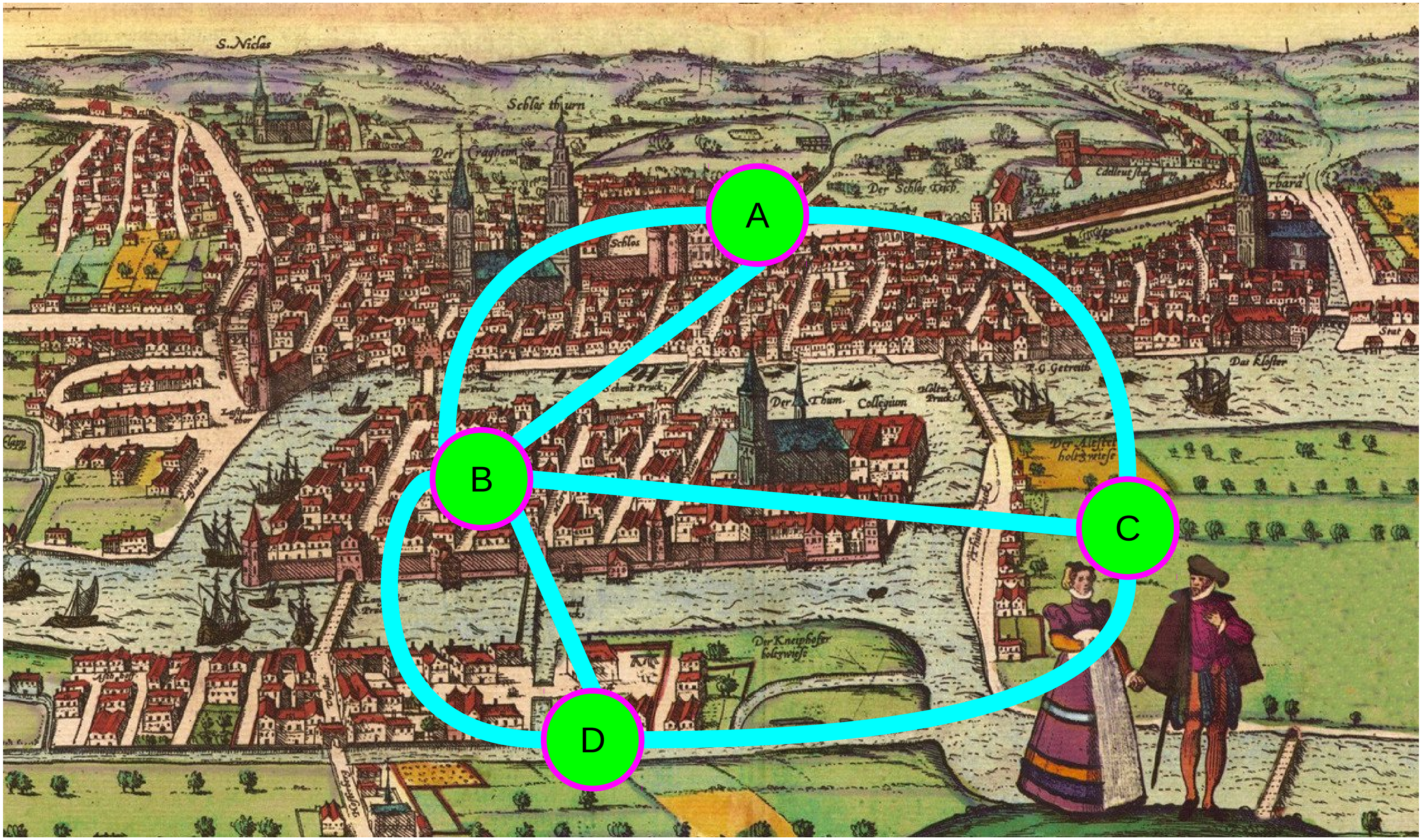
Bridges of Königsberg



Leonhard Euler
(1707-1783)

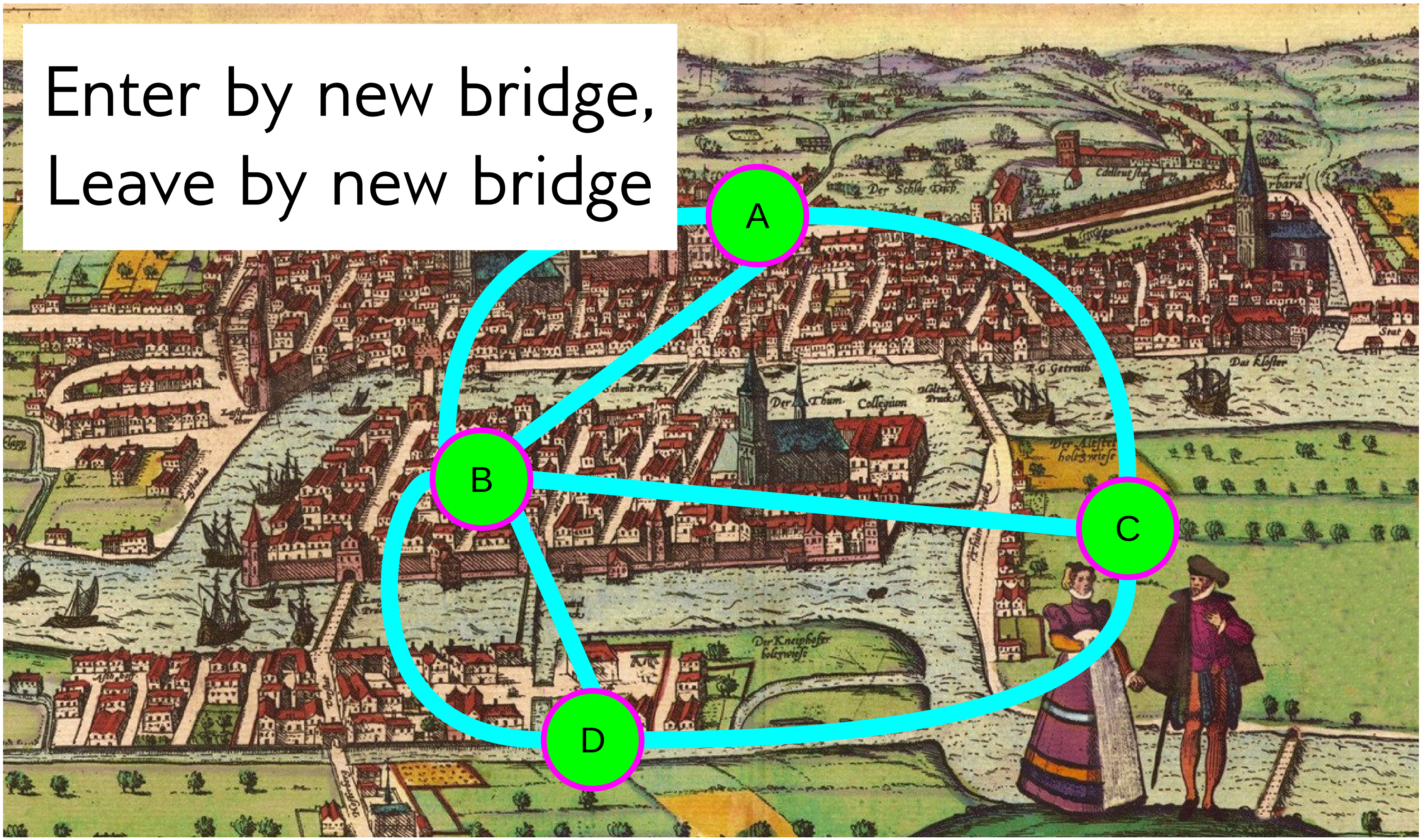
Braun & Hogenberg, "Civitates Orbis Terrarum", Cologne 1585. Photoshopped to clean up right side and add 7th bridge.

Bridges of Königsberg



Braun & Hogenberg, “Civitates Orbis Terrarum”, Cologne 1585. Photoshopped to clean up right side and add 7th bridge.

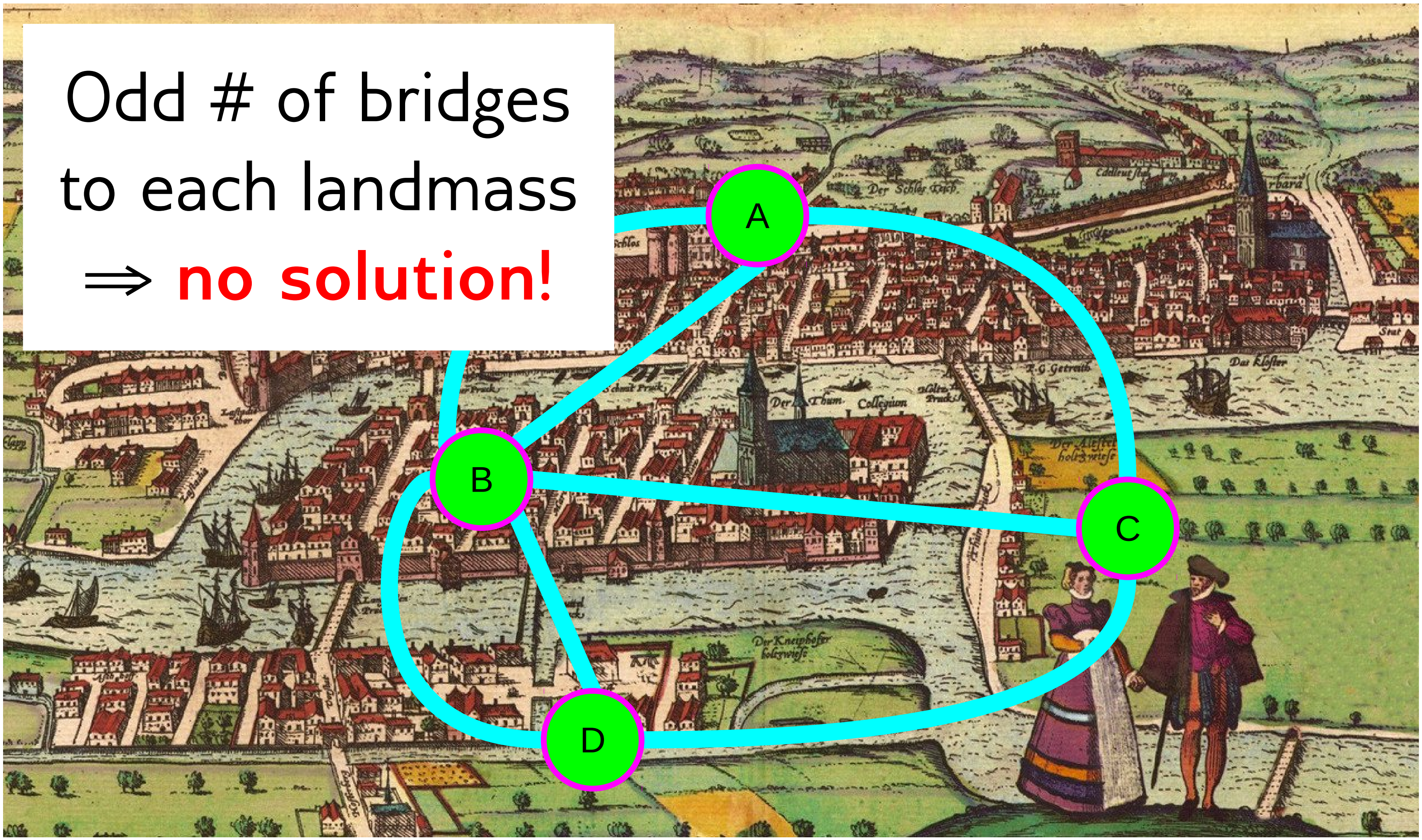
Bridges of Königsberg



Braun & Hogenberg, "Civitates Orbis Terrarum", Cologne 1585. Photoshopped to clean up right side and add 7th bridge.

Bridges of Königsberg

Odd # of bridges
to each landmass
$\Rightarrow$ **no solution!**

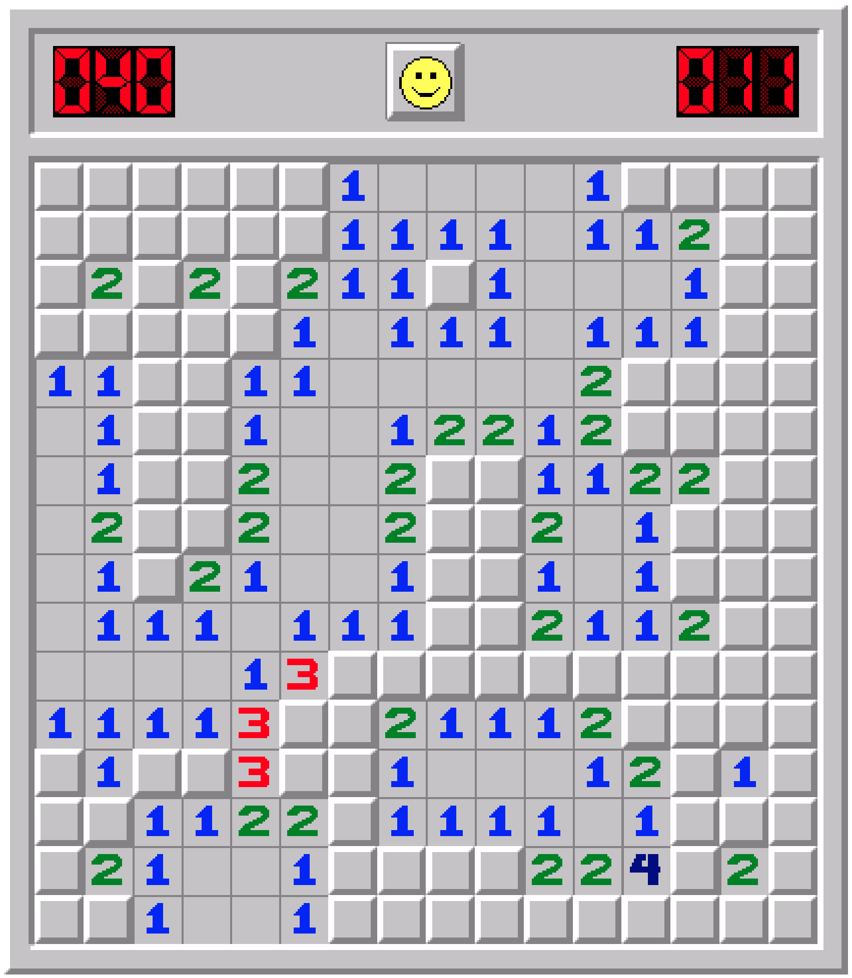


Braun & Hogenberg, “Civitates Orbis Terrarum”, Cologne 1585. Photoshopped to clean up right side and add 7th bridge.

Bridges of Königsberg

- Cross each bridge once: Euler Path
  - Easy for a computer to calculate
- Visit each landmass once: Hamiltonian Path
  - Probably very hard for a computer to calculate
  - If you can find an efficient solution, you will get $1M and undying fame (answers "P = NP?")
  - (Will also break modern crypto, collapse the banking system, revolutionize automated mathematics and science, bring about world peace…)

You'll also be terrific at Minesweeper



baslerweb.com

Discrete Structures

- Number theory
- Proof systems
- Sets, functions, relations
- Counting and probability
- Graph theory
- Models of computation, automata, complexity

This sentence is false.

This sentence is false.

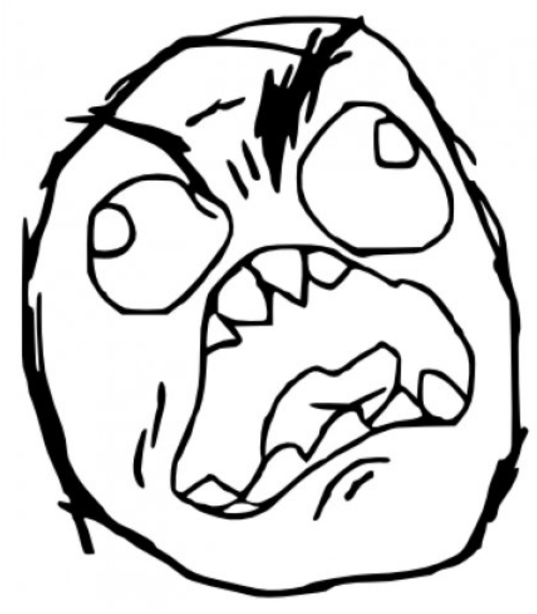
If true, it is false

If false, it is true

This sentence is false.

If true, it is false

If false, it is true



Discrete Structures

- Number theory
- Proof systems
- Sets, functions, relations
- Counting and probability
- Graph theory
- Models of computation, automata, complexity
- Logic
- Decidability, computability

warrenphotographic.co.uk, auntiedogmasgardenspot.wordpress.com

One running theme of the course:

- How to prove things
- How to write good proofs

That's what we'll be staring with.