

Theory of Computation CS3102– Spring 2011

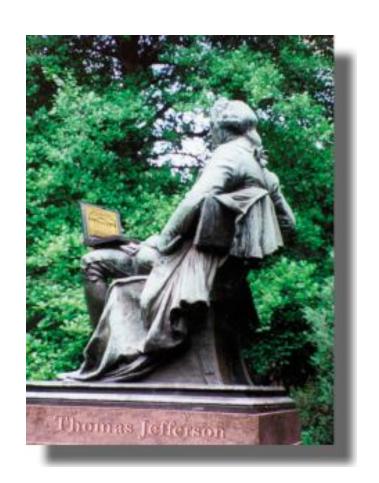
Gabriel Robins

Department of

Computer Science

University of Virginia

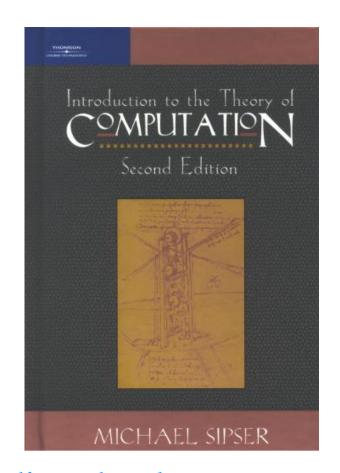
www.cs.virginia.edu/robins/theory



Theory of Computation (CS3102) - Textbook

Textbook:

Introduction to the Theory of Computation, by Michael Sipser (MIT), 2nd Edition, 2006



Good Articles / videos:

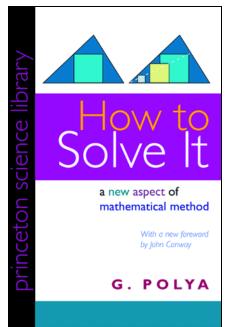
www.cs.virginia.edu/~robins/CS_readings.html

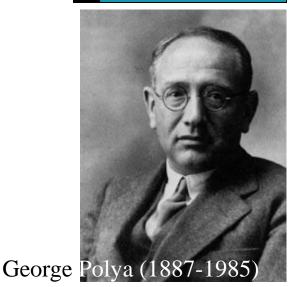
Theory of Computation (CS3102)

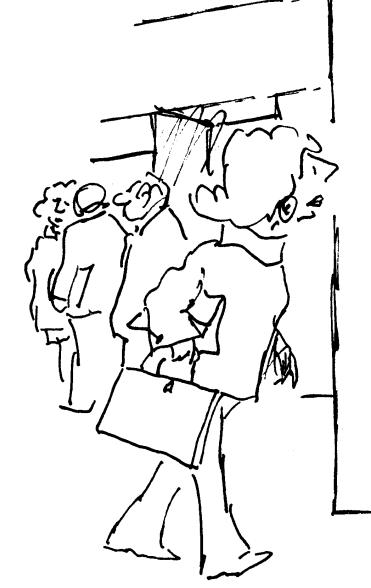
Supplemental reading:

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

A classic on problem solving







SCHOOL OF OLOGY

ANTHROP 301

ARCHAE 126

BACTERI 109

BI 326

ENTOM 217

ETYM 221

GE 204

PALEONT 113

PHYSI 312

PSYCH 2019

TOXIC 307

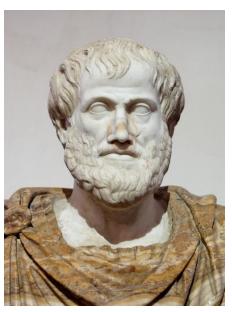
三

J. 45

Theory of Computation (CS3102) - Syllabus

A brief history of computing:

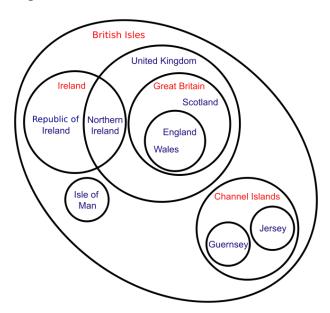
- Aristotle, Euclid, Archimedes, Eratosthenes
- Abu Ali al-Hasan ibn al-Haytham
- Fibonacci, Descartes, Fermat, Pascal
- Newton, Euler, Gauss, Hamilton
- Boole, De Morgan, Babbage, Ada Agusta
- Venn, Carroll, Cantor, Hilbert, Russell
- Hardy, Ramanujan, Ramsey
- Godel, Church, Turing, von Neumann
- Shannon,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

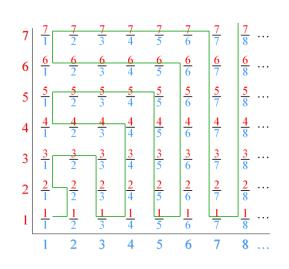




Fundamentals:

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

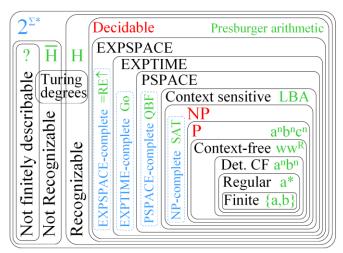


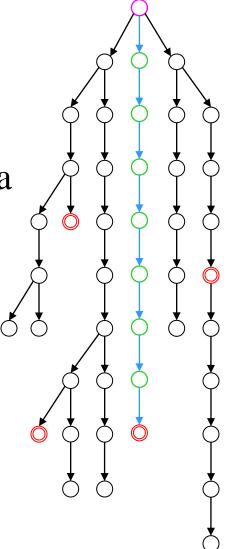


Formal languages and machine models:

- 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

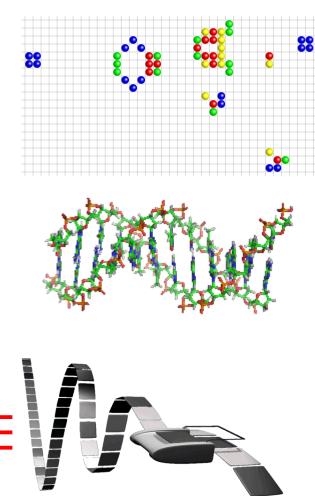
The Extended Chomsky Hierarchy





Computability and undecidability:

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

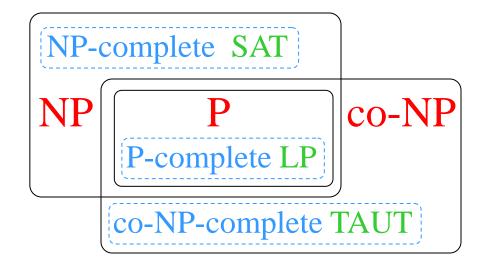


NP-completeness:

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



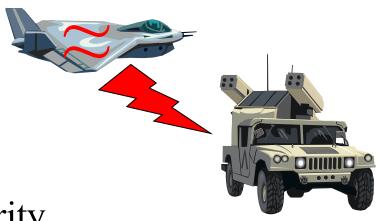


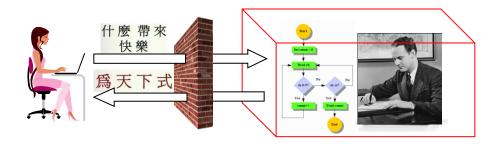


Other topics (as time permits):

- 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

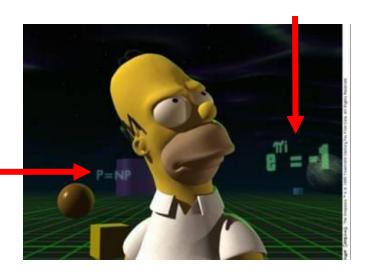


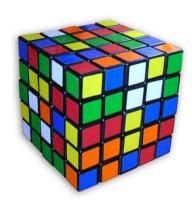




Overarching Philosophy

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

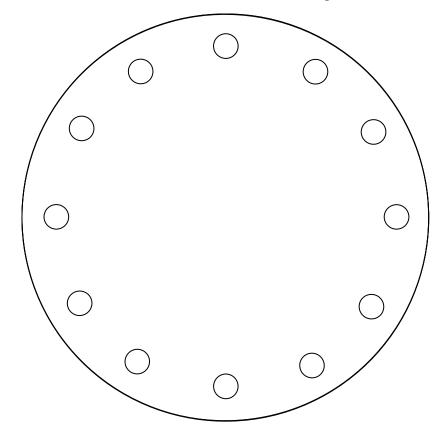






Problem: Can 5 test tubes be spun simultaneously in a 12-hole centrifuge in a balanced way?





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

Prerequisites

Some discrete math & algorithms knowldege

• Ideally, should have taken CS2102

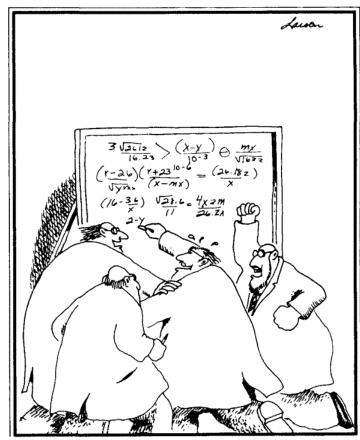
Course will "bootstrap"
 (albeit quickly) from first principles

• 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
 - Many exam questions will come from homeworks!
- 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



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

Grading Scheme

• Midterm 35%

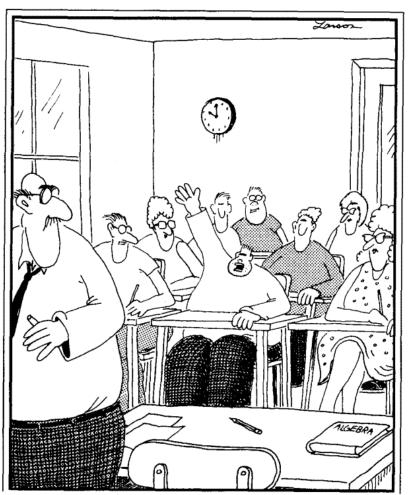
• Final 35%

• Project 30%

• Extra credit 10%

Best strategy:

Solve lots of problems!



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

Contact Information

Professor Gabriel Robins

Office: 210 Olsson Hall

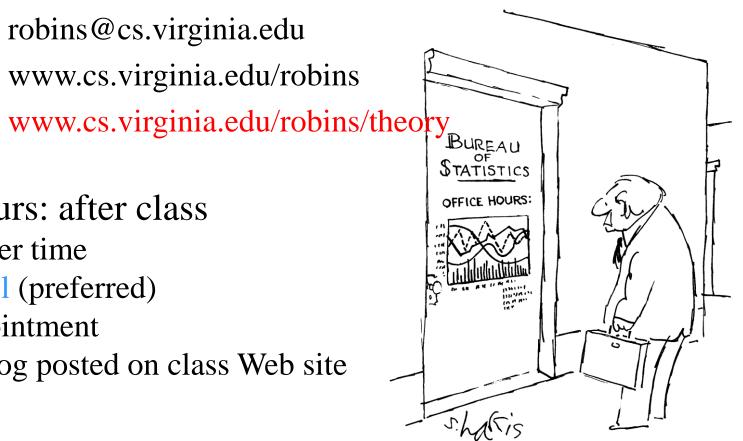
Phone: (434) 982-2207

Email: robins@cs.virginia.edu

www.cs.virginia.edu/robins Web:

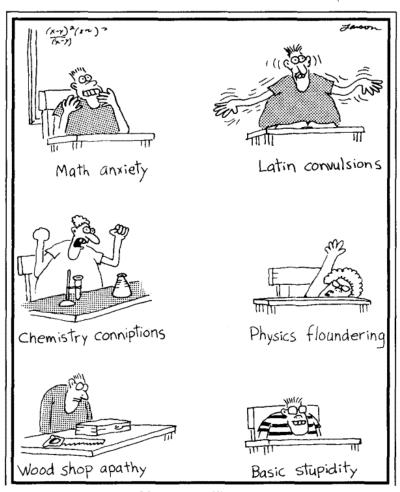
Office hours: after class

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



Good Advice

- Ask questions ASAP
- Do homeworks ASAP
- Work in study groups
- Do not fall behind
- "Cramming" won't work
- Start on project early
- Attend every lecture
- Read Email often
- Solve lots of problems



Classroom afflictions

www.cs.virginia.edu/robins/CS_readings.html

• Great videos:

- Randy Pausch's "Last Lecture", 2007
- Randy Pausch's "Time Management", 2007
- "Powers of Ten", Charles and Ray Eames, 1977





























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.

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.

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.

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 Poweder, Tim Hornyak, Scientific American, February 2008, pp. 68-71.
- Can Phishing be Foiled, Lorrie Cranor, Scientific American,
 December 2008, pp. 104-110.

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.

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

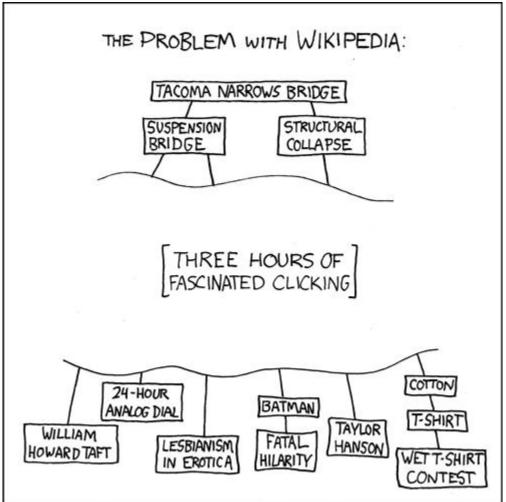


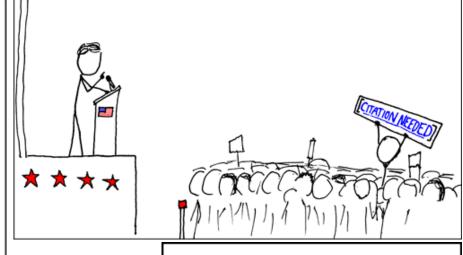
www.cs.virginia.edu/robins/CS_readings.html

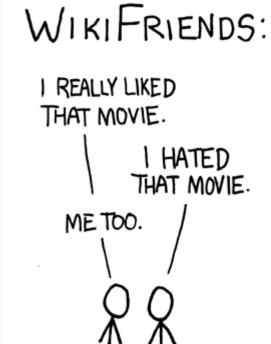
- The Wikipedia Math Portal:
 - Problem solving
 - List of Mathematical lists
 - Sets and Infinity
 - Discrete mathematics
 - Proof techniques and list of proofs
 - Information theory & randomness
 - Game theory
- Mathematica's "Math World"











Historical Perspectives



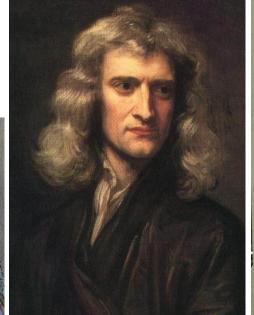
Historical Perspectives

- 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 Agusta
- Venn, Carroll



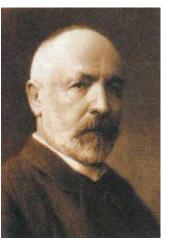




"Standing on the Shoulders of Giants"

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

Many others...









Curie Galileo G. Pasteur



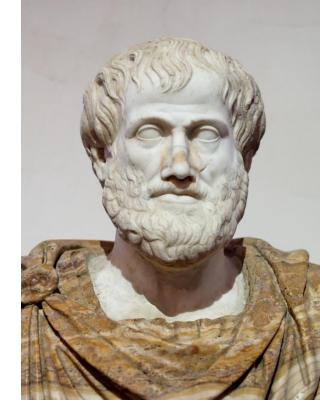
MAKING PHILOSOPHY ACCESSIBLE: POP-UP PLATO



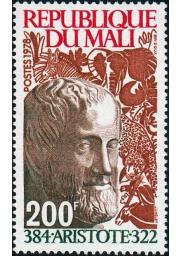
Historical Perspectives

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









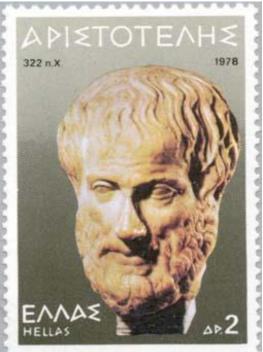


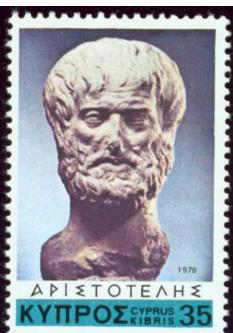




- Aristotle (384-322 B.C.)

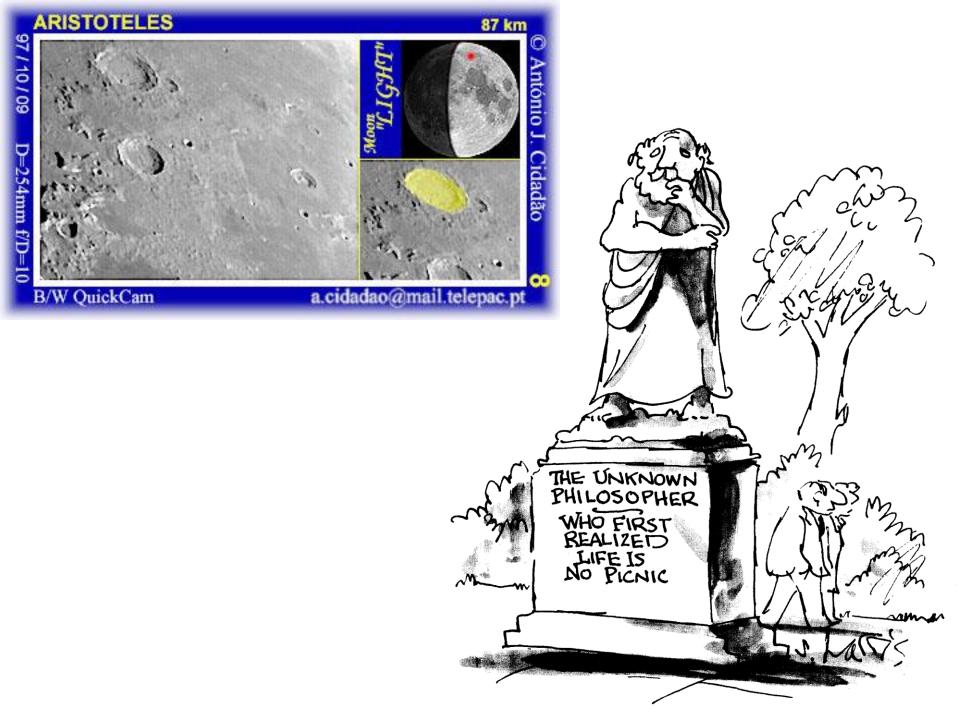








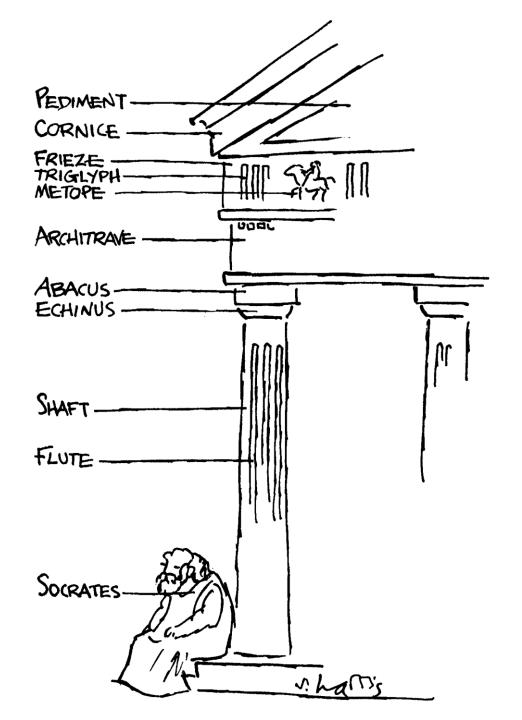








"What I especially like about being a philosopher-scientist is that I don't have to get my hands dirty."



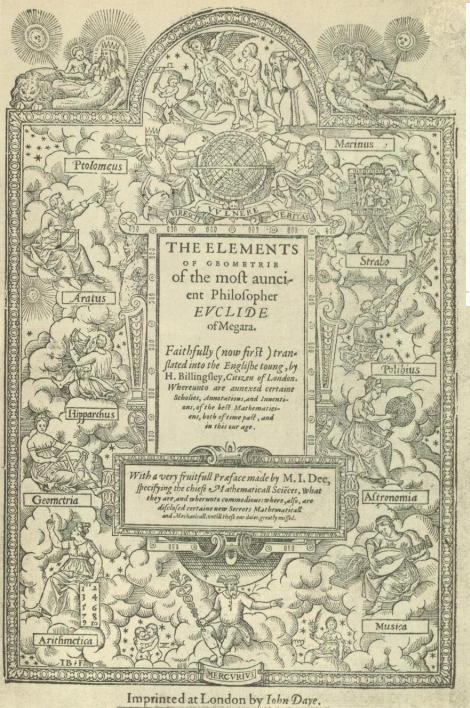
Historical Perspectives

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

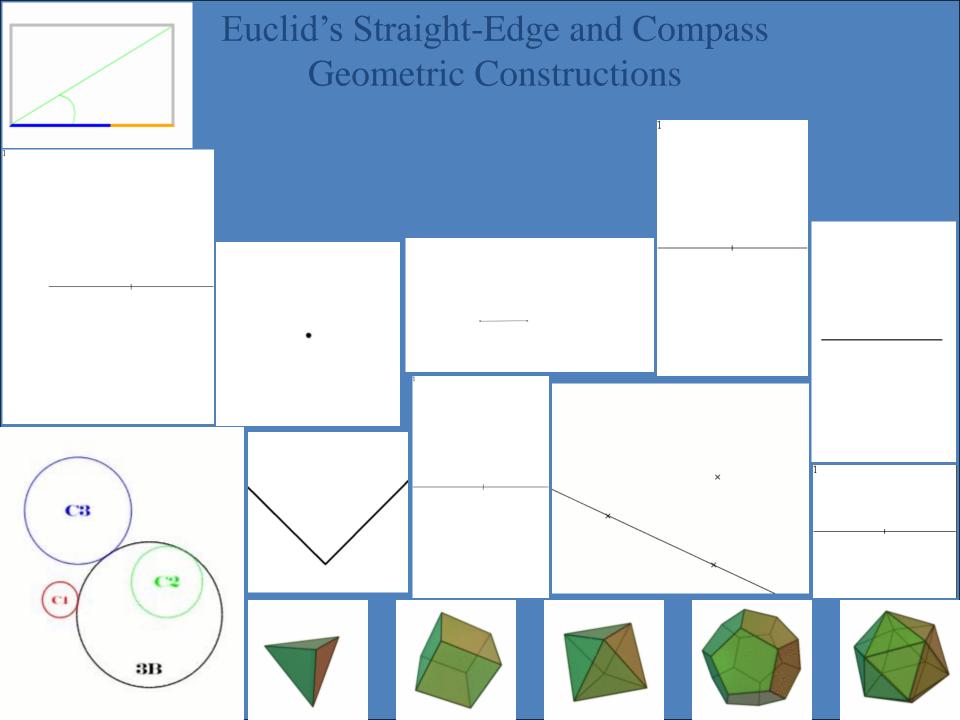








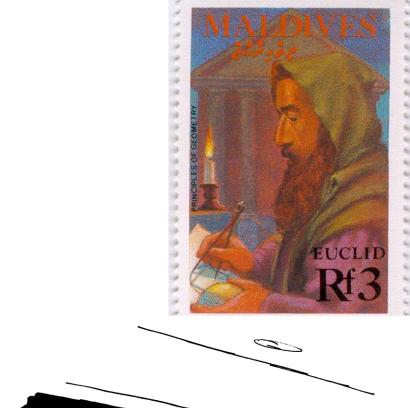


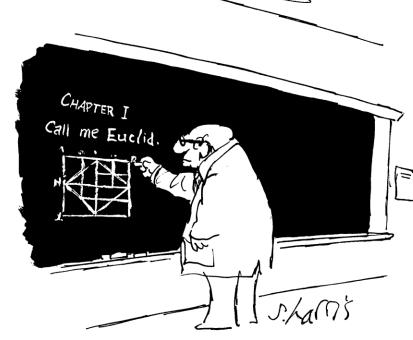












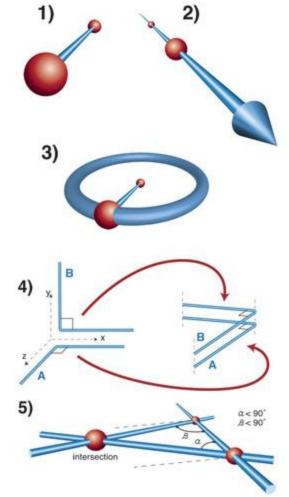
Euclid's Axioms

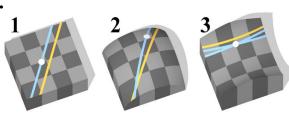
- 1: Any two points can be connected by exactly one straight line.
- 2: Any segment can be extended indefinitely into a straight line.
- 3: A circle exists for any given center and radius.
- 4: All right angles are equal to each other.
- 5: The parallel postulate: Given a line and a point off that line,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

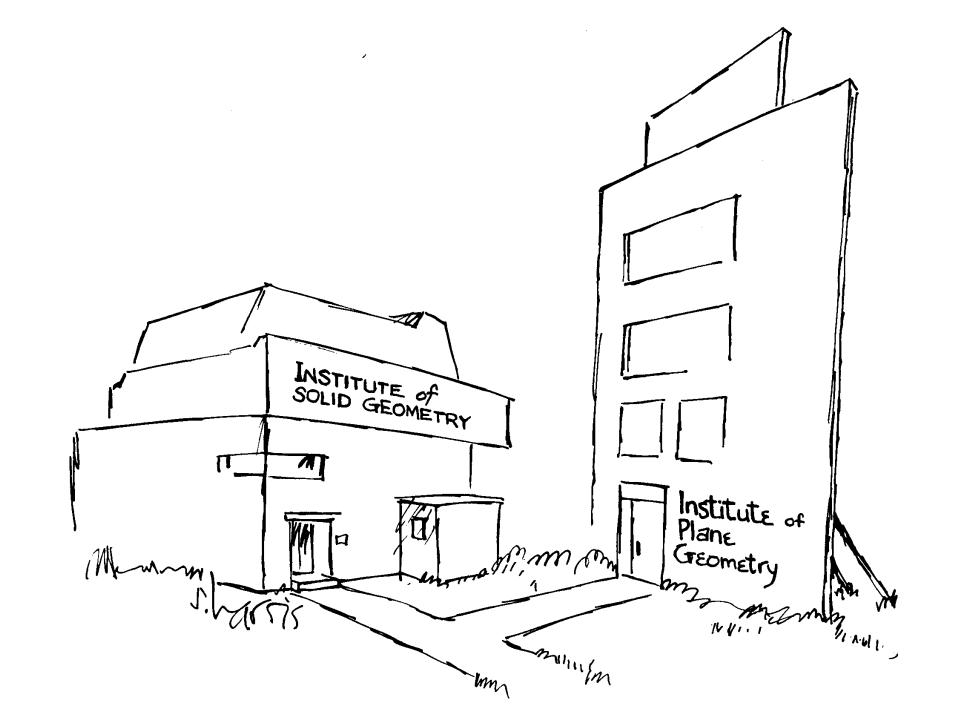
The first 28 propositions of Euclid's Elements were proven without using the parallel postulate!

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!



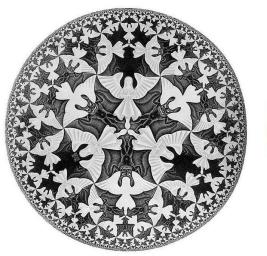




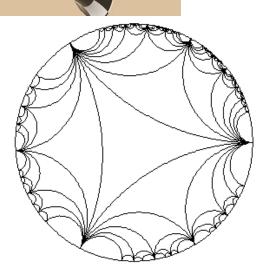
Non-Euclidean Geometries

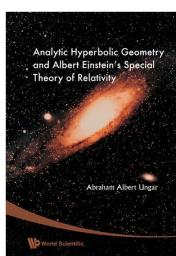
Hyperbolic geometry: Given a line and a point off that line, there are an infinity of lines passing through that point that do not intersect the first line.

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







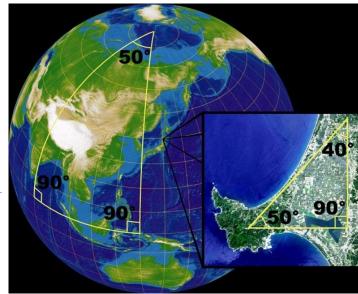


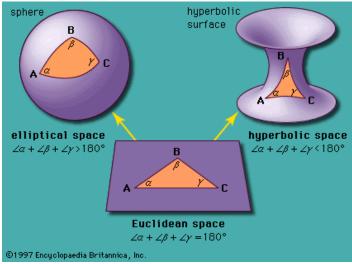
Non-Euclidean Geometries

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





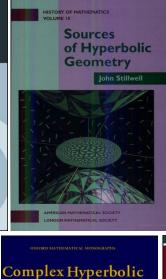


James W. Anderson

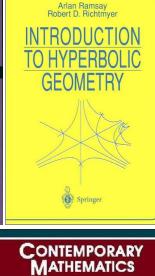


Hyperbolic Geometry





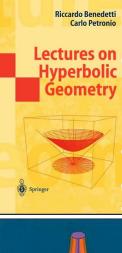
Geometry

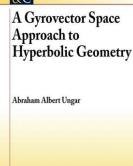


Complex Manifolds and Hyperbolic Geometry

Clifford J. Earle

William J. Harvey Sev'ı n Recilias-Pishmish



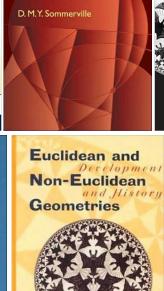


SYNTHESIS LECTURES ON MATHEMATICS AND STATISTICS

NON-EUCLIDEAN

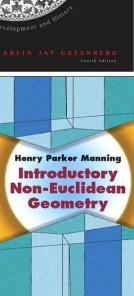
GEOMETRY

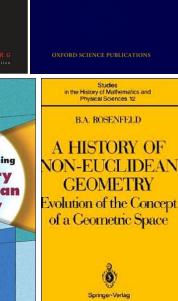
H. S. M. COXETER



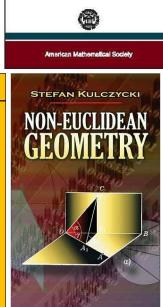
Marvin Jay Greenberg

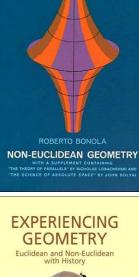
THE ELEMENTS OF NON-EUCLIDEAN GEOMETRY









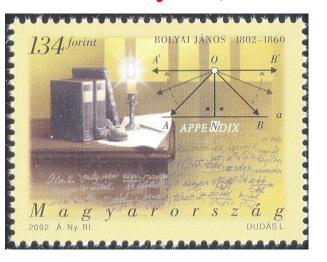






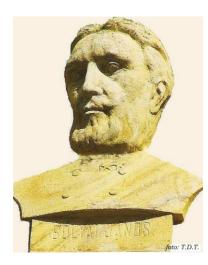
Founders of Non-Euclidean Geometry

János Bolyai (1802-1860)









Nikolai Ivanovich Lobachevsky (1792-1856)

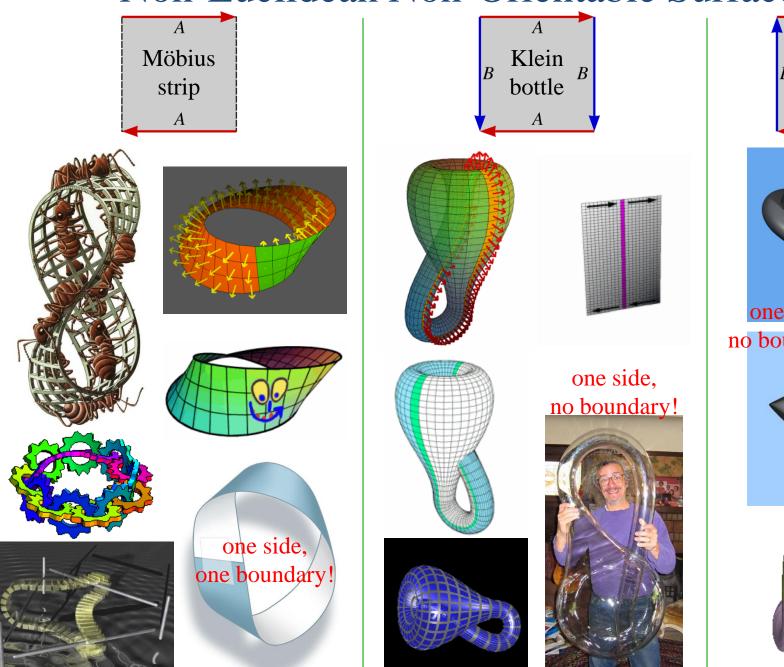


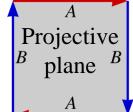


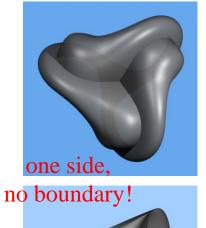


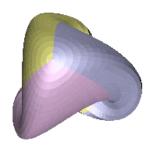


Non-Euclidean Non-Orientable Surfaces

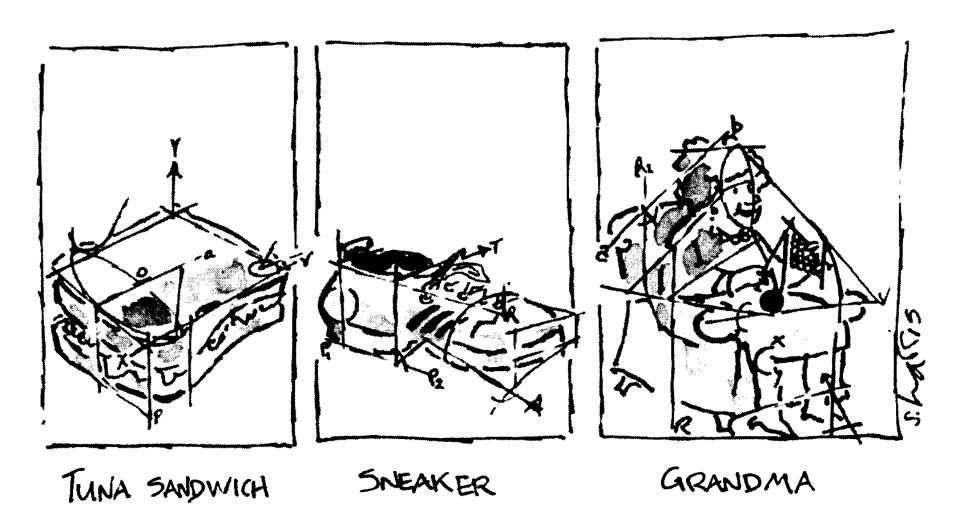








THE GEOMETRY OF EVERYDAY LIFE



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?

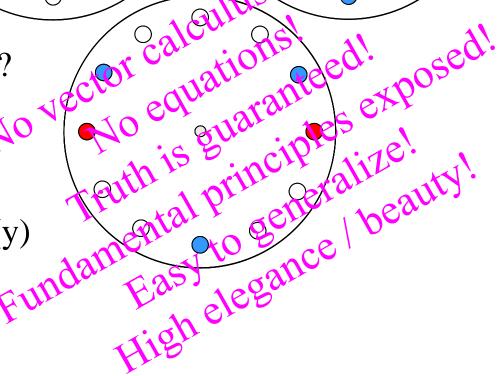
Problem: Can 5 test tubes be spun simultaneously in a

12-hole centrifuge in a balanced way?





- 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...



Problem:
$$1 + 2 + 3 + 4 + ... + 100 = ?$$

Proof: Induction...

=(100*101)/2

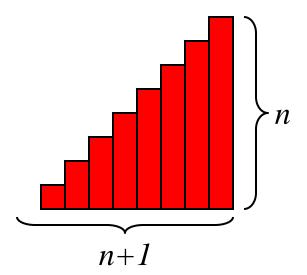
=5050

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

$$100 + 99 + 98 + ... + 2 + 1$$

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

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



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



I.e., almost never!

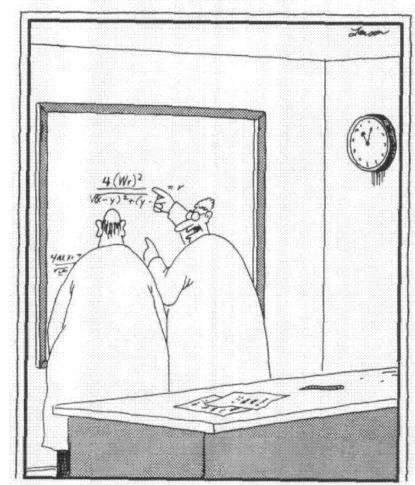


Problem: $1^3 + 2^3 + 3^3 + 4^3 + ... + n^3 = ?$

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

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: $(1/8) + (1/8)^2 + (1/8)^3 + (1/8)^4 + ... = ?$

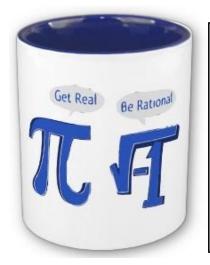
$$\sum_{i=1}^{\infty} \frac{1}{8^i} = ?$$

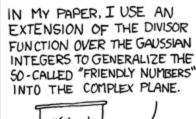
Extra Credit:

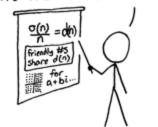
Find a short, geometric, induction-free proof.

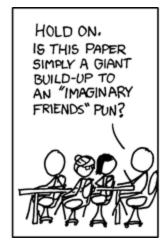
Problem: Are the complex numbers closed under exponentiation? E.g., what is the value of iⁱ?

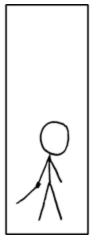


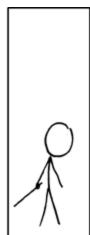


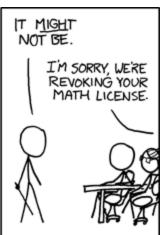












Problem: Prove that there are an infinity of primes.

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

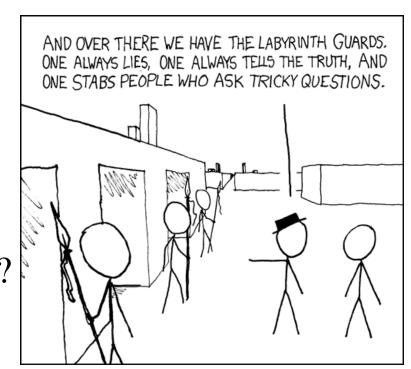
- What approaches fail?
- What techniques work and why?
- Lessons and generalizations



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

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

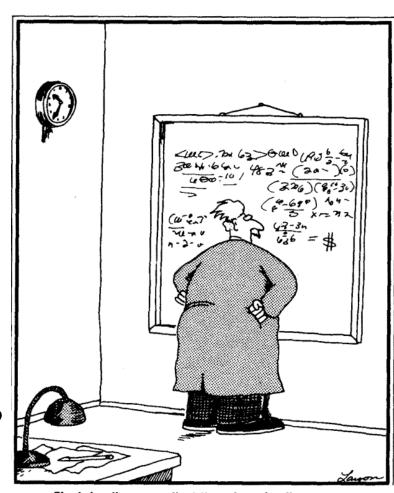
- What approaches fail?
- What techniques work and why?
- Lessons and generalizations



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

