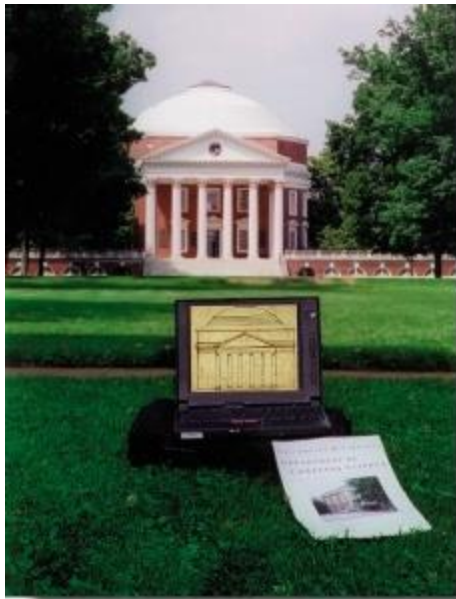


# Theory of Computation

## CS3102



Gabriel Robins

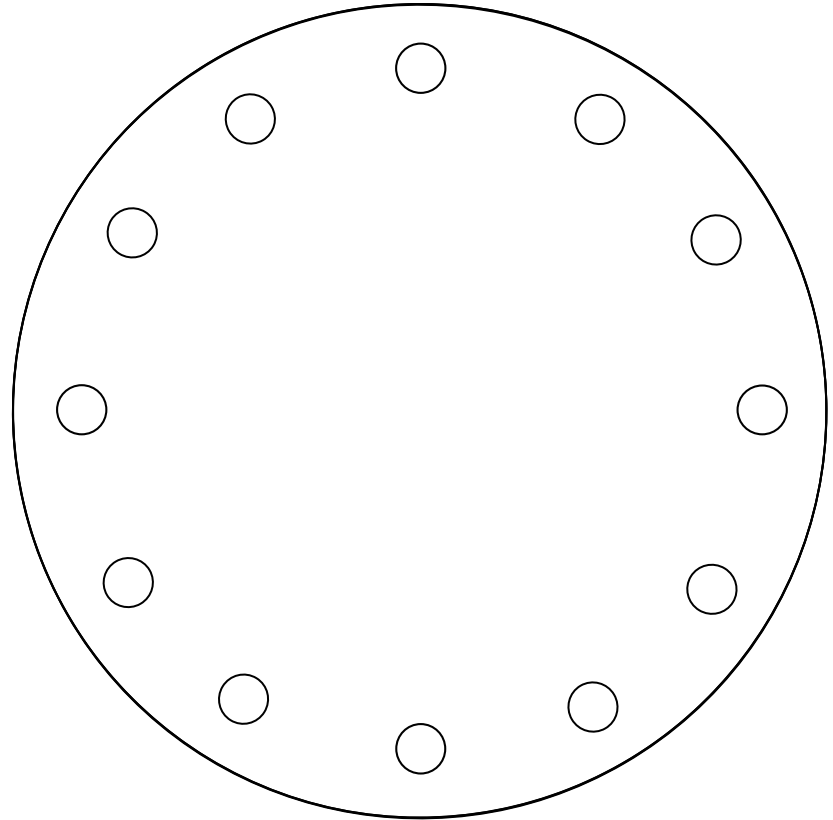
Department of  
Computer Science

University of Virginia

[www.cs.virginia.edu/robins/theory](http://www.cs.virginia.edu/robins/theory)



**Problem:** Can 5 test tubes be spun simultaneously in a 12-hole centrifuge in a balanced way?



- What approaches fail?
- What techniques work and why?
- Lessons and generalizations

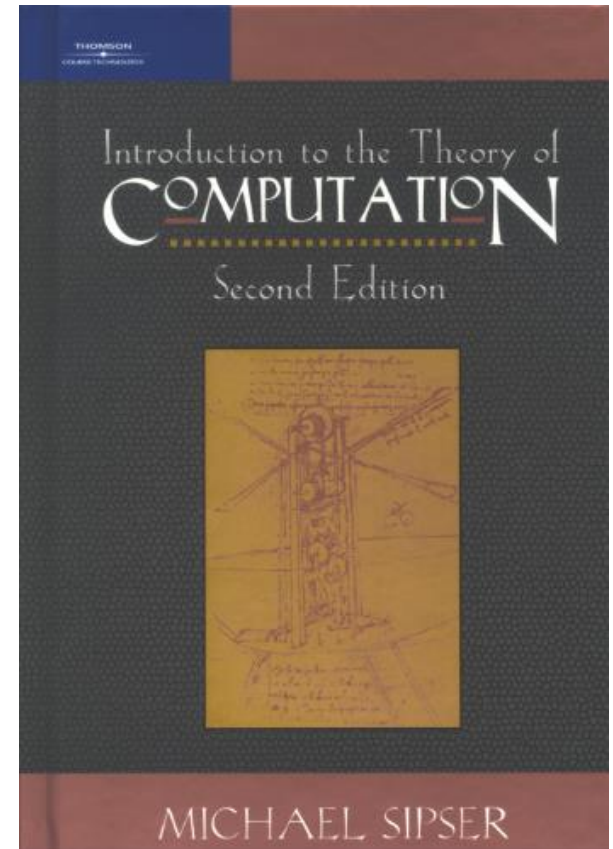
# Theory of Computation (CS3102) - Textbook

Textbook:

Introduction to the Theory of  
Computation, by Michael Sipser  
(MIT), 2<sup>nd</sup> Edition, 2005

Good Articles / videos:

[www.cs.virginia.edu/~robins/CS\\_readings.html](http://www.cs.virginia.edu/~robins/CS_readings.html)

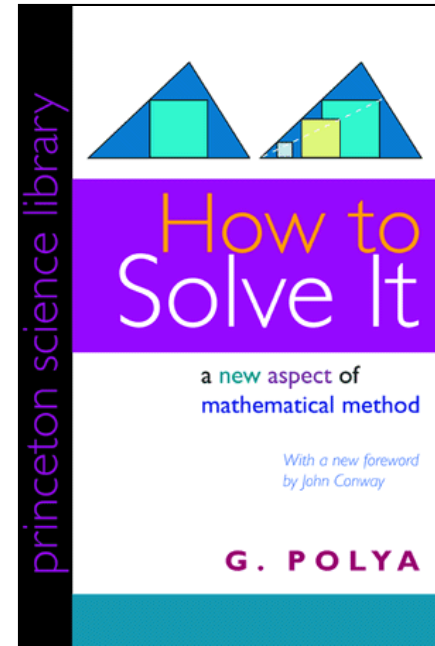


# Theory of Computation (CS3102)

Required reading:

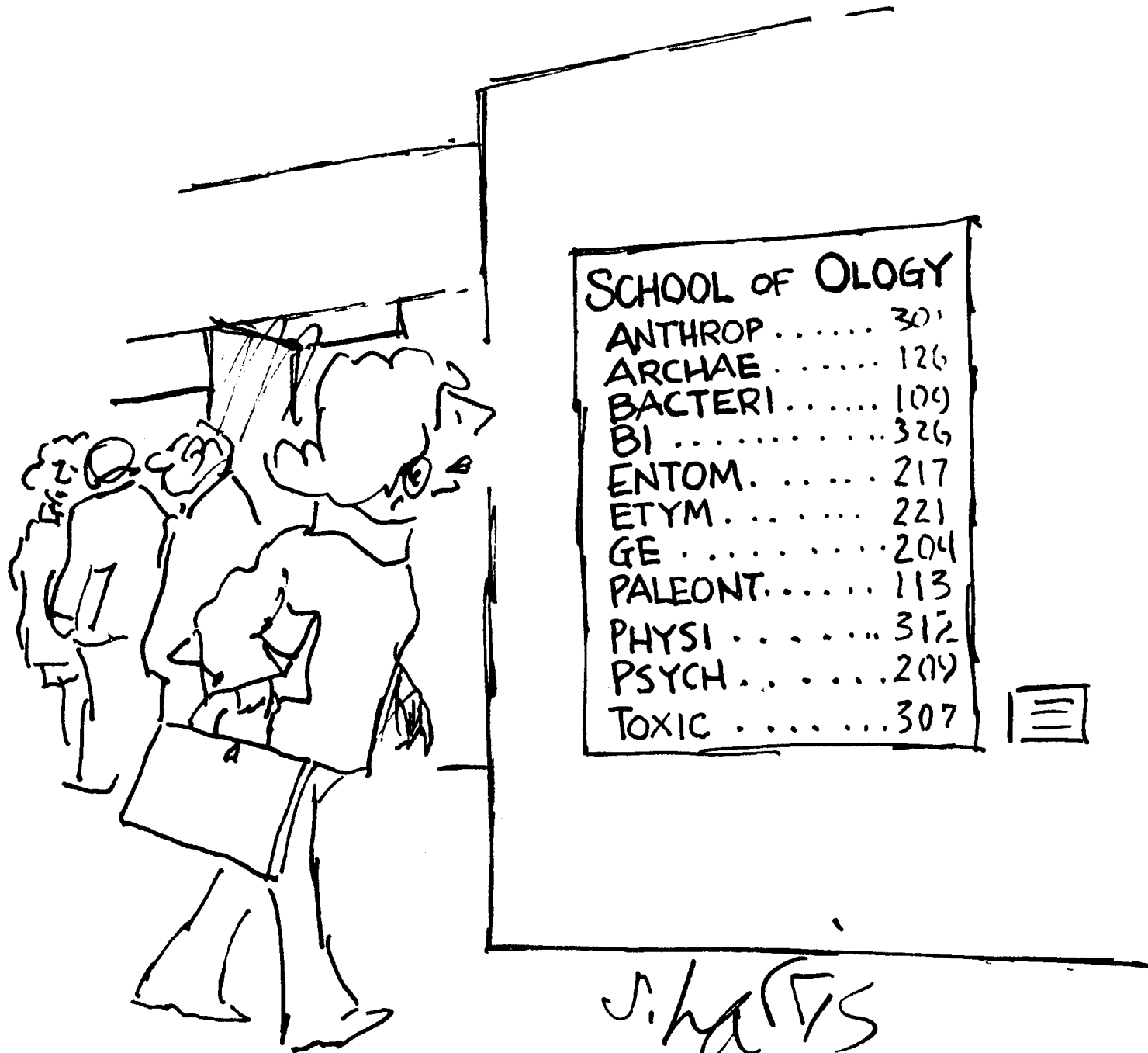
**How to Solve It**, by George Polya  
(MIT), Princeton University Press, 1945

- A classic on **problem solving**



George Polya (1887-1985)

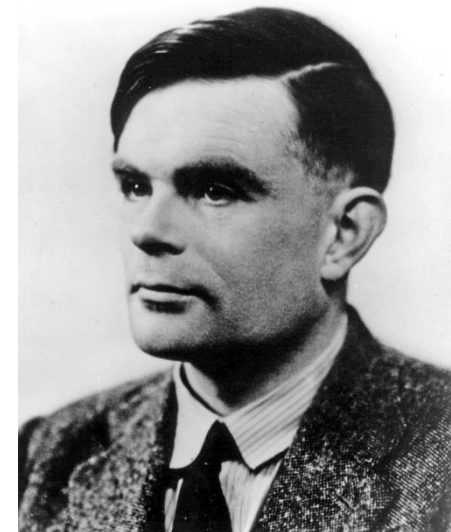
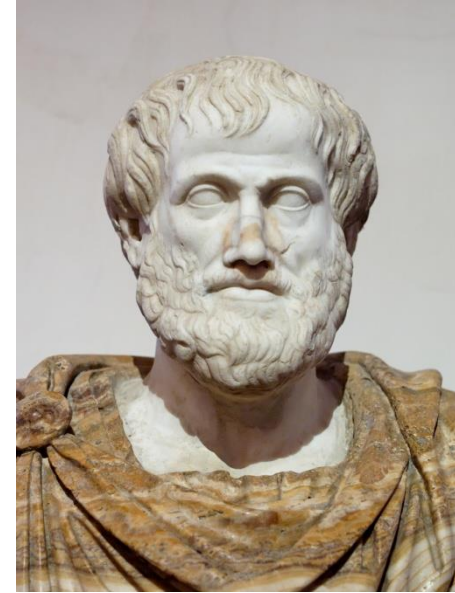




# Theory of Computation (CS3102) - Syllabus

## A brief history of computing:

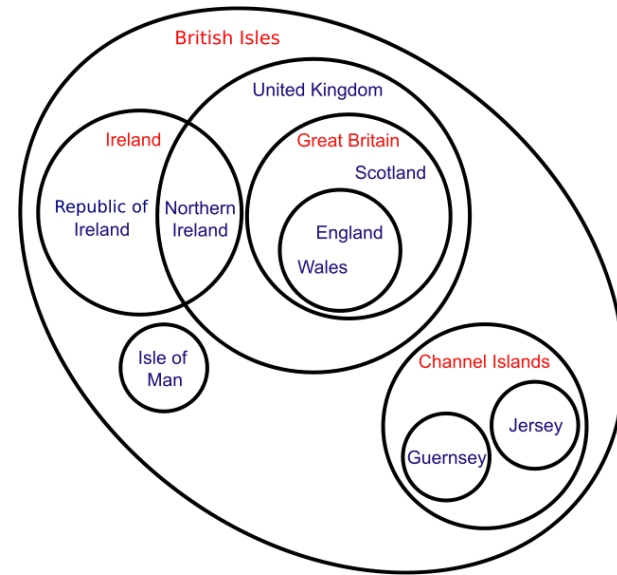
- Aristotle, **Euclid**, Archimedes, Eratosthenes
- Abu Ali al-Hasan ibn al-Haytham
- Fibonacci, Descartes, Fermat, Pascal
- Newton, Euler, Gauss, Hamilton
- **Boole**, **De Morgan**, **Babbage**, Ada Augusta
- Venn, Carroll, **Cantor**, **Hilbert**, **Russell**
- Hardy, Ramanujan, Ramsey
- Godel, **Church**, **Turing**, **von Neumann**
- Shannon, **Kleene**, **Chomsky**



# Theory of Computation Syllabus (continued)

## Fundamentals:

- Set theory
- Predicate logic
- Formalisms and notation
- Infinities and countability
- Dovetailing / diagonalization
- Proof techniques
- Problem solving
- Asymptotic growth
- Review of graph theory

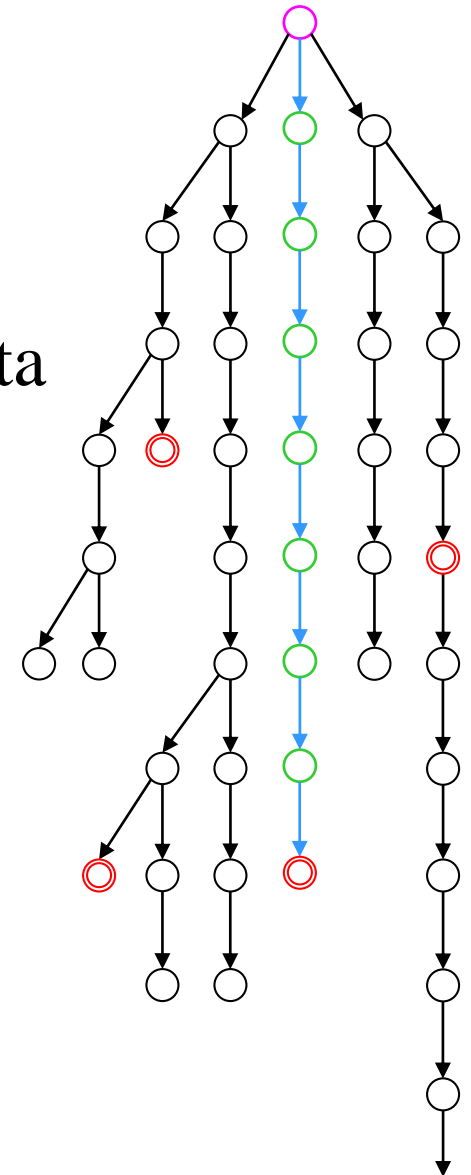


7	$\frac{7}{1}$	$\frac{7}{2}$	$\frac{7}{3}$	$\frac{7}{4}$	$\frac{7}{5}$	$\frac{7}{6}$	$\frac{7}{7}$	$\frac{7}{8}$	...
6	$\frac{6}{1}$	$\frac{6}{2}$	$\frac{6}{3}$	$\frac{6}{4}$	$\frac{6}{5}$	$\frac{6}{6}$	$\frac{6}{7}$	$\frac{6}{8}$	...
5	$\frac{5}{1}$	$\frac{5}{2}$	$\frac{5}{3}$	$\frac{5}{4}$	$\frac{5}{5}$	$\frac{5}{6}$	$\frac{5}{7}$	$\frac{5}{8}$	...
4	$\frac{4}{1}$	$\frac{4}{2}$	$\frac{4}{3}$	$\frac{4}{4}$	$\frac{4}{5}$	$\frac{4}{6}$	$\frac{4}{7}$	$\frac{4}{8}$	...
3	$\frac{3}{1}$	$\frac{3}{2}$	$\frac{3}{3}$	$\frac{3}{4}$	$\frac{3}{5}$	$\frac{3}{6}$	$\frac{3}{7}$	$\frac{3}{8}$	...
2	$\frac{2}{1}$	$\frac{2}{2}$	$\frac{2}{3}$	$\frac{2}{4}$	$\frac{2}{5}$	$\frac{2}{6}$	$\frac{2}{7}$	$\frac{2}{8}$	...
1	$\frac{1}{1}$	$\frac{1}{2}$	$\frac{1}{3}$	$\frac{1}{4}$	$\frac{1}{5}$	$\frac{1}{6}$	$\frac{1}{7}$	$\frac{1}{8}$	...
	1	2	3	4	5	6	7	8	...

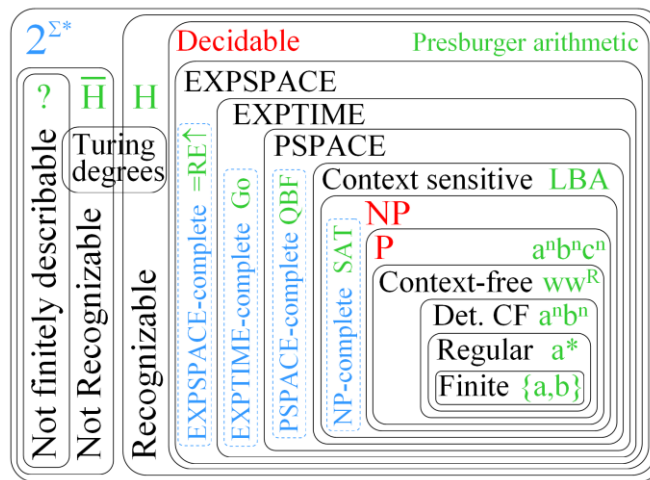
# Theory of Computation Syllabus (continued)

## Formal languages and machine models:

- The Chomsky hierarchy
- Regular languages / finite automata
- Context-free grammars / pushdown automata
- Unrestricted grammars / Turing machines
- Non-determinism
- Closure operators
- Pumping lemmas
- Non-closures
- Decidable properties



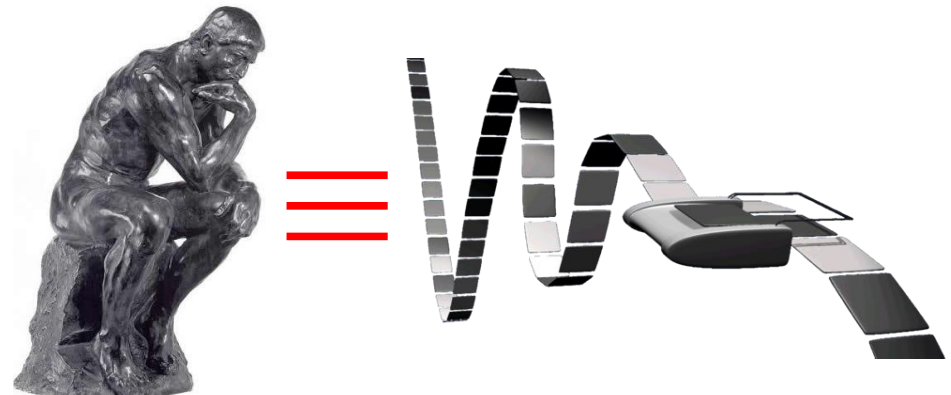
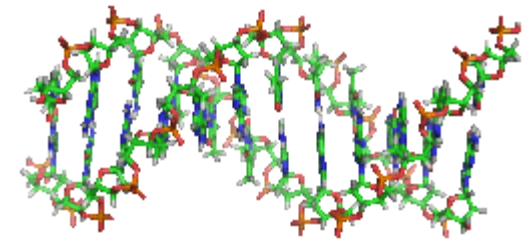
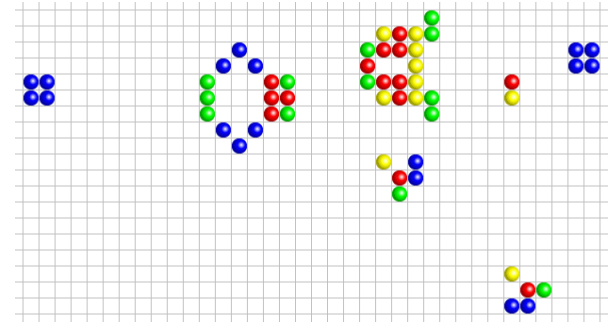
The Extended Chomsky Hierarchy



# Theory of Computation Syllabus (continued)

## Computability and undecidability:

- Basic models
- Modifications and extensions
- Computational universality
- Decidability
- Recognizability
- Undecidability
- Church-Turing thesis
- Rice's theorem

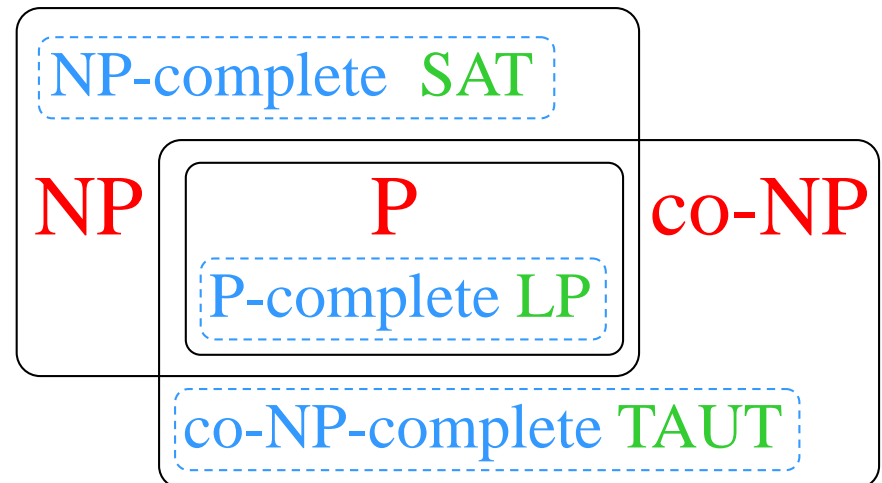




# Theory of Computation Syllabus (continued)

## NP-completeness:

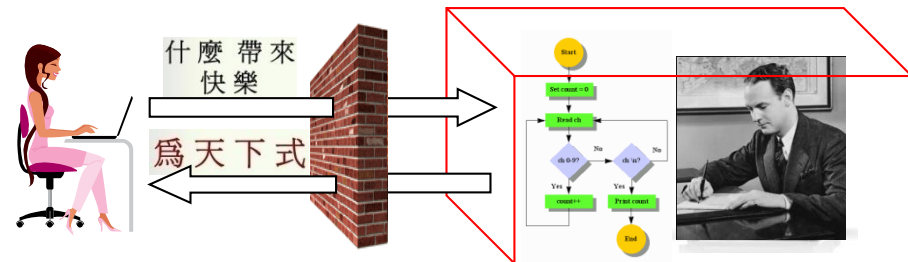
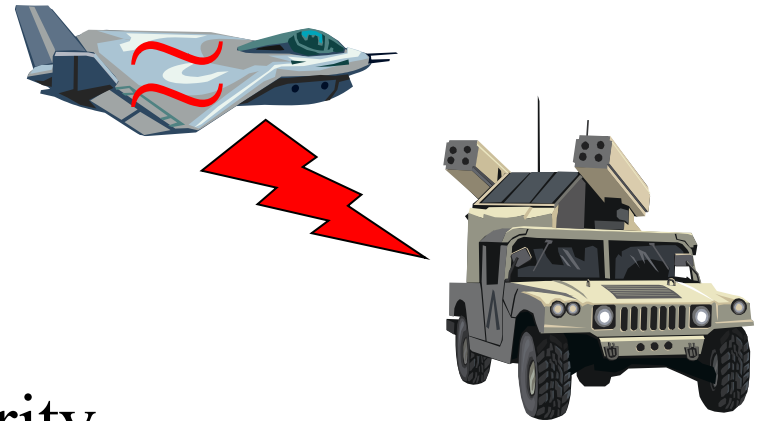
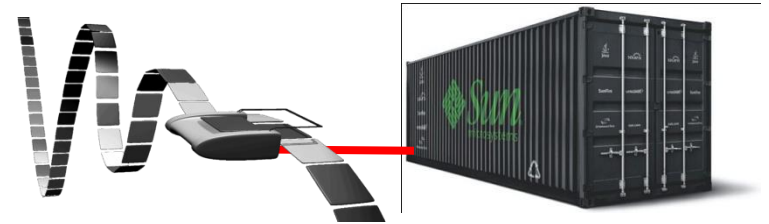
- Resource-constrained computation
- Complexity classes
- Intractability
- Boolean satisfiability
- Cook-Levin theorem
- Transformations
- Graph clique problem
- Independent sets
- Hamiltonian cycles
- Colorability problems
- Heuristics



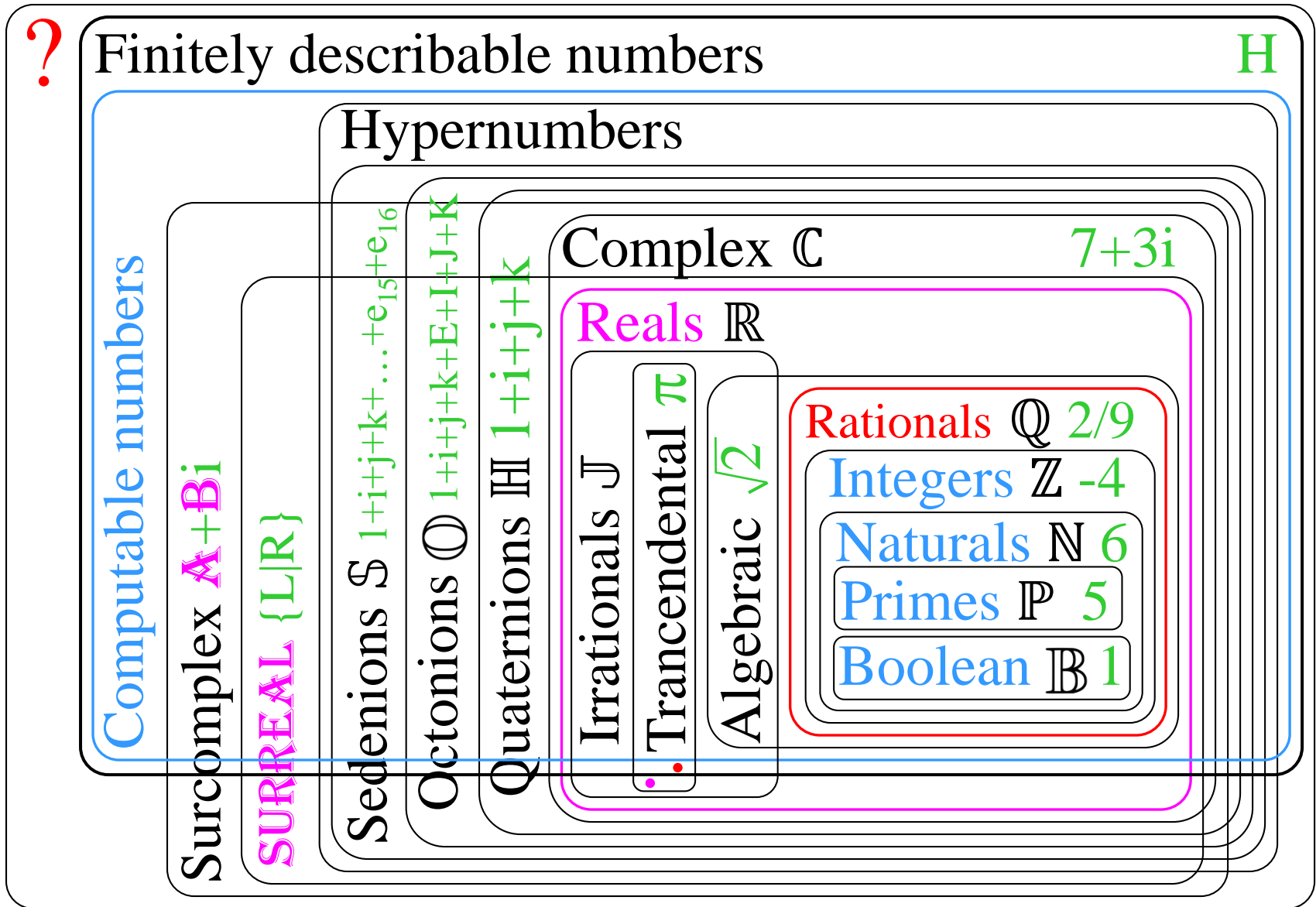
# Theory of Computation Syllabus (continued)

## Other topics (as time permits):

- Generalized number systems
- Oracles and relativization
- Zero-knowledge proofs
- Cryptography & mental poker
- The Busy Beaver problem
- Randomness and compressibility
- The Turing test
- AI and the Technological Singularity



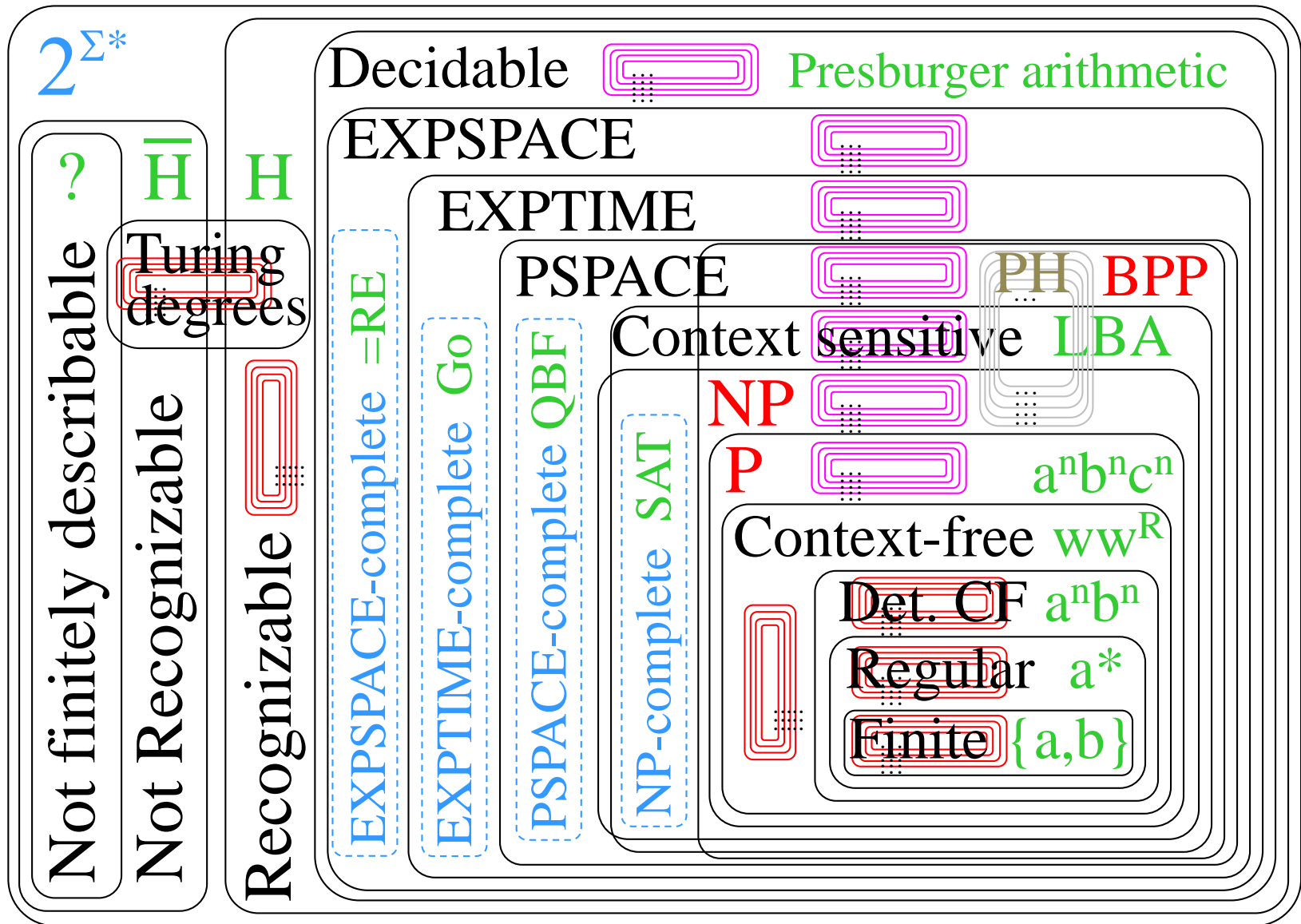
# Generalized Numbers



Theorem: some real numbers are not finitely describable!

Theorem: some finitely describable real numbers are not computable!

# The Extended Chomsky Hierarchy

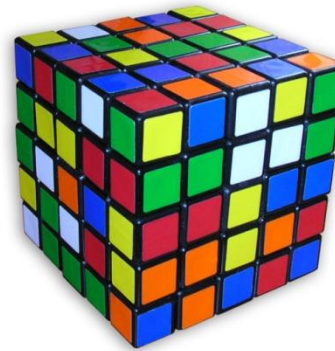


Dense infinite time & space complexity hierarchies 

Other infinite complexity & descriptive hierarchies 

# Overarching Philosophy

- Focus on the “big picture” & “scientific method”
- Emphasis on **problem solving** & creativity
- Discuss applications & practice
- A primary objective: have **fun!**





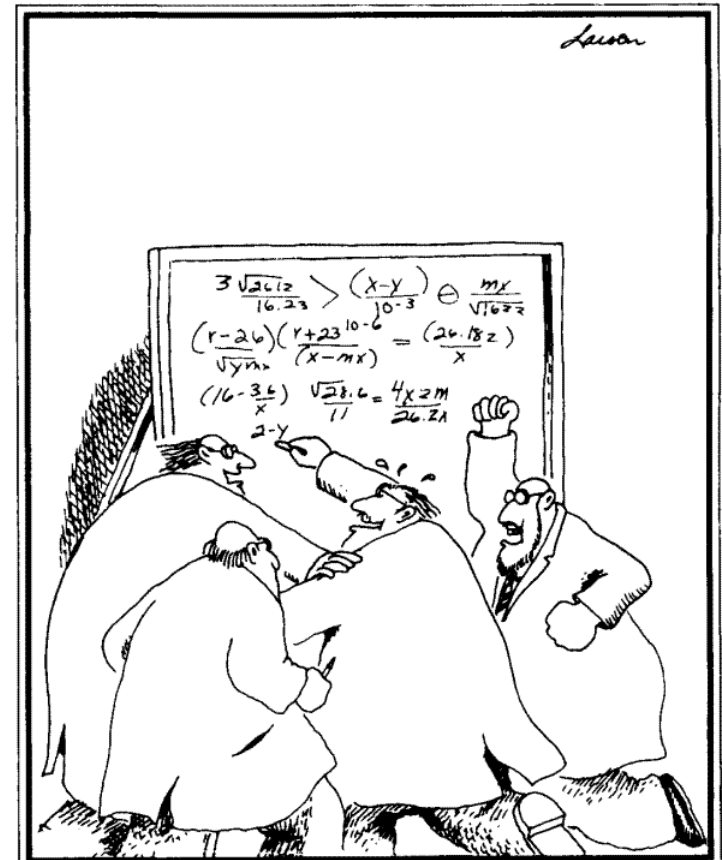
# Prerequisites

- Some **discrete math & algorithms** knowledge
- Ideally, should have taken CS2102
- Course will “**bootstrap**” (albeit quickly) from **first principles**
- Critical: **Tenacity**, **patience**



# Course Organization

- **Exams:** probably take home
  - Decide by vote
  - Flexible exam schedule
- **Problem sets:**
  - Lots of problem solving
  - **Work in groups!**
  - Not formally graded
  - **Most exam questions will come from these sets!**
- **Readings:** papers / books / videos
- **Extra credit** problems
  - In class & take-home
  - Find mistakes in slides, handouts, etc.
- Course materials posted on Web site  
[www.cs.virginia.edu/robins/theory](http://www.cs.virginia.edu/robins/theory)



"Go for it, Sidney! You've got it! You've got it! Good hands! Don't choke!"

# Contact Information

Professor Gabriel Robins

Office: 409 Rice Hall

Phone: (434) 982-2207

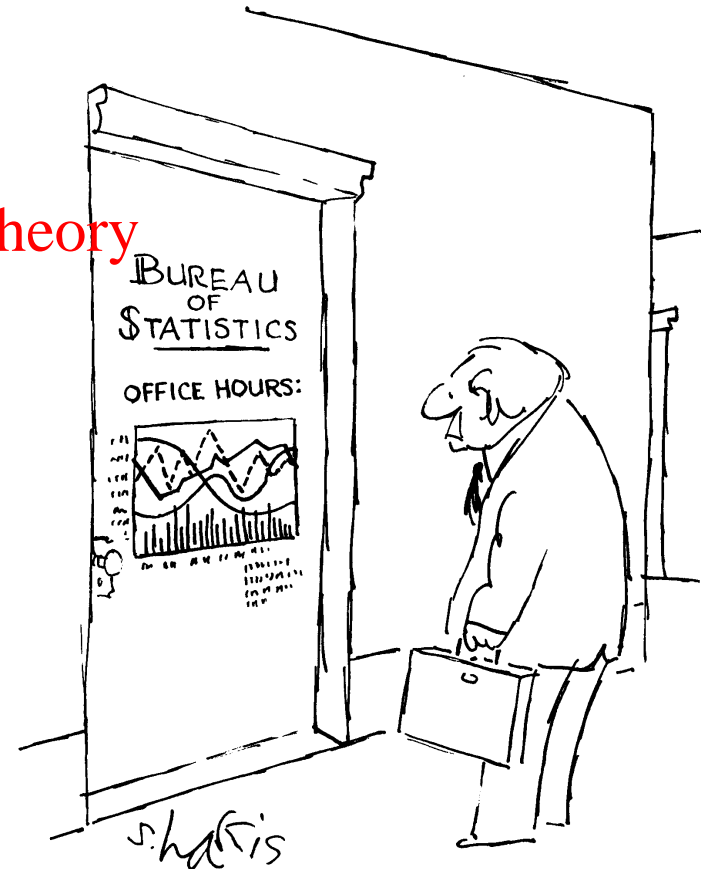
Email: [robins@cs.virginia.edu](mailto:robins@cs.virginia.edu)

Web: [www.cs.virginia.edu/robins](http://www.cs.virginia.edu/robins)

[www.cs.virginia.edu/robins/theory](http://www.cs.virginia.edu/robins/theory)

Office hours: after class

- Any other time
- [By email](#) (preferred)
- By appointment
- Q&A blog posted on class Web site



# Grading Scheme

- Midterm 35%
- Final 35%
- Readings 30%
- Extra credit 10%

Best strategy:

- Solve lots of problems!
- Do lots of readings / EC!



"Mr. Osborne, may I be excused? My brain is full."

# Course Readings

[www.cs.virginia.edu/robins/CS\\_readings.html](http://www.cs.virginia.edu/robins/CS_readings.html)

**Goal:** broad exposure to lots of cool ideas & technologies!

- **Required:** total of at least 50 items over the semester
- **Diversity:** minimums in each of 3 categories:
  1. Minimum of 20 videos
  2. Minimum of 20 papers / Web sites
  3. Minimum of 10 books
- More than 50 is even better! (extra credit)
- Some required items in each category
  - Remaining “elective” items should be a diverse mix
- Email all submissions to: [homework.cs3102@gmail.com](mailto:homework.cs3102@gmail.com)



# Required Readings

[www.cs.virginia.edu/robins/CS\\_readings.html](http://www.cs.virginia.edu/robins/CS_readings.html)

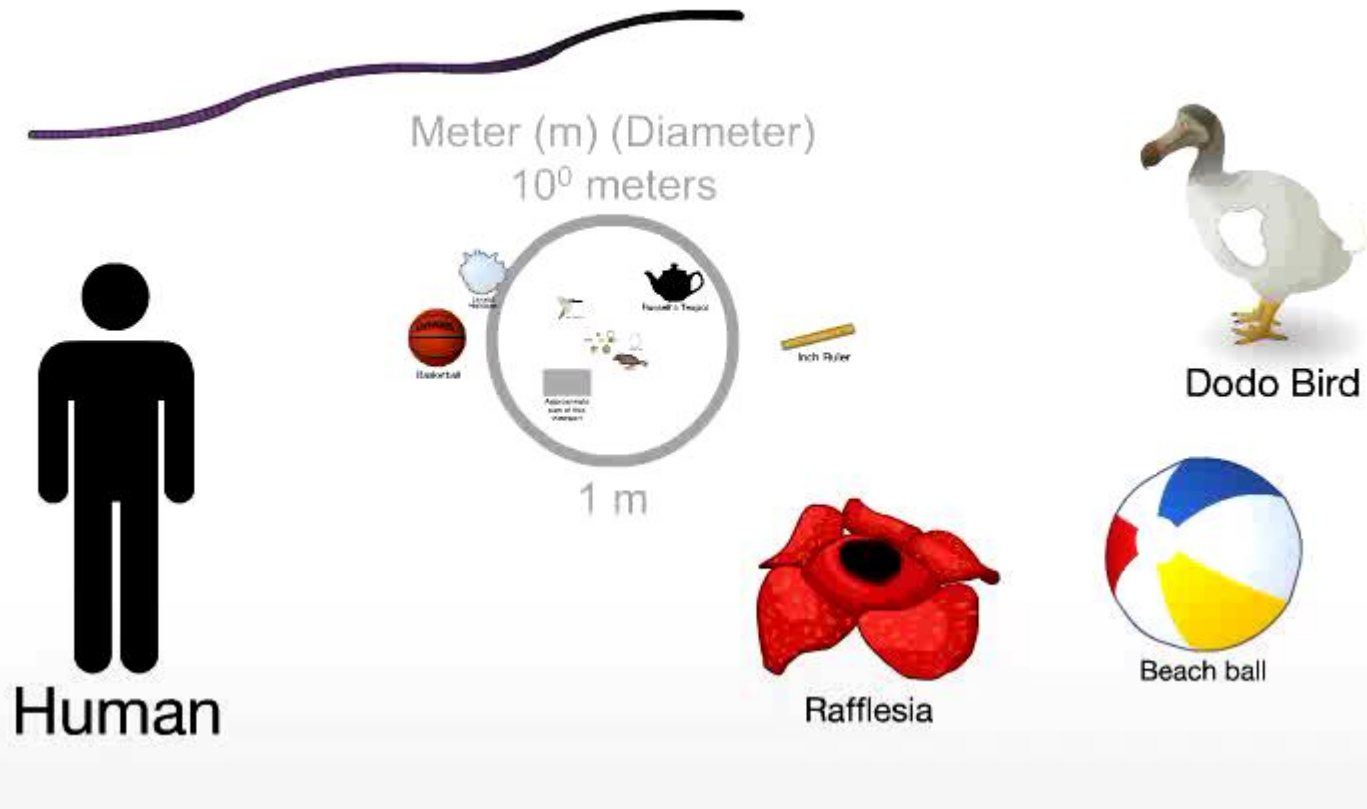
- **Required** videos:
  - Last Lecture, Randy Pausch, 2007
  - Time Management, Randy Pausch, 2007
  - Powers of Ten, Charles and Ray Eames, 1977



# Required Reading

- “[Scale of the Universe](#)”, Cary and Michael Huang, 2012

## Giant Earthworm



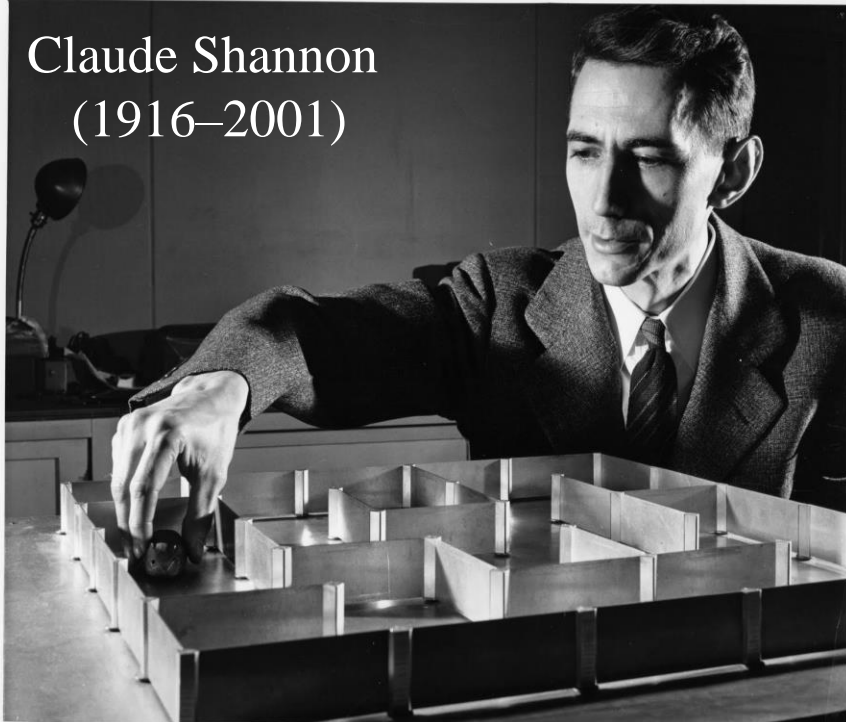
- $10^{-24}$  to  $10^{26}$  meters  $\Rightarrow$  50 orders of magnitude!

# Required Readings

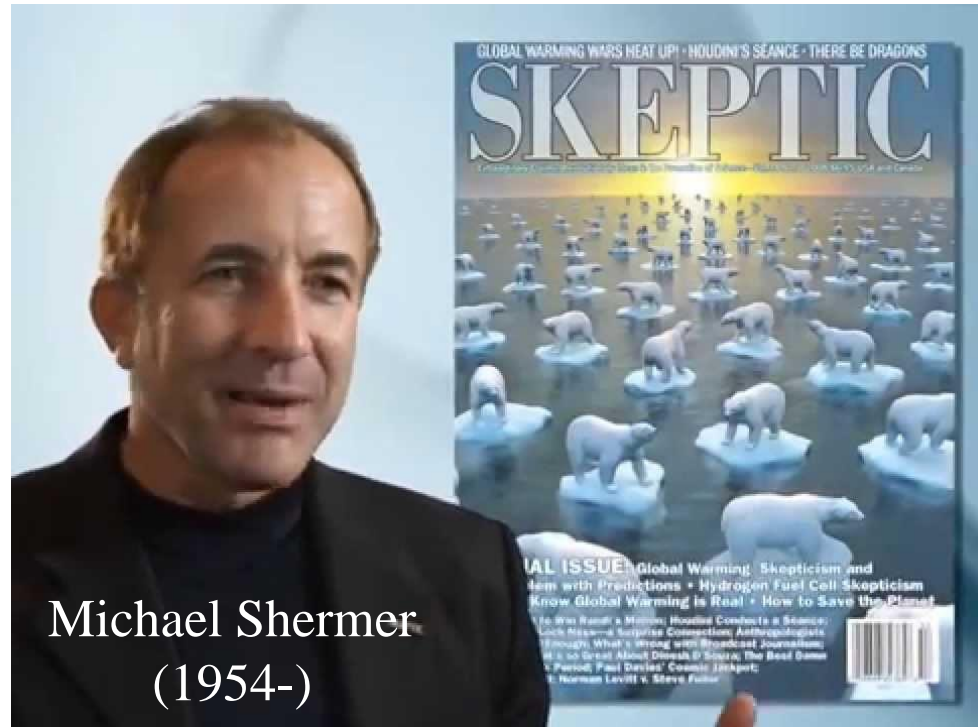
[www.cs.virginia.edu/robins/CS\\_readings.html](http://www.cs.virginia.edu/robins/CS_readings.html)

- More **required** videos:
  - Claude Shannon - Father of the Information Age, UCTV
  - [The Pattern Behind Self-Deception](#), Michael Shermer, 2010

Claude Shannon  
(1916–2001)



Michael Shermer  
(1954-)

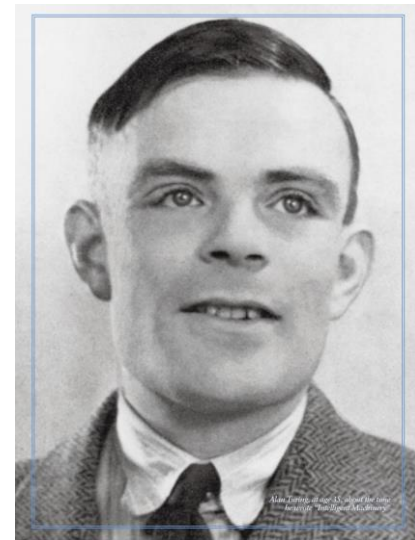
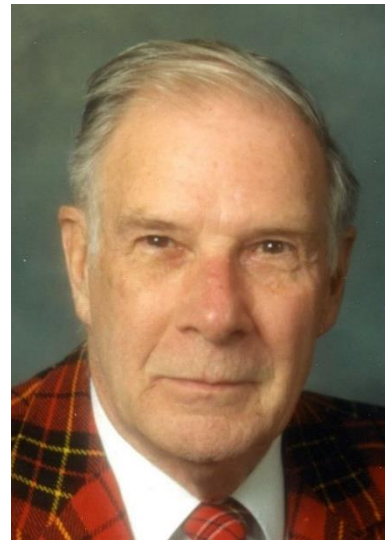




# Required Readings

[www.cs.virginia.edu/robins/CS\\_readings.html](http://www.cs.virginia.edu/robins/CS_readings.html)

- **Required** articles:
  - Decoding an Ancient Computer, Freeth, 2009
  - **Who Can Name the Bigger Number**, Scott Aaronson, 1999
  - You and Your Research, Richard Hamming, 1986
  - Alan Turing's Forgotten Ideas, Copeland and Proudfoot, 1999









# Basic Concepts and Notation

Gabriel Robins

*"When I use a word," Humpty Dumpty said, in a rather scornful tone, "it means just what I choose it to mean -- neither more nor less."*

Required reading

A **set** is formally an undefined term, but intuitively it is a (possibly empty) collection of arbitrary objects. A set is usually denoted by curly braces and some (optional) restrictions. Examples of sets are  $\{1,2,3\}$ ,  $\{\text{hi, there}\}$ , and  $\{k \mid k \text{ is a perfect square}\}$ . The symbol  $\in$  denotes set **membership**, while the symbol  $\notin$  denotes set **non-membership**; for example,  $7 \in \{p \mid p \text{ prime}\}$  states that 7 is a prime number, while  $q \notin \{0,2,4,6,\dots\}$  states that  $q$  is not an even number.

Some **common sets** are denoted by special notation:

The **natural numbers**:

$$\mathbb{N} = \{1,2,3,\dots\}$$

The **integers**:

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

The **rational numbers**:

$$\mathbb{Q} = \left\{ \frac{a}{b} \mid a,b \in \mathbb{Z}, b \neq 0 \right\}$$

The **real numbers**:

$$\mathbb{R} = \{x \mid x \text{ is a real number}\}$$

The **empty set**:

$$\emptyset = \{\}$$

# JOHANNES KEPLER'S UPHILL BATTLE

...SO, YOU SEE, THE ORBIT OF A PLANET IS ELLIPTICAL.

WHAT'S AN ORBIT?

WHAT'S A PLANET?

WHAT'S 'ELLIPTICAL'?



J. HARRIS

# Discrete Math Review Slides

## Symbolic Logic

Def: *proposition* - statement either true (T) or false (F)

Ex:  $1 + 1 = 2$

$2 + 2 = 3$

$3 < 7$

$x + 4 = 5$

"today is Monday"

## Boolean Functions

- "and"  $\wedge$
- "or"  $\vee$
- "not"  $\neg$
- "xor"  $\oplus$
- "nand"  $\bar{\wedge}$
- "nor"  $\bar{\vee}$
- "implication"  $\Rightarrow$
- "equivalence"  $\Leftrightarrow$

## Logical Implication

"implies"  $\Rightarrow$   
Truth table:

p	q	$p \Rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

Ex:  $(x < 0) \wedge (x > 0) \Rightarrow (x = 0)$   
 $1 < x < y \Rightarrow x^3 < y^3$   
"today is Sunday"  $\Rightarrow 1 + 1 = 3$

## Logical Equivalence

- "biconditional"  $\Leftrightarrow$
- or "if and only if" ("iff")
- or "necessary and sufficient"
- or "logically equivalent" =

Truth table:

p	q	$p \Leftrightarrow q$
T	T	T
T	F	F
F	T	F
F	F	T

Ex:  $p \Leftrightarrow q$   
 $[(x=0) \vee (y=0)] \Leftrightarrow (xy=0)$   
 $\min(x,y) = \max(x,y) \Leftrightarrow x=y$

## Predicates

Def: *predicate* - a function or formula involving some variables

Ex: let  $P(x) = "x > 3"$   
 $x$  is the variable  
" $x > 3$ " is the predicate

$P(5)$

$P(1)$

Ex:  $Q(x,y,z) = "x^2 + y^2 = z^2"$

$Q(2,3,4)$

$Q(3,4,5)$

## Quantifiers

- Universal: "for all"  $\forall$   
 $\forall x P(x)$   
 $\Leftrightarrow P(x_1) \wedge P(x_2) \wedge P(x_3) \wedge \dots$   
Ex:  $\forall x \ x < x + 1$   
 $\forall x \ x < x^2$
- Existential: "there exists"  $\exists$   
 $\exists x P(x)$   
 $\Leftrightarrow P(x_1) \vee P(x_2) \vee P(x_3) \vee \dots$   
Ex:  $\exists x \ x = x^2$   
 $\exists x \ x < x - 1$
- Combinations:  
 $\forall x \exists y \ y > x$

## Sets

Def: *set* - an unordered collection of elements

Ex:  $\{1, 2, 3\}$  or  $\{x \mid x \text{ is here}\}$

Venn Diagram:



Def: two sets are *equal* iff they contain the same elements

Ex:  $\{1, 2, 3\} = \{2, 3, 1\}$

$\{0\} \neq \{1\}$

$\{3, 5\} = \{3, 5, 3, 3, 5\}$

## Common Sets

Naturals:  $\mathbb{N} = \{1, 2, 3, 4, \dots\}$

Integers:  $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$

Rationals:  $\mathbb{Q} = \{\frac{a}{b} \mid a, b \in \mathbb{Z}, b \neq 0\}$

Reals:  $\mathbb{R} = \{x \mid x \text{ a real } \# \}$

Empty set:  $\emptyset = \{ \}$

$\mathbb{Z}^+$  = non-negative integers

$\mathbb{R}^-$  = non-positive reals, etc.

## Subsets

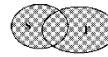
- Subset notation:  $\subseteq$   
 $S \subseteq T \Leftrightarrow (x \in S \Rightarrow x \in T)$



- Proper subset:  $\subset$   
 $S \subset T \Leftrightarrow ((S \subseteq T) \wedge (S \neq T))$   
 $S = T \Leftrightarrow ((T \subseteq S) \wedge (S \subseteq T))$   
 $\forall S \ \emptyset \subseteq S$   
 $\forall S \ S \subseteq S$

## Union:

$S \cup T = \{x \mid x \in S \vee x \in T\}$



## Intersection:

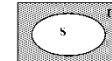
$S \cap T = \{x \mid x \in S \wedge x \in T\}$



- Universal set:  $U$  (everything)

- Set complement:  $S'$  or  $\bar{S}$

$S' = \{x \mid x \notin S\} = U - S$



- Disjoint sets:  $S \cap T = \emptyset$

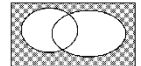


$S - T = S \cap T'$

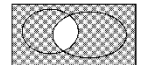
$S - S = \emptyset$

## DeMorgan's Laws

$(S \cup T)' = S' \cap T'$



$(S \cap T)' = S' \cup T'$



Boolean logic version:

$(X \wedge Y)' = X' \vee Y'$

$(X \vee Y)' = X' \wedge Y'$

## Function Types

- One-to-one** function: "1-1"  
 $a, b \in S \wedge a \neq b \Rightarrow f(a) \neq f(b)$

Ex:  $f: \mathbb{R} \rightarrow \mathbb{R}, f(x) = 2x$  is 1-1  
 $g(x) = x^2$  is not 1-1

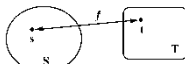
- Onto** function:

$\forall t \in T \ \exists s \in S \ \ni f(s) = t$

Ex:  $f: \mathbb{Z} \rightarrow \mathbb{Z}, f(x) = 13 - x$  is onto  
 $g(x) = x^2$  is not onto

## 1-to-1 Correspondence

- 1-to-1 correspondence:  $f: S \leftrightarrow T$   
 $f$  is both 1-1 and onto



Ex:  $f: \mathbb{R} \leftrightarrow \mathbb{R} \ \ni f(x) = x$  (identity)

$h: \mathbb{N} \leftrightarrow \mathbb{Z} \ \ni h(x) = \frac{x-1}{2}, x \text{ odd},$

$\frac{-x}{2}, x \text{ even}.$

## Generalized Cardinality

- $S$  is **at least as large** as  $T$ :  
 $|S| \geq |T| \Rightarrow \exists f: S \rightarrow T, f$  onto  
i.e., " $S$  covers  $T$ "

Ex:  $r: \mathbb{R} \rightarrow \mathbb{Z}, r(x) = \text{round}(x)$   
 $\Rightarrow |\mathbb{R}| \geq |\mathbb{Z}|$

- $S$  and  $T$  have **same cardinality**:  
 $|S| = |T| \Rightarrow |S| \geq |T| \wedge |T| \geq |S|$   
or  
 $\exists$  1-1 correspondence  $S \leftrightarrow T'$

- Generalizes finite cardinality:  
 $\{1, 2, 3, 4, 5\} \geq \{a, b, c\}$

## Infinite Sets

- Infinite set**:  $|S| > k \ \forall k \in \mathbb{Z}$   
or  
 $\exists$  1-1 corres.  $f: S \leftrightarrow T, S \subset T$

Ex:  $\{p \mid p \text{ prime}\}, \mathbb{R}$

- Countable set**:  $|S| \leq \mathbb{N}$

Ex:  $\emptyset, \{p \mid p \text{ prime}\}, \mathbb{N}, \mathbb{Z}$

- $S$  is **strictly smaller** than  $T$ :

$|S| < |T| \Rightarrow |S| \leq |T| \wedge |S| \neq |T|$

- Uncountable set**:  $|\mathbb{N}| < |S|$

Ex:  $|\mathbb{N}| < \mathbb{R}$   
 $|\mathbb{N}| < [0, 1] = \{x \mid x \in \mathbb{R}, 0 \leq x \leq 1\}$

**Thm:**  $\exists$  1-1 correspondence  $\mathbb{Q} \leftrightarrow \mathbb{N}$   
**Pf** (dove-tailing):

1	1	1	1	1	1	1	1
2	1	2	1	2	1	2	1
3	1	2	3	1	2	3	1
4	1	2	3	4	1	2	3
5	1	2	3	4	5	1	2
6	1	2	3	4	5	6	1
7	1	2	3	4	5	6	7
8	1	2	3	4	5	6	7
9	1	2	3	4	5	6	7
10	1	2	3	4	5	6	7

**Thm:**  $|\mathbb{R}| > |\mathbb{N}|$

**Pf** (diagonalization):

Assume  $\exists$  1-1 corres.  $f: \mathbb{R} \leftrightarrow \mathbb{N}$

Construct  $X \in \mathbb{R}$ :

$f(1) = 2.718281828\dots \rightarrow ?$

$f(2) = 2.718281828\dots \rightarrow ?$

$f(3) = 2.718281828\dots \rightarrow ?$

$X = 0.718281828\dots \forall k \in \mathbb{N}$

$\Rightarrow f$  not a 1-1 correspondence

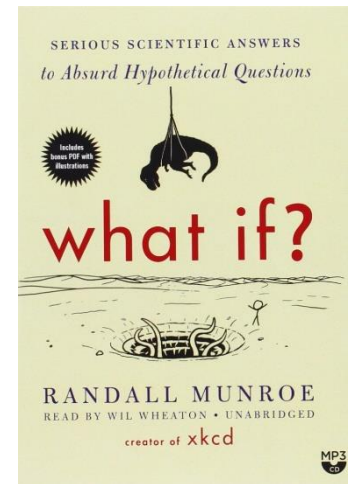
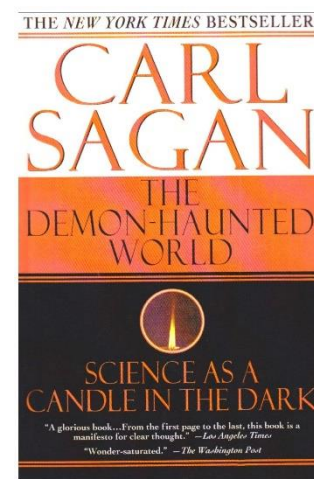
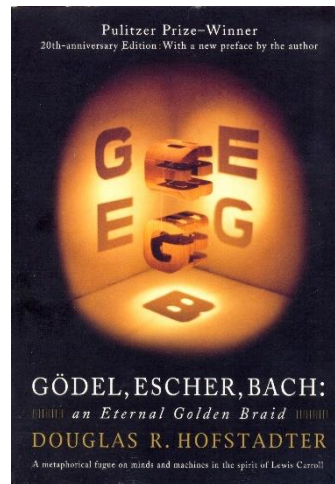
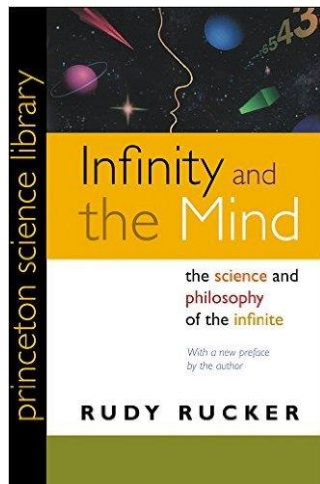
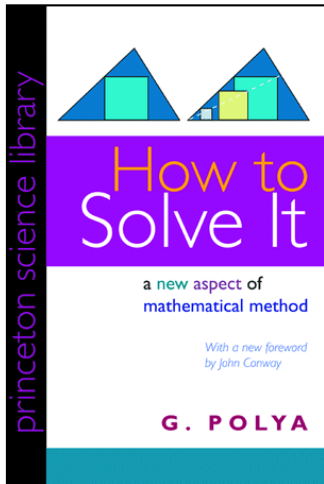
$\rightarrow$  contradiction

$\Rightarrow \mathbb{R}$  is uncountable

# Required Readings

[www.cs.virginia.edu/robins/CS\\_readings.html](http://www.cs.virginia.edu/robins/CS_readings.html)

- **Required** books:
  - [How to Solve It](#), Polya, 1957
  - [Infinity and the Mind](#), Rucker, 1995
  - [Godel, Escher, Bach, Hofstadter](#), 1979
  - [The Demon Hunted World](#), Sagan, 2009
  - [What If - Serious Scientific Answers to Absurd Hypothetical Questions](#), Munroe, 2014



# Required Readings

[www.cs.virginia.edu/robins/CS\\_readings.html](http://www.cs.virginia.edu/robins/CS_readings.html)

- Other videos / articles / books are “electives”
- Pacing: at least 3 submissions per week (due Monday)
- Length: 1-2 paragraphs per article / video  
1-2 pages per book
- Books are worth more credit than articles / videos
- Email all submissions to: [homework.cs3102@gmail.com](mailto:homework.cs3102@gmail.com)
- Additional readings beyond 50 are welcome!  
=> Extra credit

# Other Readings

[www.cs.virginia.edu/robins/CS\\_readings.html](http://www.cs.virginia.edu/robins/CS_readings.html)

- Theory and Algorithms:

- **Who Can Name the Bigger Number**, Scott Aaronson, 1999
- The Limits of Reason, Gregory Chaitin, Scientific American, March 2006, pp. 74-81.
- Breaking Intractability, Joseph Traub and Henryk Wozniakowski, Scientific American, January 1994, pp. 102-107.
- Confronting Science's Logical Limits, John Casti, Scientific American, October 1996, pp. 102-105.
- **Go Forth and Replicate**, Moshe Sipper and James Reggia, Scientific American, August 2001, pp. 34-43.
- The Science Behind Sudoku, Jean-Paul Delahaye, Scientific American, June 2006, pp. 80-87.
- The Traveler's Dilemma, Kaushik Basu, Scientific American, June 2007, pp. 90-95.

# Other Readings

[www.cs.virginia.edu/robins/CS\\_readings.html](http://www.cs.virginia.edu/robins/CS_readings.html)

- **Biological Computing:**

- Computing with DNA, Leonard Adleman, Scientific American, August 1998, pp. 54-61.
- Bringing DNA Computing to Life, Ehud Shapiro and Yaakov Benenson, Scientific American, May 2006, pp. 44-51.
- Engineering Life: Building a FAB for Biology, David Baker et al., Scientific American, June 2006, pp. 44-51.
- Big Lab on a Tiny Chip, Charles Choi, Scientific American, October 2007, pp. 100-103.
- DNA Computers for Work and Play, Macdonald et al, Scientific American, November 2007, pp. 84-91.

Email all submissions to: [homework.cs3102@gmail.com](mailto:homework.cs3102@gmail.com)



# Other Readings

[www.cs.virginia.edu/robins/CS\\_readings.html](http://www.cs.virginia.edu/robins/CS_readings.html)

- **Quantum Computing:**

- Quantum Mechanical Computers, Seth Lloyd, Scientific American, 1997, pp. 98-104.
- Quantum Computing with Molecules, Gershenfeld and Chuang, Scientific American, June 1998, pp. 66-71.
- Black Hole Computers, Seth Lloyd and Jack Ng, Scientific American, November 2004, pp. 52-61.
- Computing with Quantum Knots, Graham Collins, Scientific American, April 2006, pp. 56-63.
- **The Limits of Quantum Computers**, Scott Aaronson, Scientific American, March 2008, pp. 62-69.
- Quantum Computing with Ions, Monroe and Wineland, Scientific American, August 2008, pp. 64-71.

# Other Readings

[www.cs.virginia.edu/robins/CS\\_readings.html](http://www.cs.virginia.edu/robins/CS_readings.html)

- **History of Computing:**
  - **Alan Turing's Forgotten Ideas**, B. Jack Copeland and Diane Proudfoot, Scientific American, May 1999, pp. 98-103.
  - **Ada and the First Computer**, Eugene Kim and Betty Toole, Scientific American, April 1999, pp. 76-81.
- **Security and Privacy:**
  - Malware Goes Mobile, Mikko Hypponen, Scientific American, November 2006, pp. 70-77.
  - RFID Powder, Tim Hornyak, Scientific American, February 2008, pp. 68-71.
  - Can Phishing be Foiled, Lorrie Cranor, Scientific American, December 2008, pp. 104-110.

# Other Readings

[www.cs.virginia.edu/robins/CS\\_readings.html](http://www.cs.virginia.edu/robins/CS_readings.html)

- **Future of Computing:**

- **Microprocessors in 2020**, David Patterson, Scientific American, September 1995, pp. 62-67.
- Computing Without Clocks, Ivan Sutherland and Jo Ebergen, Scientific American, August 2002, pp. 62-69.
- Making Silicon Lase, Bahram Jalali, Scientific American, February 2007, pp. 58-65.
- **A Robot in Every Home**, Bill Gates, Scientific Am, January 2007, pp. 58-65.
- Ballbots, Ralph Hollis, Scientific American, October 2006, pp. 72-77.
- Dependable Software by Design, Daniel Jackson, Scientific American, June 2006, pp. 68-75.
- Not Tonight Dear - I Have to Reboot, Charles Choi, Scientific American, March 2008, pp. 94-97.
- Self-Powered Nanotech, Zhong Lin Wang, Scientific American, January 2008, pp. 82-87.

# Other Readings

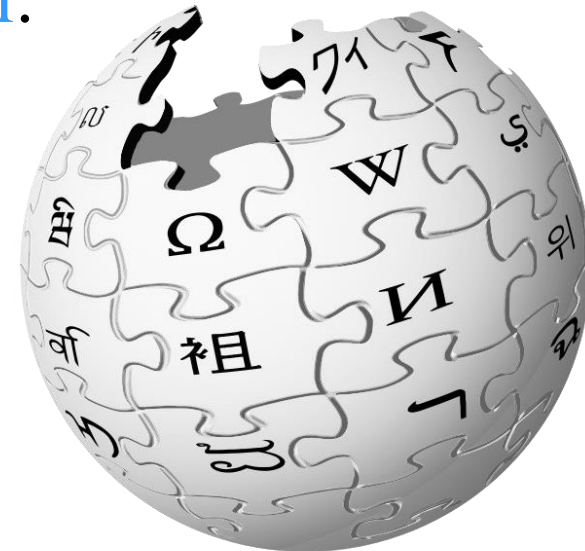
[www.cs.virginia.edu/robins/CS\\_readings.html](http://www.cs.virginia.edu/robins/CS_readings.html)

- **The Web:**

- The Semantic Web in Action, Lee Feigenbaum et al., Scientific American, December 2007, pp. 90-97.
- **Web Science Emerges**, Nigel Shadbolt and Tim Berners-Lee, Scientific American, October 2008, pp. 76-81.

- **The Wikipedia Computer Science Portal:**

- Theory of computation and Automata theory
- Formal languages and grammars
- Chomsky hierarchy and the Complexity Zoo
- Regular, context-free & Turing-decidable languages
- Finite & pushdown automata; Turing machines
- Computational complexity
- List of data structures and algorithms



Email all submissions to: [homework.cs3102@gmail.com](mailto:homework.cs3102@gmail.com)

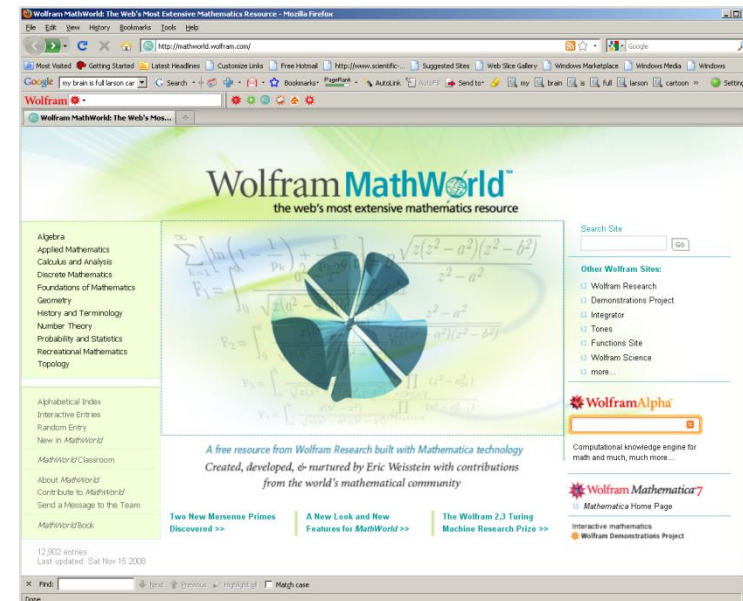
# Other Readings

[www.cs.virginia.edu/robins/CS\\_readings.html](http://www.cs.virginia.edu/robins/CS_readings.html)

- The Wikipedia Math Portal:
  - Problem solving
  - List of Mathematical lists
  - Sets and Infinity
  - Discrete mathematics
  - Proof techniques and list of proofs
  - Information theory & randomness
  - Game theory
- Mathematica's “Math World”

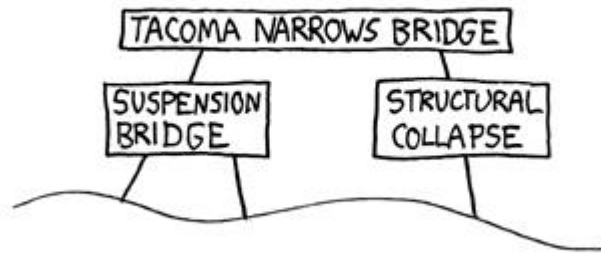


**WIKIPEDIA**  
*The Free Encyclopedia*

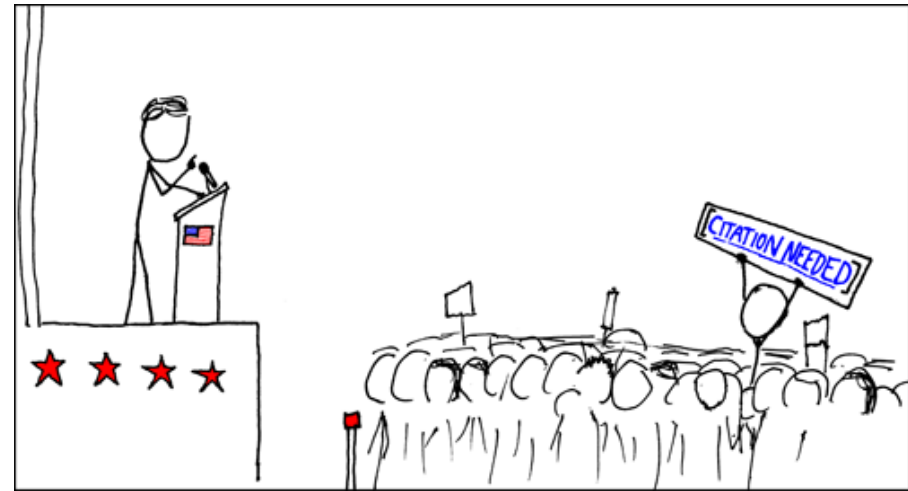
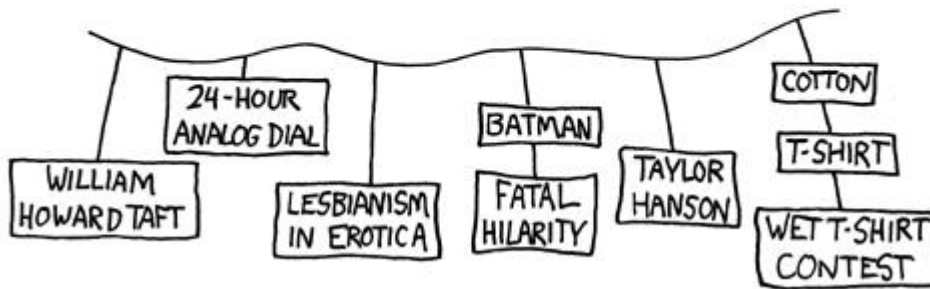


Email all submissions to: [homework.cs3102@gmail.com](mailto:homework.cs3102@gmail.com)

# THE PROBLEM WITH WIKIPEDIA:



[THREE HOURS OF  
FASCINATED CLICKING]



# WIKIFRIENDS:

I REALLY LIKED  
THAT MOVIE.

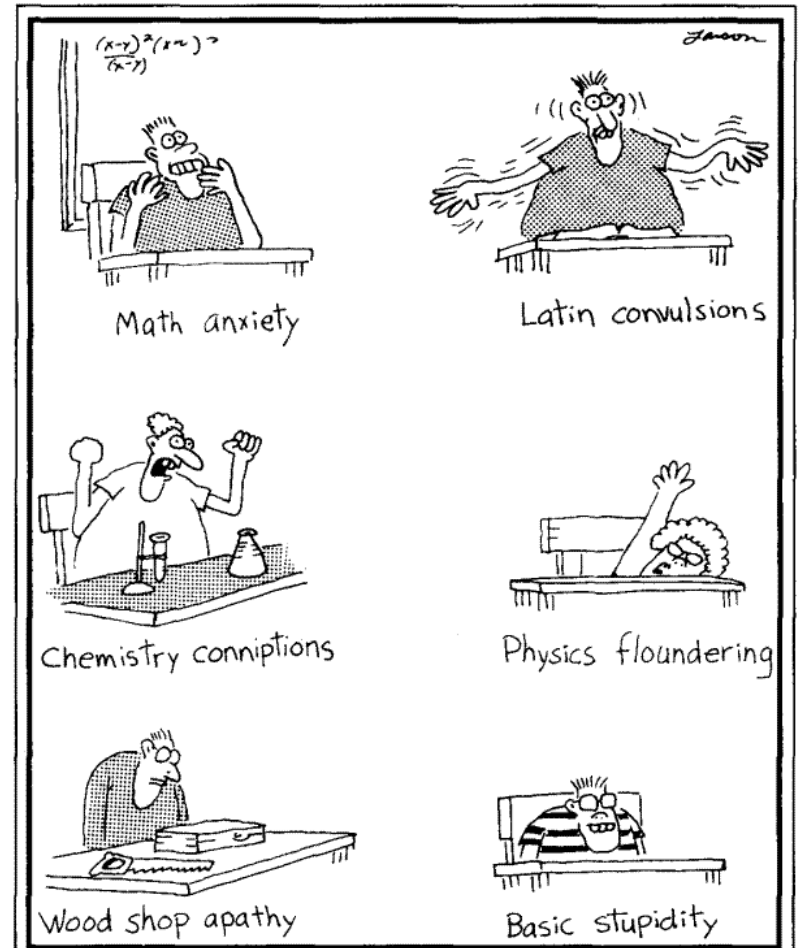
I HATED  
THAT MOVIE.

ME TOO.



# Good Advice

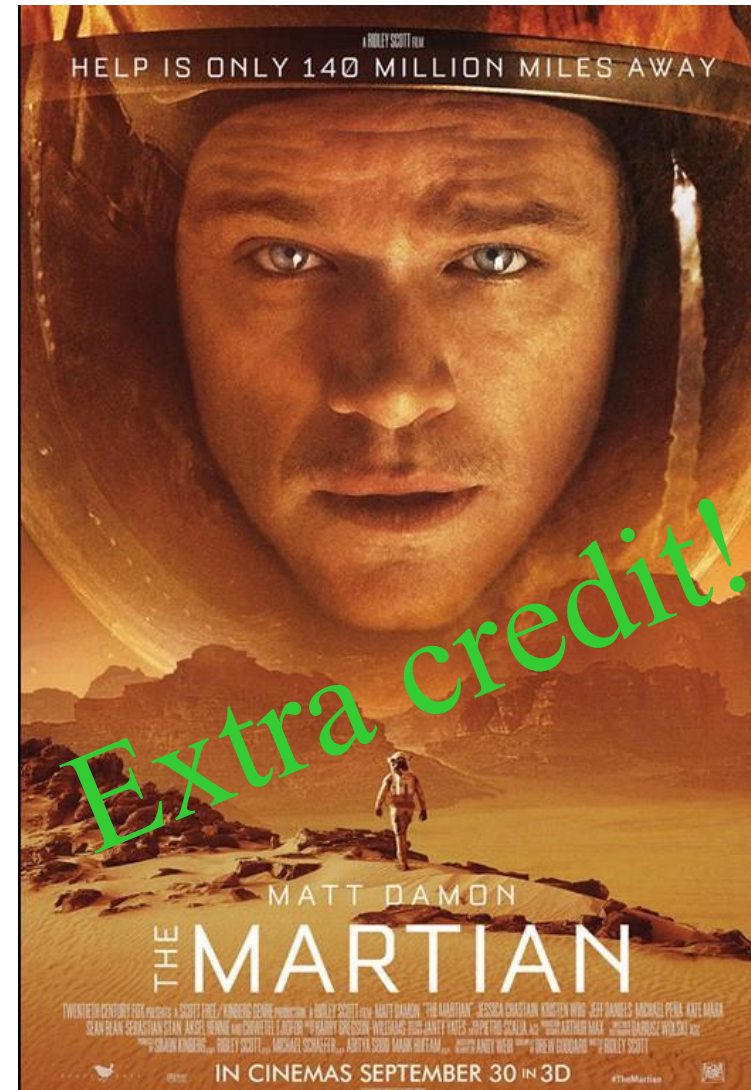
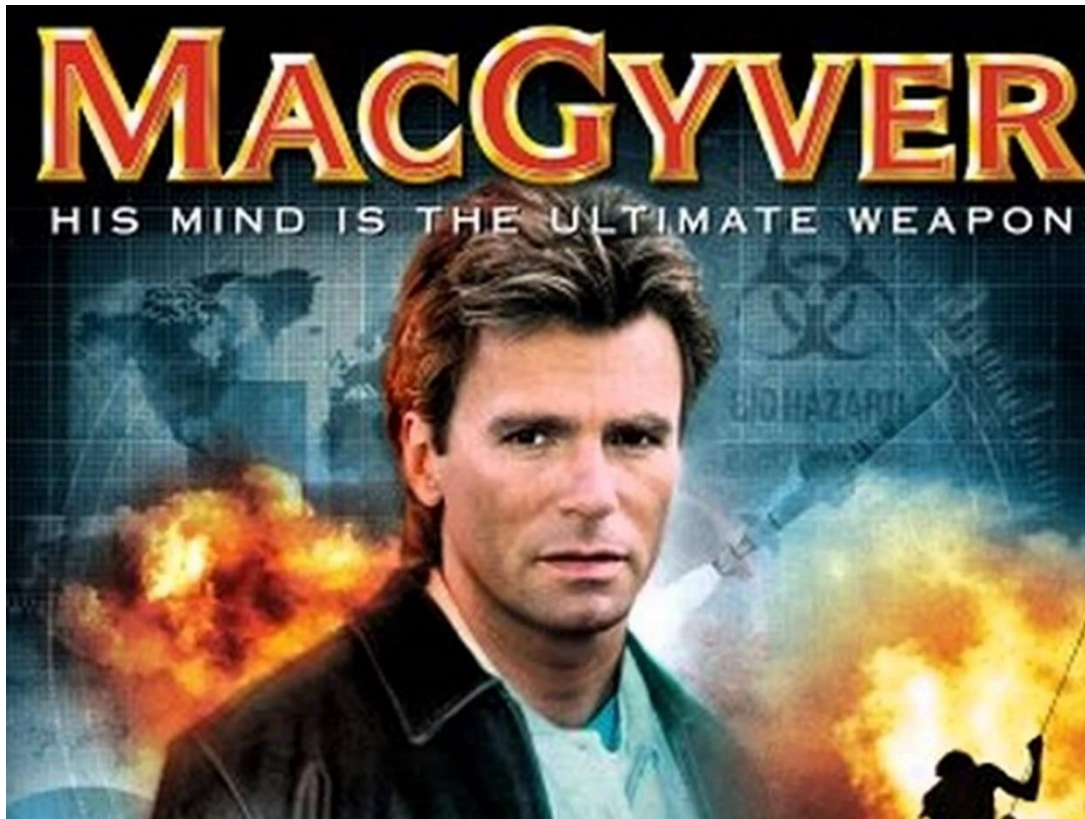
- Ask questions ASAP
- Solve problems ASAP
- **Work in study groups**
- Do not fall behind
- “Cramming” won’t work
- Do lots of extra credit
- Attend every lecture
- Visit class Website often
- **Solve lots of problems**



Classroom afflictions

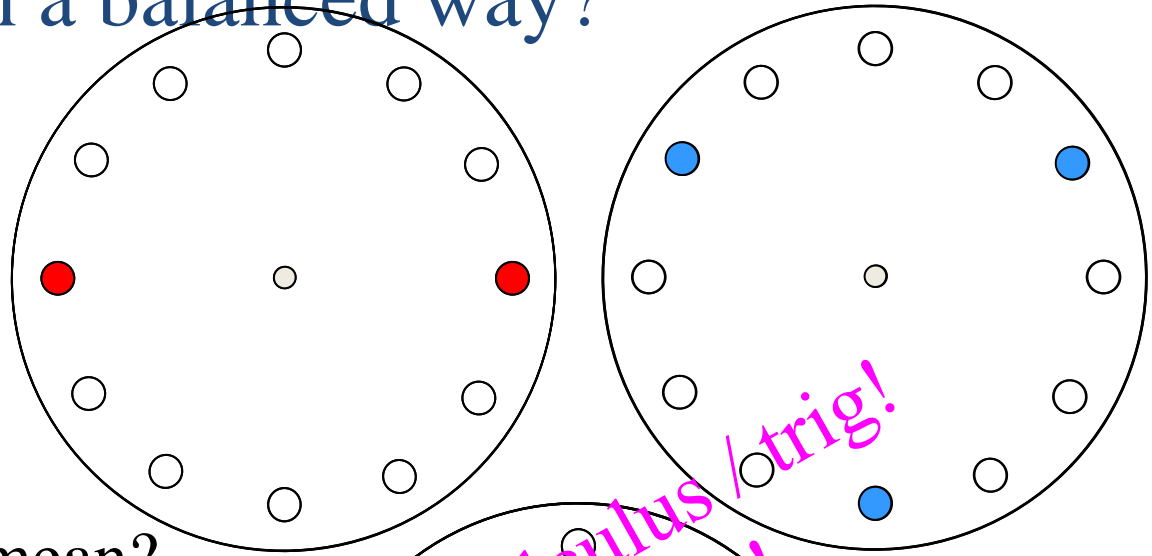


**Goal:** Become a more effective problem solver!



Email all submissions to: [homework.cs3102@gmail.com](mailto:homework.cs3102@gmail.com)

# Problem: Can 5 test tubes be spun simultaneously in a 12-hole centrifuge in a balanced way?



- What does “balanced” mean?
- Why are 3 test tubes balanced?
- **Symmetry!**
- Can you merge solutions?
- **Superposition!**
- **Linearity!**  $f(x + y) = f(x) + f(y)$
- Can you spin 7 test tubes?
- **Complementarity!**
- Empirical testing...

No vector calculus / trig!  
No equations!  
Truth is guaranteed!  
Fundamental principles exposed!  
Easy to generalize!  
High elegance / beauty!

**Problem:**  $1 + 2 + 3 + 4 + \dots + 100 = ?$

**Proof:** ~~Induction...~~

$$= (100 * 101) / 2$$

$$= 5050$$

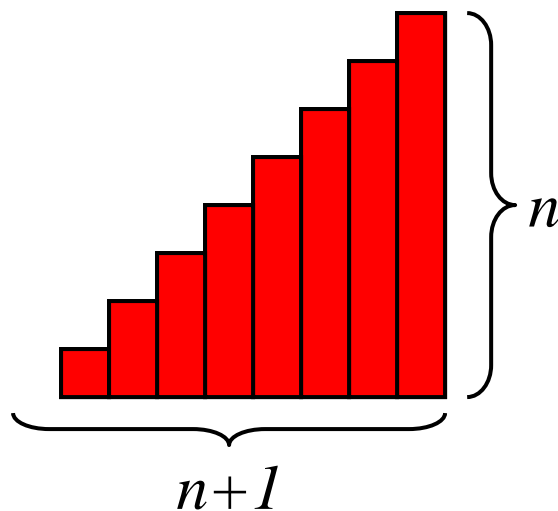
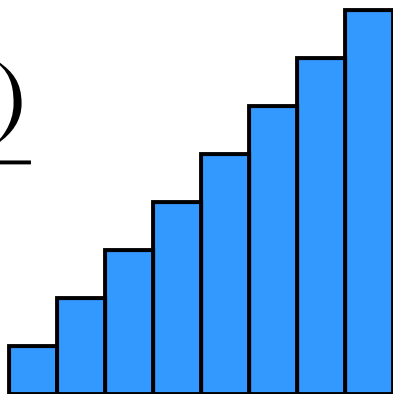
$$1 + 2 + 3 + \dots + 99 + 100$$

$$100 + 99 + 98 + \dots + 2 + 1$$

---

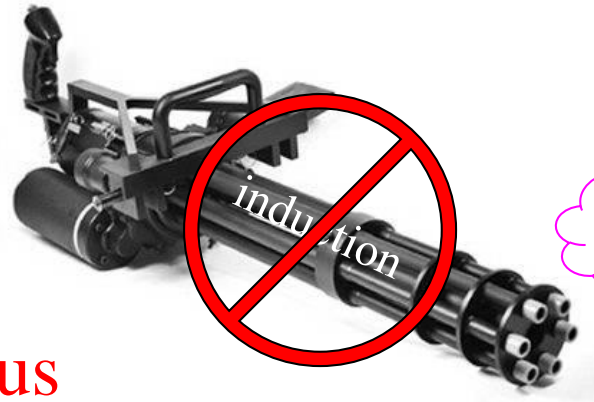
$$101 + 101 + 101 + \dots + 101 + 101 = 100 * 101$$

$$\sum_{i=1}^n i = \frac{n(n+1)}{2}$$



# Drawbacks of Induction

- You must **a priori** know the formula / result
- Easy to make **mistakes** in inductive proof
- Mostly “mechanical” – **ignores intuitions**
- **Tedious** to construct
- **Difficult** to check
- **Hard** to understand
- **Not very convincing**
- Generalizations **not obvious**
- Does not “**shed light on truth**”
- **Obfuscates** connections



**Conclusion:** only use induction as a **last resort!**

I.e., **almost never!**

# Historical Perspectives



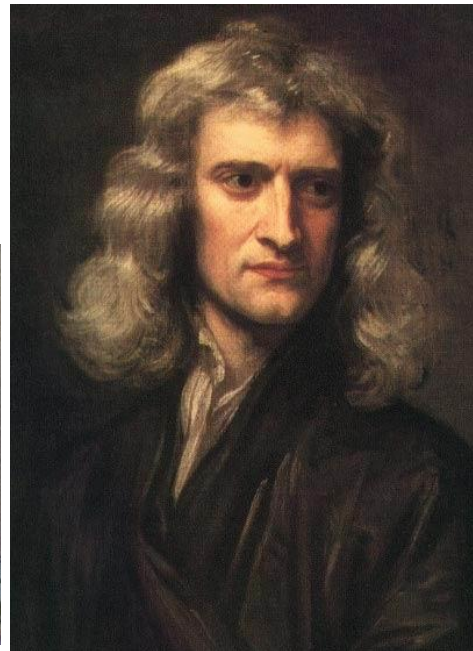
# Historical Perspectives

- Science and mathematics **builds heavily** on past
- Often the **simplest** ideas are the most **subtle**
- Most **fundamental progress** was done by a few
- We **learn** much by observing the best minds
- Research benefits from seeing **connections**
- The field of computer science has many “**parents**”
- We get **inspired** and motivated by excellence
- The giants can show us what is **possible to achieve**
- It is **fun** to know these things!



# “Standing on the Shoulders of Giants”

- Aristotle, Euclid, Archimedes, Eratosthenes
- Abu Ali al-Hasan ibn al-Haytham
- Fibonacci, Descartes, Fermat, Pascal
- Newton, Euler, Gauss, Hamilton
- **Boole, De Morgan**
- **Babbage, Ada Augusta**
- Venn, Carroll

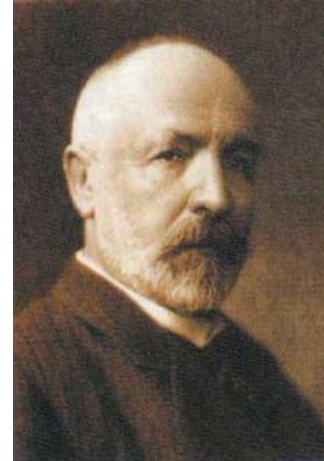


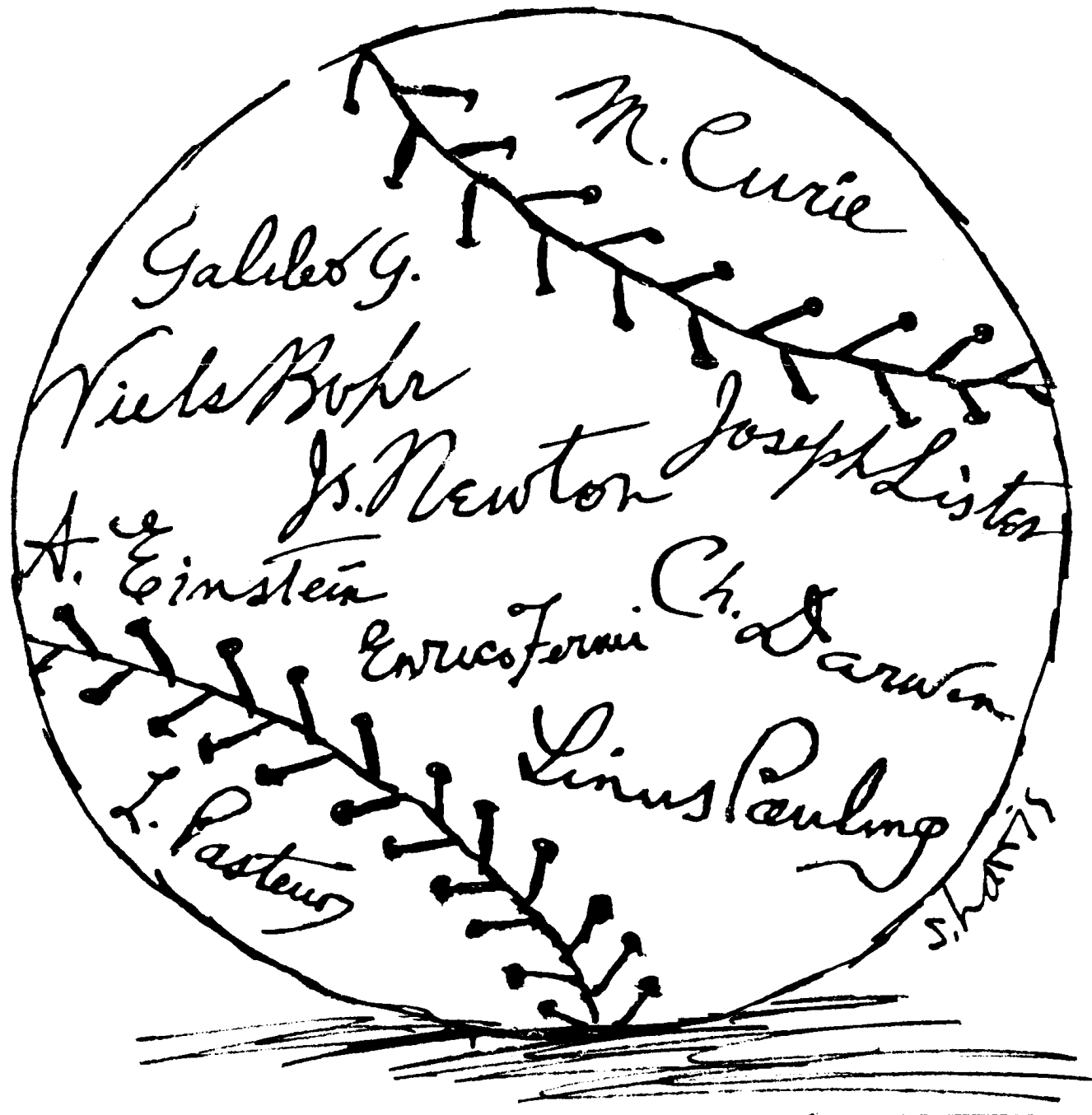


# “Standing on the Shoulders of Giants”

- Cantor, Hilbert, Russell
- Hardy, Ramanujan, Ramsey
- Godel, Church, **Turing**
- **von Neumann**, Shannon
- Kleene, **Chomsky**
- Hoare, McCarthy, Erdos
- Knuth, Backus, Dijkstra

Many others...





Galileo G.

M. Curie

Niels Bohr

J. Newton Joseph Lister

A. Einstein

Enrico Fermi Ch. Darwin

I. Pasteur

Linus Pauling

SHARIN

Gauss  
 Newton  
 Archimedes  
 Euler  
 Cauchy  
 Poincare  
 Riemann  
 Cantor  
 Cayley  
 Hamilton  
 Eisenstein  
 Pascal  
 Abel  
 Hilbert  
 Klein  
 Leibniz  
 Descartes  
 Galois  
 Mobius  
 Jacob  
 Johann Bernoulli  
 Daniel Bernoulli  
 Dirichlet  
 Fermat  
 Pythagoras  
 Laplace  
 Lagrange  
 Kronecker  
 Jacobi  
 Bolyai  
 Lobatchewsky  
 Noether  
 Germain  
 Euclid  
 Legendre

$$(p/q)(q/p) = -1^{(p-1)(q-1)/4}$$

$$\text{num} = \Delta + \Delta + \Delta$$

$$\pi(n) = \frac{n}{\ln n}$$

$$(a/p) = -1^{\eta(p,a)}$$



$$\int_b^a f(x) dx = F(b) - F(a); \quad x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}$$

$$F(s) = s^{-2}$$

$$(abcdef) = (ab)(ac)(ad)(ae)(af)$$

$$\int_{\gamma} f(z) dz = 0$$

$$|a \cdot b| \leq |a||b|$$



$$\frac{F(Ax + B)}{Cz + D} = F(z)$$

$$\text{Gal}(E/F);$$

$$E_H = \{x \in E \mid \phi(x) = x \forall \phi \in H\}$$

$$f'(c)(b - a) = f(b) - f(a)$$

$$u_{tt} = c^2 u_{xx}; \quad 0 < x < 1$$

$$u(0,t) = 0 = u(1,t)$$

$$\frac{\partial^2 u}{\partial x^2} + \frac{\partial^2 u}{\partial y^2} + \frac{\partial^2 u}{\partial z^2} = 0$$

$$D = R[x]$$





MAKING PHILOSOPHY ACCESSIBLE: POP-UP PLATO

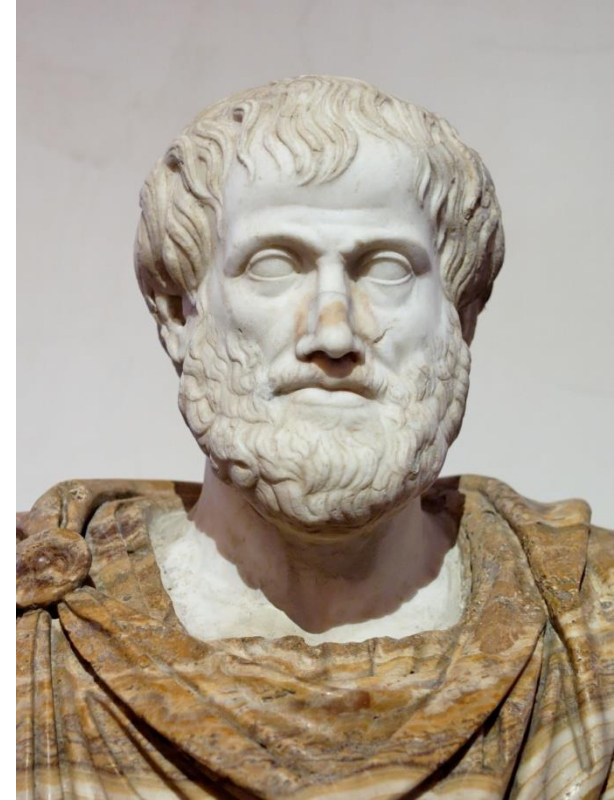


# Historical Perspectives

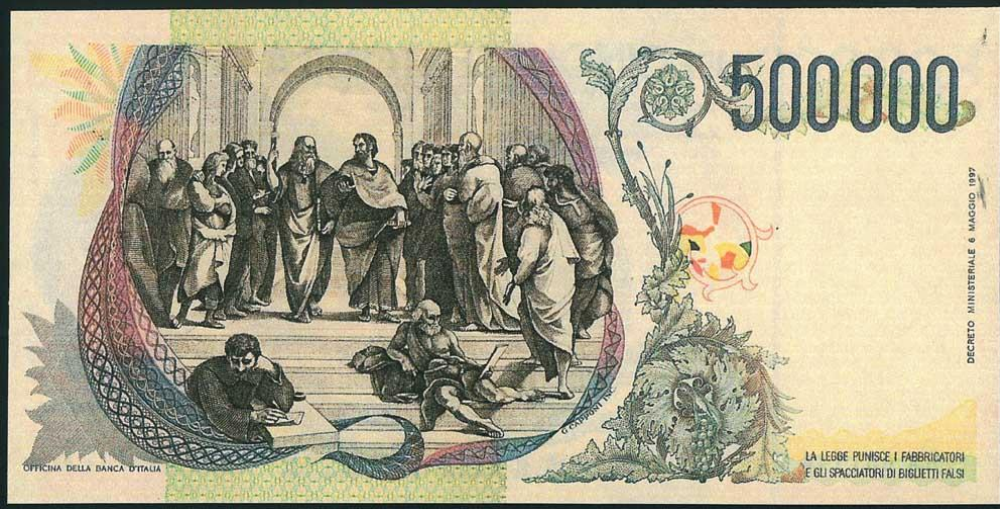
## Aristotle (384BC-322BC)

- Founded Western philosophy
- Student of Plato
- Taught Alexander the Great
- “Aristotelianism”
- Developed the “scientific method”
- One of the most influential people ever
- Wrote on physics, theatre, poetry, music, logic, rhetoric, politics, government, ethics, biology, zoology, morality, optics, science, aesthetics, psychology, metaphysics, ...
- Last person to know everything known in his own time!

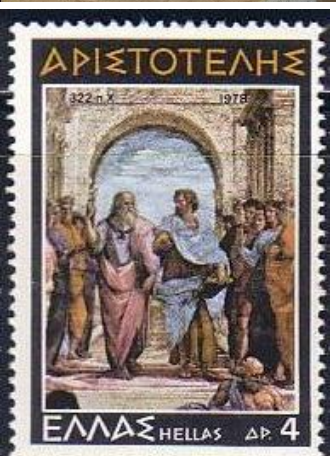
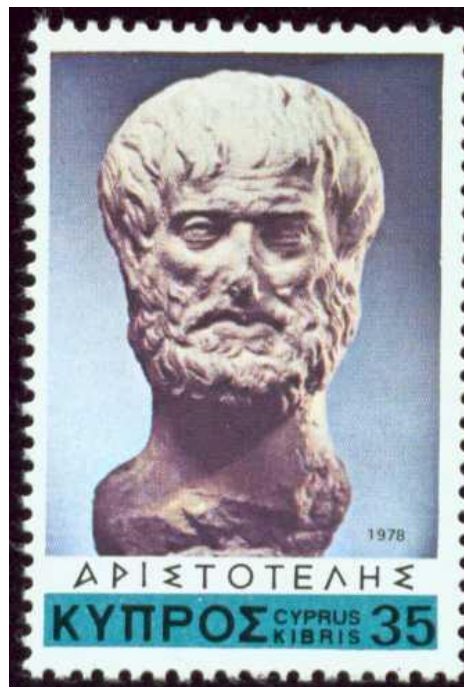
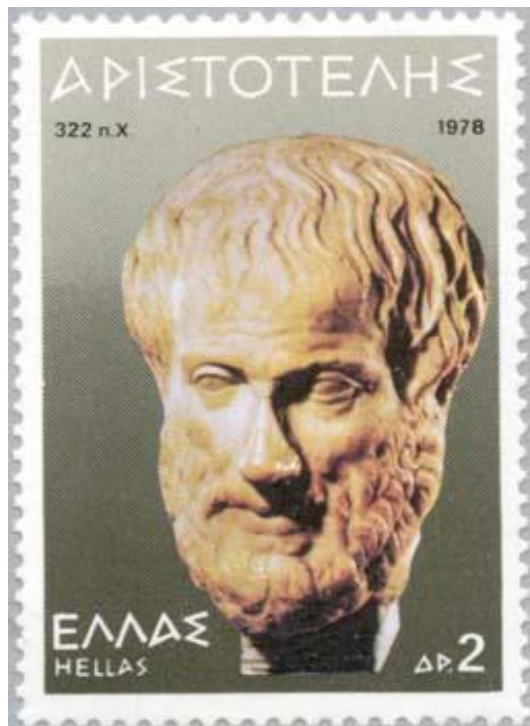
“Almost every serious intellectual advance has had to begin with an attack on some Aristotelian doctrine.” – Bertrand Russell







“Wit is educated insolence.”  
- Aristotle (384-322 B.C.)









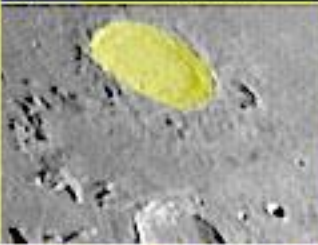
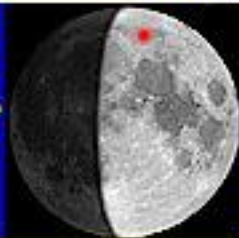
# ARISTOTELES

87 km

97 / 10 / 09 D=254mm FD=10



"LIGIA"  
Moon



© Antonio J. Cidadão

8

B/W QuickCam

a.cidadao@mail.telepac.pt



Birds fly because they're  
lighter than air.  
Some trees have different  
fruits each year.  
At night, clouds rest on  
the ground.

Are you sure  
he's Aristotle?





“What I especially like about being a philosopher-scientist is that I don’t have to get my hands dirty.”

PEDIMENT

CORNICE

FRIEZE

TRIGLYPH

METOPÉ

ARCHITRAVE

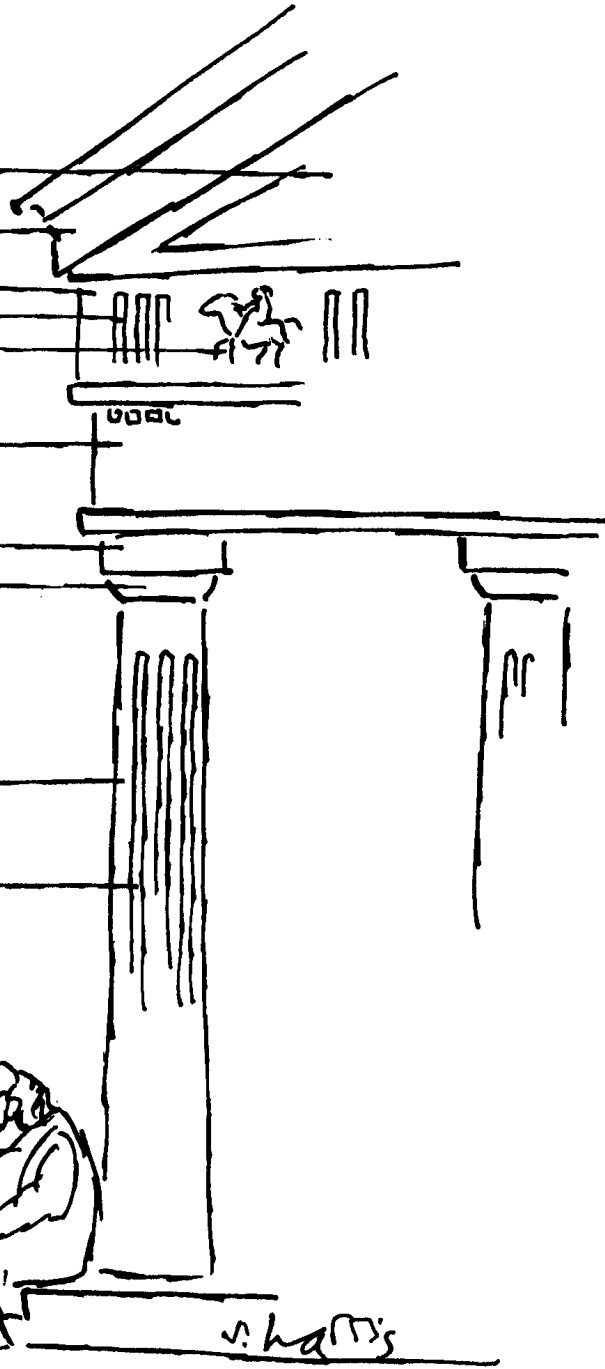
ABACUS

ECHINUS

SHAFT

FLUTE

SOCRATES

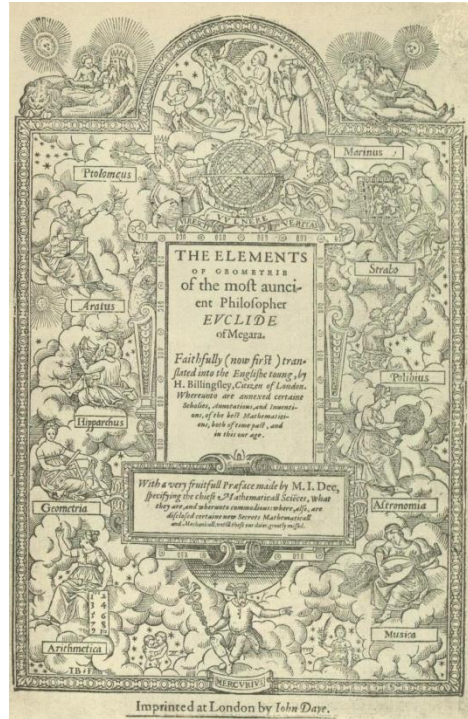


v. hartis

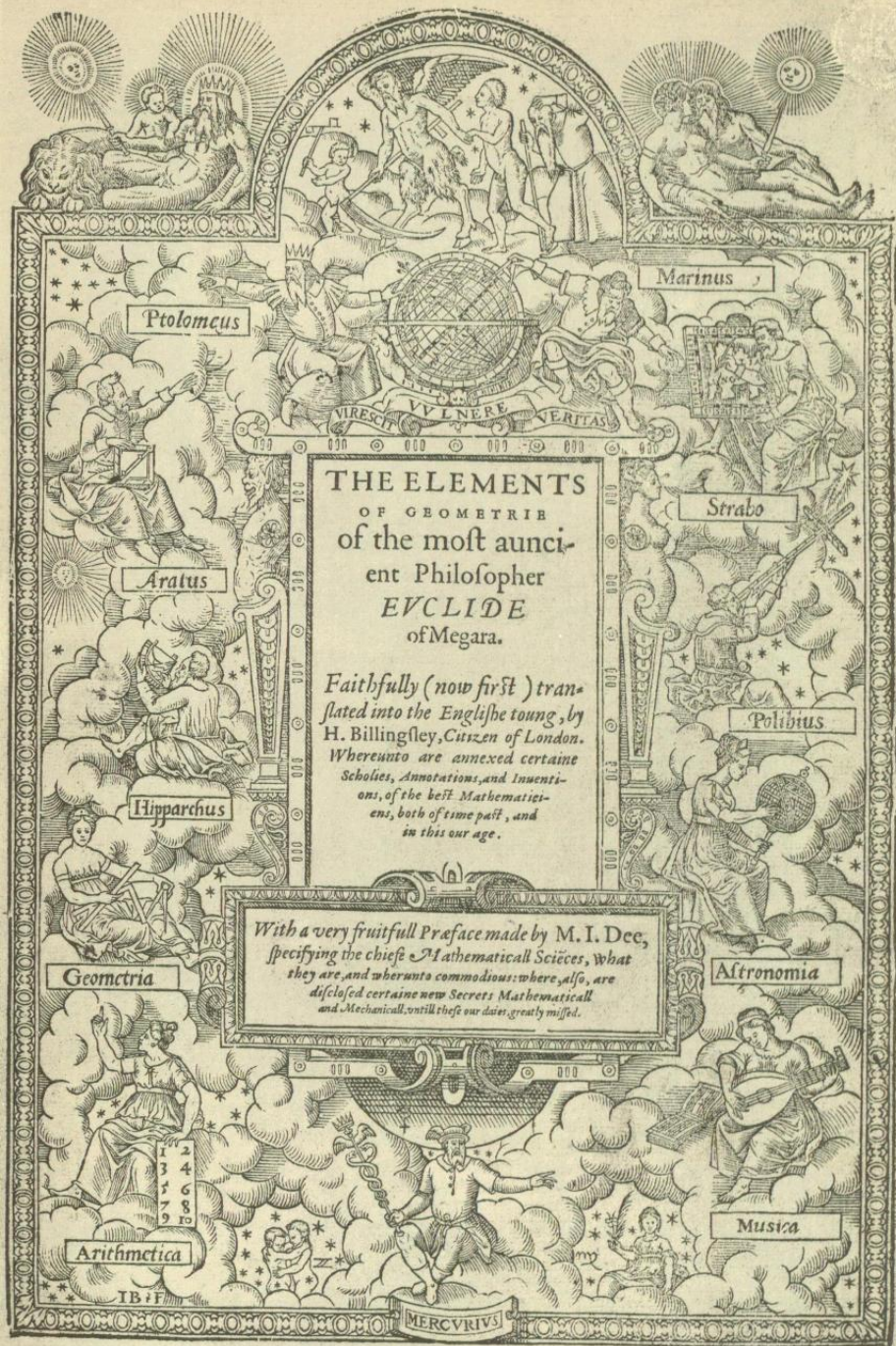
# Historical Perspectives

## Euclid (325BC-265BC)

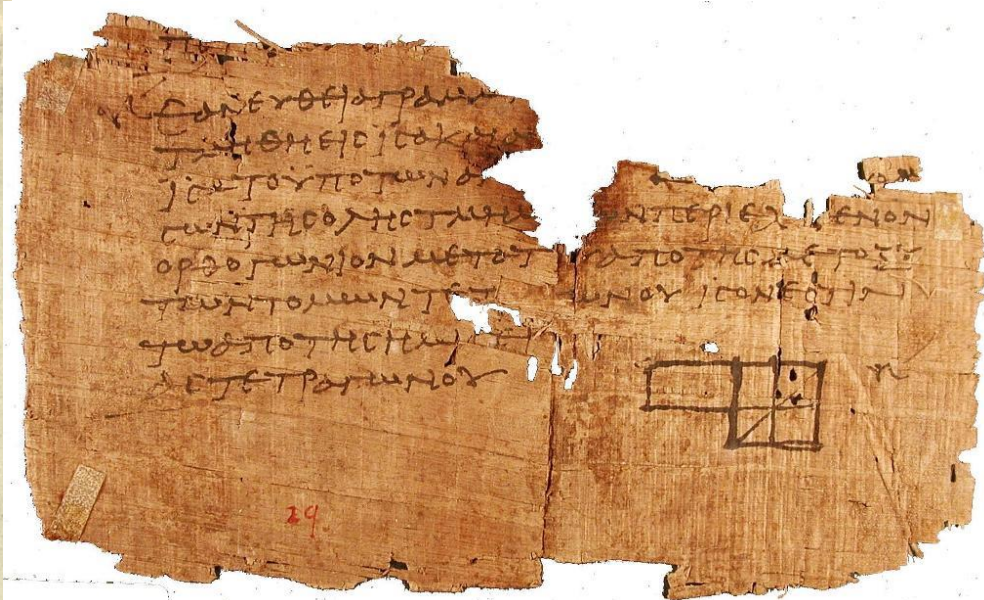
- Founder of geometry & the **axiomatic method**
- “**Elements**” – oldest and most impactful textbook
- Unified logic & math
- Introduced rigor and “**Euclidean**” geometry
- Influenced all other fields of science: Copernicus, Kepler, Galileo, Newton, Russell, Lincoln, Einstein & many others





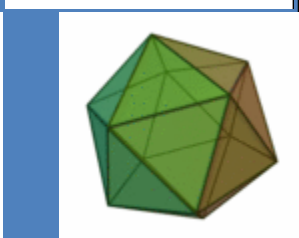
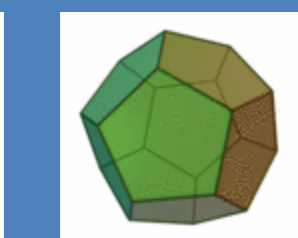
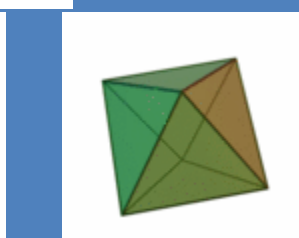
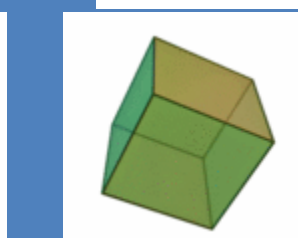
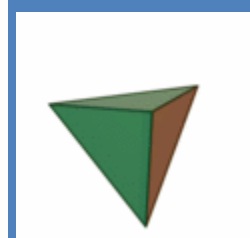
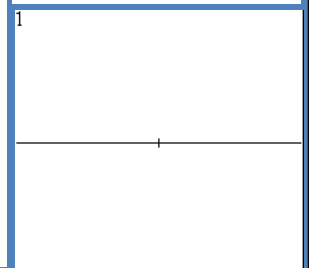
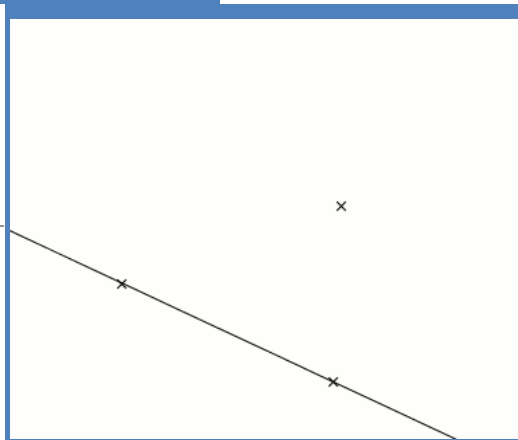
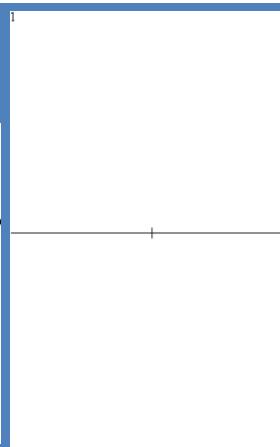
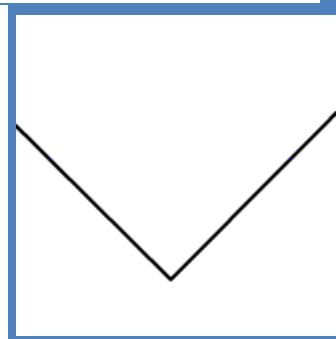
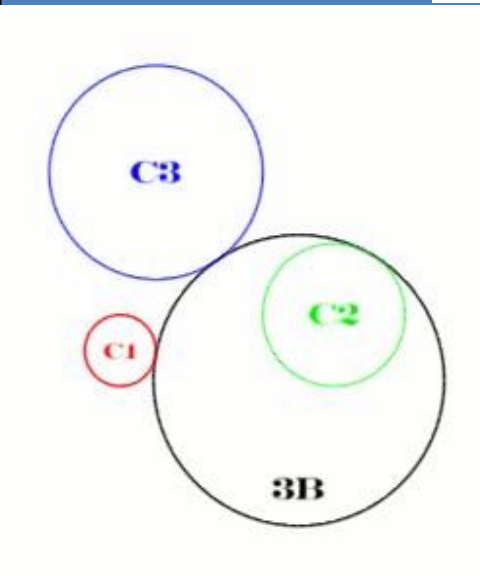
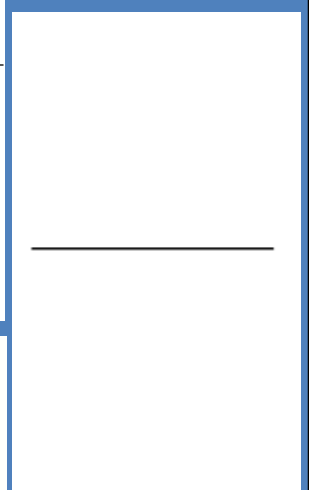
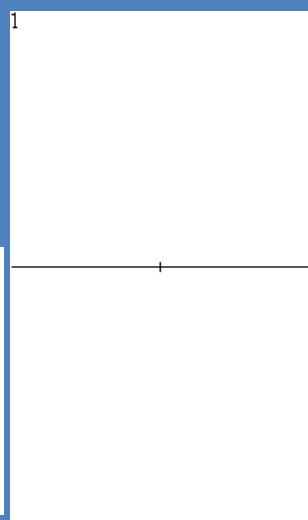
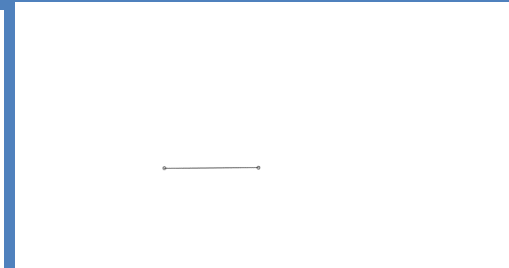
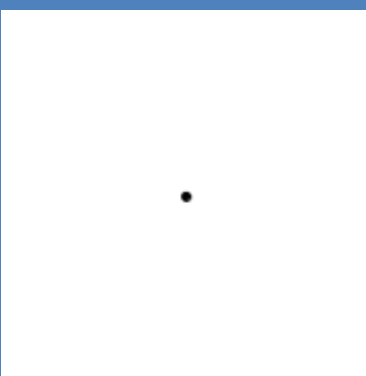
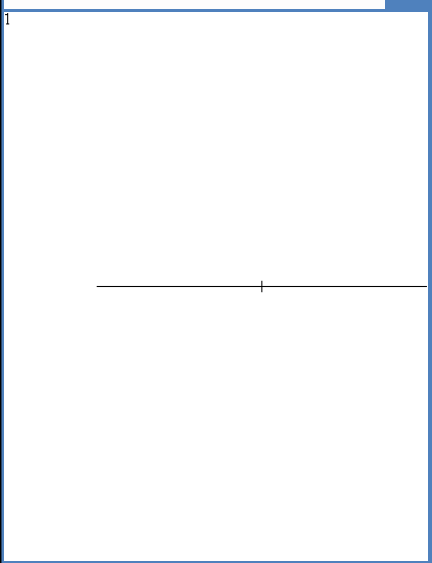
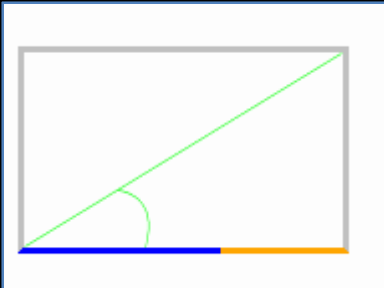


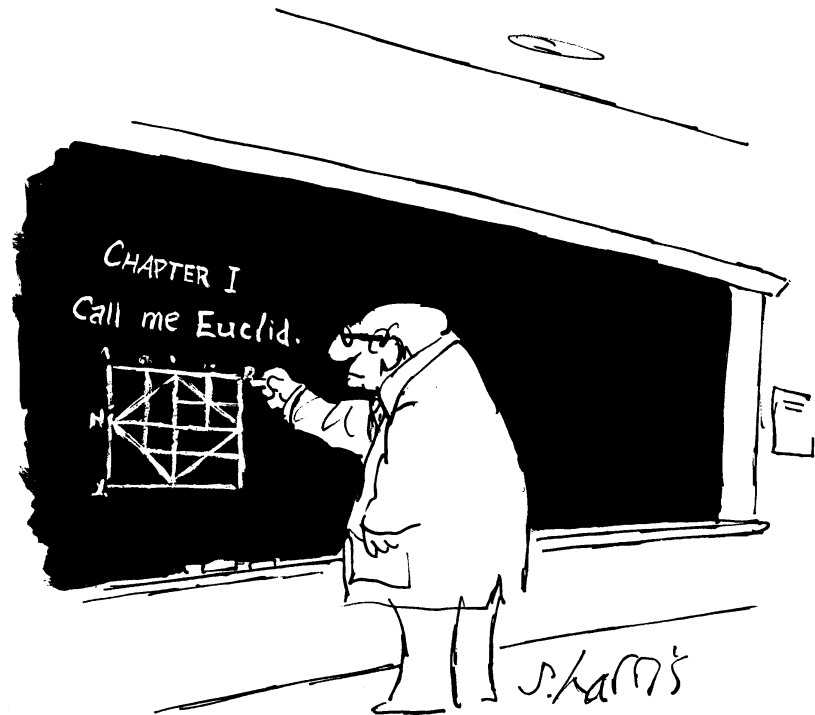
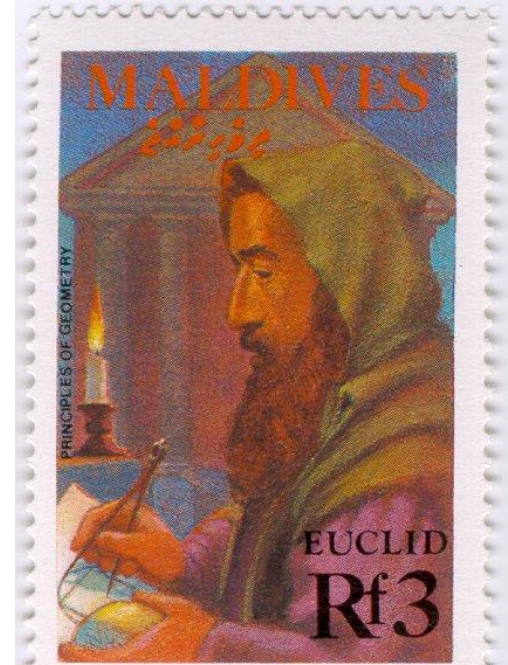
Imprinted at London by Iohn Daye.





# Euclid's Straight-Edge and Compass Geometric Constructions



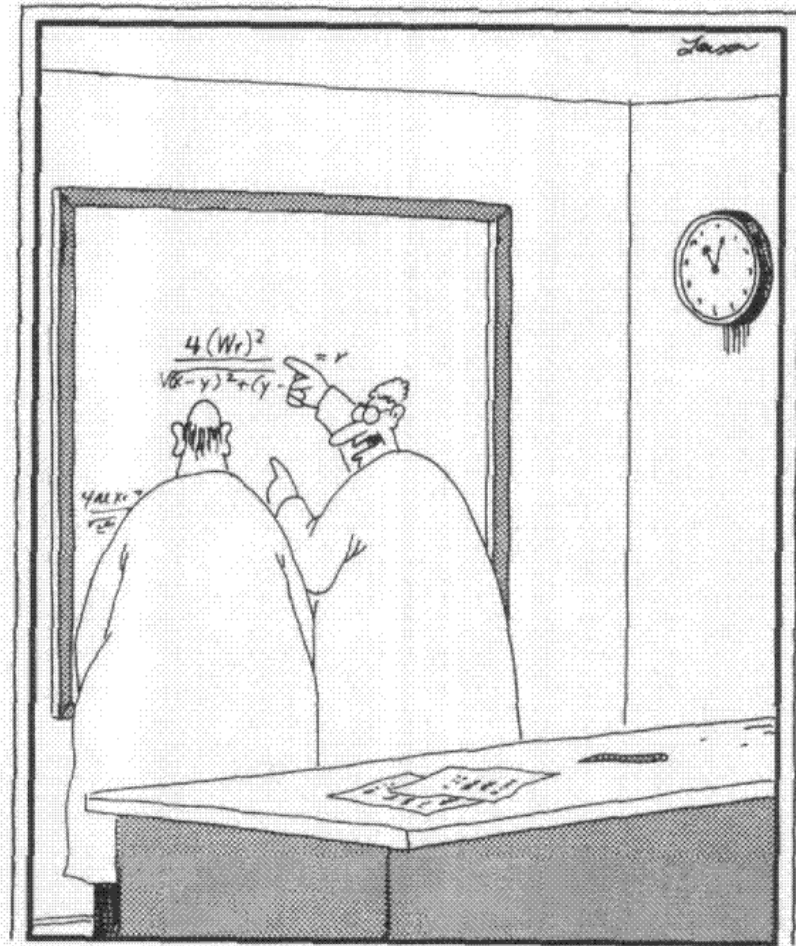


**Problem:**  $1^3 + 2^3 + 3^3 + 4^3 + \dots + n^3 = ?$

$$\sum_{i=1}^n i^3 = ?$$

**Extra Credit:**

find a short, **geometric**,  
induction-free proof.



"Yes, yes, I know that, Sidney ... everybody knows that! ... But look: Four wrongs squared, minus two wrongs to the fourth power, divided by this formula, do make a right."

**Problem:**  $(1/4) + (1/4)^2 + (1/4)^3 + (1/4)^4 + \dots = ?$

$$\sum_{i=1}^{\infty} \frac{1}{4^i} = ?$$

**Extra Credit:**

Find a short, **geometric**, induction-free proof.

**Problem:**  $(1/8) + (1/8)^2 + (1/8)^3 + (1/8)^4 + \dots = ?$

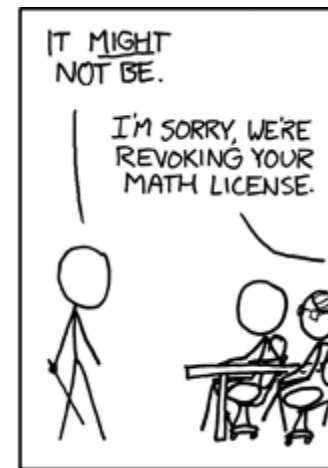
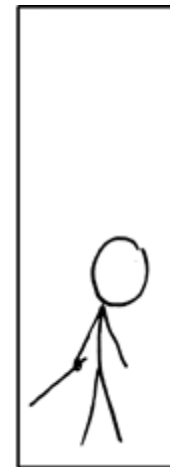
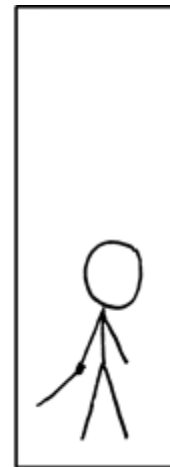
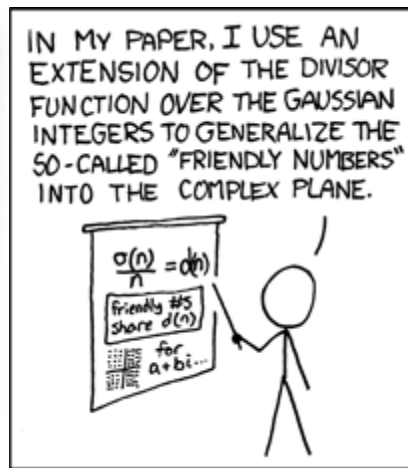
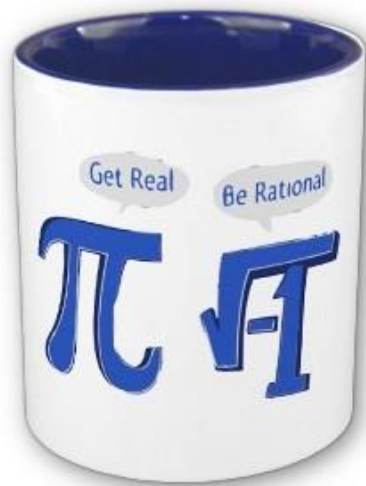
$$\sum_{i=1}^{\infty} \frac{1}{8^i} = ?$$

**Extra Credit:**

Find a short, **geometric**, induction-free proof.



**Problem:** Are the complex numbers closed under exponentiation ? E.g., what is the value of  $i^i$ ?



**Problem:** Prove that there are an infinity of primes.

**Extra Credit:** Find a short, induction-free proof.

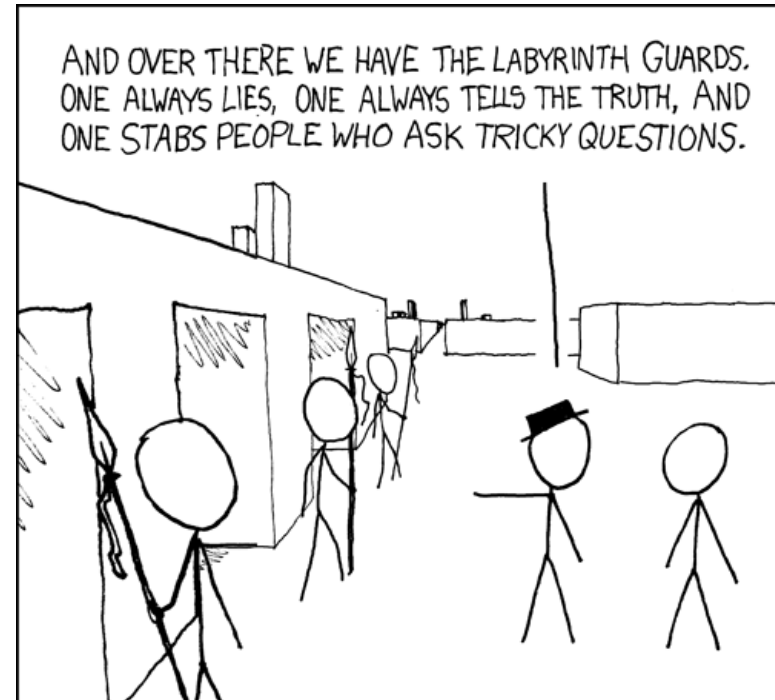
- What approaches fail?
- What techniques work and why?
- Lessons and generalizations



**Problem:** True or false: there arbitrary long blocks of consecutive composite integers.

**Extra Credit:** find a short, induction-free proof.

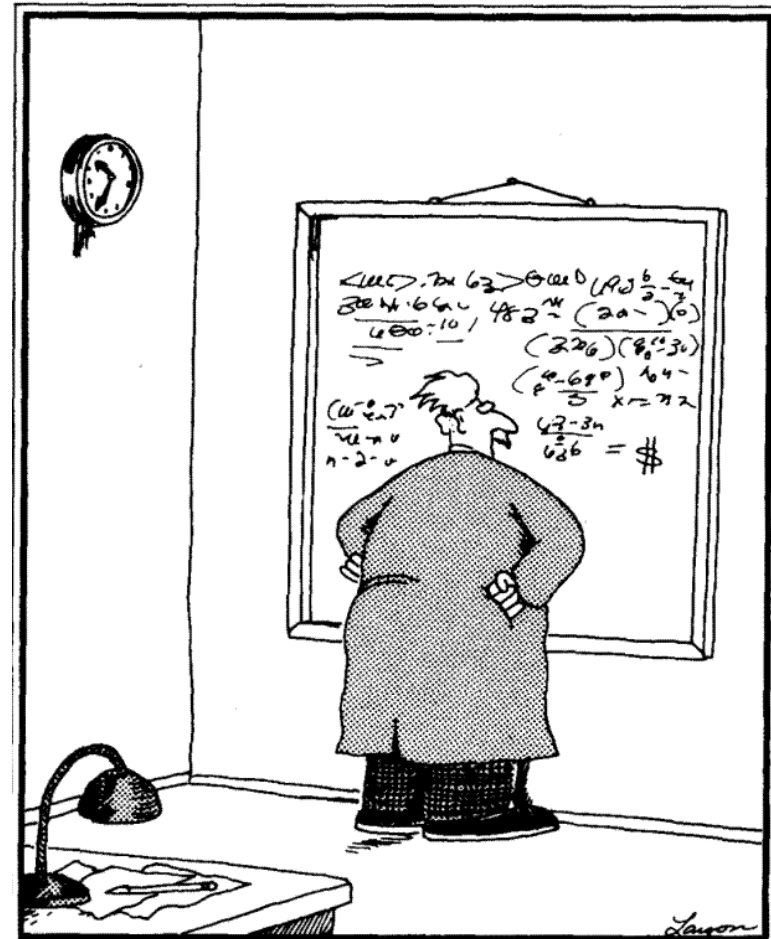
- What approaches fail?
- What techniques work and why?
- Lessons and generalizations



**Problem:** Prove that  $\sqrt{2}$  is irrational.

**Extra Credit:** find a short, induction-free proof.

- What approaches fail?
- What techniques work and why?
- Lessons and generalizations



Einstein discovers that time is actually money.

**Problem:** Does exponentiation preserve irrationality?  
i.e., are there two irrational numbers  $x$  and  $y$  such  
that  $x^y$  is rational?

**Extra Credit:** find a short, induction-free proof.

- What approaches fail?
- What techniques work and why?
- Lessons and generalizations



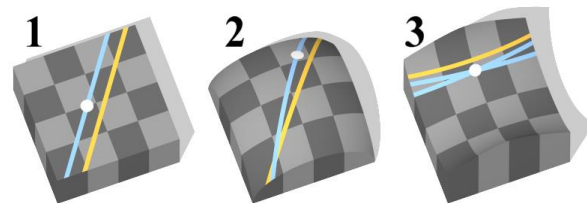
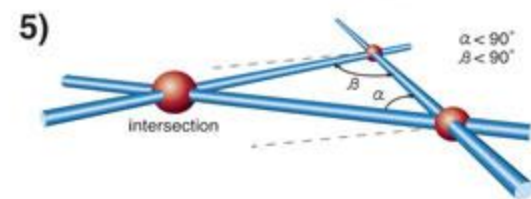
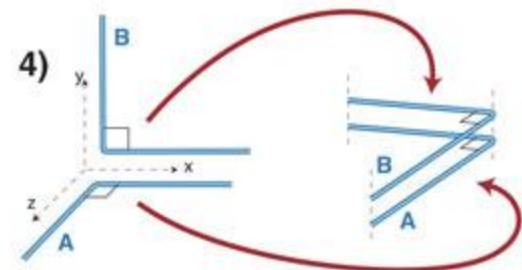
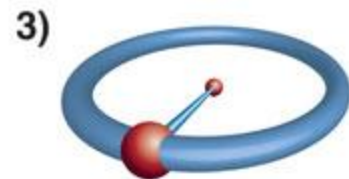
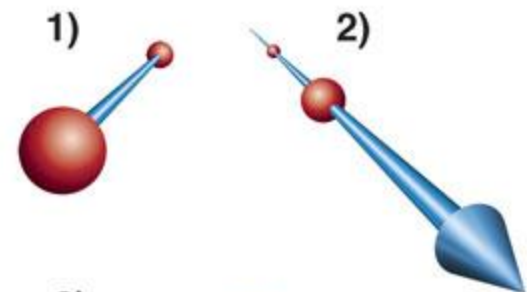
# Euclid's Axioms

- 1: Any two points can be connected by exactly one straight line.
- 2: Any segment can be extended indefinitely into a straight line.
- 3: A circle exists for any given center and radius.
- 4: All right angles are equal to each other.
- 5: The **parallel postulate**: Given a line and a point off that line, there is exactly one line passing through the point, which does not intersect the first line.

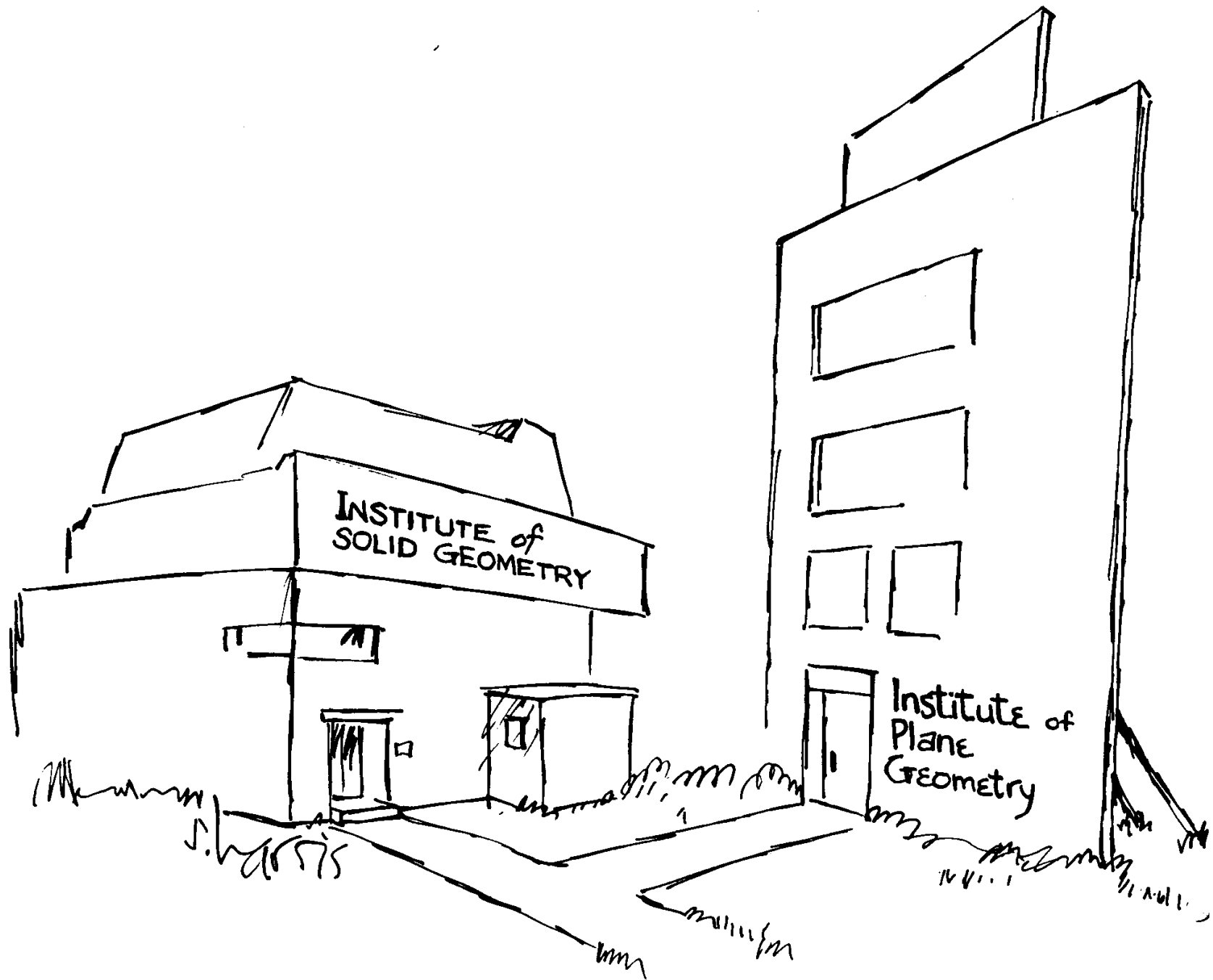
The first 28 propositions of Euclid's Elements were proven without using the parallel postulate!

**Theorem** [Beltrami, 1868]: The parallel postulate is **independent** of the other axioms of Euclidean geometry.

The parallel postulate can be **modified** to yield **non-Euclidean geometries**!







INSTITUTE of  
SOLID GEOMETRY

Institute of  
Plane  
Geometry

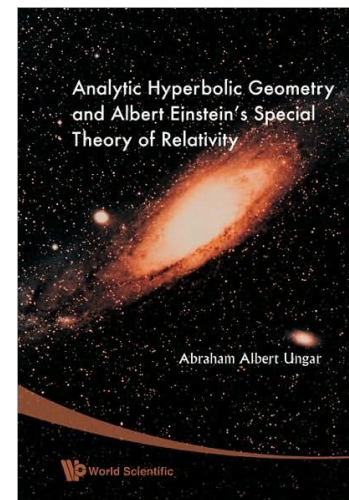
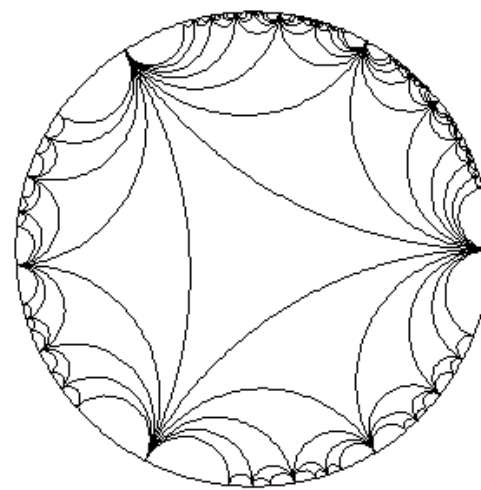
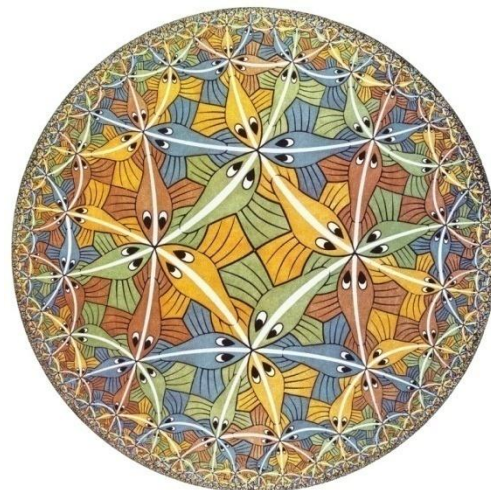
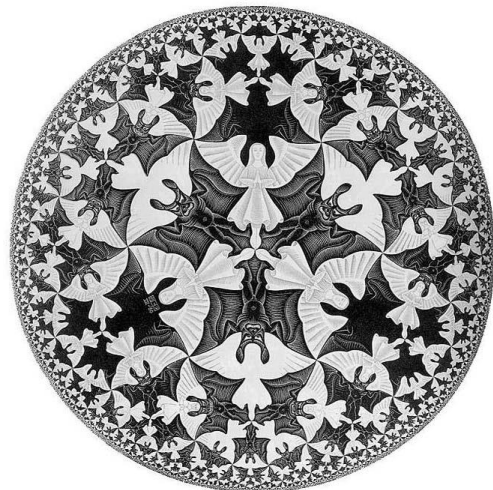
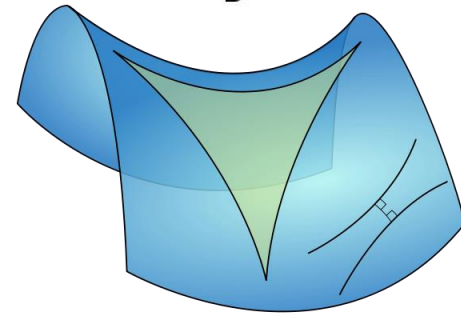
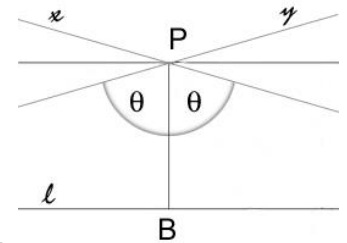
S. S. S. S.

14.11.11

# Non-Euclidean Geometries

**Hyperbolic geometry:** Given a line and a point off that line, there are an **infinity of lines** passing through that point that do not intersect the first line.

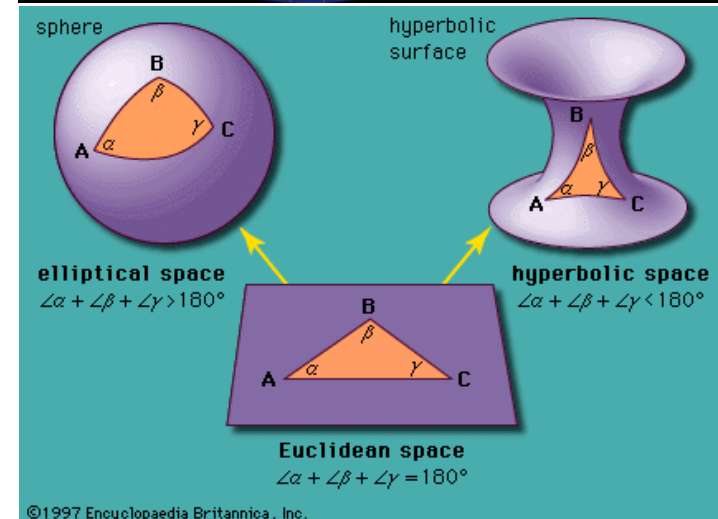
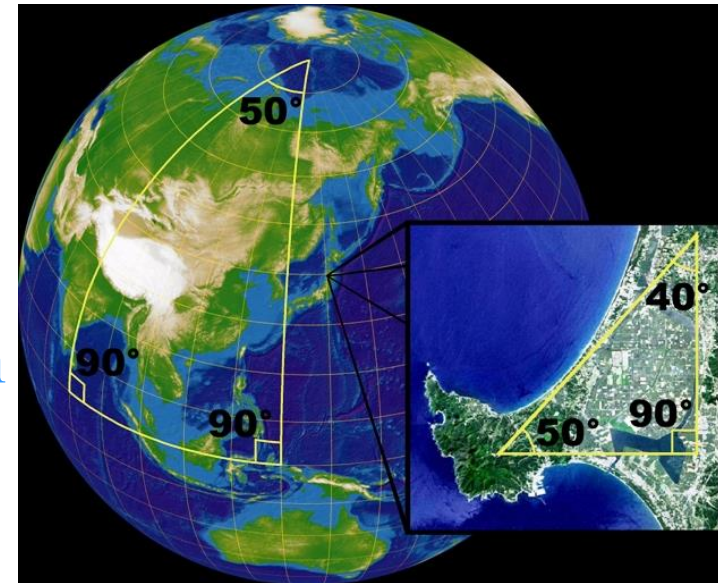
- Sum of triangle angles is less than  $180^\circ$
- Not all triangles have the same angle sum
- Triangles with same angles have same area
- There are no similar triangles
- Used in relativity theory



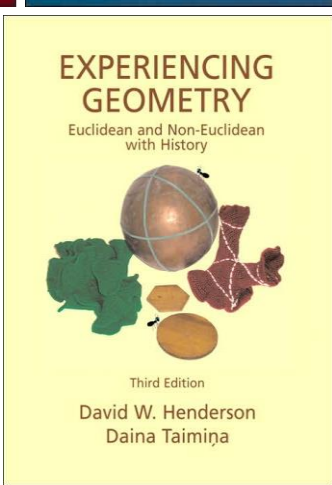
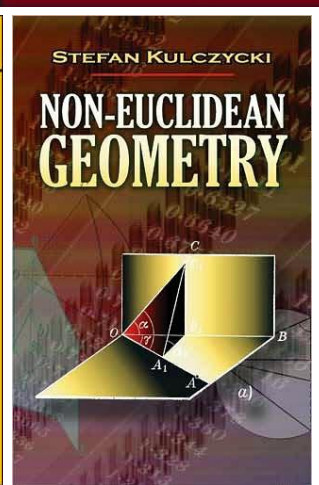
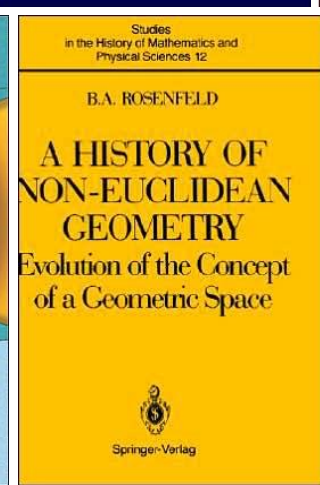
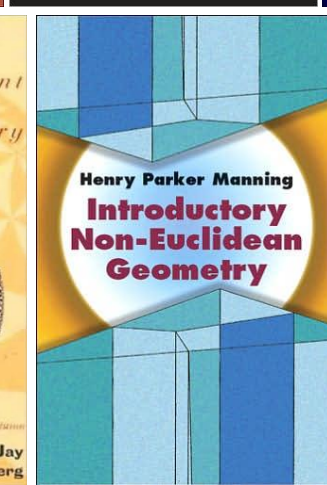
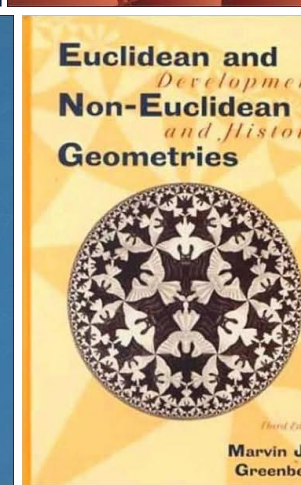
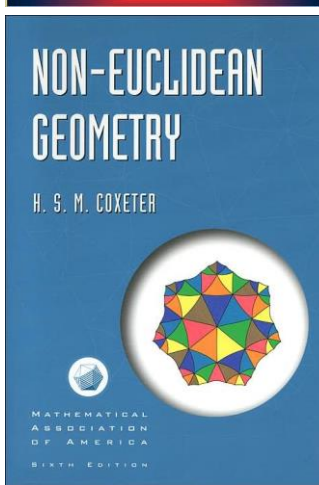
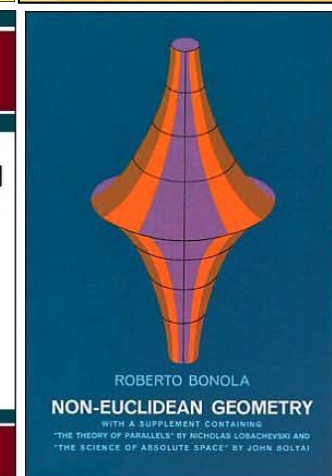
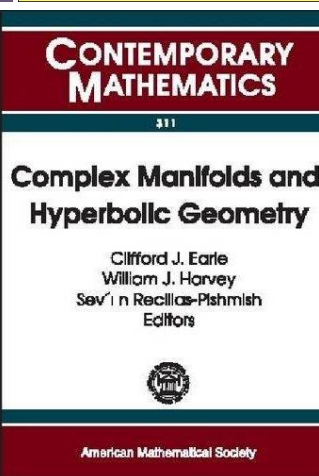
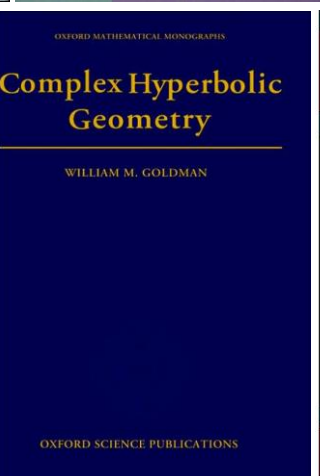
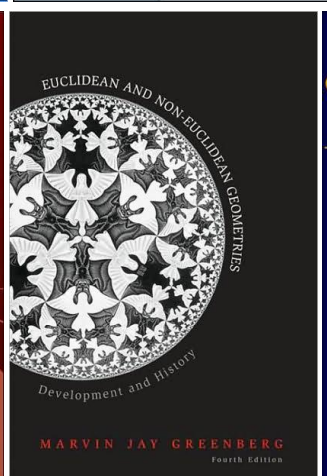
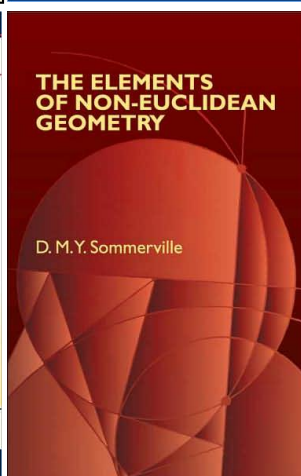
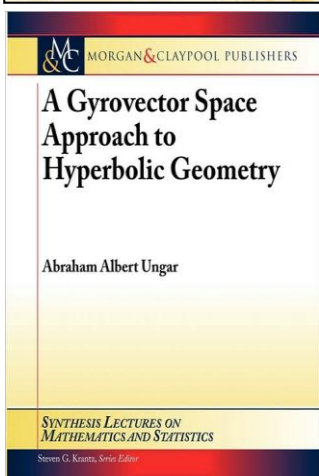
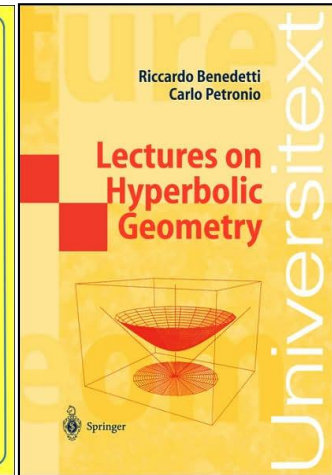
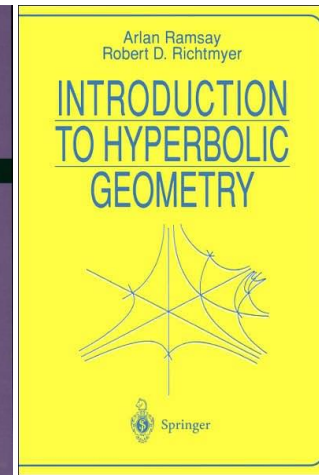
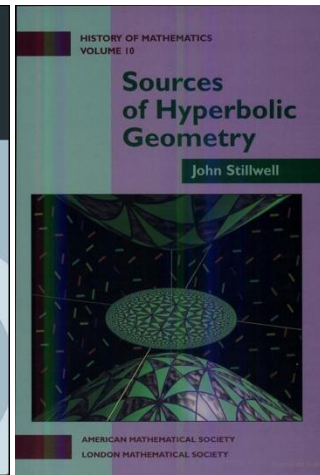
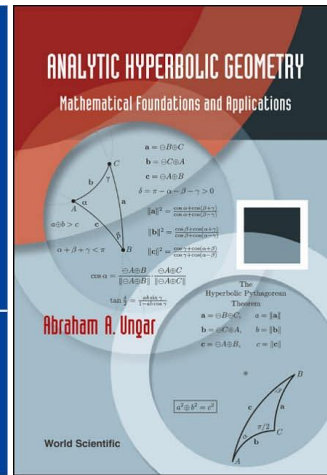
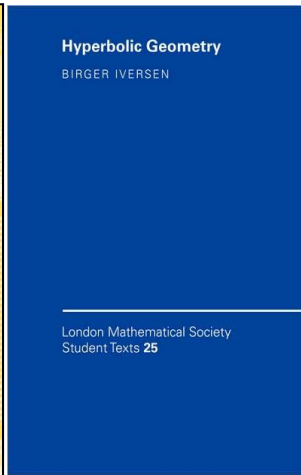
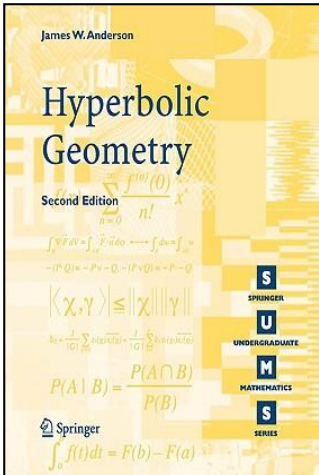
# Non-Euclidean Geometries

**Spherical / Elliptic geometry:** Given a line and a point off that line, there are **no lines** passing through that point that do not intersect the first line.

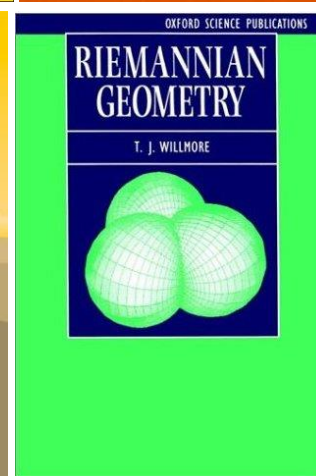
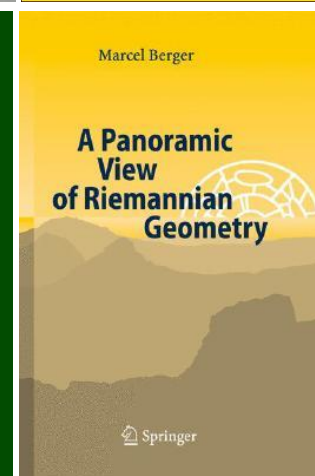
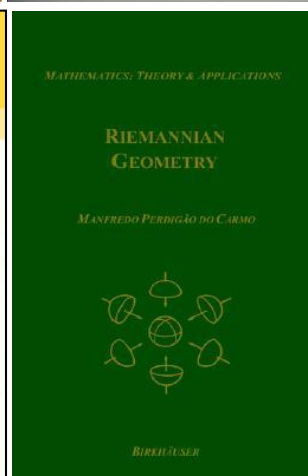
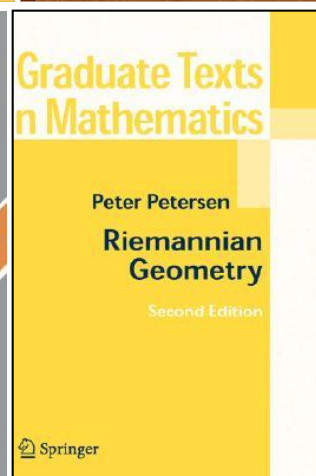
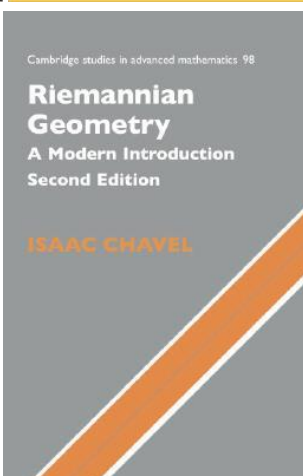
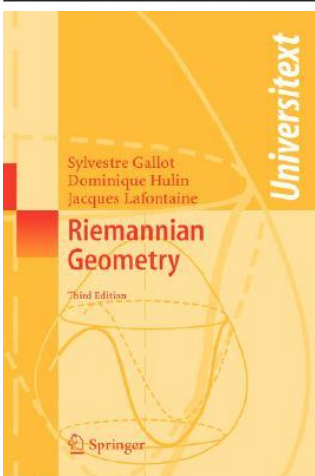
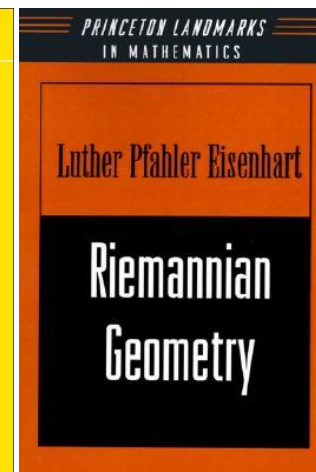
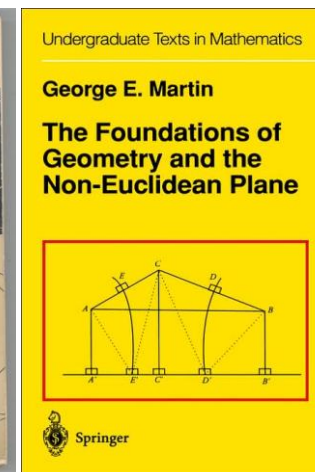
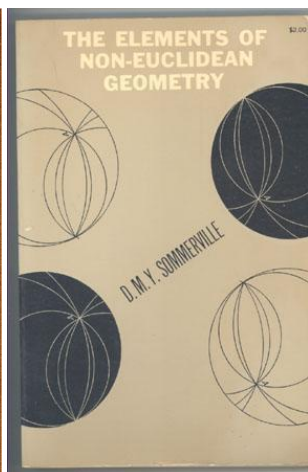
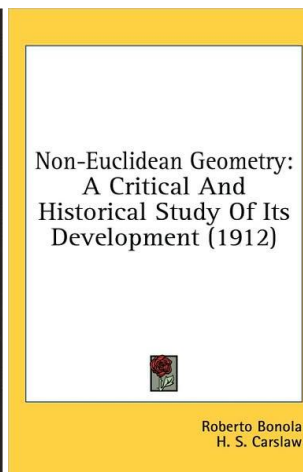
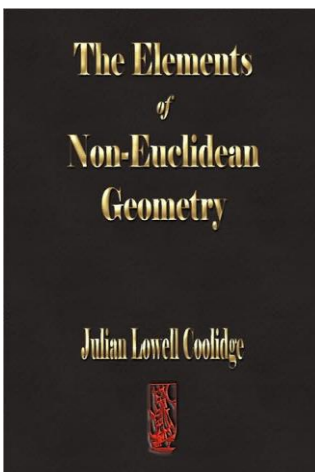
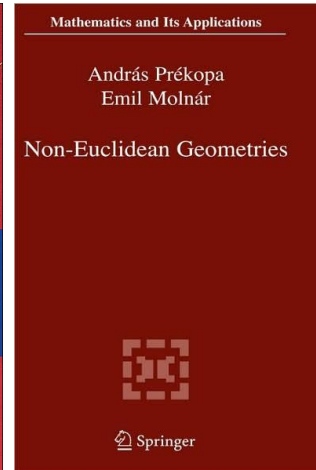
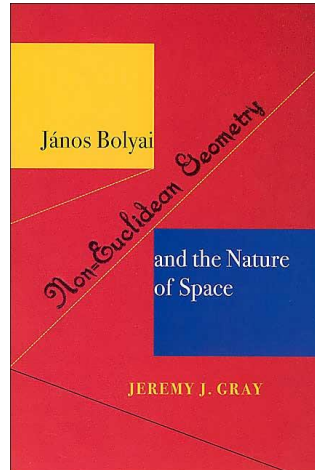
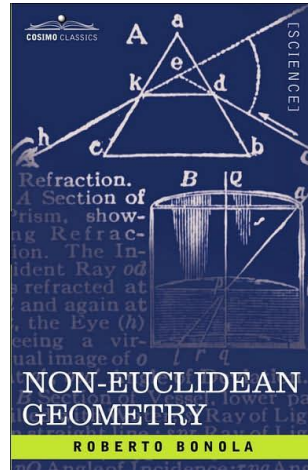
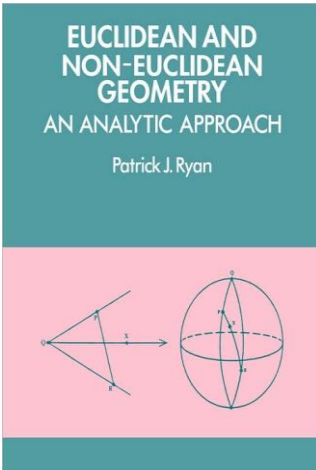
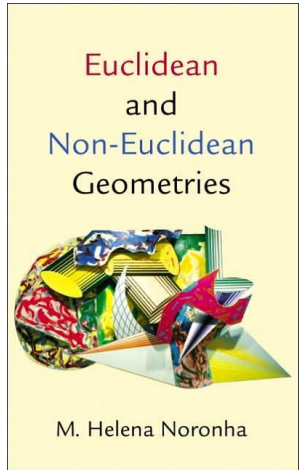
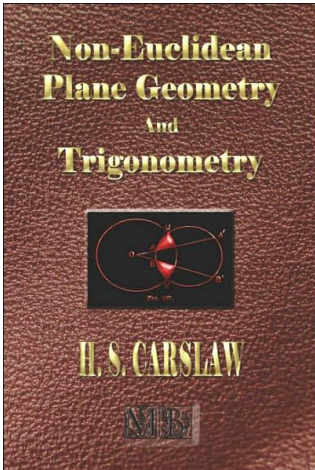
- Lines are **geodesics** - “great circles”
- Sum of triangle angles is  $> 180^\circ$
- Not all triangles have same **angle sum**
- Figures can not scale up indefinitely
- **Area** does not scale as the **square**
- **Volume** does not scale as the **cube**
- The **Pythagorean theorem** fails
- **Self-consistent**, and **complete**







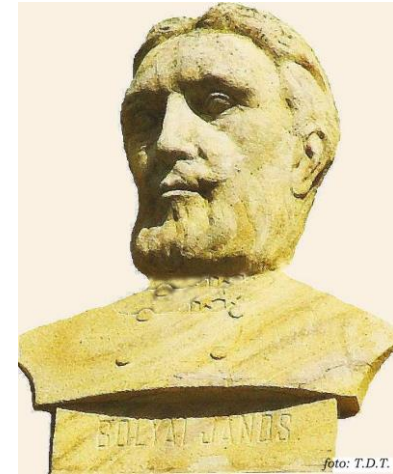
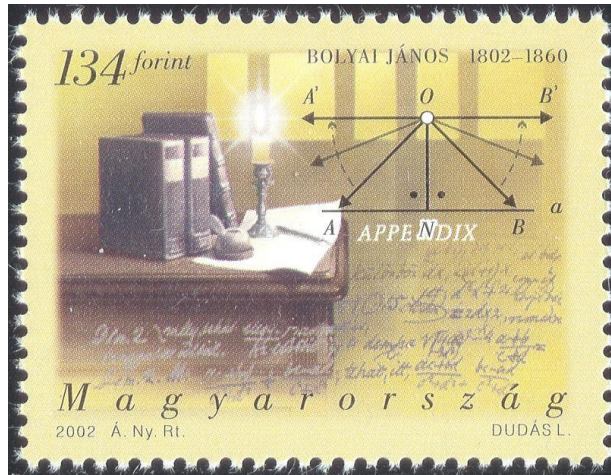




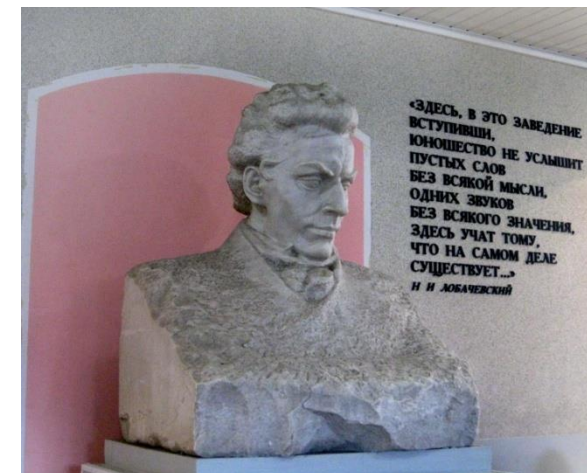


# Founders of Non-Euclidean Geometry

János **Bolyai** (1802-1860)

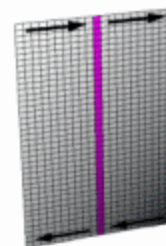
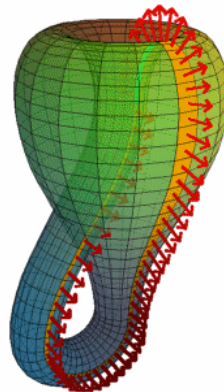
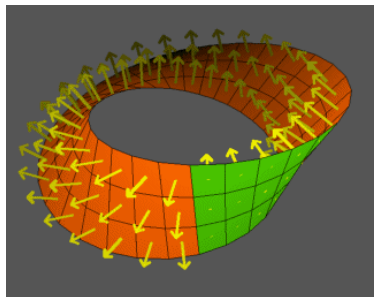
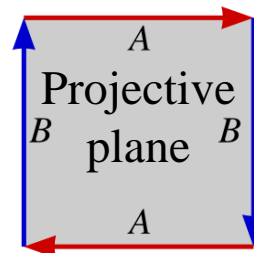
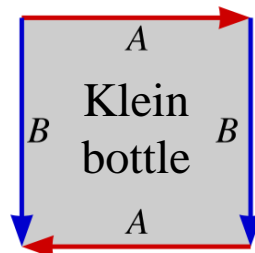
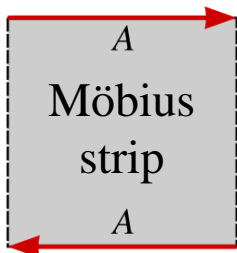


Nikolai Ivanovich **Lobachevsky** (1792-1856)

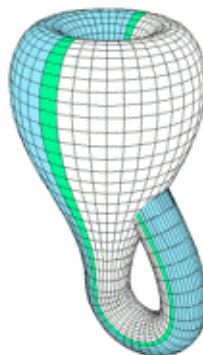
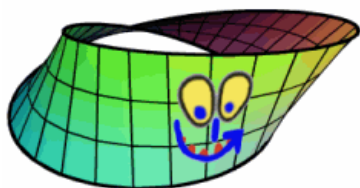




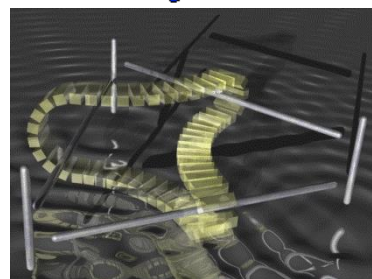
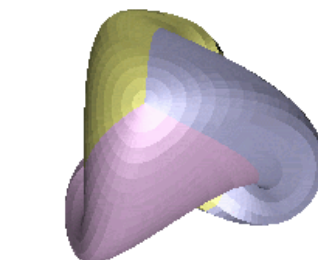
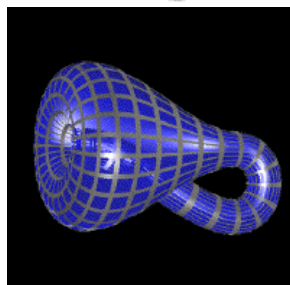
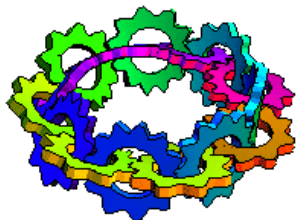
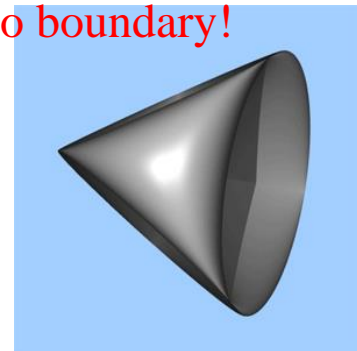
# Non-Euclidean Non-Orientable Surfaces



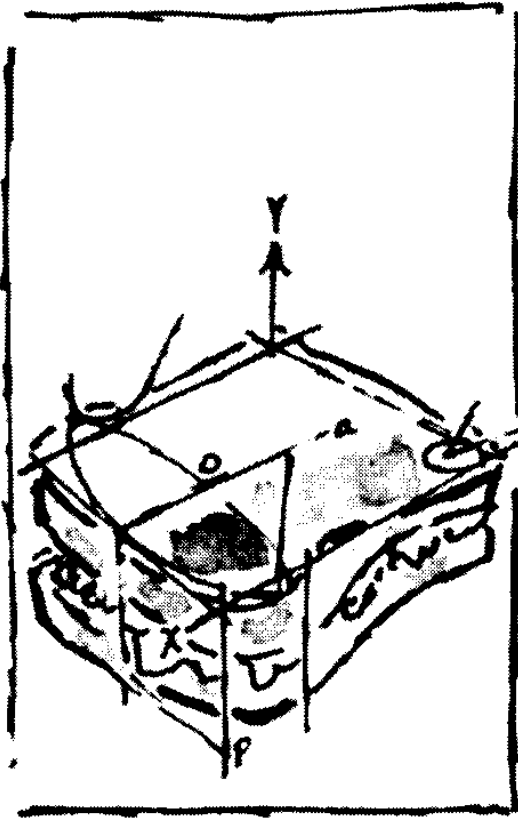
one side,  
no boundary!



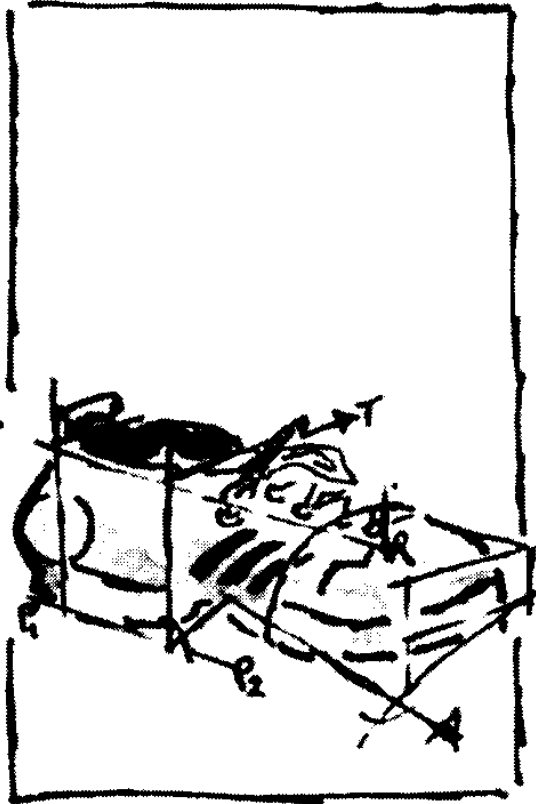
one side,  
no boundary!



# THE GEOMETRY OF EVERYDAY LIFE



TUNA SANDWICH



SNEAKER

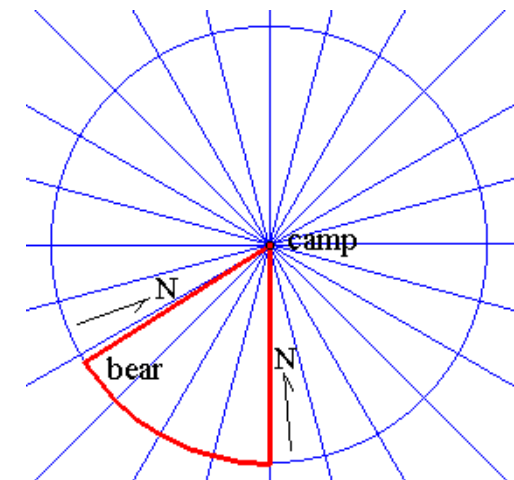


GRANDMA

sharis



**Problem:** A man leaves his house and walks one mile south. He then walks one mile west and sees a Bear. Then he walks one mile north back to his house. What color was the bear?



**Problem:** Is the house location unique?