

# Foreword

By Reuben Hersh

Every November, some thousand middle- and high-school students in dozens of schools all over New Mexico gather to spend up to three hours playing and struggling with a set of elementary but tricky math problems. It's Round One of the New Mexico High School Math Contest. Then, the following February, the highest-scoring two hundred or so are invited to the campus of the University of New Mexico in Albuquerque. They hear a talk by a famous mathematician (Paul Erdős, Peter Lax, John Conway, Serge Lang, Bill Thurston, and Ron Graham have done it), have lunch, and then dig in to Round Two, a more rigorous and demanding set of mathematical mind-twisters.

In April, at a banquet in Albuquerque, prizes are awarded by grades from seventh to twelfth. Top prizes are books, money and scholarships. Everybody who does the second round gets a free T-shirt, such as the one I am wearing as I write this.

For many students, this contest has led to steps, decisions, and, ultimately, successful careers in mathematics and science. Some parents sing the praises of an event, uncommon in parts of our state, that publicizes and glorifies the work of the mind (a kind of activity not always and everywhere rewarded among high-school kids in the present day U.S.).

All this takes time and money. At the first round, local teachers volunteer as coaches and proctors. At the second round and for the grading, faculty and graduate students at the University of New Mexico volunteer. The costs of the banquet and the prizes are graciously met by the PNM Foundation. The University of New Mexico contributes the use of its facilities and perhaps part-time release from teaching for a faculty member responsible for organizing all this.

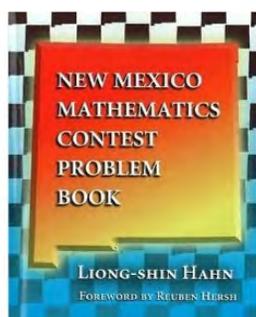
The key element, of course, is the questions themselves. They must be attractive, intriguing, and

suggestive to teenage contestants. They must require an insight, a spark, beyond routine application of a standard recipe. They must be solvable with no knowledge beyond that to be expected of a high-school student. And they should be original, not retreads of familiar chestnuts in old problem books. Such are the creations of Liong-shin Hahn—"L.S.," as he allows himself to be called by those who are shy of pronouncing his full name. Rather than cite examples, I invite you to open this book and read from any page.

The New Mexico Mathematics Contest is part of a long tradition with roots in Hungary; the story brings together mathematicians from three continents. The recently retired director of the contest, Professor Liong-shin Hahn, whose remarkable collection of problems you are now holding, was born in 1932 in Taiwan into a family of physicians. He calls himself a "black sheep" for having strayed into mathematics. He got his Ph.D. at Stanford in 1966 with Karel deLeeuw, was an instructor at Johns Hopkins, and came to New Mexico in 1968.

In 1998 Professor Hahn received the "Citation for Public Service" from the American Mathematical Society at their national meeting in Baltimore. The citation says, "Professor Hahn is being honored for carrying forward and developing the New Mexico High School Mathematics Contest and for exposition and popularization of mathematics attractive and suitable for potential candidates for the contest and others with similar intellectual interest." The reference to exposition and publication recognizes Hahn's two excellent books, *Classical Complex Analysis* (with Bernard Epstein) and *Complex Numbers and Geometry*. The latter is an original unique work, easily accessible to high-school students and teachers.

The history of the contest can be traced back to 1894, when a "Pupils' Mathematical Competition" was established by the Mathematical and Physical Society of Hungary. It became one of the decisive influences that made tiny Hungary one of the major contributors to twentieth-century mathematics. For decades the contest was known as the Eötvös Competition, in honor of the Society's founder and president, the physicist and Minister of Education, Baron Loránd



# Foreword

By Reuben Hersh

Every November, some thousand middle- and high-school students in dozens of schools all over New Mexico gather to spend up to three hours playing and struggling with a set of elementary but tricky math problems. It's Round One of the New Mexico High School Math Contest. Then, the following February, the highest-scoring two hundred or so are invited to the campus of the University of New Mexico in Albuquerque. They hear a talk by a famous mathematician (Paul Erdős, Peter Lax, John Conway, Serge Lang, Bill Thurston, and Ron Graham have done it), have lunch, and then dig in to Round Two, a more rigorous and demanding set of mathematical mind-twisters.

In April, at a banquet in Albuquerque, prizes are awarded by grades from seventh to twelfth. Top prizes are books, money and scholarships. Everybody who does the second round gets a free T-shirt, such as the one I am wearing as I write this.

For many students, this contest has led to steps, decisions, and, ultimately, successful careers in mathematics and science. Some parents sing the praises of an event, uncommon in parts of our state, that publicizes and glorifies the work of the mind (a kind of activity not always and everywhere rewarded among high-school kids in the present day U.S.).

All this takes time and money. At the first round, local teachers volunteer as coaches and proctors. At the second round and for the grading, faculty and graduate students at the University of New Mexico volunteer. The costs of the banquet and the prizes are graciously met by the PNM Foundation. The University of New Mexico contributes the use of its facilities and perhaps part-time release from teaching for a faculty member responsible for organizing all this.

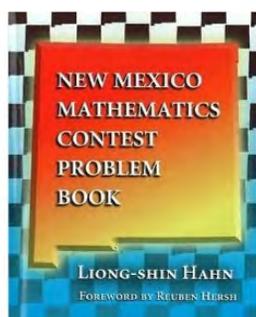
The key element, of course, is the questions themselves. They must be attractive, intriguing, and

suggestive to teenage contestants. They must require an insight, a spark, beyond routine application of a standard recipe. They must be solvable with no knowledge beyond that to be expected of a high-school student. And they should be original, not retreads of familiar chestnuts in old problem books. Such are the creations of Liong-shin Hahn—"L.S.," as he allows himself to be called by those who are shy of pronouncing his full name. Rather than cite examples, I invite you to open this book and read from any page.

The New Mexico Mathematics Contest is part of a long tradition with roots in Hungary; the story brings together mathematicians from three continents. The recently retired director of the contest, Professor Liong-shin Hahn, whose remarkable collection of problems you are now holding, was born in 1932 in Taiwan into a family of physicians. He calls himself a "black sheep" for having strayed into mathematics. He got his Ph.D. at Stanford in 1966 with Karel deLeeuw, was an instructor at Johns Hopkins, and came to New Mexico in 1968.

In 1998 Professor Hahn received the "Citation for Public Service" from the American Mathematical Society at their national meeting in Baltimore. The citation says, "Professor Hahn is being honored for carrying forward and developing the New Mexico High School Mathematics Contest and for exposition and popularization of mathematics attractive and suitable for potential candidates for the contest and others with similar intellectual interest." The reference to exposition and publication recognizes Hahn's two excellent books, *Classical Complex Analysis* (with Bernard Epstein) and *Complex Numbers and Geometry*. The latter is an original unique work, easily accessible to high-school students and teachers.

The history of the contest can be traced back to 1894, when a "Pupils' Mathematical Competition" was established by the Mathematical and Physical Society of Hungary. It became one of the decisive influences that made tiny Hungary one of the major contributors to twentieth-century mathematics. For decades the contest was known as the Eötvös Competition, in honor of the Society's founder and president, the physicist and Minister of Education, Baron Loránd



# Foreword

By Reuben Hersh

Every November, some thousand middle- and high-school students in dozens of schools all over New Mexico gather to spend up to three hours playing and struggling with a set of elementary but tricky math problems. It's Round One of the New Mexico High School Math Contest. Then, the following February, the highest-scoring two hundred or so are invited to the campus of the University of New Mexico in Albuquerque. They hear a talk by a famous mathematician (Paul Erdős, Peter Lax, John Conway, Serge Lang, Bill Thurston, and Ron Graham have done it), have lunch, and then dig in to Round Two, a more rigorous and demanding set of mathematical mind-twisters.

In April, at a banquet in Albuquerque, prizes are awarded by grades from seventh to twelfth. Top prizes are books, money and scholarships. Everybody who does the second round gets a free T-shirt, such as the one I am wearing as I write this.

For many students, this contest has led to steps, decisions, and, ultimately, successful careers in mathematics and science. Some parents sing the praises of an event, uncommon in parts of our state, that publicizes and glorifies the work of the mind (a kind of activity not always and everywhere rewarded among high-school kids in the present day U.S.).

All this takes time and money. At the first round, local teachers volunteer as coaches and proctors. At the second round and for the grading, faculty and graduate students at the University of New Mexico volunteer. The costs of the banquet and the prizes are graciously met by the PNM Foundation. The University of New Mexico contributes the use of its facilities and perhaps part-time release from teaching for a faculty member responsible for organizing all this.

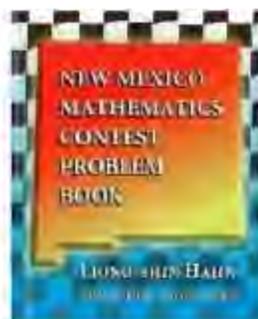
The key element, of course, is the questions themselves. They must be attractive, intriguing, and

suggestive to teenage contestants. They must require an insight, a spark, beyond routine application of a standard recipe. They must be solvable with no knowledge beyond that to be expected of a high-school student. And they should be original, not retreads of familiar chestnuts in old problem books. Such are the creations of Liong-shin Hahn—"L.S.," as he allows himself to be called by those who are shy of pronouncing his full name. Rather than cite examples, I invite you to open this book and read from any page.

The New Mexico Mathematics Contest is part of a long tradition with roots in Hungary; the story brings together mathematicians from three continents. The recently retired director of the contest, Professor Liong-shin Hahn, whose remarkable collection of problems you are now holding, was born in 1932 in Taiwan into a family of physicians. He calls himself a "black sheep" for having strayed into mathematics. He got his Ph.D. at Stanford in 1966 with Karel deLeeuw, was an instructor at Johns Hopkins, and came to New Mexico in 1968.

In 1998 Professor Hahn received the "Citation for Public Service" from the American Mathematical Society at their national meeting in Baltimore. The citation says, "Professor Hahn is being honored for carrying forward and developing the New Mexico High School Mathematics Contest and for exposition and popularization of mathematics attractive and suitable for potential candidates for the contest and others with similar intellectual interest." The reference to exposition and publication recognizes Hahn's two excellent books, *Classical Complex Analysis* (with Bernard Epstein) and *Complex Numbers and Geometry*. The latter is an original unique work, easily accessible to high-school students and teachers.

The history of the contest can be traced back to 1894, when a "Pupils' Mathematical Competition" was established by the Mathematical and Physical Society of Hungary. It became one of the decisive influences that made tiny Hungary one of the major contributors to twentieth-century mathematics. For decades the contest was known as the Eötvös Competition, in honor of the Society's founder and president, the physicist and Minister of Education, Baron Loránd



# Foreword

By Reuben Hersh

Every November, some thousand middle- and high-school students in dozens of schools all over New Mexico gather to spend up to three hours playing and struggling with a set of elementary but tricky math problems. It's Round One of the New Mexico High School Math Contest. Then, the following February, the highest-scoring two hundred or so are invited to the campus of the University of New Mexico in Albuquerque. They hear a talk by a famous mathematician (Paul Erdős, Peter Lax, John Conway, Serge Lang, Bill Thurston, and Ron Graham have done it), have lunch, and then dig in to Round Two, a more rigorous and demanding set of mathematical mind-twisters.

In April, at a banquet in Albuquerque, prizes are awarded by grades from seventh to twelfth. Top prizes are books, money and scholarships. Everybody who does the second round gets a free T-shirt, such as the one I am wearing as I write this.

For many students, this contest has led to steps, decisions, and, ultimately, successful careers in mathematics and science. Some parents sing the praises of an event, uncommon in parts of our state, that publicizes and glorifies the work of the mind (a kind of activity not always and everywhere rewarded among high-school kids in the present day U.S.).

All this takes time and money. At the first round, local teachers volunteer as coaches and proctors. At the second round and for the grading, faculty and graduate students at the University of New Mexico volunteer. The costs of the banquet and the prizes are graciously met by the PNM Foundation. The University of New Mexico contributes the use of its facilities and perhaps part-time release from teaching for a faculty member responsible for organizing all this.

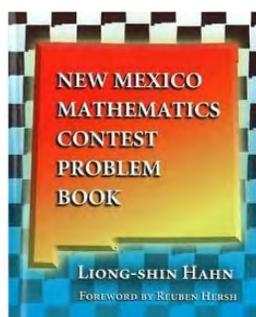
The key element, of course, is the questions themselves. They must be attractive, intriguing, and

suggestive to teenage contestants. They must require an insight, a spark, beyond routine application of a standard recipe. They must be solvable with no knowledge beyond that to be expected of a high-school student. And they should be original, not retreads of familiar chestnuts in old problem books. Such are the creations of Liong-shin Hahn—"L.S.," as he allows himself to be called by those who are shy of pronouncing his full name. Rather than cite examples, I invite you to open this book and read from any page.

The New Mexico Mathematics Contest is part of a long tradition with roots in Hungary; the story brings together mathematicians from three continents. The recently retired director of the contest, Professor Liong-shin Hahn, whose remarkable collection of problems you are now holding, was born in 1932 in Taiwan into a family of physicians. He calls himself a "black sheep" for having strayed into mathematics. He got his Ph.D. at Stanford in 1966 with Karel deLeeuw, was an instructor at Johns Hopkins, and came to New Mexico in 1968.

In 1998 Professor Hahn received the "Citation for Public Service" from the American Mathematical Society at their national meeting in Baltimore. The citation says, "Professor Hahn is being honored for carrying forward and developing the New Mexico High School Mathematics Contest and for exposition and popularization of mathematics attractive and suitable for potential candidates for the contest and others with similar intellectual interest." The reference to exposition and publication recognizes Hahn's two excellent books, *Classical Complex Analysis* (with Bernard Epstein) and *Complex Numbers and Geometry*. The latter is an original unique work, easily accessible to high-school students and teachers.

The history of the contest can be traced back to 1894, when a "Pupils' Mathematical Competition" was established by the Mathematical and Physical Society of Hungary. It became one of the decisive influences that made tiny Hungary one of the major contributors to twentieth-century mathematics. For decades the contest was known as the Eötvös Competition, in honor of the Society's founder and president, the physicist and Minister of Education, Baron Loránd



# Foreword

By Reuben Hersh

Every November, some thousand middle- and high-school students in dozens of schools all over New Mexico gather to spend up to three hours playing and struggling with a set of elementary but tricky math problems. It's Round One of the New Mexico High School Math Contest. Then, the following February, the highest-scoring two hundred or so are invited to the campus of the University of New Mexico in Albuquerque. They hear a talk by a famous mathematician (Paul Erdős, Peter Lax, John Conway, Serge Lang, Bill Thurston, and Ron Graham have done it), have lunch, and then dig in to Round Two, a more rigorous and demanding set of mathematical mind-twisters.

In April, at a banquet in Albuquerque, prizes are awarded by grades from seventh to twelfth. Top prizes are books, money and scholarships. Everybody who does the second round gets a free T-shirt, such as the one I am wearing as I write this.

For many students, this contest has led to steps, decisions, and, ultimately, successful careers in mathematics and science. Some parents sing the praises of an event, uncommon in parts of our state, that publicizes and glorifies the work of the mind (a kind of activity not always and everywhere rewarded among high-school kids in the present day U.S.).

All this takes time and money. At the first round, local teachers volunteer as coaches and proctors. At the second round and for the grading, faculty and graduate students at the University of New Mexico volunteer. The costs of the banquet and the prizes are graciously met by the PNM Foundation. The University of New Mexico contributes the use of its facilities and perhaps part-time release from teaching for a faculty member responsible for organizing all this.

The key element, of course, is the questions themselves. They must be attractive, intriguing, and

suggestive to teenage contestants. They must require an insight, a spark, beyond routine application of a standard recipe. They must be solvable with no knowledge beyond that to be expected of a high-school student. And they should be original, not retreads of familiar chestnuts in old problem books. Such are the creations of Liong-shin Hahn—"L.S.," as he allows himself to be called by those who are shy of pronouncing his full name. Rather than cite examples, I invite you to open this book and read from any page.

The New Mexico Mathematics Contest is part of a long tradition with roots in Hungary; the story brings together mathematicians from three continents. The recently retired director of the contest, Professor Liong-shin Hahn, whose remarkable collection of problems you are now holding, was born in 1932 in Taiwan into a family of physicians. He calls himself a "black sheep" for having strayed into mathematics. He got his Ph.D. at Stanford in 1966 with Karel deLeeuw, was an instructor at Johns Hopkins, and came to New Mexico in 1968.

In 1998 Professor Hahn received the "Citation for Public Service" from the American Mathematical Society at their national meeting in Baltimore. The citation says, "Professor Hahn is being honored for carrying forward and developing the New Mexico High School Mathematics Contest and for exposition and popularization of mathematics attractive and suitable for potential candidates for the contest and others with similar intellectual interest." The reference to exposition and publication recognizes Hahn's two excellent books, *Classical Complex Analysis* (with Bernard Epstein) and *Complex Numbers and Geometry*. The latter is an original unique work, easily accessible to high-school students and teachers.

The history of the contest can be traced back to 1894, when a "Pupils' Mathematical Competition" was established by the Mathematical and Physical Society of Hungary. It became one of the decisive influences that made tiny Hungary one of the major contributors to twentieth-century mathematics. For decades the contest was known as the Eötvös Competition, in honor of the Society's founder and president, the physicist and Minister of Education, Baron Loránd

## NEW MEXICO MATH CONTEST

Prof. Conway from Princeton University will give a very special talk for the participants in the last round of the New Mexico Math Contest.

- **Speaker:** Prof. John H. Conway (Princeton University).
- **Title:** *TANGLES, BANGLES AND KNOTS*.
- **Time:** Saturday February 6th, 10:30am.
- **Place:** Anthropology Building Room 163 (West of the Chapel).

**ABSTRACT:** *How would you describe a knot to your friend over the telephone? I'll discuss a way to understand some of the geometry of knots in elementary arithmetical terms. Come prepared to dance!*

**Who is J. H. Conway?** John H. Conway is the John Von Neumann Professor of Mathematics at Princeton University. A native of England, Conway received his PhD from Cambridge University and was professor of mathematics there until 1986 when he moved to Princeton.

Prof. Conway has made substantial contributions to several branches of mathematics: set theory, number theory, finite groups, quadratic forms, game theory, and combinatorics. He is best known, in a popular sense, for his work in the theory of games, especially the Game of "Life" and his invention of a theory of numbers that has its origins on games. Conway's enchantment with games is reflected in the title of one of his papers: *All games bright and beautiful*. In Conway's theory of numbers, every two-person game is a number! Don Knuth, the noted computer scientist, was so taken with Conway's new theory of numbers that he wrote *Surreal Numbers*, a novel that explains the theory to students.

In 1969 he discovered a simple group, the Conway group, and is the senior author of the *Atlas of Finite Groups*. He is also the author of *On numbers and Games*; *Sphere Packing, Lattices and Groups* (with Neil Sloane); *Winning Ways for your Mathematical Plays* (with Elwyn Berlekamp and Richard Guy); *The Book of Numbers* (with Richard Guy); and *The Sensual (Quadratic) Form*.

Conway has earned many honors, including election as Fellow of the Royal Society of London.

You are all welcome to come, it should be a very entertaining lecture! Needless to say this is an exceptional opportunity to meet one of the most famous mathematicians in the world.



John 'Horned' (Horton) Conway

# New Mexico Math Contest

## Lectures

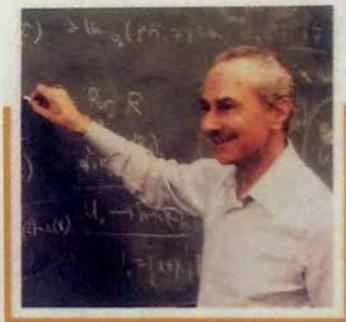
Speaker: *Prof. Serge Lang* (from Yale University)

### Official lecture

Title: *The abc polynomial theorem and the abc conjecture*

Saturday February 5, 2000  
10:30am Dane Smith Hall 125

*Abstract:* The abc polynomial theorem is due to Stothers and Mason (early '80's). We will give a proof due to Noah Snyder (a high school student in 1998). We will formulate an analogue for integers, in which case it is a great conjecture due to Masser and Oesterle (1986). The theorem (resp. conjecture) imply Fermat's last theorem, thus showing their power.



*Warm up lecture*  
(especially for the young ones)

Title: *Review of polynomials*

Saturday February 5, 2000  
9:15am Dane Smith Hall 125

You are all welcome to come. These should be very entertaining lectures! This is an exceptional opportunity to meet a very distinguished mathematician.

*Refreshments will be served*

**Reminder:** The second round of the Math Contest will be held promptly at 1:00pm in Dane Smith Hall 125

# *New Mexico Math Contest Lecture*

***Speaker: Prof. Fernando Rodriguez Villegas***  
*(From the University of Texas at Austin)*

***Title: Lattice Polygons: What's 12 got to  
do with it?***

***Saturday February 3, 2001  
10:30am, Woodward Hall 101  
University of New Mexico***



***Abstract:*** *I will discuss an elementary theorem about polygons in the plane with integer vertices. Its proof will take us through some interesting group theory ending with a challenging puzzle.*

You are all welcome to come. This should be a very entertaining lecture from an excellent mathematician!!

**Reminder:** The second round of the Math Contest will be held promptly at 1:00 pm in Woodward Hall 101



# UNM-PNM Math Contest Lecture



**Speaker:** Prof. Roger Howe (Yale University)

**Title:** Mirrors and Reflections - Symmetry  
from several viewpoints

Saturday Feb 2nd, 2002 10:30am  
Woodward Hall 101

**Abstract:**

Symmetry is often first encountered in the context of repeating patterns and symmetric designs. The aesthetic aspects of symmetry contribute beauty to many parts of our lives. However, the mathematical ideas of symmetry go far beyond artistic issues, and lies at the heart of our understanding of geometry and physics. This talk will attempt to provide a brief glimpse into the power of symmetry principles in geometry.

You are all welcome to come.

This should be a very entertaining lecture!

This is an exceptional opportunity to meet a very distinguished mathematician.

Refreshments will be served at 10:00am

# MATH CONTEST LECTURE

The Department of Mathematics and Statistics at UNM  
has the pleasure to invite you to the 2003 Math Contest Lecture  
by distinguished mathematician Ron Graham.

Sponsored by the Efroymsen and PNM Foundations

**Professor Ron Graham**

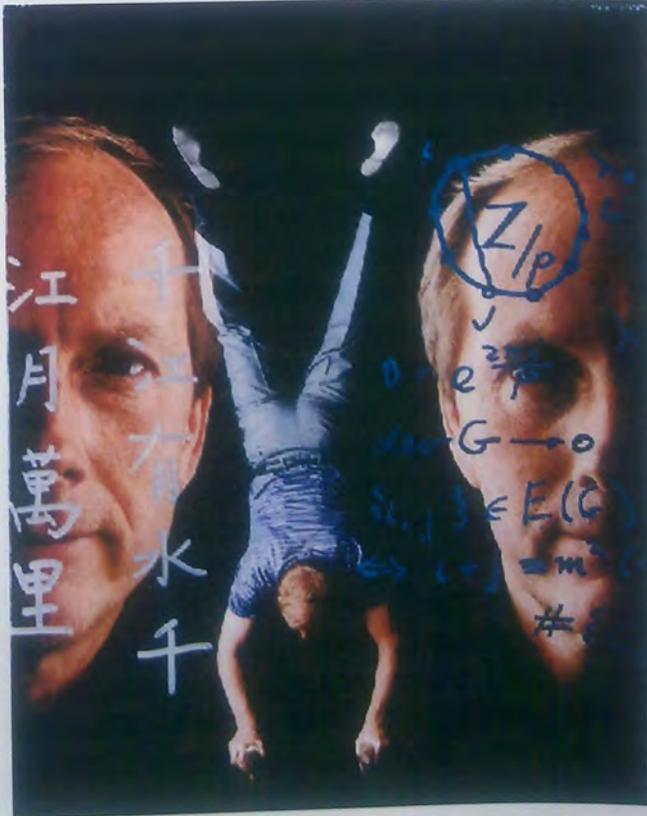
University of California at San Diego

“Mathematics and Computers: Problems and Prospects”

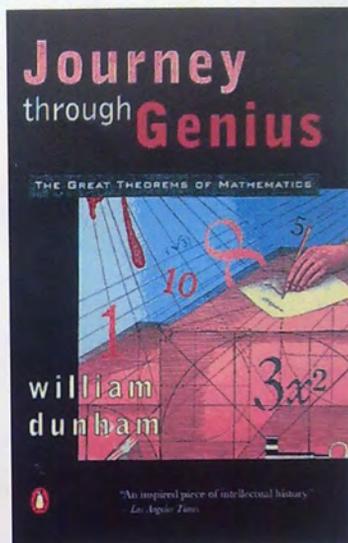
**Saturday February 1st, 2003, 10:30 am Woodward Hall 101**

**Abstract:** In this talk, I will describe a variety of mathematical problems, all of which are easy to state. For some of them, computers were essential in their solution, and for others, computers may prove to be useful in the future. However, I will also describe problems for which computers will apparently be of no use whatsoever!

Ron Graham's invaluable contributions to discrete mathematics earned him the 2003 Steele Prize for Lifetime Achievement presented by the American Mathematical Society. His contributions to number theory and other realm of mathematics earned him the prestigious Polya Prize in 1972, and membership into the National Academy of Sciences in 1985. He spent 32 years at Bell Labs, eventually as chief scientist, and built it into world a class center for research in discrete mathematics and theoretical computer science. He is currently the Irwin and Joan Jacobs Chair of Computer and Information Science at the University of California, San Diego, as well as Chief Scientist of the California Institute for Telecommunications and Information Technology. Graham's non-mathematical feats are equally diverse. He is an expert in juggling, gymnastics, ping-pong and fluent in Mandarin.



# UNM – PNM State Mathematics Contest Lecture Series Presents



## William Dunham

Truman Koehler Professor of Mathematics, Muhlenberg College

### Author of:

Journey Through Genius: The Great Theorems of Mathematics

The Mathematical Universe

Euler: The Master of Us All

The Calculus Gallery: Masterpieces from Newton to Lebesque

### All interested are invited to attend:

Feb 4, 2005

“The Calculus Gallery”	Refreshments:	Humanities 446	3:00 pm
Department Colloquium		Mitchell Hall	3:30 pm

Feb 5, 2005

“Newton & Leibniz: Mathematicians at War”	Refreshments:	10:00 am
Math Contest Lecture Series	Woodward Hall 101	10:30 am

# UNM – PNM State Mathematics Contest Lecture Series Presents



Bjorn Poonen received the A.B. degree from Harvard, and the Ph.D. degree from the University of California at Berkeley, where he is now Professor of Mathematics.

His main research is in number theory and algebraic geometry, but he has published also in combinatorics and probability.

He wrote problems for the U.S.A. Mathematical Olympiad for 14 years, and has published the book “The William Lowell Putnam Mathematical Competition 1985-2000: Problems, Solutions, and Commentary” with K. Kedlaya and R. Vakil.

## Bjorn Poonen

Professor of Mathematics, University of California, Berkeley

All are invited to attend the Talk

Title: Elliptic curves

Saturday, February 4, 2006

10:30-11:30 am

Northrop Hall Room 122

(refreshments at 10am at the same place)

# Fractals, Chaos & the Patterns of Nature

Feb 3rd, 10:30AM

Woodward Hall room 101



Join Dr. Jonathan Wolfe of the Fractal Foundation for a dazzling and entertaining presentation about fractals and chaos theory. Learn about the beautiful connections between math, science and art.



[www.FractalFoundation.org](http://www.FractalFoundation.org)

Sponsored by the UNM-PNM Statewide Mathematics Contest and the PNM Foundation



## UNM-PNM STATEWIDE MATHEMATICS CONTEST LECTURE



**Professor Alex Solynin**  
Texas Tech University

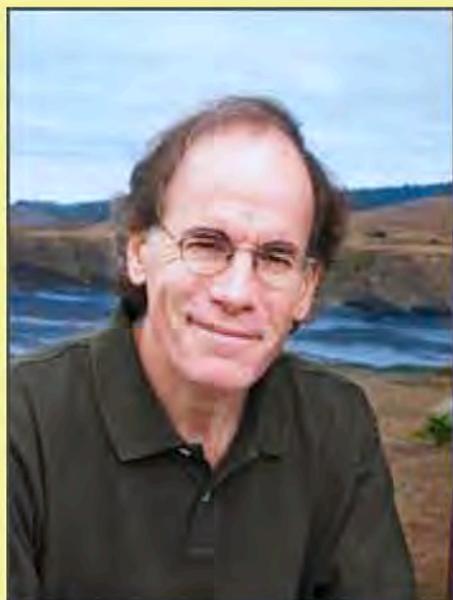
### **Symmetry and Isoperimetric Inequalities**

*Among all simple closed plane curves of given length  $L$ , the circle of circumference  $L$  encloses the maximum area. Nowadays the isoperimetric problem is understood in a very broad sense where we fix a geometric parameter of a domain and try to optimize a given quantity dependent on the domain. Physical problems leading to isoperimetric problems include torsional rigidity, electrostatic capacity, vibrations (lowest fundamental frequency), black holes. The study of isoperimetric problems involves geometry, analysis and differential equations, and very often leads to a solution with a lot of symmetries. Professor Solynin is one of the world experts in isoperimetric problems.*

**Saturday, February 7, 2009**  
**Woodward Hall Room 101, 10:00am.**



UNM-PNM STATEWIDE  
MATHEMATICS CONTEST  
LECTURE



*A Mathematical Mystery  
Tour*

*Richard Gardner  
Western Washington University*

*How do you become a mathematician? Can mathematics be beautiful? Can you square a circle? What is the plank problem? How can you get an elephant into a one-inch cube? What is Geometric Tomography? Some or all of these questions, and others, may or may not be answered in this talk!*

**Saturday, February 6, 2010**

**Anthropology 163, 10:00am**

Refreshments before lecture. All are welcome.

# UNM-PNM STATEWIDE MATHEMATICS CONTEST LECTURE

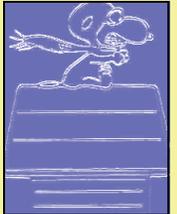


## *Discrete Wavelets and Image Compression*

*Catherine Bénéteau  
University of South Florida*



How does the FBI store so many fingerprints in their database? How can you compress a digital image? How can you detect an art forgery? I will discuss how researchers from many different areas such as electrical engineering, physics, mathematics, and computer science came together in the late 1980s and 1990s to answer these questions by using what are called discrete wavelet transformations, and how these transformations are connected to some beautiful mathematics.



Public Lecture in Science and Math Learning Center,  
February 5, 2011, Room 102 at 11am  
Refreshments before lecture. All are welcome.



# UNM-PNM STATEWIDE MATHEMATICS CONTEST LECTURE

## *From Algebra to Astrophysics*



*Dmitry Khavinson  
University of South Florida*

*How many roots does a polynomial equation of degree  $n$  have? For polynomials of a complex variable the answer is given by the celebrated Fundamental Theorem of Algebra: the number is the same as the degree of the polynomial (counting multiplicities). Yet, for more general polynomials the situation is far from clear.*

*If the light from a distant star is bent (in accordance with the relativity theory) when it passes near another massive star, a small galaxy, or a quasar, how many twin copies of the original star will our telescope detect?*

*What do these two questions have in common? We shall see that in more ways than one they are actually equivalent, and the answers to the first one, a purely mathematical query, shed light on the second one, resolving one of the problems in today's astrophysics.*

Public Lecture in Science and Math Learning Center,  
February 5, 2011, Room 102 at 10am  
Refreshments before lecture. All are welcome.



## UNM-PNM STATEWIDE MATHEMATICS CONTEST LECTURE



### *Archimedes' Law of the Lever and how he used it to deduce the volume of the sphere*

*Mike Raugh*

*Retired professor of Mathematics Harvey Mudd College & director of  
IPAM's—Research in Industrial Projects for Students (RIPS) Program*

Archimedes' marvelous proof of the law of the lever is summarized along with comments about lingering questions surrounding his proof. Generalizing the law of the lever in our modern formulation of the center of gravity as centroid allows us to show with elementary algebra or calculus that a static object suspended freely from a point on the object hangs so that the vertical line passing through the point passes through the center of gravity of the object. But Archimedes already knew this. His "method" used comparisons of cross sections to determine volumes, like Cavalieri's principle in calculus. An inspiring example is Archimedes' derivation of the volume of a sphere using levers.

Archimedes was a physicist as well as a mathematician of great power and insight, maybe the most creative of all. Even today, his ideas stand out for their brilliance and originality.

Public Lecture in Science and Math Learning Center,  
Saturday, February 4, 2012, Room 102 at 10am

Refreshments served before lecture. All are welcome.

<http://mathcontest.unm.edu/>



## UNM-PNM STATEWIDE MATHEMATICS CONTEST LECTURE



*Why math competitions?*

*Dr. Titu Andreescu*

*University of Texas Dallas*

Dr. Titu Andreescu is past chairman of the USA Mathematical Olympiad, director of the MAA American Mathematics Competitions (1998–2003), coach of the USA International Mathematical Olympiad Team (1993–2008), director of the Mathematical Olympiad Summer Program (1995–2002), and leader of the USA IMO Team (1995–2002). In 2002 he was elected member of the IMO Advisory Board, the governing body of the world's most prestigious mathematics competition. Professor Andreescu co-founded in 2006 and is the director of the AwesomeMath Summer Program (AMSP). He received the Edyth May Sliffe Award for Distinguished High School Mathematics Teaching from the MAA in 1994 and a "Certificate of Appreciation" from the president of the MAA in 1995 for his outstanding service as coach in preparing the US team for its perfect performance at the 1994 IMO. His contributions to numerous textbooks and problem books are valued worldwide.

Public Lecture in Science and Math Learning Center,  
Saturday, February 2, 2013, Room 102 at 10am

Refreshments served before lecture. All are welcome.

<http://mathcontest.unm.edu/>



## UNM-PNM STATEWIDE MATHEMATICS CONTEST LECTURE



### **Mathematics and Phylogenetics**

**Elizabeth Allman**

**University of Alaska Fairbanks**

Phylogenetics is the field of biology concerned with determining the evolutionary relationship between species. Are humans closest relatives among the great apes gorillas or chimpanzees? When did the human species arise on earth? Cutting-edge research by biologists, mathematicians, statisticians, and computer scientists seeks to answer these and related questions.

This talk will give a short overview to the field of mathematical phylogenetics, and describe how one can mathematically model the evolution of present-day DNA sequences from a common ancestor.

Dr. Elizabeth Allman is Professor of Mathematics at the University of Alaska Fairbanks, a Senior Research Associate at the Institute for Arctic Biology and a Fellow of the American Mathematical Society. Her interests include Biomathematics and Algebraic Statistics, but a common theme throughout is her use of Algebra.

Public Lecture in Science and Math Learning Center,  
Saturday, February 1, 2014, Room 102 at 10am

Refreshments served before lecture. All are welcome.

<http://mathcontest.unm.edu/>



## UNM-PNM STATEWIDE MATHEMATICS CONTEST LECTURE



### **The beauty, mystery, and utility of prime numbers**

**Tom Marley**

**University of Nebraska**

Ever since the days of Euclid, mathematicians (novice and professional) have been fascinated by prime numbers. While many centuries-old questions about prime numbers remain unsolved to this day, there have been exciting recent discoveries which may lead to their ultimate solutions. And it turns out, not only are prime numbers interesting and fun objects of study, they also play a critical role in cyber security in today's information age.

Dr. Tom Marley is Professor of Mathematics and Chief Undergraduate Advisor at the University of Nebraska. In addition, he directs the successful Nebraska IMMERSE Program which strengthens the preparation of students who are entering their first year of graduate study in mathematics and also develops the teaching, research and mentoring skills of graduate students and early-career faculty. His area of expertise is commutative algebra, a branch of mathematics focused on the study of algebraic equations and their solutions.

Public Lecture in Science and Math Learning Center,  
Saturday, February 7, 2015, Room 102 at 10am

Refreshments served before lecture. All are welcome.

<http://mathcontest.unm.edu/>



## UNM-PNM STATEWIDE MATHEMATICS CONTEST LECTURE



### *The Curvature of Space*

**John M. Lee**

**Professor of Mathematics  
University of Washington**

Do you think that everything there is to know about geometry was already discovered ages ago? Think again. Since the time of Euclid, the history of geometry has been a dramatic saga that your high-school teachers might not tell you about. It led, more than a century ago, to the mind-bending mathematical discovery that the three-dimensional space we live in might be "curved," in much the same way as the two-dimensional surface of the earth is curved.

In this talk you'll have a chance to learn what it could possibly mean mathematically for space to be curved, how we can detect it, and the fascinating story of how we got from Euclid to here. Along the way, you'll find out about "proofs" by professional mathematicians that turned out to be wrong, a million-dollar prize for solving a mathematical problem, and a mysterious modern-day Russian mathematician who earned it but doesn't want it.

Public Lecture in Science and Math Learning Center,  
Saturday, February 6, 2016, Room 102 at 10am

Refreshments served before lecture. All are welcome.

<http://mathcontest.unm.edu/>



## **UNM-PNM STATEWIDE MATHEMATICS CONTEST LECTURE**



### **Splendor in the Graphs**

**Jennifer Beineke  
Professor of Mathematics  
Western New England University**

**Graph theory can provide an entertaining analysis of certain games and puzzles. Using elementary results, we will explore brainteasers such as: Dots-and-Boxes, Bridg-It, Paradoxical Pennies, and Perplexing Prisoners. That should be preparation enough to set us off on a mathematical sort of safari.**

**Public Lecture in Science and Math Learning Center,  
Saturday, February 4, 2017, Room 102 at 10am**

**Refreshments served before lecture. All are welcome.**

**<http://mathcontest.unm.edu/>**



## **UNM-PNM STATEWIDE MATHEMATICS CONTEST LECTURE**



### **Practical Uses of Complex Analysis**

#### **Loredana Lanzani**

#### **Professor of Mathematics**

#### **Syracuse University**

Conformal maps are used by mathematicians, physicists and engineers to change regions with complicated shapes into much simpler ones, in a way that preserves shape on a small scale (that is, when viewed up close). This makes it possible to “transpose” a problem that was formulated for the complicated-looking region into another, related problem for the simpler region (where it can be easily solved) -- then one uses conformal mapping to “move” the solution of the problem over the simpler region, back to a solution of the original problem (over the complicated region). The beauty of conformal mapping is that its governing principle is based on a very simple idea that is easy to explain and to understand (much like the statement of Fermat's celebrated last theorem) .

In the first part of this talk I will introduce the notion of conformal mapping and will briefly go over its basic properties and some of its history (including a historical mystery going back to Galileo Galilei). I will then describe some of the many real-life applications of conformal maps, including: cartography; airplane wing design (transonic flow); art (in particular, the so-called “Droste effect” in the work of M. C. Escher). Time permitting, I will conclude by highlighting a 2013 paper by McArthur fellow L. Mahadevan that uses the related notion of *quasi-conformal mapping* to link D'Arcy Thompson's iconic work *On Shape and Growth* (published in 1917) with modern morphometric analysis (a discipline in biology that studies, among other things, how living organisms evolve over time).

No previous knowledge of complex analysis is needed to enjoy this talk.

**Public Lecture in Science and Math Learning Center**

**Saturday, February 3, 2018, Room 102 at 10am**

**Refreshments served before lecture. All are welcome.**

**<http://mathcontest.unm.edu/>**

# **From Algebra to Astrophysics**

Dmitry Khavinson  
University of South Florida

February 2011

“The miracle of the appropriateness of the language of mathematics to the formulation of the laws of physics is a wonderful gift which we neither understand nor deserve” .

Eugene P. Wigner (1902 - 1995), 1963  
Physics Nobel Prize Laureate.



## Solving Algebraic Equations

Recall quadratic equations:

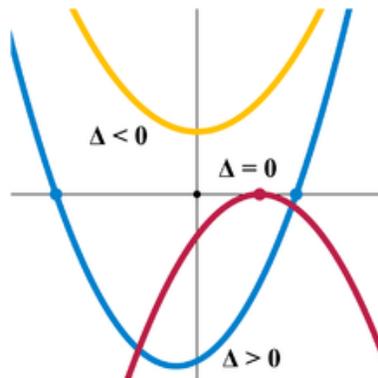
$$ax^2 + bx + c = 0,$$

where  $a, b, c$  are given real numbers (coefficients).

Completing the square we can easily derive

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} = \frac{-b \pm \sqrt{\Delta}}{2a},$$

where  $\Delta = b^2 - 4ac$ , the discriminant. Then, the number of **real** solutions of the equation depends on  $\Delta$ . Yet, the number of **complex** solutions counting multiplicities is always 2!



## A Brief History

Quadratic Equations - 1800-1600 B.C., Babylonians

Cubic Equations - 16th century A. D. (S. del Ferro, N. Tartaglia, G. Cardano)

Quartic Equations - 16th century A.D., (L. Ferrari)

*All the above solutions are expressed as explicit formulas.*

19th century - N.-H. Abel, E. Galois proved that general equations of degree 5 and higher **CANNOT** be solved by explicit formulas.

**Question:** How many many complex solutions does an equation of degree  $n \geq 1$  have?

## Fundamental Theorem of Algebra

**Theorem 1.** *Every complex polynomial  $p(z) := a_n z^n + \dots + a_0$ ,  $a_n \neq 0$  of degree  $n$  has precisely  $n$  complex roots (counted with multiplicities).*

First proved in 1799 by C. F. Gauss (1777-1855).



In the 1990s T. Sheil-Small, A. Wilmshurst proposed to extend FTA to a larger class of polynomials, harmonic polynomials.

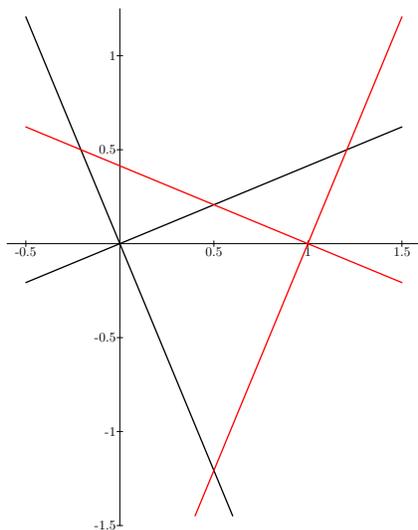
$$h(z) := p(z) - \overline{q(z)}, n := \deg p > m := \deg q.$$

(For a complex number  $a+ib$ ,  $a, b \in \mathbf{R}$ ,  $\overline{a+ib} = a - ib$ .)

**Theorem 2.** (A. Wilmshurst, '92)

$$\#\{z : h(z) = 0\} \leq n^2.$$

Moreover, there exist  $p, q : \deg q = n - 1$  such that the upper bound  $n^2$  is attained.



Wilmshurst's example for  $n = 2$ .

$$h(z) := \operatorname{Im}(e^{-\frac{i\pi}{4}} z^n) + i \operatorname{Im}(e^{\frac{i\pi}{4}} (z - 1)^n).$$

A little bit of algebra gives a more elegant example:

$$h(z) := z^n + (z - 1)^n + i\bar{z}^n - i(\bar{z} - 1)^n.$$

Note:  $m=n-1$ .

**Question:** If  $m \ll n$ , what is the precise upper bound for the number of zeros of the polynomial  $p(z) - \overline{q(z)}$ ?

**Conjecture 1.** (*A. Wilmshurst, '92*)

$$\#\{z : p(z) - \overline{q(z)} = 0\} \leq m(m - 1) + 3n - 2.$$

For  $m = n - 1$ , the above example shows that Conjecture 1 holds and is sharp. For  $m = 1$ , it becomes

**Conjecture 2.** (*T. Sheil-Small - A. Wilmshurst, '92*)

$$\#\{z : p(z) - \bar{z} = 0, n > 1\} \leq 3n - 2.$$

## History of Conjecture 2

- In the 1990s D. Sarason and B. Crofoot and, independently, D. Bshouty, A. Lyzzaik and W. Hengartner verified it for  $n = 2, 3$ .
- In 2001, using elementary complex dynamics and the argument principle for harmonic mappings, G. Swiatek and DK proved Conjecture 2 for all  $n > 1$ .
- In 2003-2005 L. Geyer showed, using dynamics, that  $3n - 2$  bound is sharp for all  $n$ .

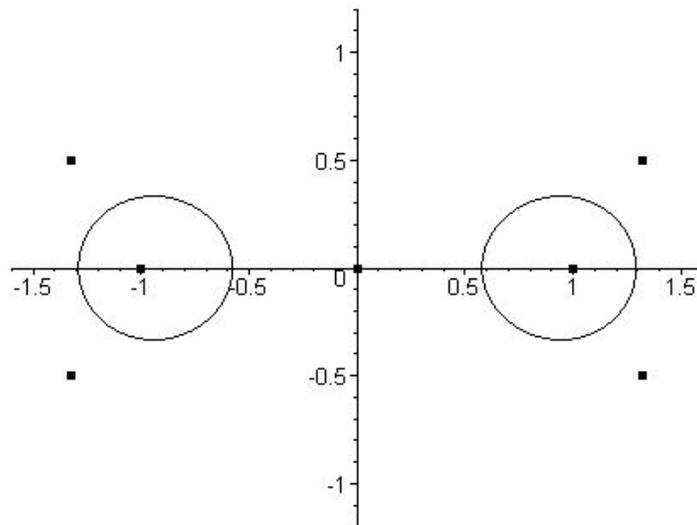
**Theorem 3.** (G. Swiatek -DK, '01)

$$\#\{z : p(z) - \bar{z} = 0, n > 1\} \leq 3n - 2.$$

The bound  $3n - 2$  is sharp for all  $n$  (L. Geyer, '03 -'05).

**Example.** Consider

$h(z) = z - \overline{\frac{1}{2}(3z - z^3)}$ ,  $n = 3$ . It has  $3 \times 3 - 2 = 7$  zeros  $0, \pm 1, \frac{1}{2}(\pm\sqrt{7} \pm i)$ .



Let  $r(z) := \frac{p(z)}{q(z)}$  be a rational function,  $p(z), q(z)$  are polynomials.  $\deg r := \max\{\deg p, \deg q\}$ . For example,

$$r(z) = \sum_{j=1}^n \frac{a_j}{z - z_j}.$$

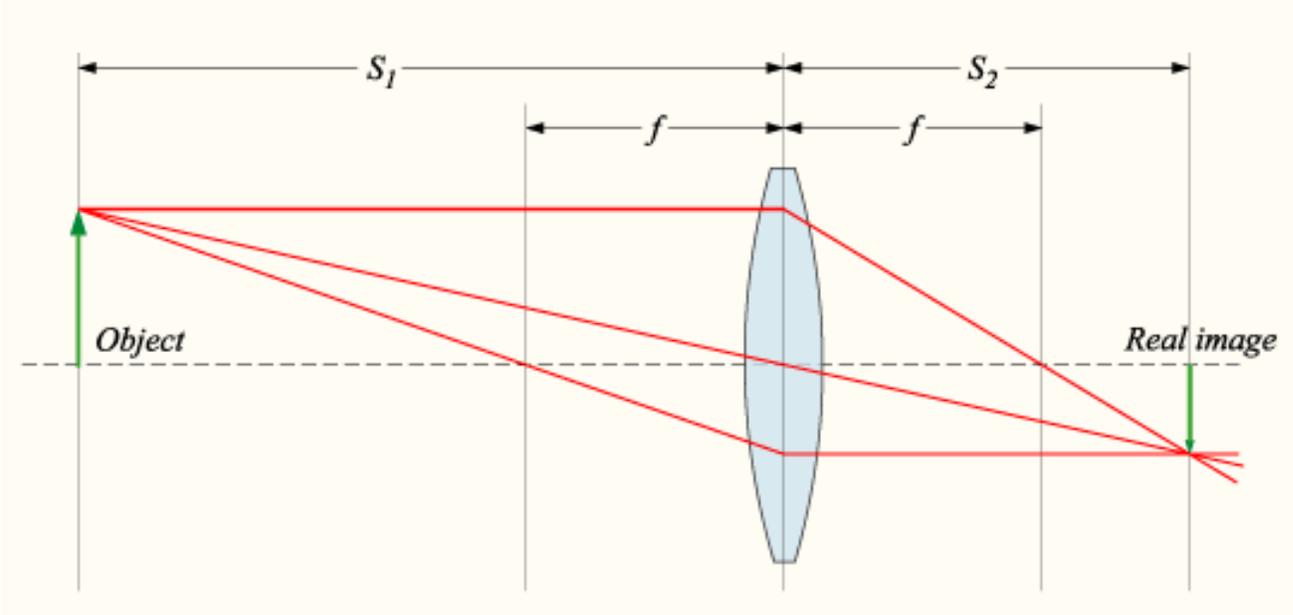
**Theorem 4.** (*G. Neumann -DK, '05*)

$$\#\{z : r(z) - \bar{z} = 0, n := \deg r > 1\} \leq 5n - 5.$$

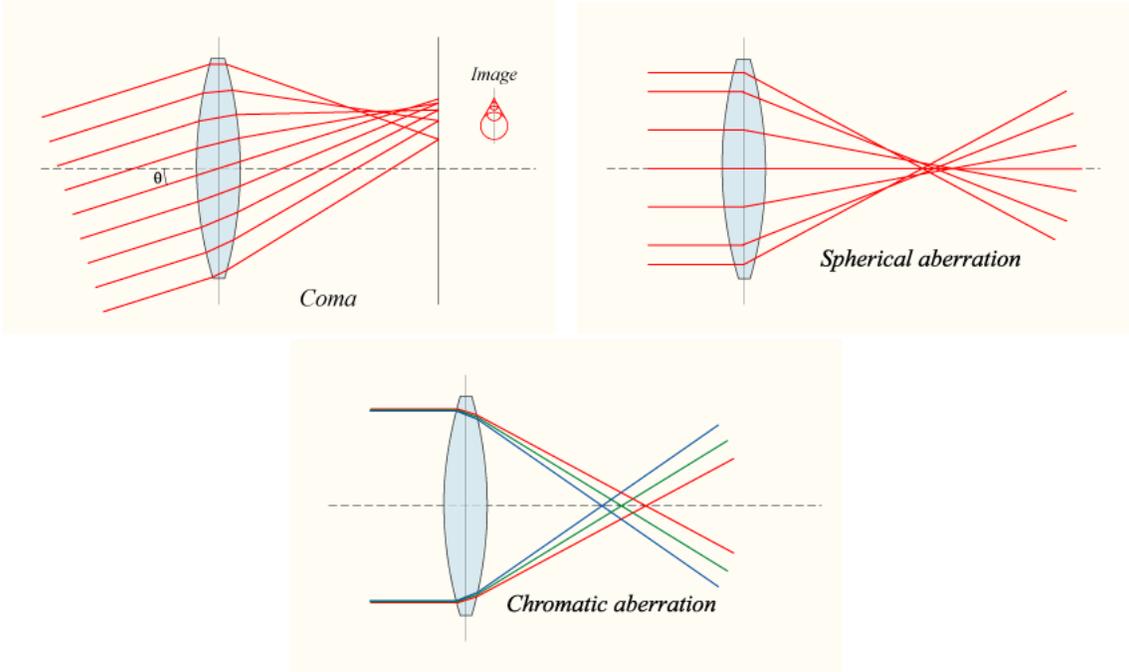
*The bound  $5n - 5$  is sharp for all  $n$  (S. Rhie, '03).*

**It turns out that this result opens a door to another world.**

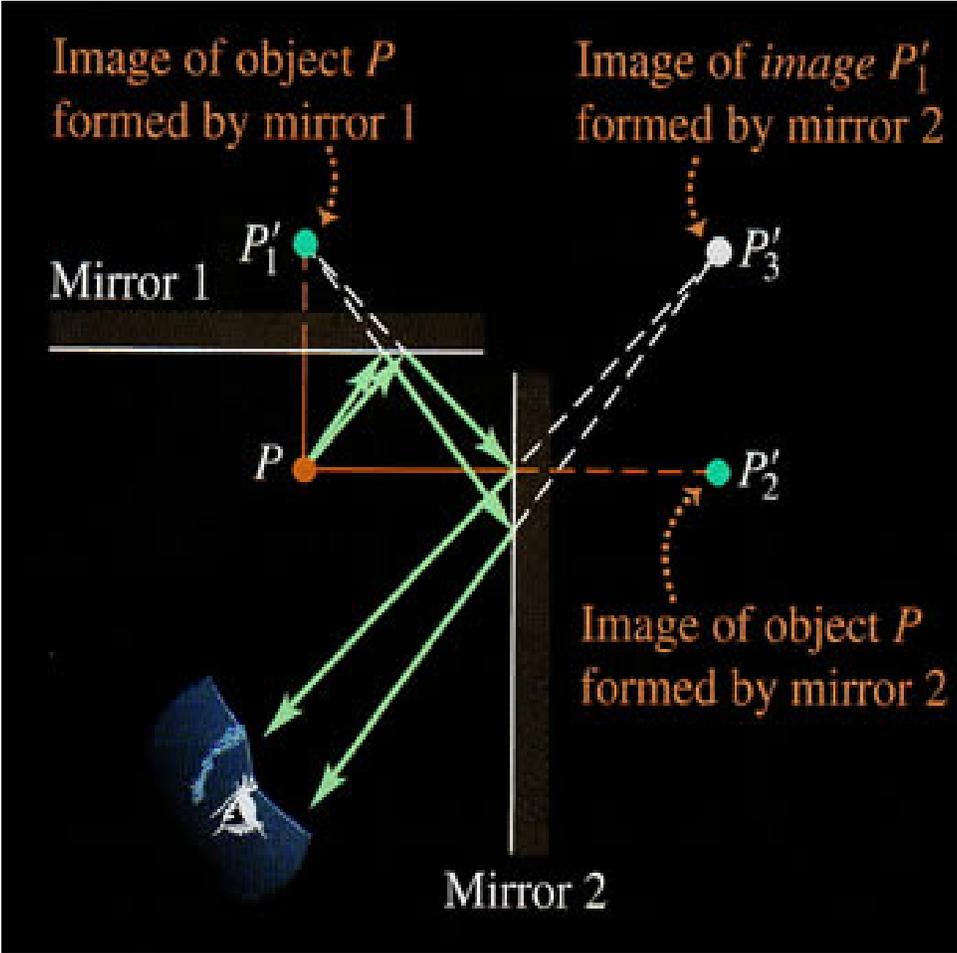
# Geometric Optics in the Perfect World



# Optics in Less Than Perfect World

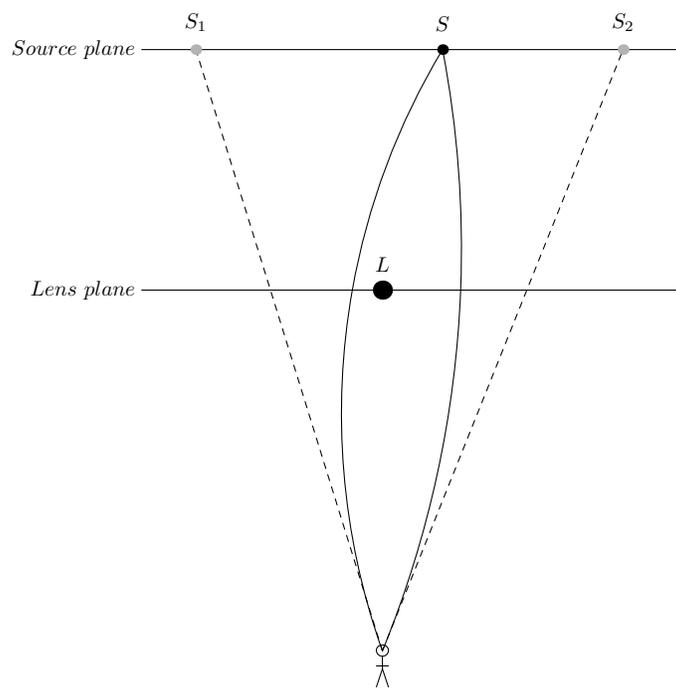


# Multiple Images by a System of Mirrors



## Gravitational Microlensing

- $n$  co-planar point-masses (e.g. condensed galaxies, black holes, etc.) in *lens plane* or *deflector plane*.
- Consider a light source in the plane parallel to the lens plane (*source plane*) and perpendicular to the line of sight from the observer.
- Due to deflection of light by masses multiple images of the source are formed. This phenomenon is known as *gravitational microlensing*.



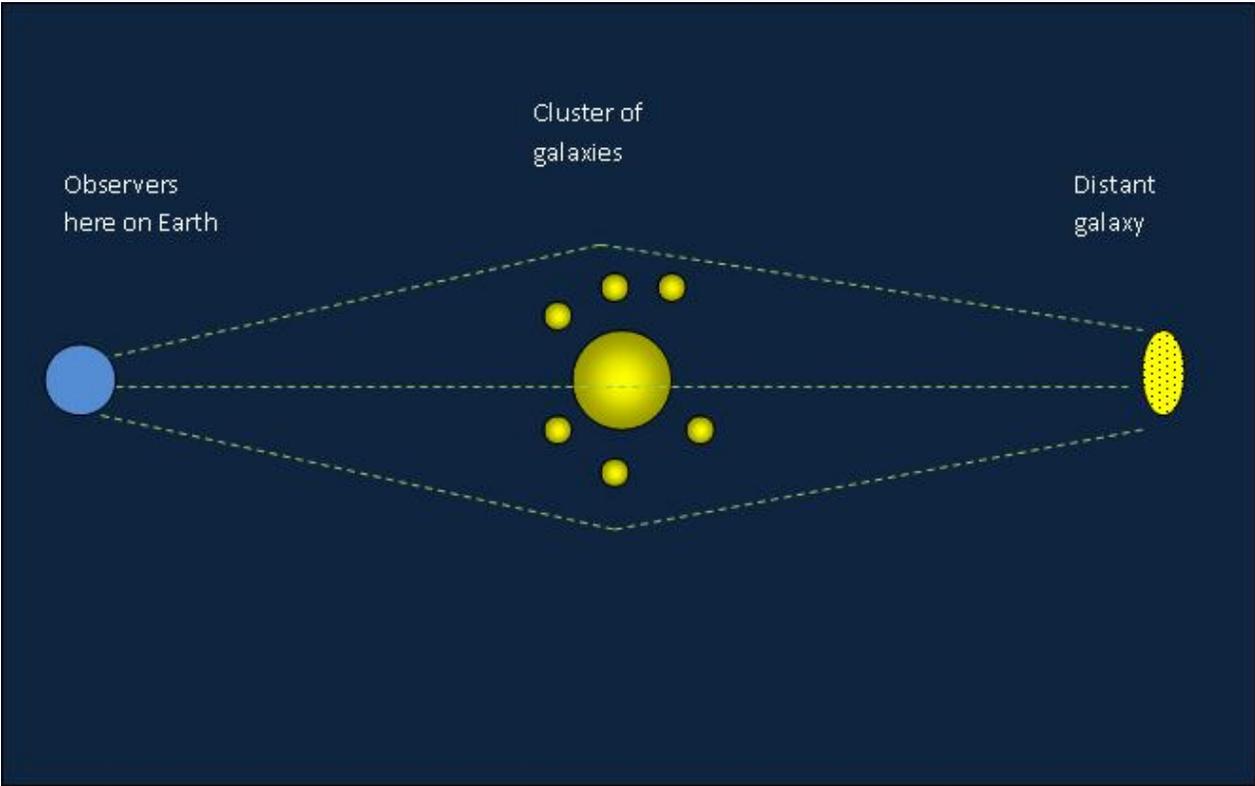
Basics of gravitational lensing.

**Gravitational lensing: the gravitational field of a massive object(s) acts as a lens for background sources**



**Exciting fact: the map from the distorted picture to the original is a planar harmonic map.**

# Lensing by Multiple Massive Objects



## Lens Equation

Light source is located in the position  $w$  in the *source plane*. The lensed image is located at the position  $z$  in the *lens plane* while the masses are located at the positions  $z_j$  in the *lens plane*.

$$w = z - \sum_1^n \sigma_j / (\bar{z} - \bar{z}_j),$$

where  $\sigma_j \neq 0$  are real constants.

Letting  $r(z) = \sum_1^n \sigma_j / (z - z_j) + \bar{w}$ , the lens equation becomes

$$z - \overline{r(z)} = 0, \text{ deg } r = n.$$

The number of solutions = the number of “lensed” images.



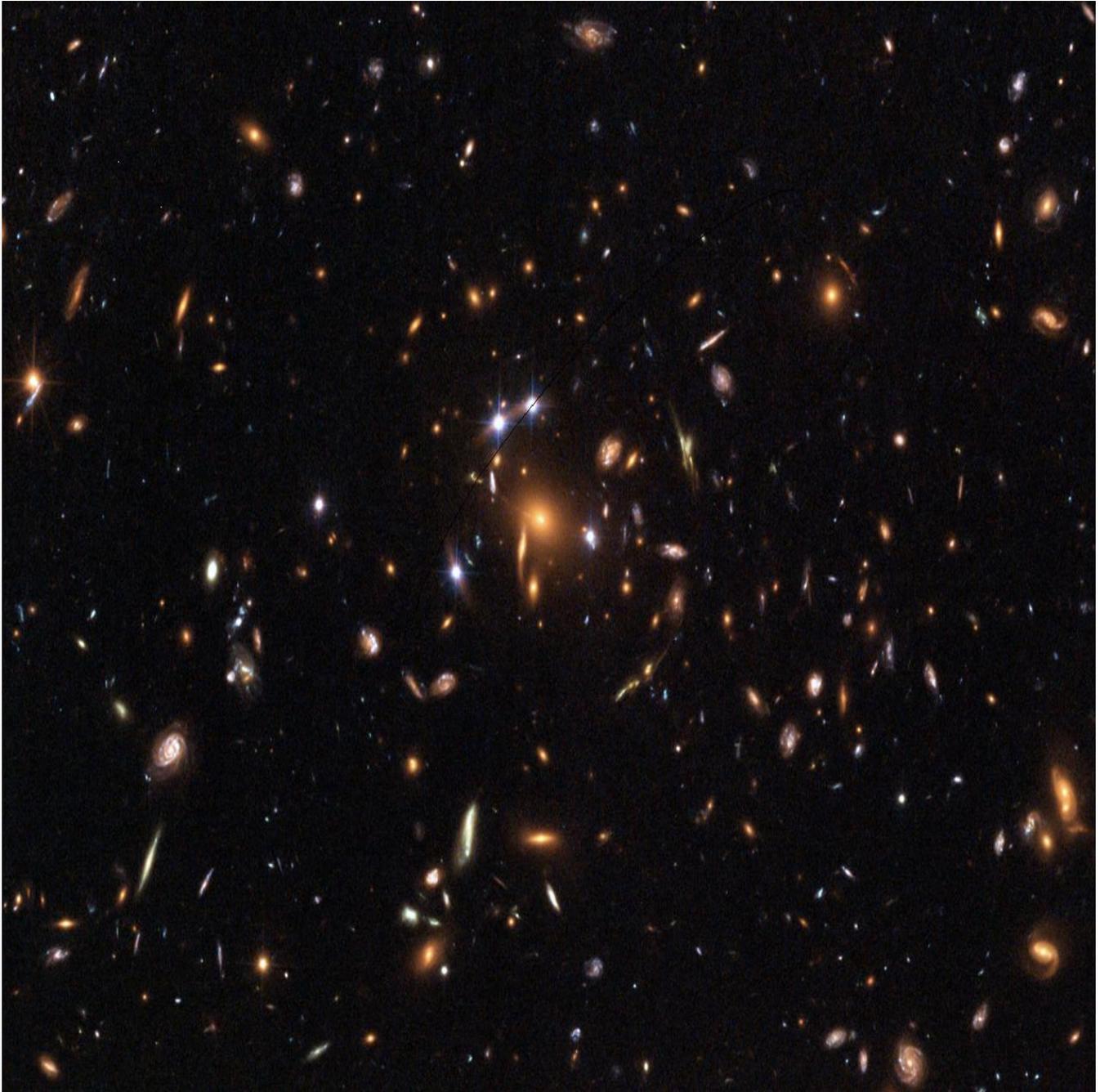
**Gravitational Lens  
Galaxy Cluster 0024+1654**

**HST · WFPC2**

PRC96-10 · ST ScI OPO · April 24, 1996

W.N. Colley (Princeton University), E. Turner (Princeton University),

J.A. Tyson (AT&T Bell Labs) and NASA



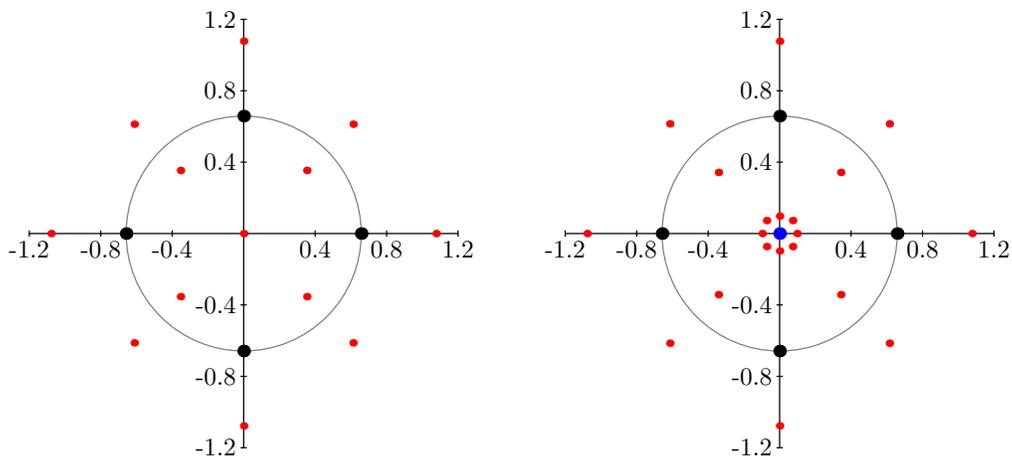
5 images of a quasar=quasi-stellar-radio object

## History

- $n = 1$  (one mass) A. Einstein (1912 - 1933), either two images or the whole circle (“Einstein ring”).
- H. Witt ('90) For  $n > 1$  the maximum number of observed images is  $\leq n^2 + 1$ . S. Mao, A. Petters and H. Witt ('97) showed that the maximum is  $\geq 3n + 1$ .
- S.H. Rhie ('01) conjectured the upper bound for the number of lensed images for an  $n$ -lens is  $5n - 5$ .

**Corollary 1.** (*G. Neumann-DK, '05*). *The number of lensed images by an  $n$ -mass lens cannot exceed  $5n - 5$  and this bound is sharp (Rhie, '03). Moreover, it follows from the proof that the number of images is even when  $n$  is odd and vice versa.*

## Rhie's Construction



**13 images for the non-perturbed lens and  
20 images after adding a small mass at  
the origin.**

## Questions

1. How many zeros can a polynomial

$$h := \bar{z}^m - p(z), \deg p = n > m$$

have?

Wilmshurst's conjecture for  $m = 2$  suggests the upper bound  $3n$ . Is it true?

2. *Lensing*. G. Neumann-DK's theorem applies to  $n$  "spherically symmetric" mass distributions in the lens plane and gives at most  $5n - 5$ -lensed images outside the support of the mass distribution.

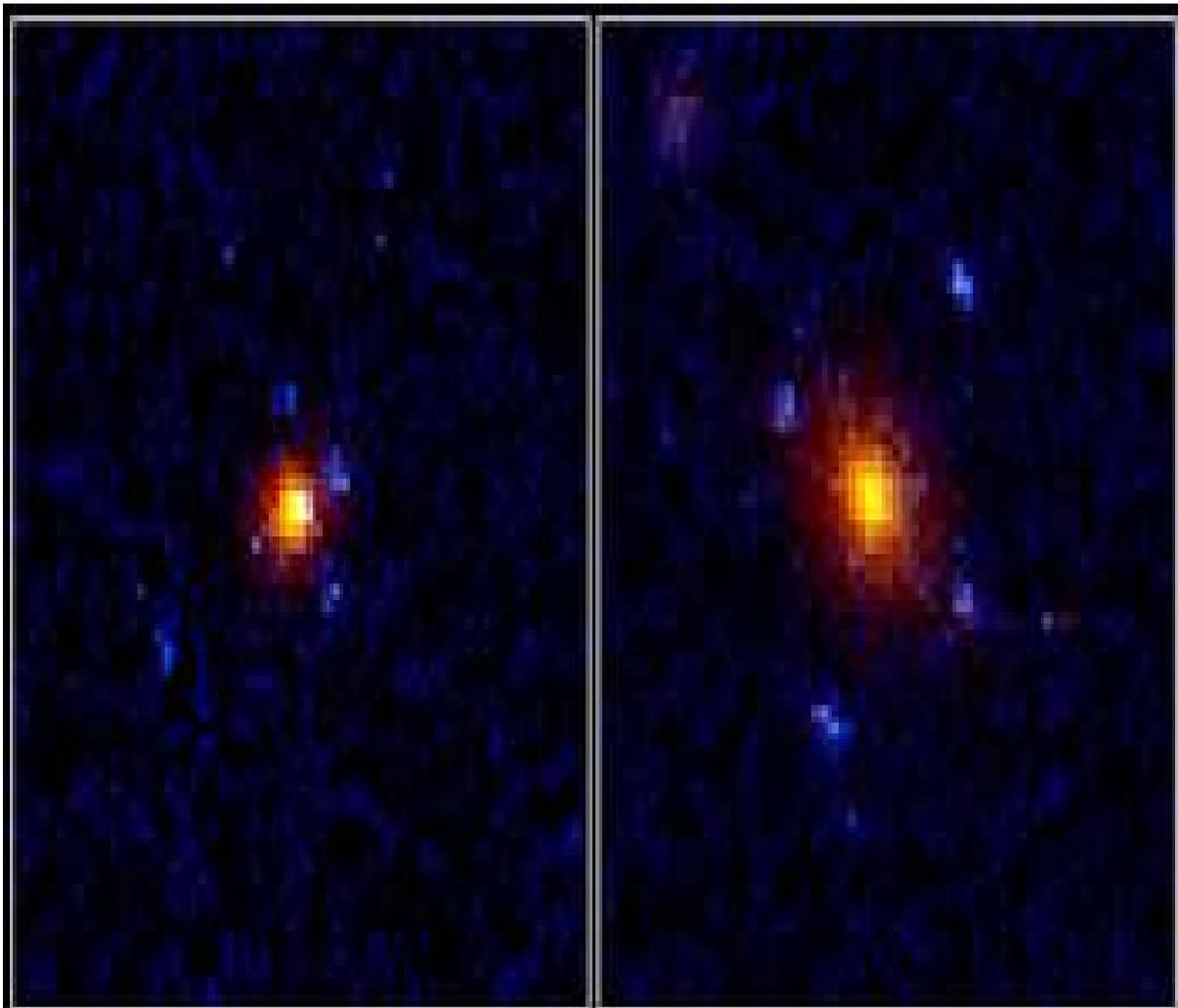
**Question.** How many lensed images can a uniform elliptic mass distribution produce?

**Theorem 5.** (*C. Fassnacht - C. Keeton - DK, '07.*)

*An elliptic galaxy  $\Omega$  with a uniform mass density may produce at most 4 “bright” lensing images of a point light source outside  $\Omega$ , and at most one “dim” image inside  $\Omega$ , i.e., at most 5 lensing images altogether.*

*Moreover, an elliptic galaxy  $\Omega$  with mass density that is constant on ellipses confocal with  $\Omega$ , may produce at most 4 “bright” lensing images of a point light source outside  $\Omega$ .*

## An “Astronomical” Proof



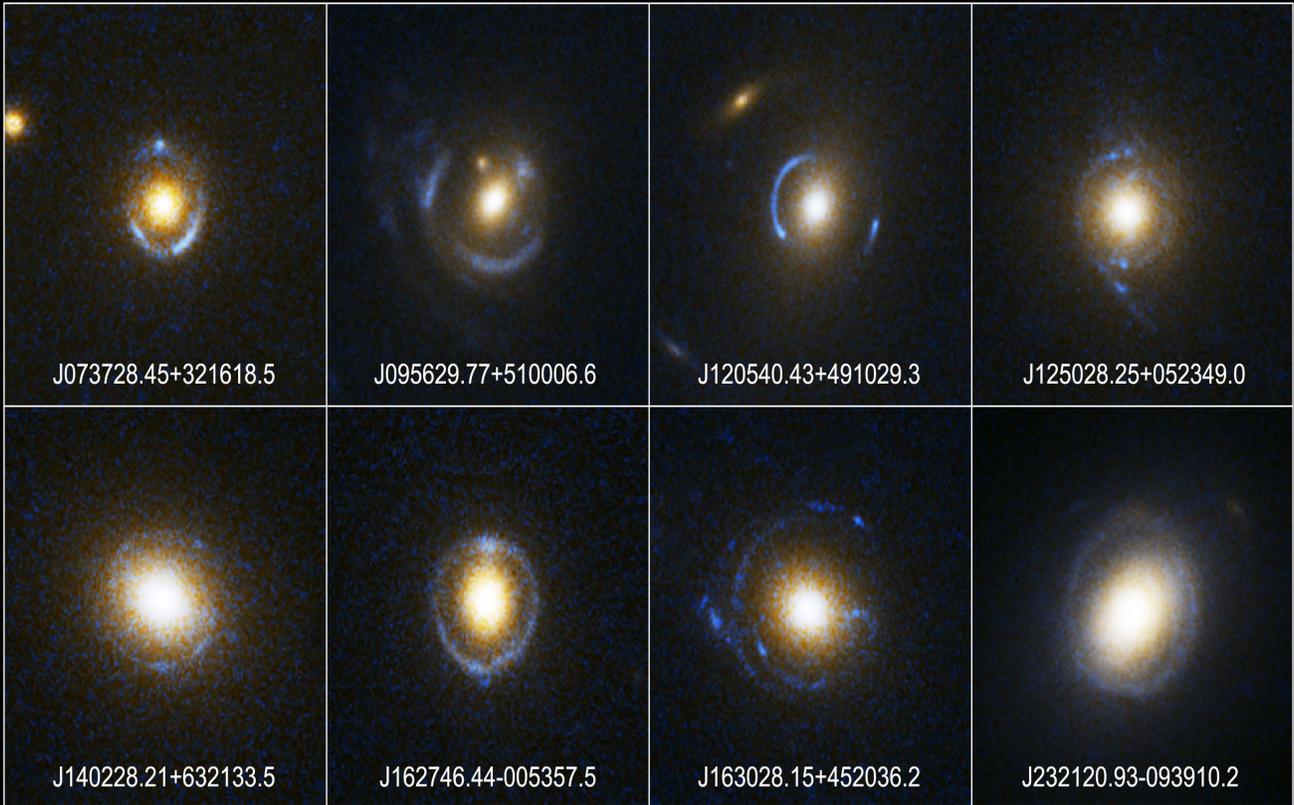
**Gravitational Lenses**

**HST - WFPC2**

PRC95-43 - ST ScI OPO - October 18, 1995 - K. Ratnatunga (JHU), NASA

## Einstein Rings are Ellipses

**Theorem 6.** (*Fassnacht - Keeton - DK, '07.*)  
*For any lens  $\mu$ , if the lensing produces an image “curve” surrounding the lens, it is either a circle in the case when the shear, i.e., a gravitational “pull” by a galaxy “far, far away”,  $= 0$ , or an ellipse.*



**Einstein Ring Gravitational Lenses**  
*Hubble Space Telescope • Advanced Camera for Surveys*

NASA, ESA, A. Bolton (Harvard-Smithsonian CfA), and the SLACS Team

STScI-PRC05-32

## “Isothermal” Elliptical Lenses

- The density, important from the physical viewpoint, is a so-called “isothermal density” obtained by projecting onto the lens plane the “realistic” three-dimensional density  $\sim 1/\rho^2$ , where  $\rho$  is the (three-dimensional) distance from the origin. It could be included into the whole class of densities that are constant on all ellipses *homothetic* rather than confocal with the given one.
- Lens equation becomes transcendental.

$$z - \text{const} \int_0^1 \frac{dt}{\sqrt{\bar{z}^2 - c^2 t^2}} - \gamma \bar{z} = w.$$

## Final Remarks

- An isothermal sphere with a shear is covered by '06 DK -G. Neumann theorem and may produce at most 4 images (observed).
- DK and E. Lundberg ('09) have proved that an isothermal elliptical lens without a shear may produce up to 8 bright images. Instantly, Bergweiler and Eremenko improved the estimate to 6 images, and showed that 6 is sharp. No more than 5 images (4 bright +1 dim) have been observed up to now.
- In 2000 Ch. Keeton, S. Mao and H. J. Witt constructed models with a tidal gravitational perturbation (shear) having 9, (8 bright + 1 dim), images.

## Three-Dimensional Lensing

- The 3-dimensional lens equation with mass-distribution  $dm(y)$  with source at  $\vec{w}$  becomes

$$\vec{x} - \nabla_x \left( \int \frac{dm(y)}{|x-y|} \right) = \vec{w}.$$

- If the mass-distribution  $dm(y)$  consists of  $n$  point-masses, there are some estimates for the maximal number of images (A. Petters, '90s) based on geometric topology (Morse theory). No sharp estimates are known.
- A difficult Maxwell's problem concerns a number of stationary points of the Newtonian potential of  $n$  point-masses (conjectured  $\leq (n-1)^2$ ). Most recent progress due to Eremenko, Gabrielov, D. Novikov, B. Shapiro. But this is the beginning of a new tale.

THANK YOU!

# DISCRETE HAAR WAVELET TRANSFORMS

Catherine Bénéteau

University of South Florida  
Tampa, FL USA

UNM - PNM Statewide Mathematics Contest, 2011

# A MINI HISTORY OF WAVELETS

- ▶ In the late 1970s, Morlet (trained at the Ecole Polytechnique), a geophysicist, became interested in signals that carried information related to geological layers.

## A MINI HISTORY OF WAVELETS

- ▶ In the late 1970s, Morlet (trained at the Ecole Polytechnique), a geophysicist, became interested in signals that carried information related to geological layers.
- ▶ **The problem:** Fourier analysis techniques lacked the ability to *zoom in* on a signal and find short varying high frequencies.

# A MINI HISTORY OF WAVELETS

- ▶ In the late 1970s, Morlet (trained at the Ecole Polytechnique), a geophysicist, became interested in signals that carried information related to geological layers.
- ▶ **The problem:** Fourier analysis techniques lacked the ability to *zoom in* on a signal and find short varying high frequencies.
- ▶ Morlet represented his signals via a special kind of function that is an ancestor of what we would call a wavelet today.

## A MINI HISTORY OF WAVELETS

- ▶ In the late 1970s, Morlet (trained at the Ecole Polytechnique), a geophysicist, became interested in signals that carried information related to geological layers.
- ▶ **The problem:** Fourier analysis techniques lacked the ability to *zoom in* on a signal and find short varying high frequencies.
- ▶ Morlet represented his signals via a special kind of function that is an ancestor of what we would call a wavelet today.
- ▶ But Morlet was a geophysicist, and wanted to make sure his work made sense mathematically, so he contacted Grossman (a quantum physicist), who gave an elegant proof that Morlet's representation worked.

## A MINI HISTORY OF WAVELETS

- ▶ In the late 1970s, Morlet (trained at the Ecole Polytechnique), a geophysicist, became interested in signals that carried information related to geological layers.
- ▶ **The problem:** Fourier analysis techniques lacked the ability to *zoom in* on a signal and find short varying high frequencies.
- ▶ Morlet represented his signals via a special kind of function that is an ancestor of what we would call a wavelet today.
- ▶ But Morlet was a geophysicist, and wanted to make sure his work made sense mathematically, so he contacted Grossman (a quantum physicist), who gave an elegant proof that Morlet's representation worked.
- ▶ In 1984, Yves Meyer (a mathematician) became acquainted with Morlet's work, and noticed right away that Morlet's functions were connected to some deep mathematics that had been worked on in the 1960s, and the subject took off from there.

# ENOUGH OF THIS HISTORY!

What would a math lecture be without an exam? It's time to take a test!

You are going to see three images. One is the original image consisting of **149604** bytes of information. A second image is a wavelet-compressed version of the original using **12253** bytes (about 8% of the original size), and another image is a wavelet-compressed version of the original using only **4452** bytes (about 3% of the original size)!

# ENOUGH OF THIS HISTORY!

**Question:** Which is which?

*The following images come from a really neat site developed and maintained by Osmar R. Zaïane at Simon Fraser University in Canada.*

# ENOUGH OF THIS HISTORY!



Image A

# ENOUGH OF THIS HISTORY!



Image B

# ENOUGH OF THIS HISTORY!



Image C

## ENOUGH OF THIS HISTORY!

## The Answer Key:

Image	Number of Bytes	Transfer Time*
Image A	4452	0.15 seconds
Image B	149604	5.00 seconds
Image C	12253	0.40 seconds

*\*This rate assumes a standard 56K dial up modem that typically connects at about 30K.*

## SO WHY WAVELETS?

- ▶ It is definitely new math - the subject took off in the late 80's/early 90's.

## SO WHY WAVELETS?

- ▶ It is definitely new math - the subject took off in the late 80's/early 90's.
- ▶ If you ask engineering or physics students to name some of the top accomplishments in their respective fields in the past 100 years, they can.

## SO WHY WAVELETS?

- ▶ It is definitely new math - the subject took off in the late 80's/early 90's.
- ▶ If you ask engineering or physics students to name some of the top accomplishments in their respective fields in the past 100 years, they can.
- ▶ Mathematics students, when asked the same question, typically struggle to name one or two.

## SO WHY WAVELETS?

- ▶ It is definitely new math - the subject took off in the late 80's/early 90's.
- ▶ If you ask engineering or physics students to name some of the top accomplishments in their respective fields in the past 100 years, they can.
- ▶ Mathematics students, when asked the same question, typically struggle to name one or two.
- ▶ The reason is most of the math we cover was developed hundreds of years ago and most of those famous mathematicians are ...

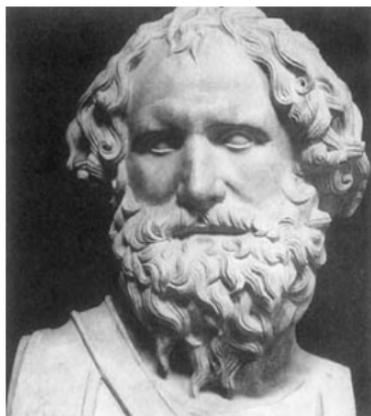
# SO WHY WAVELETS?



Isaac Newton - Dead ... for a VERY long time.



# SO WHY WAVELETS?



Archimedes - Fossilized.

## SO WHY WAVELETS?



C.F. Gauss - Dead .... But Brain is Still Around.

## SO WHY WAVELETS?



Alfred Haar - Dead .... Ok, so we're still talking about him.

# SO WHY WAVELETS?

But wavelet theory is *new* math and the major players are...

# SO WHY WAVELETS?



Ingrid Daubechies - Still Alive!

# SO WHY WAVELETS?



David Donoho - Still Alive!

# SO WHY WAVELETS?



Yves Meyer - Blurry, But Still Alive!



## SO WHY WAVELETS?

Applications involving wavelets are numerous. Here are two:

- ▶ The **FBI** uses wavelets to digitally compress fingerprints. The compression factor is between 40 and 100 times the original size of the fingerprint!

## SO WHY WAVELETS?

Applications involving wavelets are numerous. Here are two:

- ▶ The **FBI** uses wavelets to digitally compress fingerprints. The compression factor is between 40 and 100 times the original size of the fingerprint!
- ▶ Starting in 2000, the **Joint Photographic Experts Group**, designers of the popular **.jpg** image format used on the web, began implementing wavelet techniques in their format scheme.

## SO WHY WAVELETS?

And two more:

- ▶ **Kodak Polychrome Graphics**, a Twin Cities' based company, produces extremely high resolution digital images for advertisements that appear in publications like **Time Magazine**. They use wavelets to allow their clients to quickly analyze parts of the image.

## SO WHY WAVELETS?

And two more:

- ▶ **Kodak Polychrome Graphics**, a Twin Cities' based company, produces extremely high resolution digital images for advertisements that appear in publications like **Time Magazine**. They use wavelets to allow their clients to quickly analyze parts of the image.
- ▶ Wavelets have been heavily utilized in the modeling of distant galaxies. Wavelets have helped astronomers locate a subcluster of galaxies in the Coma supercluster of 1,400 galaxies! (*Quantum Vol. 15 No. 3*)

## SO WHY WAVELETS?

And one more:

- ▶ Musicologists restore an 1889 recording of Brahms playing his **Hungarian Dance Number 1** from a wax cylinder recording in such bad shape that many listeners failed to recognize that a piano was even being played. (*Quantum Vol. 15 No. 3*)

# DIGITAL IMAGES

## GRAYSCALE IMAGE BASICS

# DIGITAL IMAGES

## GRAYSCALE IMAGE BASICS

- ▶ A *bit* is a fundamental unit on a computer - either 0 or 1.

# DIGITAL IMAGES

## GRAYSCALE IMAGE BASICS

- ▶ A *bit* is a fundamental unit on a computer - either 0 or 1.
- ▶ A *byte* is 8 bits. There are  $2^8 = 256$  possible bytes. There are also 256 characters on a standard keyboard!

# DIGITAL IMAGES

## GRAYSCALE IMAGE BASICS

- ▶ A *bit* is a fundamental unit on a computer - either 0 or 1.
- ▶ A *byte* is 8 bits. There are  $2^8 = 256$  possible bytes. There are also 256 characters on a standard keyboard!
- ▶ The **A**merican **S**tandard **C**ode for **I**nformation **I**nterchange (ASCII) assigns to each byte a *character*.

# DIGITAL IMAGES

## GRAYSCALE IMAGE BASICS

- ▶ A *bit* is a fundamental unit on a computer - either 0 or 1.
- ▶ A *byte* is 8 bits. There are  $2^8 = 256$  possible bytes. There are also 256 characters on a standard keyboard!
- ▶ The **A**merican **S**tandard **C**ode for **I**nformation **I**nterchange (ASCII) assigns to each byte a *character*.
- ▶ Some of these characters are visible on a standard computer keyboard (eg., *y* is 121 and *0* is 48).

# DIGITAL IMAGES

## GRAYSCALE IMAGE BASICS

Dec	Hex	Char	Dec	Hex	Char	Dec	Hex	Char	Dec	Hex	Char
0	00	Null	32	20	Space	64	40	@	96	60	`
1	01	Start of heading	33	21	!	65	41	A	97	61	a
2	02	Start of text	34	22	"	66	42	B	98	62	b
3	03	End of text	35	23	#	67	43	C	99	63	c
4	04	End of transmit	36	24	\$	68	44	D	100	64	d
5	05	Enquiry	37	25	%	69	45	E	101	65	e
6	06	Acknowledge	38	26	&	70	46	F	102	66	f
7	07	Audible bell	39	27	'	71	47	G	103	67	g
8	08	Backspace	40	28	(	72	48	H	104	68	h
9	09	Horizontal tab	41	29	)	73	49	I	105	69	i
10	0A	Line feed	42	2A	*	74	4A	J	106	6A	j
11	0B	Vertical tab	43	2B	+	75	4B	K	107	6B	k
12	0C	Form feed	44	2C	,	76	4C	L	108	6C	l
13	0D	Carriage return	45	2D	-	77	4D	M	109	6D	m
14	0E	Shift out	46	2E	.	78	4E	N	110	6E	n
15	0F	Shift in	47	2F	/	79	4F	O	111	6F	o
16	10	Data link escape	48	30	0	80	50	P	112	70	p
17	11	Device control 1	49	31	1	81	51	Q	113	71	q
18	12	Device control 2	50	32	2	82	52	R	114	72	r
19	13	Device control 3	51	33	3	83	53	S	115	73	s
20	14	Device control 4	52	34	4	84	54	T	116	74	t
21	15	Neg. acknowledge	53	35	5	85	55	U	117	75	u
22	16	Synchronous idle	54	36	6	86	56	V	118	76	v
23	17	End trans. block	55	37	7	87	57	W	119	77	w
24	18	Cancel	56	38	8	88	58	X	120	78	x
25	19	End of medium	57	39	9	89	59	Y	121	79	y
26	1A	Substitution	58	3A	:	90	5A	Z	122	7A	z
27	1B	Escape	59	3B	;	91	5B	[	123	7B	(
28	1C	File separator	60	3C	<	92	5C	\	124	7C	
29	1D	Group separator	61	3D	=	93	5D	]	125	7D	)
30	1E	Record separator	62	3E	>	94	5E	^	126	7E	~
31	1F	Unit separator	63	3F	?	95	5F	_	127	7F	□

## DIGITAL IMAGES

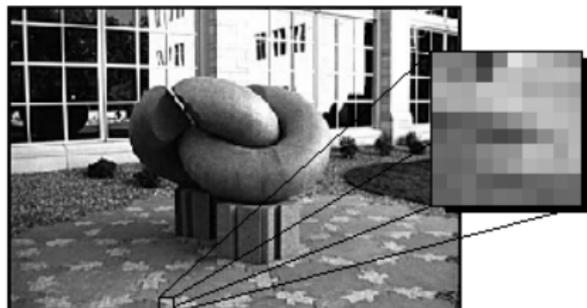
## GRAYSCALE IMAGE BASICS

Dec	Hex	Char									
128	80	Ç	160	A0	á	192	C0	Ł	224	E0	α
129	81	ü	161	A1	í	193	C1	ł	225	E1	β
130	82	é	162	A2	ó	194	C2	ŧ	226	E2	Γ
131	83	á	163	A3	ú	195	C3	ł	227	E3	π
132	84	ä	164	A4	ř	196	C4	—	228	E4	Σ
133	85	å	165	A5	Ň	197	C5	†	229	E5	σ
134	86	ã	166	A6	ª	198	C6	‡	230	E6	μ
135	87	ç	167	A7	º	199	C7	‡	231	E7	τ
136	88	ê	168	A8	¿	200	C8	£	232	E8	φ
137	89	ë	169	A9	ƒ	201	C9	ƒ	233	E9	θ
138	8A	è	170	AA	ŕ	202	CA	£	234	EA	Ω
139	8B	ì	171	AB	½	203	CB	ƒ	235	EB	δ
140	8C	í	172	AC	¾	204	CC	ƒ	236	EC	∞
141	8D	î	173	AD	ı	205	CD	=	237	ED	ø
142	8E	ÿ	174	AE	«	206	CE	‡	238	EE	τ
143	8F	ÿ	175	AF	»	207	CF	£	239	EF	∩
144	90	Ë	176	B0	⋮	208	DO	£	240	FO	≡
145	91	æ	177	B1	⋮	209	D1	ƒ	241	F1	±
146	92	Æ	178	B2	■	210	D2	ƒ	242	F2	≥
147	93	ó	179	B3		211	D3	£	243	F3	≤
148	94	ö	180	B4	†	212	D4	£	244	F4	{
149	95	õ	181	B5	†	213	D5	ƒ	245	F5	}
150	96	ù	182	B6		214	D6	ƒ	246	F6	÷
151	97	ù	183	B7		215	D7	‡	247	F7	⁄
152	98	ÿ	184	B8	¶	216	D8	†	248	F8	*
153	99	ÿ	185	B9	¶	217	D9	‡	249	F9	.
154	9A	Û	186	BA		218	DA	ƒ	250	FA	·
155	9B	ö	187	BB	¶	219	DB	■	251	FB	√
156	9C	£	188	BC	¶	220	DC	■	252	FC	°
157	9D	¥	189	BD	¶	221	DD		253	FD	°
158	9E	£	190	BE	¶	222	DE		254	FE	■
159	9F	f	191	BF	¶	223	DF	■	255	FF	□

# DIGITAL IMAGES

## GRAYSCALE IMAGE BASICS

An *8-bit* digital image can be viewed as a matrix whose entries (known as *pixels*) range from 0 (black) to 255 (white).



$$\begin{bmatrix}
 129 & 128 & 121 & 51 & 127 & 224 & 201 & 179 & 159 & 140 \\
 148 & 116 & 130 & 75 & 184 & 191 & 182 & 185 & 186 & 180 \\
 175 & 169 & 166 & 195 & 195 & 192 & 168 & 173 & 166 & 158 \\
 157 & 171 & 169 & 182 & 199 & 205 & 191 & 191 & 180 & 172 \\
 73 & 89 & 96 & 100 & 122 & 143 & 166 & 190 & 188 & 180 \\
 93 & 107 & 103 & 81 & 70 & 77 & 106 & 139 & 165 & 181 \\
 106 & 105 & 112 & 132 & 144 & 147 & 189 & 183 & 158 & 184 \\
 102 & 100 & 106 & 124 & 140 & 157 & 179 & 175 & 168 & 175 \\
 91 & 105 & 112 & 93 & 86 & 85 & 100 & 104 & 110 & 106 \\
 97 & 97 & 112 & 102 & 113 & 111 & 105 & 94 & 103 & 104
 \end{bmatrix}$$

# DIGITAL IMAGES

## GRAYSCALE IMAGE BASICS

- ▶ Thus if we store an intensity value, say 121, to disk, we don't store 121, we store its ASCII character  $y$ .

# DIGITAL IMAGES

## GRAYSCALE IMAGE BASICS

- ▶ Thus if we store an intensity value, say 121, to disk, we don't store 121, we store its ASCII character  $y$ .
- ▶  $y$  also has a binary representation:  $01111001_2$ .

# DIGITAL IMAGES

## GRAYSCALE IMAGE BASICS

- ▶ Thus if we store an intensity value, say 121, to disk, we don't store 121, we store its ASCII character  $y$ .
- ▶  $y$  also has a binary representation:  $01111001_2$ .
- ▶ Thus if an image has dimensions  $N \times M$ , we need  $8MN$  bits to store it on disk (modulo some header information).

# DIGITAL IMAGES

## GRAYSCALE IMAGE BASICS

- ▶ Thus if we store an intensity value, say 121, to disk, we don't store 121, we store its ASCII character  $y$ .
- ▶  $y$  also has a binary representation:  $01111001_2$ .
- ▶ Thus if an image has dimensions  $N \times M$ , we need  $8MN$  bits to store it on disk (modulo some header information).
- ▶ We will refer to the stored image as the *bitstream* and note that the bits per pixel (*bpp*) is 8.

# HUFFMAN CODING

- ▶ In 1952, **David Huffman** made a simple observation:

# HUFFMAN CODING

- ▶ In 1952, **David Huffman** made a simple observation:
- ▶ *Rather than use the same number of bits to represent each character, why not use a short bit stream for characters that appear often in an image and a longer bit stream for characters that appear infrequently in the image?*

# HUFFMAN CODING

- ▶ In 1952, **David Huffman** made a simple observation:
- ▶ *Rather than use the same number of bits to represent each character, why not use a short bit stream for characters that appear often in an image and a longer bit stream for characters that appear infrequently in the image?*
- ▶ He then developed an algorithm to do just that. We refer to his simple algorithm as **Huffman coding**. We will illustrate the algorithm via an example.

# HUFFMAN CODING

- ▶ Suppose you want to perform Huffman coding on the word **seesaws**.

# HUFFMAN CODING

- ▶ Suppose you want to perform Huffman coding on the word **seesaws**.
- ▶ First observe that *s* appears three times (24 bits), *e* appears twice (16 bits), and *a* and *w* each appear once (16 bits) so the total number of bits needed to represent *seesaws* is 56.

## HUFFMAN CODING

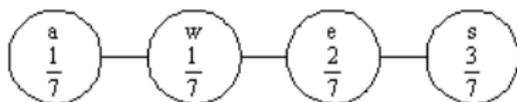
Char.	ASCII	Binary	Frequency
s	115	01110011 <sub>2</sub>	3
e	101	01100101 <sub>2</sub>	2
a	97	01100001 <sub>2</sub>	1
w	119	01110111 <sub>2</sub>	1

So in terms of bits, the word **seesaws** is

01110011 01100101 01100101 01110011 01100001 01110111 01110011

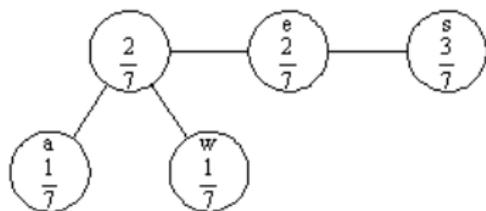
# HUFFMAN CODING

The first step in Huffman coding is as follows: Assign probabilities to each character and then sort from smallest to largest. We will put the probabilities in circles called **nodes** and connect them with lines (**branches**).



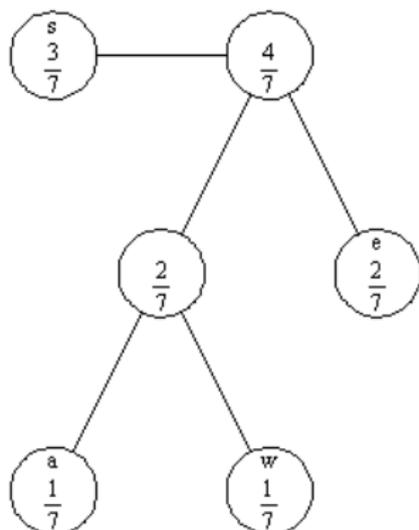
## HUFFMAN CODING

Now simply add the two smallest probabilities to create a new node with probability  $2/7$ . Branch the two small nodes off this one and resort the three remaining nodes:



# HUFFMAN CODING

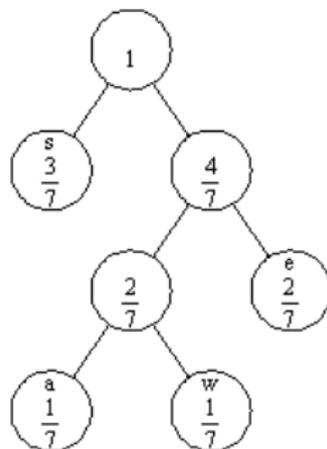
Again we add the smallest two probabilities on the top row ( $2/7 + 2/7 = 4/7$ ), create a new node with everything below these nodes as branches and sort again:



# HUFFMAN CODING

Since only two nodes remain on top, we simply add the probabilities of these nodes together to get 1 and obtain our finished tree:

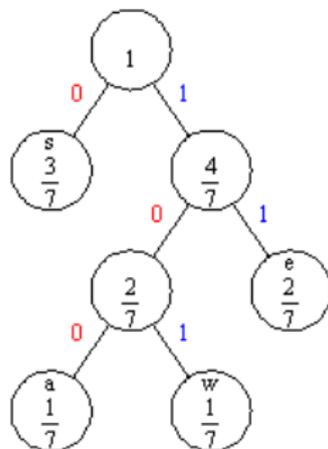
## HUFFMAN CODING



# HUFFMAN CODING

Now assign to each left branch the value 0 and to each right branch the value 1:

## HUFFMAN CODING



# HUFFMAN CODING

- ▶ We can read the new bit stream for each character right off the tree!

# HUFFMAN CODING

- ▶ We can read the new bit stream for each character right off the tree!
- ▶ Here are the new bit streams for the four characters:

## HUFFMAN CODING

Char.	Binary
s	$0_2$
e	$11_2$
a	$100_2$
w	$101_2$

# HUFFMAN CODING

- ▶ Since  $s$  appears three times in *seesaws*, we need 3 bits to represent them. The character  $e$  appears twice (4 bits), and  $a$  and  $w$  each appear once (3 bits each).

# HUFFMAN CODING

- ▶ Since  $s$  appears three times in *seesaws*, we need 3 bits to represent them. The character  $e$  appears twice (4 bits), and  $a$  and  $w$  each appear once (3 bits each).
- ▶ The total number of bits we need to represent the word *seesaws* is 13 bits! Recall without Huffman coding, we needed 56 bits so we have reduced the number of bits needed by a factor of 4!

# HUFFMAN CODING

- ▶ Since *s* appears three times in *seesaws*, we need 3 bits to represent them. The character *e* appears twice (4 bits), and *a* and *w* each appear once (3 bits each).
- ▶ The total number of bits we need to represent the word *seesaws* is 13 bits! Recall without Huffman coding, we needed 56 bits so we have reduced the number of bits needed by a factor of 4!
- ▶ Here is the word *seesaws* using the Huffman codes for each character:

0111101001010

## ENCODING AN IMAGE

- ▶ The example is a bit of a sales job - of course we will enjoy great savings with only 4 distinct characters. What happens when we apply Huffman coding to a digital image?
- ▶ Consider the  $200 \times 200$  image



# ENCODING AN IMAGE

- ▶ Unencoded, we need 320000 bits or 8 *bits per pixel* (bpp) to represent the image.

## ENCODING AN IMAGE

- ▶ Unencoded, we need 320000 bits or 8 *bits per pixel* (bpp) to represent the image.
- ▶ Using Huffman encoding, we only need 266993 bits to store the image.

## ENCODING AN IMAGE

- ▶ Unencoded, we need 320000 bits or 8 *bits per pixel* (bpp) to represent the image.
- ▶ Using Huffman encoding, we only need 266993 bits to store the image.
- ▶ This constitutes a 16.5% savings or an average of 6.67bpp.

## ENCODING AN IMAGE

- ▶ Unencoded, we need 320000 bits or 8 *bits per pixel* (bpp) to represent the image.
- ▶ Using Huffman encoding, we only need 266993 bits to store the image.
- ▶ This constitutes a 16.5% savings or an average of 6.67bpp.
- ▶ We should be able to do better . . .

## ENCODING AN IMAGE

- ▶ Unencoded, we need 320000 bits or 8 *bits per pixel* (bpp) to represent the image.
- ▶ Using Huffman encoding, we only need 266993 bits to store the image.
- ▶ This constitutes a 16.5% savings or an average of 6.67bpp.
- ▶ We should be able to do better . . .
- ▶ What really helps an encoding method is a *preprocessor* that transforms the image to a setting that is a bit more amenable to the encoding scheme.

## ENCODING AN IMAGE

- ▶ Unencoded, we need 320000 bits or 8 *bits per pixel* (bpp) to represent the image.
- ▶ Using Huffman encoding, we only need 266993 bits to store the image.
- ▶ This constitutes a 16.5% savings or an average of 6.67bpp.
- ▶ We should be able to do better . . .
- ▶ What really helps an encoding method is a *preprocessor* that transforms the image to a setting that is a bit more amenable to the encoding scheme.
- ▶ That's where the discrete wavelet transform comes in!

# CHALLENGE PROBLEMS

- ▶ Get with a partner, and each partner should choose a word or short phrase and determine the Huffman codes for each letter.

# CHALLENGE PROBLEMS

- ▶ Get with a partner, and each partner should choose a word or short phrase and determine the Huffman codes for each letter.
- ▶ Write the word as a binary string using the Huffman codes.

# CHALLENGE PROBLEMS

- ▶ Get with a partner, and each partner should choose a word or short phrase and determine the Huffman codes for each letter.
- ▶ Write the word as a binary string using the Huffman codes.
- ▶ Give the string and the codes (dictionary) to your partner.

# CHALLENGE PROBLEMS

- ▶ Get with a partner, and each partner should choose a word or short phrase and determine the Huffman codes for each letter.
- ▶ Write the word as a binary string using the Huffman codes.
- ▶ Give the string and the codes (dictionary) to your partner.
- ▶ The partner should determine the word or phrase.

# CHALLENGE PROBLEMS

- ▶ Get with a partner, and each partner should choose a word or short phrase and determine the Huffman codes for each letter.
- ▶ Write the word as a binary string using the Huffman codes.
- ▶ Give the string and the codes (dictionary) to your partner.
- ▶ The partner should determine the word or phrase.
- ▶ Given the Huffman codes  $g = 10$ ,  $n = 01$ ,  $o = 00$ , space key =  $110$ ,  $e = 1110$ , and  $i = 1111$ , decode the bit stream  $1000111101101101000111101101101000011110$ .

# CHALLENGE PROBLEMS

- ▶ Are Huffman codes unique? In other words, given a word or a phrase, is it possible to have more than one Huffman code for that word or phrase?

# CHALLENGE PROBLEMS

- ▶ Are Huffman codes unique? In other words, given a word or a phrase, is it possible to have more than one Huffman code for that word or phrase?
- ▶ Are Huffman codes invertible? In other words, given a bit stream and a Huffman code tree or dictionary, can I *always* translate the bit stream?

# CHALLENGE PROBLEMS

- ▶ Are Huffman codes unique? In other words, given a word or a phrase, is it possible to have more than one Huffman code for that word or phrase?
- ▶ Are Huffman codes invertible? In other words, given a bit stream and a Huffman code tree or dictionary, can I *always* translate the bit stream?
- ▶ Is it possible to design a word so that one letter has as its code 0 and the other letter has as its code 1?

# CHALLENGE PROBLEMS

- ▶ Are Huffman codes unique? In other words, given a word or a phrase, is it possible to have more than one Huffman code for that word or phrase?
- ▶ Are Huffman codes invertible? In other words, given a bit stream and a Huffman code tree or dictionary, can I *always* translate the bit stream?
- ▶ Is it possible to design a word so that one letter has as its code 0 and the other letter has as its code 1?
- ▶ For a word of length greater than 2, is it possible for all the letters to have the same code length?

# NAIVE DATA APPROXIMATION

- ▶ Suppose you are given  $N$  values

$$\mathbf{x} = (x_1, x_2, \dots, x_N)$$

where  $N$  is even.

# NAIVE DATA APPROXIMATION

- ▶ Suppose you are given  $N$  values

$$\mathbf{x} = (x_1, x_2, \dots, x_N)$$

where  $N$  is even.

- ▶ **Your task:** Send an approximation  $\mathbf{s}$  (a list of numbers) of this data via the internet to a colleague.

# NAIVE DATA APPROXIMATION

- ▶ Suppose you are given  $N$  values

$$\mathbf{x} = (x_1, x_2, \dots, x_N)$$

where  $N$  is even.

- ▶ **Your task:** Send an approximation  $\mathbf{s}$  (a list of numbers) of this data via the internet to a colleague.
- ▶ In order to reduce transfer time, the length of your approximation must be  $N/2$ .

# NAIVE DATA APPROXIMATION

- ▶ Suppose you are given  $N$  values

$$\mathbf{x} = (x_1, x_2, \dots, x_N)$$

where  $N$  is even.

- ▶ **Your task:** Send an approximation  $\mathbf{s}$  (a list of numbers) of this data via the internet to a colleague.
- ▶ In order to reduce transfer time, the length of your approximation must be  $N/2$ .
- ▶ How do you suggest we do it?

# NAIVE DATA APPROXIMATION

- ▶ One solution is to pair-wise average the numbers:

$$s_k = \frac{x_{2k-1} + x_{2k}}{2}, \quad k = 1, \dots, N/2$$

# NAIVE DATA APPROXIMATION

- ▶ One solution is to pair-wise average the numbers:

$$s_k = \frac{x_{2k-1} + x_{2k}}{2}, \quad k = 1, \dots, N/2$$

- ▶ For example:

$$\mathbf{x} = (6, 12, 15, 15, 14, 12, 120, 116) \rightarrow \mathbf{s} = (9, 15, 13, 118)$$



- ▶ Suppose now you were allowed to send extra data in addition to the pair-wise averages list  $\mathbf{s}$ .

- ▶ Suppose now you were allowed to send extra data in addition to the pair-wise averages list  $\mathbf{s}$ .
- ▶ The idea is to send a second list of data  $\mathbf{d}$  so that the original list  $\mathbf{x}$  can be recovered from  $\mathbf{s}$  and  $\mathbf{d}$ .

- ▶ Suppose now you were allowed to send extra data in addition to the pair-wise averages list  $\mathbf{s}$ .
- ▶ The idea is to send a second list of data  $\mathbf{d}$  so that the original list  $\mathbf{x}$  can be recovered from  $\mathbf{s}$  and  $\mathbf{d}$ .
- ▶ How would you do it?

- ▶ There are a couple of choices for  $d_k$  (called **directed distances**):

- ▶ There are a couple of choices for  $d_k$  (called **directed distances**):
- ▶ We could set

$$d_k = \frac{x_{2k-1} - x_{2k}}{2}, \quad k = 1, \dots, N/2$$

- ▶ There are a couple of choices for  $d_k$  (called **directed distances**):
- ▶ We could set

$$d_k = \frac{x_{2k-1} - x_{2k}}{2}, \quad k = 1, \dots, N/2$$

- ▶ or

$$d_k = \frac{x_{2k} - x_{2k-1}}{2}, \quad k = 1, \dots, N/2$$

- ▶ There are a couple of choices for  $d_k$  (called **directed distances**):
- ▶ We could set

$$d_k = \frac{x_{2k-1} - x_{2k}}{2}, \quad k = 1, \dots, N/2$$

- ▶ or

$$d_k = \frac{x_{2k} - x_{2k-1}}{2}, \quad k = 1, \dots, N/2$$

- ▶ We will use the second formula.

$$d_k = \frac{x_{2k} - x_{2k-1}}{2}, \quad k = 1, \dots, N/2$$

- ▶ The process is invertible since

$$s_k + d_k = \frac{x_{2k-1} + x_{2k}}{2} + \frac{x_{2k} - x_{2k-1}}{2} = x_{2k}$$

and

$$s_k - d_k = \frac{x_{2k-1} + x_{2k}}{2} - \frac{x_{2k} - x_{2k-1}}{2} = x_{2k-1}$$

- ▶ The process is invertible since

$$s_k + d_k = \frac{x_{2k-1} + x_{2k}}{2} + \frac{x_{2k} - x_{2k-1}}{2} = x_{2k}$$

and

$$s_k - d_k = \frac{x_{2k-1} + x_{2k}}{2} - \frac{x_{2k} - x_{2k-1}}{2} = x_{2k-1}$$

- ▶ So we map  $\mathbf{x} = (x_1, x_2, \dots, x_N)$  to  $(\mathbf{s} \mid \mathbf{d}) = (s_1, \dots, s_{N/2} \mid d_1, \dots, d_{N/2})$ .

- ▶ The process is invertible since

$$s_k + d_k = \frac{x_{2k-1} + x_{2k}}{2} + \frac{x_{2k} - x_{2k-1}}{2} = x_{2k}$$

and

$$s_k - d_k = \frac{x_{2k-1} + x_{2k}}{2} - \frac{x_{2k} - x_{2k-1}}{2} = x_{2k-1}$$

- ▶ So we map  $\mathbf{x} = (x_1, x_2, \dots, x_N)$  to  $(\mathbf{s} \mid \mathbf{d}) = (s_1, \dots, s_{N/2} \mid d_1, \dots, d_{N/2})$ .
- ▶ Using our example values we have

$$(6, 12, 15, 15, 14, 12, 120, 116) \rightarrow (9, 15, 13, 118 \mid 3, 0, -1, -2)$$

- ▶ The process is invertible since

$$s_k + d_k = \frac{x_{2k-1} + x_{2k}}{2} + \frac{x_{2k} - x_{2k-1}}{2} = x_{2k}$$

and

$$s_k - d_k = \frac{x_{2k-1} + x_{2k}}{2} - \frac{x_{2k} - x_{2k-1}}{2} = x_{2k-1}$$

- ▶ So we map  $\mathbf{x} = (x_1, x_2, \dots, x_N)$  to  $(\mathbf{s} \mid \mathbf{d}) = (s_1, \dots, s_{N/2} \mid d_1, \dots, d_{N/2})$ .
- ▶ Using our example values we have

$$(6, 12, 15, 15, 14, 12, 120, 116) \rightarrow (9, 15, 13, 118 \mid 3, 0, -1, -2)$$

- ▶ Why might people prefer the data in this form?

- ▶ We can identify large changes in the the differences portion  $\mathbf{d}$  of the transform.

- ▶ We can identify large changes in the the differences portion  $\mathbf{d}$  of the transform.
- ▶ It is easier to *quantize* the data in this form.

- ▶ We can identify large changes in the the differences portion  $\mathbf{d}$  of the transform.
- ▶ It is easier to *quantize* the data in this form.
- ▶ The transform concentrates the information (*energy*) in the signal in fewer values.

- ▶ We can identify large changes in the the differences portion  $\mathbf{d}$  of the transform.
- ▶ It is easier to *quantize* the data in this form.
- ▶ The transform concentrates the information (*energy*) in the signal in fewer values.
- ▶ And the obvious answer: **fewer digits!!**

- ▶ We can identify large changes in the the differences portion  $\mathbf{d}$  of the transform.
- ▶ It is easier to *quantize* the data in this form.
- ▶ The transform concentrates the information (*energy*) in the signal in fewer values.
- ▶ And the obvious answer: **fewer digits!!**
- ▶ We will talk about quantizing and image compression a little later.

- ▶ The transformation

$$\mathbf{x} = (x_1, \dots, x_N) \rightarrow (\mathbf{s} \mid \mathbf{d}) = (s_1, \dots, s_{N/2} \mid d_1, \dots, d_{N/2})$$

is (almost!) called the (1-dimensional) **Discrete Haar Wavelet Transformation**. (Actually, usually we would multiply by  $\sqrt{2}$  - why do you think we might do that?)

- ▶ The transformation

$$\mathbf{x} = (x_1, \dots, x_N) \rightarrow (\mathbf{s} \mid \mathbf{d}) = (s_1, \dots, s_{N/2} \mid d_1, \dots, d_{N/2})$$

is (almost!) called the (1-dimensional) **Discrete Haar Wavelet Transformation**. (Actually, usually we would multiply by  $\sqrt{2}$  - why do you think we might do that?)

- ▶ What does the transform look like as a matrix?

Consider applying the transform to an 8-vector. What is the matrix that works?

$$\begin{bmatrix} \phantom{x_1} \\ \phantom{x_2} \\ \phantom{x_3} \\ \phantom{x_4} \\ \phantom{x_5} \\ \phantom{x_6} \\ \phantom{x_7} \\ \phantom{x_8} \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \\ x_8 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} x_1 + x_2 \\ x_3 + x_4 \\ x_5 + x_6 \\ x_7 + x_8 \\ \hline x_2 - x_1 \\ x_4 - x_3 \\ x_6 - x_5 \\ x_8 - x_7 \end{bmatrix}$$

Consider applying the transform to an 8-vector. What is the matrix that works?

$$\begin{bmatrix}
 \frac{1}{2} & \frac{1}{2} & 0 & 0 & 0 & 0 & 0 & 0 \\
 0 & 0 & \frac{1}{2} & \frac{1}{2} & 0 & 0 & 0 & 0 \\
 0 & 0 & 0 & 0 & \frac{1}{2} & \frac{1}{2} & 0 & 0 \\
 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{2} & \frac{1}{2} \\
 \hline
 -\frac{1}{2} & \frac{1}{2} & 0 & 0 & 0 & 0 & 0 & 0 \\
 0 & 0 & -\frac{1}{2} & \frac{1}{2} & 0 & 0 & 0 & 0 \\
 0 & 0 & 0 & 0 & -\frac{1}{2} & \frac{1}{2} & 0 & 0 \\
 0 & 0 & 0 & 0 & 0 & 0 & -\frac{1}{2} & \frac{1}{2}
 \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \\ x_8 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} x_1 + x_2 \\ x_3 + x_4 \\ x_5 + x_6 \\ x_7 + x_8 \\ \hline x_2 - x_1 \\ x_4 - x_3 \\ x_6 - x_5 \\ x_8 - x_7 \end{bmatrix}$$

We will denote the transform matrix by  $W_8$ .

What about  $W_8^{-1}$ ? That is, what matrix solves

$$\begin{bmatrix} \phantom{x_1} \\ \phantom{x_2} \\ \phantom{x_3} \\ \phantom{x_4} \\ \phantom{x_5} \\ \phantom{x_6} \\ \phantom{x_7} \\ \phantom{x_8} \end{bmatrix} \cdot \left( \frac{1}{2} \begin{bmatrix} x_1 + x_2 \\ x_3 + x_4 \\ x_5 + x_6 \\ x_7 + x_8 \\ \hline x_2 - x_1 \\ x_4 - x_3 \\ x_6 - x_5 \\ x_8 - x_7 \end{bmatrix} \right) = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \\ x_8 \end{bmatrix}$$

What about  $W_8^{-1}$ ? That is, what matrix solves

$$\left[ \begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{array} \right] \cdot \left( \frac{1}{2} \begin{bmatrix} X_1 + X_2 \\ X_3 + X_4 \\ X_5 + X_6 \\ X_7 + X_8 \\ \hline X_2 - X_1 \\ X_4 - X_3 \\ X_6 - X_5 \\ X_8 - X_7 \end{bmatrix} \right) = \begin{bmatrix} X_1 \\ X_2 \\ X_3 \\ X_4 \\ X_5 \\ X_6 \\ X_7 \\ X_8 \end{bmatrix}$$

- ▶ The matrices  $W_8^{-1}$  and  $W_8^T$  are very closely connected!

- ▶ The matrices  $W_8^{-1}$  and  $W_8^T$  are very closely connected!
- ▶ In fact,  $2W_8^T = W_8^{-1}$ .

- ▶ The matrices  $W_8^{-1}$  and  $W_8^T$  are very closely connected!
- ▶ In fact,  $2W_8^T = W_8^{-1}$ .
- ▶ This makes  $W_8$  very close to being what we call an orthogonal matrix. (That's why we usually throw in a  $\sqrt{2}$ !)

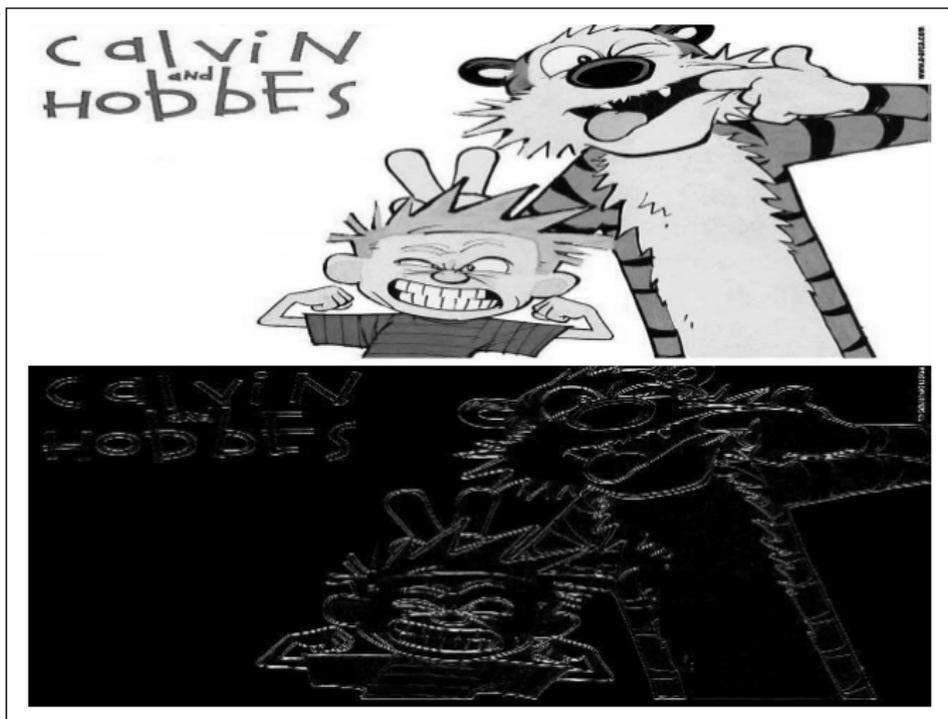
Consider the  $480 \times 640$  image (call it  $A$ )



If  $\mathbf{a}^1, \dots, \mathbf{a}^{640}$  are the columns of  $A$ , then computing  $W_{480}A$  is the same as applying the HWT to each column of  $A$ :

$$W_{480}A = (W_{480} \cdot \mathbf{a}^1, \dots, W_{480} \cdot \mathbf{a}^{640})$$

Graphically, we have



- ▶  $C = W_{480}A$  processes the **columns** of  $A$ .

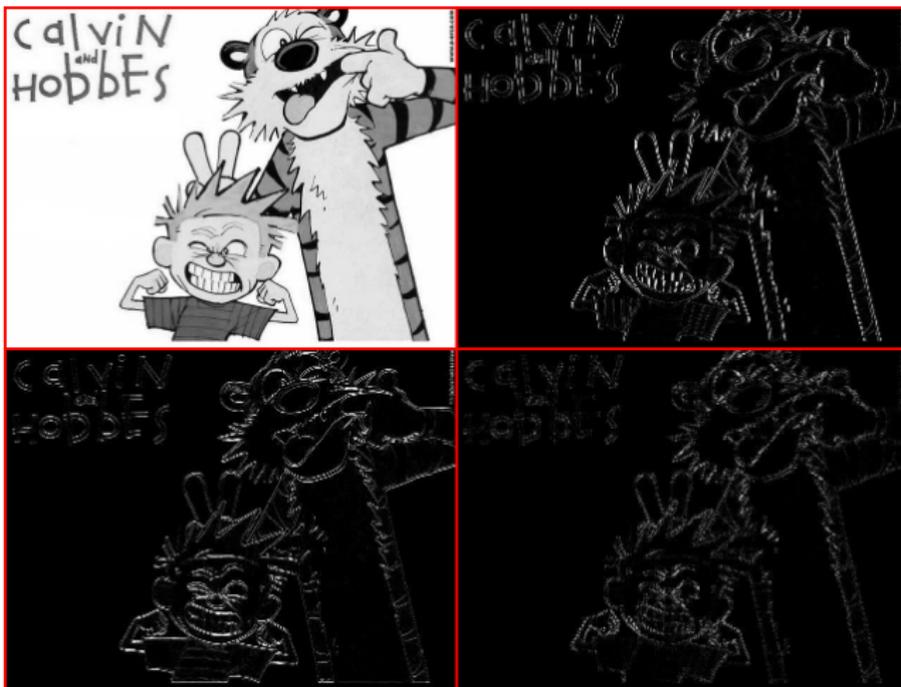
- ▶  $C = W_{480}A$  processes the **columns** of  $A$ .
- ▶ How would we process the **rows** of  $C$ ?

- ▶  $C = W_{480}A$  processes the **columns** of  $A$ .
- ▶ How would we process the **rows** of  $C$ ?
- ▶ We compute  $CW_{640}^T = W_{480}AW_{640}^T$ .

- ▶  $C = W_{480}A$  processes the **columns** of  $A$ .
- ▶ How would we process the **rows** of  $C$ ?
- ▶ We compute  $CW_{640}^T = W_{480}AW_{640}^T$ .
- ▶ The **two-dimensional Haar transform** of the  $M \times N$  matrix  $A$  is

$$B = W_M A W_N^T$$

Graphically, we have



- ▶ Can we interpret what the transformation does to the image?

- ▶ Can we interpret what the transformation does to the image?
- ▶ Suppose  $A$  is the  $4 \times 4$  matrix

$$A = \begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{bmatrix}$$

- ▶ Can we interpret what the transformation does to the image?
- ▶ Suppose  $A$  is the  $4 \times 4$  matrix

$$A = \begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{bmatrix}$$

- ▶ Partitioning  $W_4 = \begin{bmatrix} H \\ - \\ G \end{bmatrix}$ , we have

$$\begin{aligned}
 W_4 A W_4^T &= \begin{bmatrix} H \\ - \\ G \end{bmatrix} A \begin{bmatrix} H^T & | & G^T \end{bmatrix} \\
 &= \begin{bmatrix} HA \\ - \\ GA \end{bmatrix} \begin{bmatrix} H^T & | & G^T \end{bmatrix} \\
 &= \left[ \begin{array}{c|c} HA H^T & HA G^T \\ \hline GA H^T & GA G^T \end{array} \right]
 \end{aligned}$$

Let's look at each  $2 \times 2$  block individually:

$$\blacktriangleright \mathbf{HAH}^T = \frac{1}{4} \left[ \begin{array}{c|c} \mathbf{a}_{11} + \mathbf{a}_{12} + \mathbf{a}_{21} + \mathbf{a}_{22} & \mathbf{a}_{13} + \mathbf{a}_{14} + \mathbf{a}_{23} + \mathbf{a}_{24} \\ \hline \mathbf{a}_{31} + \mathbf{a}_{32} + \mathbf{a}_{41} + \mathbf{a}_{42} & \mathbf{a}_{33} + \mathbf{a}_{34} + \mathbf{a}_{43} + \mathbf{a}_{44} \end{array} \right]$$

$$\blacktriangleright \mathbf{HAH}^T = \frac{1}{4} \left[ \begin{array}{cc|cc} \mathbf{a}_{11} + \mathbf{a}_{12} + \mathbf{a}_{21} + \mathbf{a}_{22} & & \mathbf{a}_{13} + \mathbf{a}_{14} + \mathbf{a}_{23} + \mathbf{a}_{24} & \\ & & & \\ \hline \mathbf{a}_{31} + \mathbf{a}_{32} + \mathbf{a}_{41} + \mathbf{a}_{42} & & \mathbf{a}_{33} + \mathbf{a}_{34} + \mathbf{a}_{43} + \mathbf{a}_{44} & \\ & & & \end{array} \right]$$

$\blacktriangleright$  Partition  $A$  in  $2 \times 2$  blocks as

$$A = \left[ \begin{array}{cc|cc} \mathbf{a}_{11} & \mathbf{a}_{12} & \mathbf{a}_{13} & \mathbf{a}_{14} \\ \mathbf{a}_{21} & \mathbf{a}_{22} & \mathbf{a}_{23} & \mathbf{a}_{24} \\ \hline \mathbf{a}_{31} & \mathbf{a}_{32} & \mathbf{a}_{33} & \mathbf{a}_{34} \\ \mathbf{a}_{41} & \mathbf{a}_{42} & \mathbf{a}_{43} & \mathbf{a}_{44} \end{array} \right] = \left[ \begin{array}{c|c} \mathbf{A}_{11} & \mathbf{A}_{12} \\ \hline \mathbf{A}_{21} & \mathbf{A}_{22} \end{array} \right]$$

$$\blacktriangleright \mathit{HAH}^T = \frac{1}{4} \left[ \begin{array}{cc|cc} a_{11} + a_{12} + a_{21} + a_{22} & & a_{13} + a_{14} + a_{23} + a_{24} & \\ & & a_{33} + a_{34} + a_{43} + a_{44} & \\ \hline a_{31} + a_{32} + a_{41} + a_{42} & & & \end{array} \right]$$

- ▶ Partition  $A$  in  $2 \times 2$  blocks as

$$A = \left[ \begin{array}{cc|cc} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ \hline a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{array} \right] = \left[ \begin{array}{c|c} A_{11} & A_{12} \\ \hline A_{21} & A_{22} \end{array} \right]$$

- ▶ Then the  $(i, j)$  element of  $\mathit{HAH}^T$  is simply the average of the elements in  $A_{ij}$ !

$$\blacktriangleright HAH^T = \frac{1}{4} \left[ \begin{array}{cc|cc} a_{11} + a_{12} + a_{21} + a_{22} & a_{13} + a_{14} + a_{23} + a_{24} \\ a_{31} + a_{32} + a_{41} + a_{42} & a_{33} + a_{34} + a_{43} + a_{44} \end{array} \right]$$

- ▶ Partition  $A$  in  $2 \times 2$  blocks as

$$A = \left[ \begin{array}{cc|cc} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ \hline a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{array} \right] = \left[ \begin{array}{c|c} A_{11} & A_{12} \\ \hline A_{21} & A_{22} \end{array} \right]$$

- ▶ Then the  $(i, j)$  element of  $HAH^T$  is simply the average of the elements in  $A_{ij}$ !
- ▶ So  $HAH^T$  is an approximation or **blur** of the original image. We will denote  $HAH^T$  as  $\mathcal{B}$ .

- ▶ The upper right hand corner is

$$HAG^T = \frac{1}{4} \begin{bmatrix} (a_{12} + a_{22}) - (a_{11} + a_{21}) & (a_{14} + a_{24}) - (a_{13} + a_{23}) \\ (a_{32} + a_{42}) - (a_{31} + a_{41}) & (a_{34} + a_{44}) - (a_{33} + a_{43}) \end{bmatrix}$$

- ▶ The upper right hand corner is

$$HAG^T = \frac{1}{4} \begin{bmatrix} (a_{12} + a_{22}) - (a_{11} + a_{21}) & (a_{14} + a_{24}) - (a_{13} + a_{23}) \\ (a_{32} + a_{42}) - (a_{31} + a_{41}) & (a_{34} + a_{44}) - (a_{33} + a_{43}) \end{bmatrix}$$

- ▶ Partition  $A$  in  $2 \times 2$  blocks as

$$A = \left[ \begin{array}{cc|cc} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ \hline a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{array} \right] = \left[ \begin{array}{c|c} A_{11} & A_{12} \\ \hline A_{21} & A_{22} \end{array} \right]$$

- ▶ The upper right hand corner is

$$HAG^T = \frac{1}{4} \begin{bmatrix} (a_{12} + a_{22}) - (a_{11} + a_{21}) & (a_{14} + a_{24}) - (a_{13} + a_{23}) \\ (a_{32} + a_{42}) - (a_{31} + a_{41}) & (a_{34} + a_{44}) - (a_{33} + a_{43}) \end{bmatrix}$$

- ▶ Partition  $A$  in  $2 \times 2$  blocks as

$$A = \left[ \begin{array}{cc|cc} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ \hline a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{array} \right] = \left[ \begin{array}{c|c} A_{11} & A_{12} \\ \hline A_{21} & A_{22} \end{array} \right]$$

- ▶ The  $(i, j)$  element of  $HAG^T$  can be viewed as a difference between columns of  $A_{ij}$ .

- ▶ The upper right hand corner is

$$HAG^T = \frac{1}{4} \begin{bmatrix} (a_{12} + a_{22}) - (a_{11} + a_{21}) & (a_{14} + a_{24}) - (a_{13} + a_{23}) \\ (a_{32} + a_{42}) - (a_{31} + a_{41}) & (a_{34} + a_{44}) - (a_{33} + a_{43}) \end{bmatrix}$$

- ▶ Partition  $A$  in  $2 \times 2$  blocks as

$$A = \left[ \begin{array}{cc|cc} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ \hline a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{array} \right] = \left[ \begin{array}{c|c} A_{11} & A_{12} \\ \hline A_{21} & A_{22} \end{array} \right]$$

- ▶ The  $(i, j)$  element of  $HAG^T$  can be viewed as a difference between columns of  $A_{ij}$ .
- ▶ We will denote  $HAG^T$  as  $\mathcal{V}$  (for vertical differences).

- The lower left hand corner is

$$GAH^T = \frac{1}{4} \begin{bmatrix} (a_{21} + a_{22}) - (a_{12} + a_{11}) & (a_{23} + a_{24}) - (a_{13} + a_{14}) \\ (a_{31} + a_{32}) - (a_{42} + a_{41}) & (a_{43} + a_{44}) - (a_{33} + a_{34}) \end{bmatrix}$$

- ▶ The lower left hand corner is

$$GAH^T = \frac{1}{4} \begin{bmatrix} (a_{21} + a_{22}) - (a_{12} + a_{11}) & (a_{23} + a_{24}) - (a_{13} + a_{14}) \\ (a_{31} + a_{32}) - (a_{42} + a_{41}) & (a_{43} + a_{44}) - (a_{33} + a_{34}) \end{bmatrix}$$

- ▶ Partition  $A$  in  $2 \times 2$  blocks as

$$A = \left[ \begin{array}{cc|cc} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ \hline a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{array} \right] = \left[ \begin{array}{c|c} A_{11} & A_{12} \\ \hline A_{21} & A_{22} \end{array} \right]$$

- ▶ The lower left hand corner is

$$GAH^T = \frac{1}{4} \begin{bmatrix} (a_{21} + a_{22}) - (a_{12} + a_{11}) & (a_{23} + a_{24}) - (a_{13} + a_{14}) \\ (a_{31} + a_{32}) - (a_{42} + a_{41}) & (a_{43} + a_{44}) - (a_{33} + a_{34}) \end{bmatrix}$$

- ▶ Partition  $A$  in  $2 \times 2$  blocks as

$$A = \left[ \begin{array}{cc|cc} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ \hline a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{array} \right] = \left[ \begin{array}{c|c} A_{11} & A_{12} \\ \hline A_{21} & A_{22} \end{array} \right]$$

- ▶ The  $(i, j)$  element of  $HAG^T$  can be viewed as a difference between rows of  $A_{ij}$ .

- ▶ The lower left hand corner is

$$GAH^T = \frac{1}{4} \begin{bmatrix} (a_{21} + a_{22}) - (a_{12} + a_{11}) & (a_{23} + a_{24}) - (a_{13} + a_{14}) \\ (a_{31} + a_{32}) - (a_{42} + a_{41}) & (a_{43} + a_{44}) - (a_{33} + a_{34}) \end{bmatrix}$$

- ▶ Partition  $A$  in  $2 \times 2$  blocks as

$$A = \left[ \begin{array}{cc|cc} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ \hline a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{array} \right] = \left[ \begin{array}{c|c} A_{11} & A_{12} \\ \hline A_{21} & A_{22} \end{array} \right]$$

- ▶ The  $(i, j)$  element of  $HAG^T$  can be viewed as a difference between rows of  $A_{ij}$ .
- ▶ We will denote  $GAH^T$  as  $\mathcal{H}$  (for horizontal differences).

- The lower right hand corner is

$$GAG^T = \frac{1}{4} \begin{bmatrix} (a_{11} + a_{22}) - (a_{12} + a_{21}) & (a_{13} + a_{24}) - (a_{23} + a_{14}) \\ (a_{31} + a_{42}) - (a_{32} + a_{41}) & (a_{33} + a_{44}) - (a_{43} + a_{34}) \end{bmatrix}$$

- ▶ The lower right hand corner is

$$GAG^T = \frac{1}{4} \begin{bmatrix} (a_{11} + a_{22}) - (a_{12} + a_{21}) & (a_{13} + a_{24}) - (a_{23} + a_{14}) \\ (a_{31} + a_{42}) - (a_{32} + a_{41}) & (a_{33} + a_{44}) - (a_{43} + a_{34}) \end{bmatrix}$$

- ▶ Partition  $A$  in  $2 \times 2$  blocks as

$$A = \left[ \begin{array}{cc|cc} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ \hline a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{array} \right] = \left[ \begin{array}{c|c} A_{11} & A_{12} \\ \hline A_{21} & A_{22} \end{array} \right]$$

- ▶ The lower right hand corner is

$$GAG^T = \frac{1}{4} \begin{bmatrix} (a_{11} + a_{22}) - (a_{12} + a_{21}) & (a_{13} + a_{24}) - (a_{23} + a_{14}) \\ (a_{31} + a_{42}) - (a_{32} + a_{41}) & (a_{33} + a_{44}) - (a_{43} + a_{34}) \end{bmatrix}$$

- ▶ Partition  $A$  in  $2 \times 2$  blocks as

$$A = \left[ \begin{array}{cc|cc} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ \hline a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{array} \right] = \left[ \begin{array}{c|c} A_{11} & A_{12} \\ \hline A_{21} & A_{22} \end{array} \right]$$

- ▶ The  $(i, j)$  element of  $GAG^T$  can be viewed as a difference between the diagonals of  $A_{ij}$ .

- ▶ The lower right hand corner is

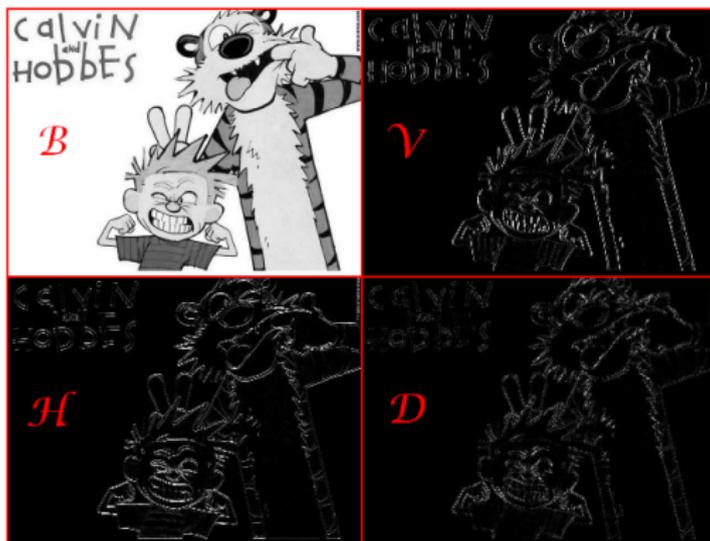
$$GAG^T = \frac{1}{4} \begin{bmatrix} (a_{11} + a_{22}) - (a_{12} + a_{21}) & (a_{13} + a_{24}) - (a_{23} + a_{14}) \\ (a_{31} + a_{42}) - (a_{32} + a_{41}) & (a_{33} + a_{44}) - (a_{43} + a_{34}) \end{bmatrix}$$

- ▶ Partition  $A$  in  $2 \times 2$  blocks as

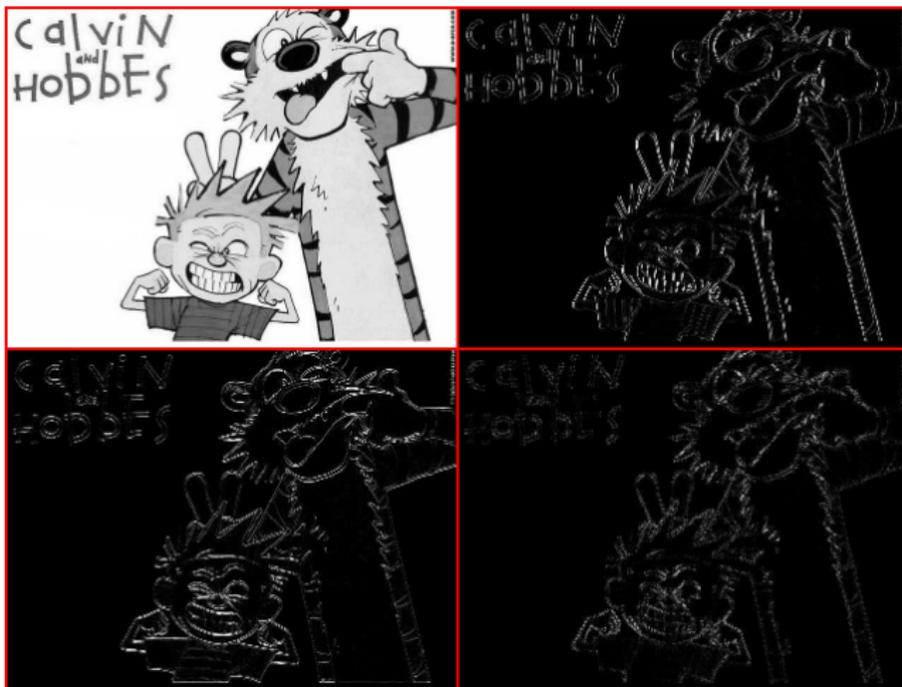
$$A = \left[ \begin{array}{cc|cc} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ \hline a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{array} \right] = \left[ \begin{array}{c|c} A_{11} & A_{12} \\ \hline A_{21} & A_{22} \end{array} \right]$$

- ▶ The  $(i, j)$  element of  $GAG^T$  can be viewed as a difference between the diagonals of  $A_{ij}$ .
- ▶ We will denote  $GAG^T$  as  $\mathcal{D}$  (for diagonal differences).

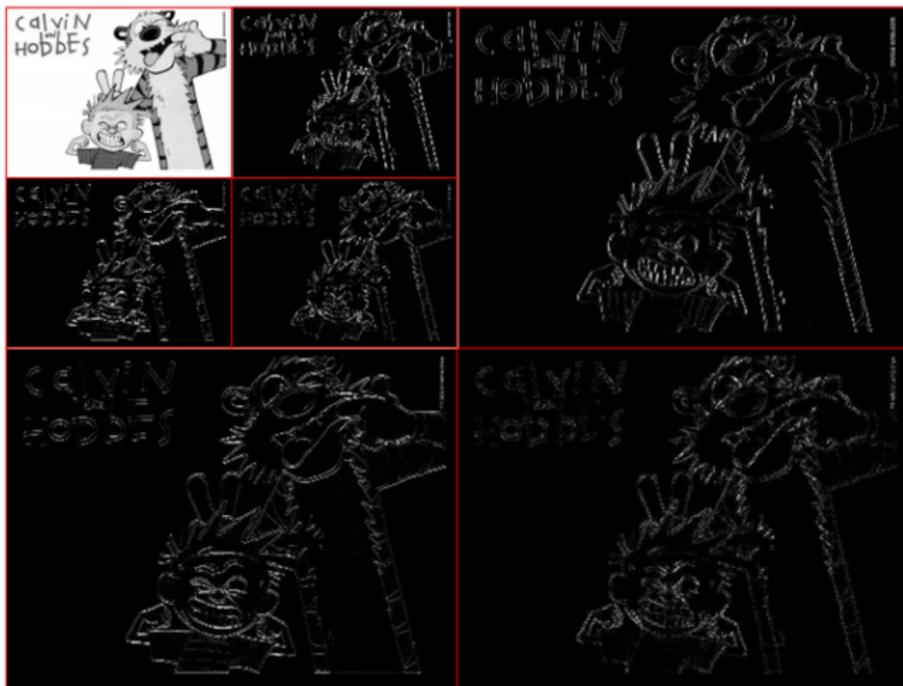
So again the transform of our image is



We can apply the HWT to the blur.



We can apply the HWT to the blur. This is called **the iterated HWT**.



# THIS IS JUST A TASTE!

- ▶ All the examples discussed today are examples of *orthogonal* wavelets - in many applications (such as JPEG2000), wavelet transforms used are *biorthogonal*.

# THIS IS JUST A TASTE!

- ▶ All the examples discussed today are examples of *orthogonal* wavelets - in many applications (such as JPEG2000), wavelet transforms used are *biorthogonal*.
- ▶ There are variations of the wavelet algorithm - FBI fingerprint compression uses what is called *wavelet packets*.

# THIS IS JUST A TASTE!

- ▶ All the examples discussed today are examples of *orthogonal* wavelets - in many applications (such as JPEG2000), wavelet transforms used are *biorthogonal*.
- ▶ There are variations of the wavelet algorithm - FBI fingerprint compression uses what is called *wavelet packets*.
- ▶ Wavelets are a great topic for undergraduates to see some modern mathematics and connections between theory and application.

# THIS IS JUST A TASTE!

- ▶ All the examples discussed today are examples of *orthogonal* wavelets - in many applications (such as JPEG2000), wavelet transforms used are *biorthogonal*.
- ▶ There are variations of the wavelet algorithm - FBI fingerprint compression uses what is called *wavelet packets*.
- ▶ Wavelets are a great topic for undergraduates to see some modern mathematics and connections between theory and application.
- ▶ Thank you for your attention! Check out the pdf file of challenge problems for the Haar wavelet transformation.

*Archimedes' Law of the Lever,  
and his Mysterious Mechanical Method  
for Finding the Volume of a Sphere*

Mike Raugh

Ph.D. in Math from Stanford

[www.mikeraugh.org](http://www.mikeraugh.org)

A Presentation for  
PNM-UNM New Mexico Math Contest  
February 4, 2012

## *Attention iPad Users!*

The iPad renders three slides incorrectly —

The ones with captions beginning:

“Cylinder”, “Cone”, and “Sphere”.

(Verified Mar 24, 2012)

# Archimedes:

He invented physical modeling

and the mathematics needed to do it!

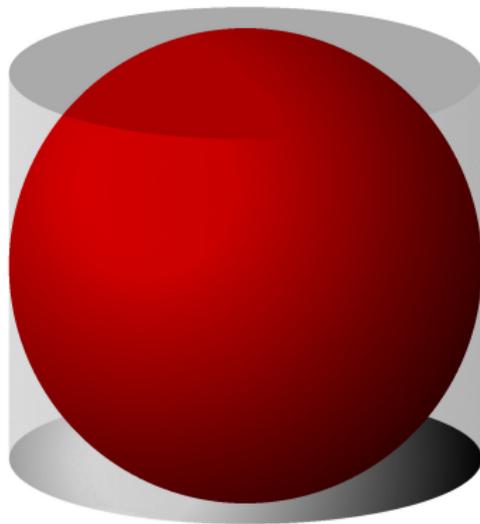
## *Little is known about him.*

- Archimedes of Syracuse, 287 ? – 212 BC
- Greek mathematician, physicist, engineer, inventor and astronomer
- Approximated  $\pi$ , determined the area of a circle and the volume of a sphere in terms of  $\pi$
- Invented the compound pulley and *explained* the mechanical advantage of the lever
- Laid foundations in hydrostatics and statics, calculated area of parabola using summation of an infinite series, and defined the spiral of Archimedes
- Killed by a Roman soldier during the capture of Syracuse.

## *Archimedes and the Roman Soldier*



## *Archimedes' Proudest Achievement*



(NYU, <http://math.nyu.edu/~corres/Archimedes/Tomb/Cicero.html>)

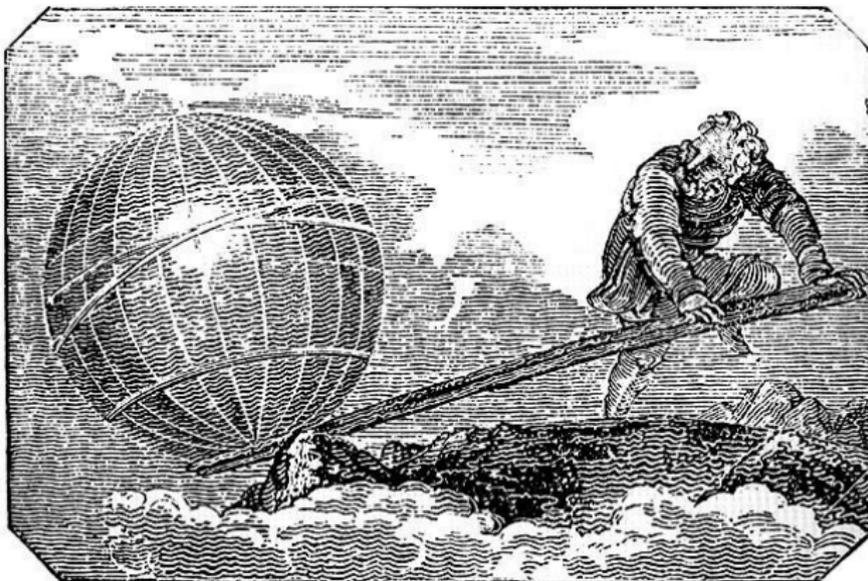
**The enclosed sphere has  $\frac{2}{3}$  the volume of the cylinder.**

In this talk we begin with the Law of the Lever, then conclude with Archimedes' use of it to determine the volume of a sphere.

# Part 1

## The Law of the Lever

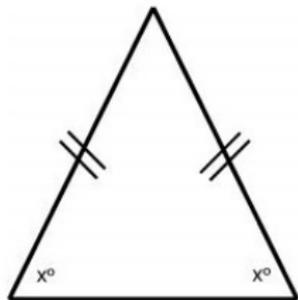
## *Archimedes' Moves the World*



(Anon.)

“Give me a lever long enough and a place to stand and I will move the world.”

*Archimedes' Law was innovative like the "Pons Asinorum" of Thales.*



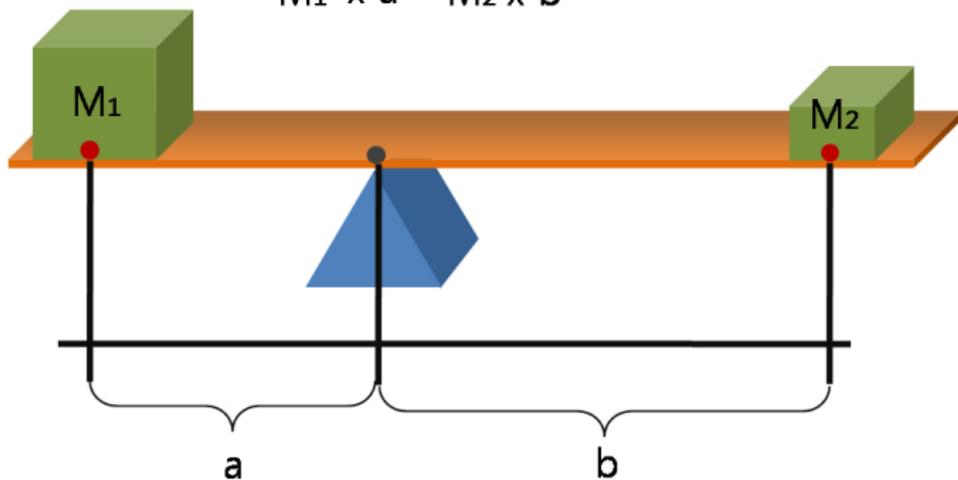
**Theorem:** Base angles of an isosceles triangle are equal.  
Seems obvious.

**But Greeks wanted strictly deductive proofs based on stated axioms** — not loose arguments like donkeys prefer.

*Pons Asinorum*, the Bridge of Asses. Theorem attributed to Thales (c 624 – 526 BC).

## The Law of the Lever

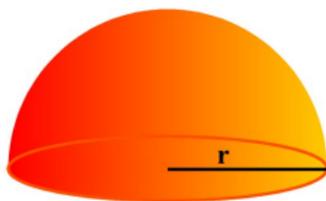
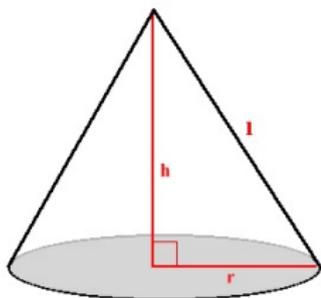
$$M_1 \times a = M_2 \times b$$



(Wikipedia)

Archimedes assumed: **A mass presses down on a static beam as if concentrated at its *center-of-mass*.**  
The beam is stiff and weightless.

## Archimedes invented the Center-of-Mass.



**Hemisphere**



(Clip Art Freeware)

**Where is the center-of-mass?** This usually needs calculus, but Archimedes understood the concept without *modern* calculus.

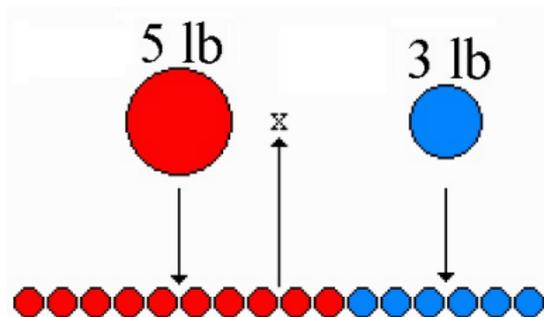
## *The Axiom of Equivalence*

A distributed mass balances like the same mass concentrated at its center-of-mass.

This is an empirical fact not deducible from geometry.

The Law of the Lever rests on the concept of center-of-mass.

## *Archimedes' Proof of the Law of the Lever*



(<http://physics.weber.edu/carroll/archimedes/leverprf.htm>)

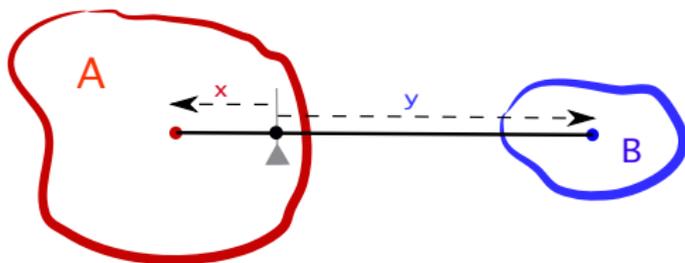
To find a balance point between two weights, divide them into commensurable units, colored red and blue. **Place the units uniformly on a beam; the balance point is at the center of the units.** The proportionate distances are measured from the center of the units, 3 : 5 in this case. So, **5** x 3 = **3** x 5.

## *Archimedes' Innovations*

Archimedes:

1. **invented** the concept of center-of-mass;
2. **introduced a rigorous mathematical model** to describe a physical phenomenon: the **Law of the Lever**;
3. **applied his law of the lever** to find the volume of a sphere — this was the mysterious Mechanical Method he referred to in his correspondence with other geometers

## *Axioms for Center-of-Mass for Areas*



Archimedes generalized the Law of the Lever. Figure illustrates two axioms for balancing *areas* in 2D:

$$(\text{Area } A) \cdot x = (\text{Area } B) \cdot y$$

Third axiom: center-of-mass of a convex area lies within the area.

Archimedes used these in his theory of bouyancy.

## *The Modern Definition of Center-of-Mass*

Given point-masses  $\{(m_i, \mathbf{x}_i), i = 1, \dots, n\}$ , their **center of mass**  $\bar{\mathbf{x}}$ , also called **centroid**, is defined

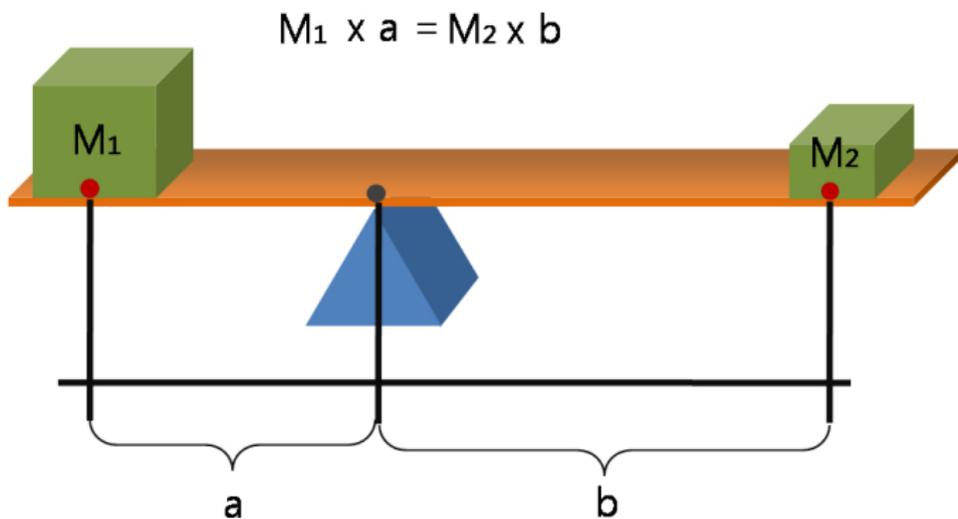
$$\bar{\mathbf{x}} = \frac{\sum_{i=1}^n m_i \mathbf{x}_i}{\sum_{i=1}^n m_i}$$

More generally,

$$\bar{\mathbf{x}} = \frac{\int_V \mathbf{x} dm}{\int_V dm}$$

These vector equations, which yield the balance point for a mass distribution in 1-D, generalize the Law of the Lever. **In 3-D they are fundamental constructs of rigid-body mechanics.**

## *The Law of the Lever*



(Wikipedia)

## Part II

### Volume of the Sphere

Archimedes' Method, unknown until 1906,  
applies the Law of the Lever.

*Archimedes explained his “Mechanical Method” in a Palimpsest discovered in 1906 in a Byzantine Crypt in Istanbul.*



(©The Owner of the Palimpsest)

Here's what it looked like when rediscovered in 1998.

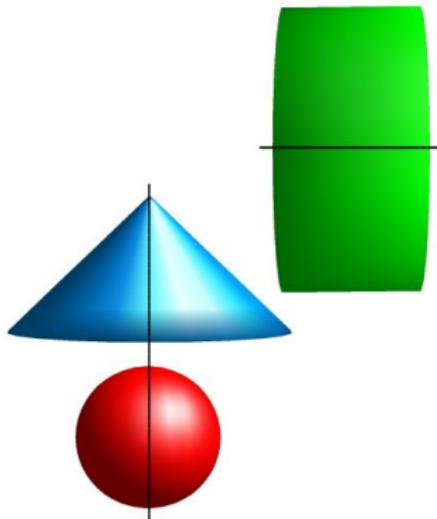
## *One Imaged Page of the Archimedes Palimpsest*



(Wikipedia)

In the early 1900s, the Danish philologist Johan Heiberg transcribed legible portions into Greek. Here is a recent scan.

*Archimedes used the Law of the Lever to compare volumes of a cylinder, cone and sphere.*

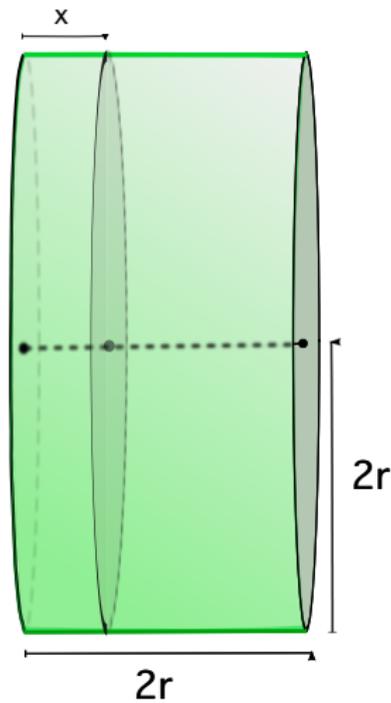


Archimedes knew the volumes of **cylinders** and **cones**, and areas of their circular cross sections. He used these to determine the volume of the **sphere**.

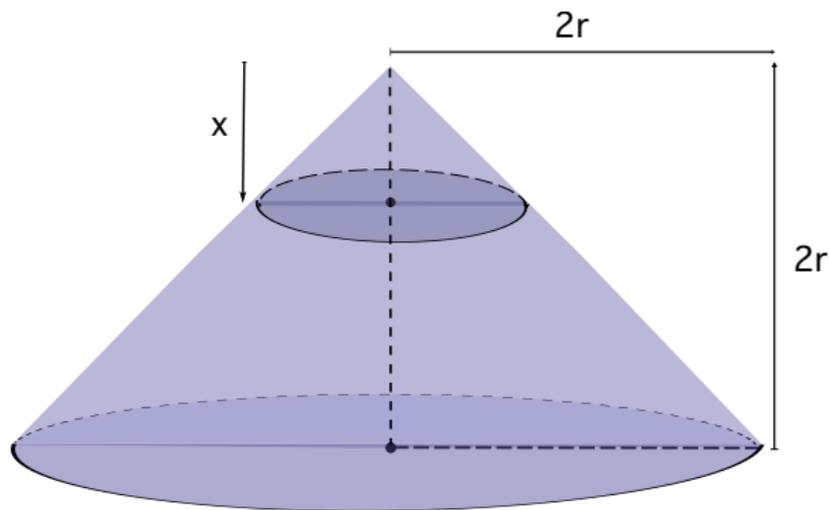
## *Cylinder: Area of $x$ -level Cross Section*

**Circular cross-section  
at level  $x$ :  $4\pi r^2$**

[Volume of cylinder =  
 $C_y = 8\pi r^3$ ]



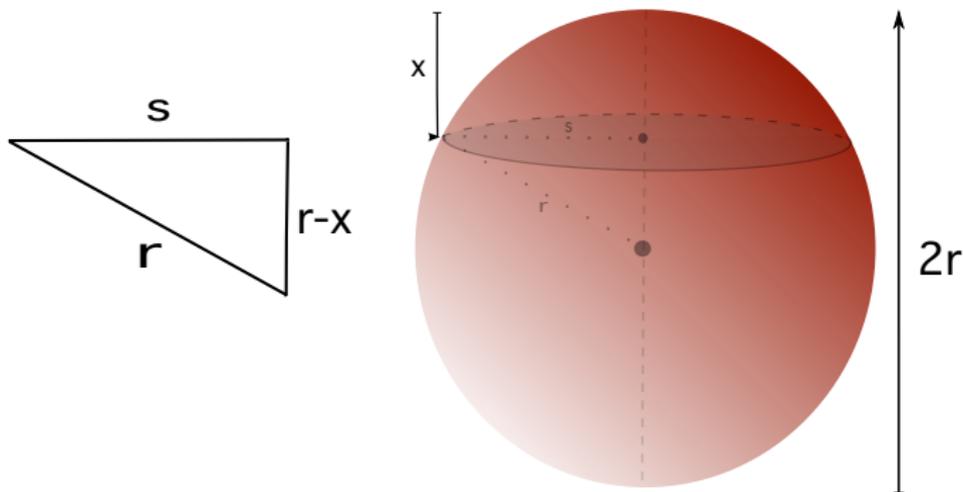
## *Cone: Area of $x$ -level Cross Section*



**Circular cross-section at level  $x$ :**  $\pi x^2$

[Volume of cone =  $C_o = \frac{8}{3}\pi r^3$ ]

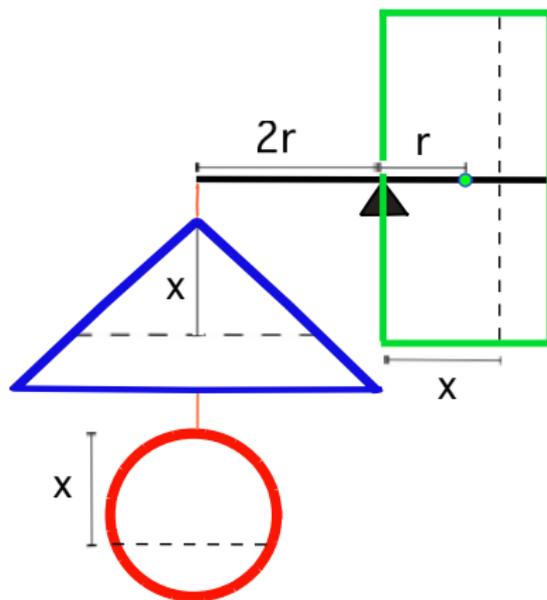
## *Sphere: Area of $x$ -level Cross Section*



**Circular cross-section at level  $x$ :**  $\pi s^2 = 2\pi r x - \pi x^2$

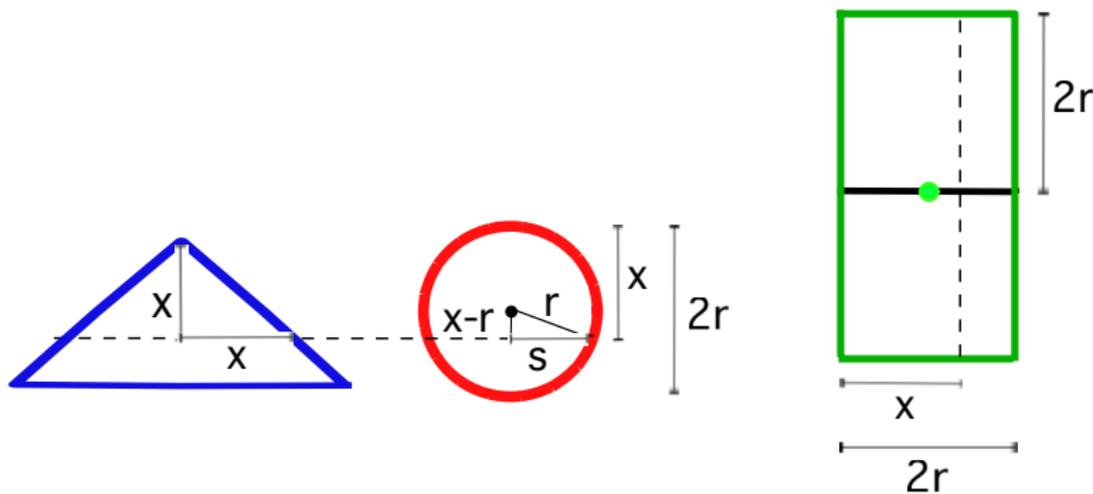
[Volume of sphere =  $S = ???$ ]

## *Method (Step 1): Three Solids in Perfect Balance*



We will see that the  $x$ -level cross sections balance. (Assuming uniform density.)

*Method (Step 2): The cross-section (CS) areas balance.*



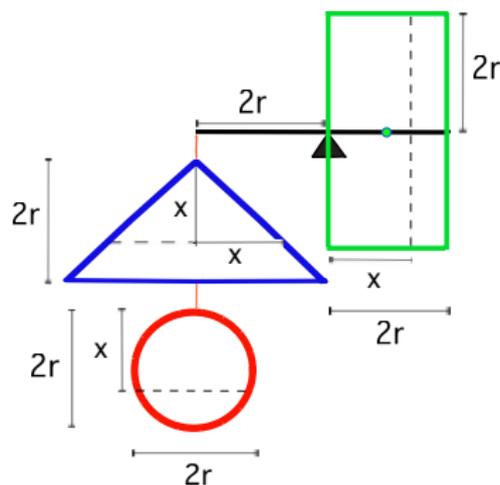
Cone CS:  $+ \pi x^2$ ;

Sphere CS:  $\pi s^2 = 2\pi r x - \pi x^2$ ;

(Cone CS + Sphere CS) =  $2\pi r x$       Cylinder CS:  $4\pi r^2$

$2r \cdot (\text{Cone CS} + \text{Sphere CS}) = 4\pi r^2 x = \text{Cylinder CS} \cdot x$       **QED**

## Method (Step 3): The Derivation



By previous slide: Each  $x$ -section of cylinder balances the combined  $x$ -sections of the hanging cone and sphere.  
 Therefore, **the volumes balance**:  $2r \cdot (C_o + S) = r \cdot C_y$ , so

$$C_o = \frac{8}{3}\pi r^3, \quad C_y = 8\pi r^3 \quad \implies \quad S = \frac{4}{3}\pi r^3$$

*Using modern terms, we would express this as:*

$$\begin{aligned} 2r(C_o + S) &= \\ \int_0^{2r} (2r)(2\pi rx) dx &= 8\pi r^4 = \int_0^{2r} (x)(4\pi r^2) dx \\ &= rC_y \end{aligned}$$

Archimedes did this nearly 2 millenia before Newton and Leibniz.

## *Archimedes' Proudest Achievement*

Archimedes asked that a cylinder and sphere be mounted on his tomb, displaying their proportional volumes.

The sphere is 2/3 the volume of a circumscribed cylinder:

$$S = \frac{4}{3}\pi r^3.$$

“Cicero discovering the Tomb of Archimedes – 1”



(Anon., 1806)

Frontispiece of Weinzierl's German translation of Cicero's  
*Tusculan Disputations*

## *“Cicero discovering the Tomb of Archimedes – 2”*



(Martin Knoller (1725-1804))

## *“Cicero discovering the Tomb of Archimedes – 3”*



(Benjamin West (1738-1820))

*“Cicero discovering the Tomb of Archimedes – 4”*



(Hubert Robert (1733-1808))

## *“Cicero Decouvrant le Tombeau d’Archimede” – 5*



(Pierre Henri de Valenciennes (1750-1819))

## Conclusion

Archimedes **invented physical modeling**, using rigorous mathematical deductions from specified physical axioms.

He formulated and **proved the Law of the Lever, based on center-of-mass**.

He **anticipated methods of integral calculus**: Cavalieri's Principle and Fubini's theorem.

And now we know his Mechanical Method, by which **he applied the Law of the Lever to determine the volume of a sphere**.

## *Recommended reading*

- Asger Aaboe, *Episodes from the early history of mathematics*, Mathematical Association of America, 1998.
- Archimedes, *The works of Archimedes*, Dover Publications, (Thomas L. Heath edition), 2002.
- E. J. Dijksterhuis, *Archimedes*, Acta Historica Scientiarum Naturalium et Medicinalium, vol 12, 1956.
- Laubenbacher and Pengelley, *Mathematical Expeditions — Chronicles by the Explorers*, Springer, 1999.
- Sherman Stein, *Archimedes: What Did He Do Besides Cry Eureka?* Mathematical Association of America, 1999.
- Nietz & Noel, *The Archimedes Codex: How a Medieval Prayer Book Is Revealing the True Genius of Antiquity's Greatest Scientist*, Da Capo Press, Jan 9, 2009.
- The Archimedes Palimpsest  
(<http://www.archimedespalimpsest.org/>)

In the Endnotes, the slides continue with:

An alternative discussion of the Law of the Lever using the concept of *torque*,

A sketch of Archimedes' derivation of the surface area of a disk ( $\pi r^2$ ) and a sphere ( $\pi D^2$ )  
and

Brief commentary.

*A text version with more details will be available on my web.*

These slides are there, too:

[www.mikeraugh.org](http://www.mikeraugh.org)

Contact me at,

Michael.Raugh@gmail.com



(Supplementary sections follow.)

## Endnote 1

Torque is defined and determined using a differential equation based on the Axiom of Equivalence.

The Law of the Lever is inferred.

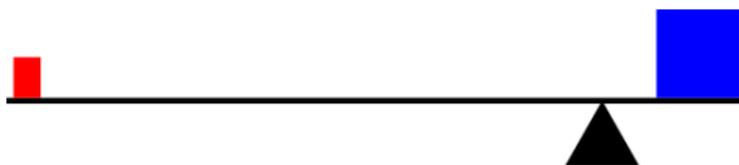
Concludes with discussion of “action at a distance” compared to “argument from cause”, with compound pulley as example.

## *First, Some Balance Axioms*

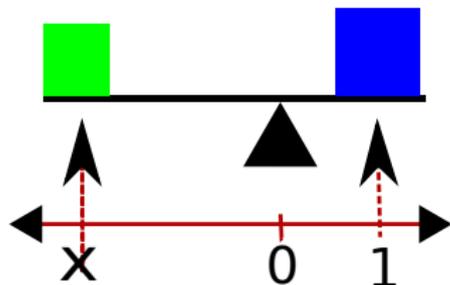
These axioms are assumed in the following derivations. They are not the same as Archimedes' axioms:

1. (**Basic**) Equal masses at equal distances are balanced.
2. (**Symmetry**) Balanced masses remain balanced under reflection about the fulcrum.
3. (**Linearity**) A balanced set of masses added to (or subtracted from) a balanced set of masses remains balanced.
4. (**Equivalence**) A distributed mass balances like the same mass concentrated at the center-of-mass.

*We begin with a graphic depiction of “torque.”*

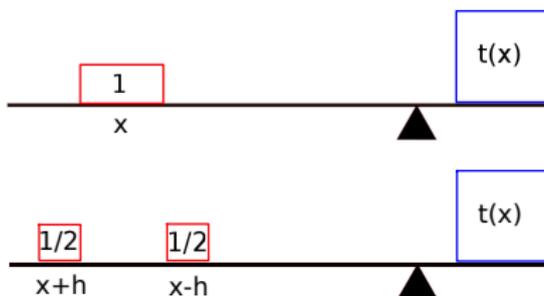


The **red**, **brown**, and **green** weights all **counterbalance** the same **blue** weight. They exert the same “**torque**”, **defined** as the **blue** weight.



We compute “torque” by solving a simple differential equation.

Let  $t(x)$  be the torque exerted by 1 unit of weight at a distance of  $x$  units from the fulcrum. By Axiom of Equivalence:



$$\frac{t(x+h) + t(x-h)}{2} = t(x) \implies$$

$$\lim_{h \rightarrow 0} \frac{t(x+h) - 2t(x) + t(x-h)}{h^2} = \frac{d^2}{dx^2} t(x) = 0$$

$$\implies t(x) = ax + b = x$$

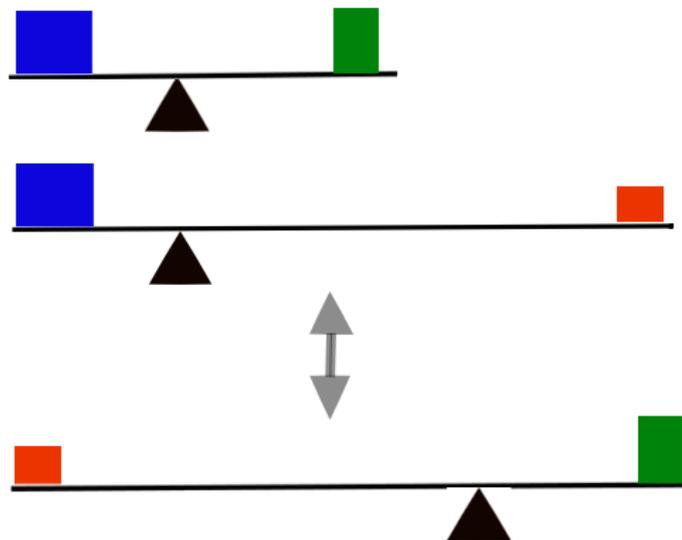
*Now we have a formula for “big- $T$ ” Torque.*

By the Axiom of Linearity the torque exerted by an arbitrary force  $F$  at a distance  $x$  from the fulcrum is  $F \cdot t(x) = F \cdot x$

A force of weight  $W$  applied at a distance  $x$  from the fulcrum exerts a torque of

$$T(W, x) = W \cdot t(x) = W \cdot x$$

## *Law of the Lever: A Proof with One Word*



$$W_1 \cdot x_1 = \text{Torque} = W_2 \cdot x_2$$

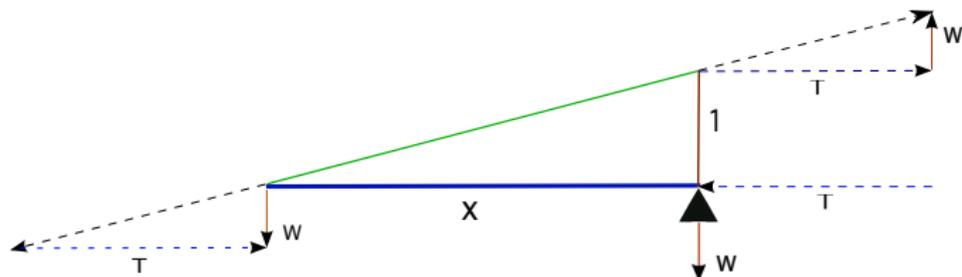
## *“Action at a Distance” vs “Argument from Cause”*

Archimedes avoided specifying cause; he did not explain how torque is transmitted through a lever. Instead he assumed the mutual influence of objects balanced on a beam according to the empirical Axiom of Equivalence, as likewise Newton based gravitation theory on observed behavior, avoiding hypotheses about the cause of attraction. Let's call this kind of unexplained force “action at a distance.”

We can incorporate cause into the derivation of torque by using the parallelogram law for composition of forces, as outlined in the next slide. The parallelogram law is itself an empirically derived axiom, developed by Stevins, Roberval and Newton. (Rene Dugas, “A History of Mechanics,” Dover Edition, 1988.)

Consider the beam as a material object that transmits pressure and tension. In the next slide, a triangle is used as example, wherein the hypotenuse (think wire) transmits tension, and the lower longitudinal leg of the triangle (think rod) transmits pressure. Torque  $T = W \cdot x$  above the fulcrum results from loading the beam with force  $W$ .

## *Archimedes Assumed Action at a Distance, But a Causal Proof is Possible*



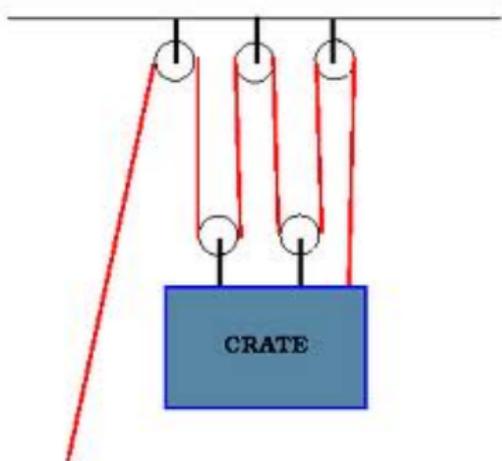
Suppose lever is triangular, loaded with weight  $W$  at lever's end.

Resolve force ( $W$ ), where torque component is  $T$ . By similar triangles:  $T = W \cdot x$

Note that the downward load at fulcrum is also  $W$ .

The same argument generalizes to a beam constructed as a truss, where  $x$  then is the length of the truss.

## *Compound Pulley: Archimedes' Other Form of "Leverage"*



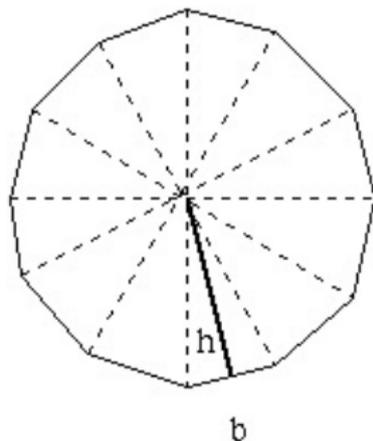
Assuming tension in rope is uniform, mechanical advantage is counted by number of segments pulling on load: 5 times in left panel, 6 times on right (at a cost of having to pull that much farther). Here the cause is self-evident: force transmitted through rope.

## Endnote 2

Archimedes' derivation of the area of a disk is sketched.

His analogous argument for determining the surface of a sphere is described.

## Surface Area of a Sphere — First the Disk



(UBC Calculus Online, [www.ugrad.math.ubc.ca](http://www.ugrad.math.ubc.ca))

Archimedes deduced disk Area as limit of  $n$  inscribed triangles:

$$(\text{as } n \rightarrow \infty) \quad h \rightarrow r, \quad \text{and } n \left( \frac{1}{2} h \frac{2\pi r}{n} \right) \rightarrow \pi r^2 = \text{Area}$$

## *Surface Area of a Sphere — Archimedes' Idea*

Same idea as for the disk:

Imagine a sphere as comprised of many thin cones with apexes at the center and bases at the surface. Say, a spherical planet platted with one-acre plots; the surface area would equal the number of plots.

Summing the conical volumes, in the limit they amount to a cone with base equal to the surface of the sphere  $S$  and height equal to the radius  $r$ .

$$\frac{4}{3}\pi r^3 = \frac{1}{3}rS \quad \rightarrow \quad S = 4\pi r^2$$

## Endnote 3

Brief Comments Interpolated in Talk

## *Quality of Archimedes' Work*

“In weightiness of matter and elegance of style, no classical mathematics treatise surpasses the works of Archimedes. This was recognized in antiquity; thus Plutarch says of Archimedes’ works:

*‘It is not possible to find in all geometry more difficult and intricate questions, or more simple and lucid explanations. Some ascribe this to his genius; while others think that incredible effort and toil produced these, to all appearances, easy and unlaboured results.’ ”*

(Aaboe in *Recommended reading*)

“Archimedes is so clever that sometimes I think that if you want an example of someone brought from outer space it would be Archimedes. Because he, in my view, is so original and so imaginative that I think he is better than Newton. Whereas Newton said, ‘I have only seen so far because I have been standing on the shoulders of other giants,’ there was nobody for Archimedes, nobody’s shoulders for Archimedes to stand on. He is the first physicist and the first applied mathematician. And he did it all on his own from nowhere.”

(Lewis Wolpert in *On Shoulders of Giants* by Melvyn Bragg, 1998)

## *Archimedes' "Method of Mechanical Theorems."*

Archimedes' geometric proof for the volume of a sphere was well known, but the method by which he discovered the result remained a mystery until 1906.

The *Archimedes Palimpsest*, in which Archimedes described his method, was found in Istanbul in a Byzantine crypt, then lost and recovered again in 1998.

The Palimpsest contained a tenth-century copy of a Greek MS that was scraped, washed and overlaid with Christian liturgy and other writings.

(See *Recommended reading*).

## *The Roman orator Cicero found the Archimedes' tomb.*

Archimedes was killed in 212 BC.

Archimedes had asked that a cylinder and sphere be mounted on his tomb, displaying their proportional volumes:  $2/3$ .

The tomb was built and lost until the figures of the cylinder and the sphere enabled Cicero to find it 137 years later.

Cicero found the tomb in 75 BC. He wrote: "So one of the most famous cities in the Greek world would have remained in total ignorance of the tomb of the most brilliant citizen it had ever produced, had a man from Arpinum not come and pointed it out!"

(Aaboe in *Recommended reading*)

# The beauty, mystery, and utility of prime numbers

Tom Marley

University of Nebraska-Lincoln

February 7, 2015

# The natural numbers

In this talk, by *number* we will mean one of the whole numbers

1, 2, 3, 4, 5, .....

Mathematicians call these the *natural numbers*.

# The natural numbers

In this talk, by *number* we will mean one of the whole numbers

1, 2, 3, 4, 5, .....

Mathematicians call these the *natural numbers*.

*“God made the natural numbers, all else is the work of man.”*  
(Leopold Kronecker, 1823-1891)

# The natural numbers

In this talk, by *number* we will mean one of the whole numbers

1, 2, 3, 4, 5, .....

Mathematicians call these the *natural numbers*.

*“God made the natural numbers, all else is the work of man.”*  
(Leopold Kronecker, 1823-1891)

By a *factor* of a number we mean a whole number which **evenly** divides the number; i.e., divides with no remainder.

# The natural numbers

In this talk, by *number* we will mean one of the whole numbers

1, 2, 3, 4, 5, .....

Mathematicians call these the *natural numbers*.

*“God made the natural numbers, all else is the work of man.”*  
(Leopold Kronecker, 1823-1891)

By a *factor* of a number we mean a whole number which *evenly* divides the number; i.e., divides with no remainder.

- 4 is a factor of 20 because 20 divided by 4 is 5 with no remainder.

# The natural numbers

In this talk, by *number* we will mean one of the whole numbers

1, 2, 3, 4, 5, .....

Mathematicians call these the *natural numbers*.

*“God made the natural numbers, all else is the work of man.”*  
(Leopold Kronecker, 1823-1891)

By a *factor* of a number we mean a whole number which *evenly* divides the number; i.e., divides with no remainder.

- 4 is a factor of 20 because 20 divided by 4 is 5 with no remainder.
- 3 is **not** a factor of 20 because 20 divided by 3 is 6 with remainder 2.

# What is a prime number?

For small numbers, we can easily list all its factors:

# What is a prime number?

For small numbers, we can easily list all its factors:

- The factors of 20 are 1, 2, 4, 5, 10, and 20.

# What is a prime number?

For small numbers, we can easily list all its factors:

- The factors of 20 are 1, 2, 4, 5, 10, and 20.
- The factors of 24 are 1, 2, 3, 4, 6, 8, 12, and 24.

# What is a prime number?

For small numbers, we can easily list all its factors:

- The factors of 20 are 1, 2, 4, 5, 10, and 20.
- The factors of 24 are 1, 2, 3, 4, 6, 8, 12, and 24.
- The factors of 23 are 1 and 23.

A *prime number* is a number that has precisely two factors: namely 1 and itself.

# What is a prime number?

For small numbers, we can easily list all its factors:

- The factors of 20 are 1, 2, 4, 5, 10, and 20.
- The factors of 24 are 1, 2, 3, 4, 6, 8, 12, and 24.
- The factors of 23 are 1 and 23.

A *prime number* is a number that has precisely two factors: namely 1 and itself.

For reasons we'll discuss later, we exclude the number 1 from being prime.

# What is a prime number?

For small numbers, we can easily list all its factors:

- The factors of 20 are 1, 2, 4, 5, 10, and 20.
- The factors of 24 are 1, 2, 3, 4, 6, 8, 12, and 24.
- The factors of 23 are 1 and 23.

A *prime number* is a number that has precisely two factors: namely 1 and itself.

For reasons we'll discuss later, we exclude the number 1 from being prime.

The first few prime numbers are:

2, 3, 5, 7, 11, 13, 17, 19, 23, ...

# Prime factorization

We learned in elementary school that every number can be factored into primes:

$$48 = 8 \times 6$$

# Prime factorization

We learned in elementary school that every number can be factored into primes:

$$\begin{aligned}48 &= 8 \times 6 \\ &= 2 \times 4 \times 2 \times 3\end{aligned}$$

# Prime factorization

We learned in elementary school that every number can be factored into primes:

$$\begin{aligned}48 &= 8 \times 6 \\ &= 2 \times 4 \times 2 \times 3 \\ &= 2 \times 2 \times 2 \times 2 \times 3\end{aligned}$$

# Prime factorization

We learned in elementary school that every number can be factored into primes:

$$\begin{aligned}48 &= 8 \times 6 \\ &= 2 \times 4 \times 2 \times 3 \\ &= 2 \times 2 \times 2 \times 2 \times 3\end{aligned}$$

Moreover, we get the same answer no matter how we do the factorization:

# Prime factorization

We learned in elementary school that every number can be factored into primes:

$$\begin{aligned}48 &= 8 \times 6 \\ &= 2 \times 4 \times 2 \times 3 \\ &= 2 \times 2 \times 2 \times 2 \times 3\end{aligned}$$

Moreover, we get the same answer no matter how we do the factorization:

$$48 = 12 \times 4$$

# Prime factorization

We learned in elementary school that every number can be factored into primes:

$$\begin{aligned}48 &= 8 \times 6 \\ &= 2 \times 4 \times 2 \times 3 \\ &= 2 \times 2 \times 2 \times 2 \times 3\end{aligned}$$

Moreover, we get the same answer no matter how we do the factorization:

$$\begin{aligned}48 &= 12 \times 4 \\ &= 3 \times 4 \times 2 \times 2\end{aligned}$$

# Prime factorization

We learned in elementary school that every number can be factored into primes:

$$\begin{aligned}48 &= 8 \times 6 \\ &= 2 \times 4 \times 2 \times 3 \\ &= 2 \times 2 \times 2 \times 2 \times 3\end{aligned}$$

Moreover, we get the same answer no matter how we do the factorization:

$$\begin{aligned}48 &= 12 \times 4 \\ &= 3 \times 4 \times 2 \times 2 \\ &= 3 \times 2 \times 2 \times 2 \times 2\end{aligned}$$

# Prime factorization

We learned in elementary school that every number can be factored into primes:

$$\begin{aligned}48 &= 8 \times 6 \\ &= 2 \times 4 \times 2 \times 3 \\ &= 2 \times 2 \times 2 \times 2 \times 3\end{aligned}$$

Moreover, we get the same answer no matter how we do the factorization:

$$\begin{aligned}48 &= 12 \times 4 \\ &= 3 \times 4 \times 2 \times 2 \\ &= 3 \times 2 \times 2 \times 2 \times 2\end{aligned}$$

This fact is known as *The Fundamental Theorem of Arithmetic*



# How many primes?

Euclid (300 BCE) was the first to prove there are infinitely many primes.

# How many primes?

Euclid (300 BCE) was the first to prove there are infinitely many primes.

How did he do this without exhibiting infinitely many primes?

# How many primes?

Euclid (300 BCE) was the first to prove there are infinitely many primes.

How did he do this without exhibiting infinitely many primes?

He did this using *Proof by Contradiction*.

# How many primes?

Euclid (300 BCE) was the first to prove there are infinitely many primes.

How did he do this without exhibiting infinitely many primes?

He did this using *Proof by Contradiction*.

This is a method of logic whereby one assumes a statement is false and shows this leads to an 'absurdity'.

# Euclid's proof

We assume there are only finitely many primes. We seek to derive an 'aburdity' from this assumption.

# Euclid's proof

We assume there are only finitely many primes. We seek to derive an 'aburdity' from this assumption.

For the purposes of this argument, let's suppose there are one million primes, but no more.

# Euclid's proof

We assume there are only finitely many primes. We seek to derive an 'aburdity' from this assumption.

For the purposes of this argument, let's suppose there are one million primes, but no more.

Multiply all of these one million primes together and then add one to the answer. Call this (huge) number  $N$ .

# Euclid's proof

We assume there are only finitely many primes. We seek to derive an 'aburdity' from this assumption.

For the purposes of this argument, let's suppose there are one million primes, but no more.

Multiply all of these one million primes together and then add one to the answer. Call this (huge) number  $N$ .

Question: What is the remainder when you divide  $N$  by one of the primes?

# Euclid's proof

We assume there are only finitely many primes. We seek to derive an 'aburdity' from this assumption.

For the purposes of this argument, let's suppose there are one million primes, but no more.

Multiply all of these one million primes together and then add one to the answer. Call this (huge) number  $N$ .

Question: What is the remainder when you divide  $N$  by one of the primes?

Answer: **One!**

# Euclid's proof

We assume there are only finitely many primes. We seek to derive an 'abudity' from this assumption.

For the purposes of this argument, let's suppose there are one million primes, but no more.

Multiply all of these one million primes together and then add one to the answer. Call this (huge) number  $N$ .

Question: What is the remainder when you divide  $N$  by one of the primes?

Answer: **One!**

This means that  $N$  is not divisible by any prime! This is our 'abusurdity'.

# A simple primality test

# A simple primality test

To see if a number is prime, we only need to check to see if it is divisible by a prime number less or equal to its square root.

This is much faster having to check all numbers less than the number!

# A simple primality test

To see if a number is prime, we only need to check to see if it is divisible by a prime number less or equal to its square root.

This is much faster having to check all numbers less than the number!

For example, it is easy to see that the only primes less than or equal to 10 are 2, 3, 5 and 7.

# A simple primality test

To see if a number is prime, we only need to check to see if it is divisible by a prime number less or equal to its square root.

This is much faster having to check all numbers less than the number!

For example, it is easy to see that the only primes less than or equal to 10 are 2, 3, 5 and 7.

So, to see if a number between 2 and 100 is prime, we just have to check if it is divisible by 2, 3, 5, or 7.

# A simple primality test

To see if a number is prime, we only need to check to see if it is divisible by a prime number less or equal to its square root.

This is much faster having to check all numbers less than the number!

For example, it is easy to see that the only primes less than or equal to 10 are 2, 3, 5 and 7.

So, to see if a number between 2 and 100 is prime, we just have to check if it is divisible by 2, 3, 5, or 7.

We can make an algorithm out of this, which is called the

*Sieve of Eratosthenes.*

# Sieve of Eratosthenes

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50

# Sieve of Eratosthenes

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50

Prime: 2

All multiples of 2 crossed out.

# Sieve of Eratosthenes

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50

Primes: 2, 3

All multiples of 2 and 3 crossed out.

# Sieve of Eratosthenes

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50

Primes: 2, 3, 5

All multiples of 2, 3, and 5 crossed out.

# Sieve of Eratosthenes

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50

Primes: 2, 3, 5, 7 and all other uncrossed numbers

All multiples of 2, 3, 5, and 7 crossed out.

# The prime number theorem

**Question:** Suppose we want to check if large number is prime. Is the Sieve a good method?

# The prime number theorem

**Question:** Suppose we want to check if large number is prime. Is the Sieve a good method?

The answer depends on how many prime numbers are less than or equal to the square root of the number.

# The prime number theorem

**Question:** Suppose we want to check if large number is prime. Is the Sieve a good method?

The answer depends on how many prime numbers are less than or equal to the square root of the number.

**The Prime Number Theorem**, which was proved around 1900, states that for an  $n$ -digit number  $N$ , the number of primes less than or equal to  $\sqrt{N}$  is (approximately) at least

$$\frac{(3.16)^n}{(1.15)n}$$

# The prime number theorem

**Question:** Suppose we want to check if large number is prime. Is the Sieve a good method?

The answer depends on how many prime numbers are less than or equal to the square root of the number.

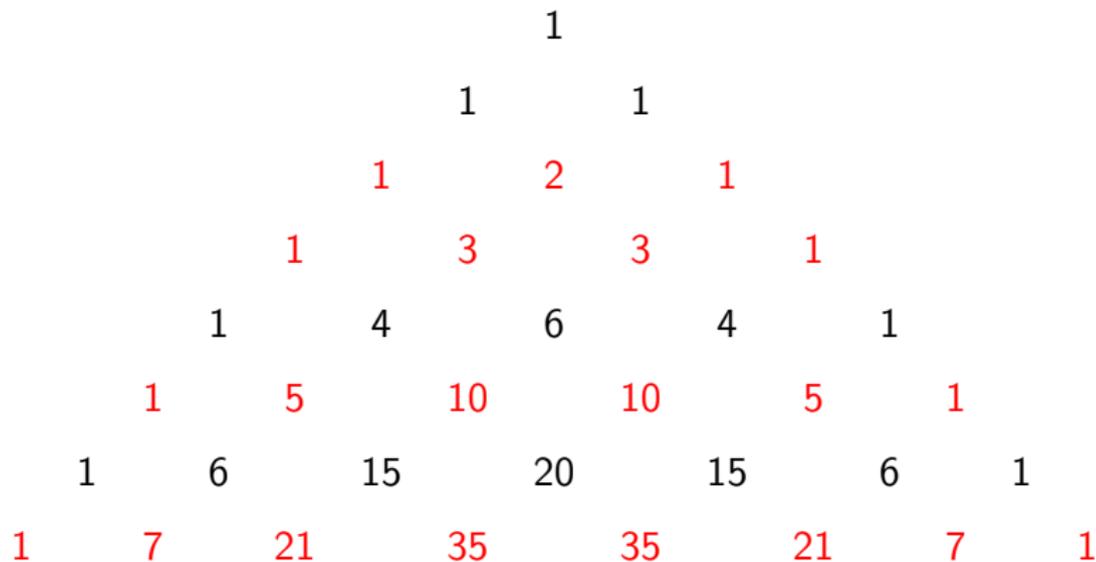
**The Prime Number Theorem**, which was proved around 1900, states that for an  $n$ -digit number  $N$ , the number of primes less than or equal to  $\sqrt{N}$  is (approximately) at least

$$\frac{(3.16)^n}{(1.15)n}$$

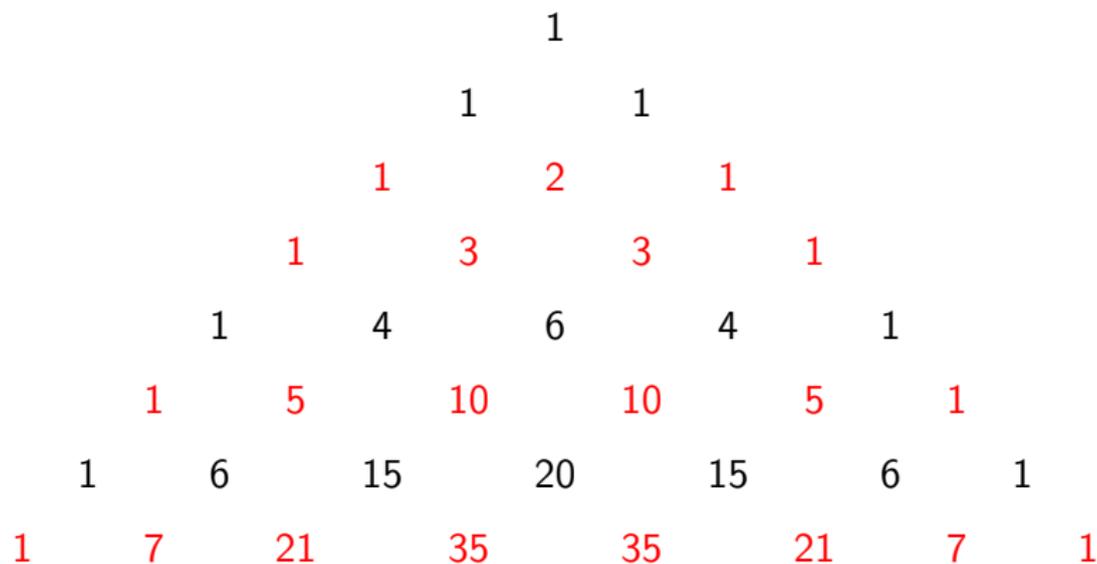
This function grows very fast with  $n$ . Consequently, it would take thousands of years for even the world's fastest supercomputers to check if a 400-digit number is prime using the Sieve.



# Pascal's Triangle



# Pascal's Triangle



**Fact:** If  $n$  is prime then  $n$  divides all the middle terms in it's row.

# Fermat's Theorem

For example,

$$(a + b)^5 = a^5 + 5a^4b + 10a^3b^2 + 10a^2b^3 + 5ab^4 + b^5.$$

# Fermat's Theorem

For example,

$$(a + b)^5 = a^5 + 5a^4b + 10a^3b^2 + 10a^2b^3 + 5ab^4 + b^5.$$

$$(a + b)^5 - a^5 - b^5 = 5(a^4b + 2a^3b^2 + 2a^2b^3 + ab^4)$$

# Fermat's Theorem

For example,

$$(a + b)^5 = a^5 + 5a^4b + 10a^3b^2 + 10a^2b^3 + 5ab^4 + b^5.$$

$$(a + b)^5 - a^5 - b^5 = 5(a^4b + 2a^3b^2 + 2a^2b^3 + ab^4)$$

In general, if  $p$  is prime then  $(a + b)^p - a^p - b^p$  is divisible by  $p$  for all numbers  $a$  and  $b$ .

# Fermat's Theorem

For example,

$$(a + b)^5 = a^5 + 5a^4b + 10a^3b^2 + 10a^2b^3 + 5ab^4 + b^5.$$

$$(a + b)^5 - a^5 - b^5 = 5(a^4b + 2a^3b^2 + 2a^2b^3 + ab^4)$$

In general, if  $p$  is prime then  $(a + b)^p - a^p - b^p$  is divisible by  $p$  for all numbers  $a$  and  $b$ .

It's a very short argument from there to...

**Fermat's Theorem:** If  $p$  is a prime number then  $p$  divides  $a^p - a$  for all numbers  $a$ .

# Carmichael numbers

**Question:** Does Fermat's Theorem only work for prime numbers?

That is, suppose  $n$  is a number and  $a^n - a$  is divisible by  $n$  for all numbers  $a$ . Must  $n$  be prime?

# Carmichael numbers

**Question:** Does Fermat's Theorem only work for prime numbers?

That is, suppose  $n$  is a number and  $a^n - a$  is divisible by  $n$  for all numbers  $a$ . Must  $n$  be prime?

Unfortunately, the answer is no! There are numbers, called **Carmichael numbers**, which have the Fermat property but are not prime. The smallest Carmichael number is  $561 = (3)(11)(17)$ .

# Carmichael numbers

**Question:** Does Fermat's Theorem only work for prime numbers?

That is, suppose  $n$  is a number and  $a^n - a$  is divisible by  $n$  for all numbers  $a$ . Must  $n$  be prime?

Unfortunately, the answer is no! There are numbers, called **Carmichael numbers**, which have the Fermat property but are not prime. The smallest Carmichael number is  $561 = (3)(11)(17)$ .

The good news is: Carmichael numbers are quite rare relative to prime numbers!

# A probabilistic primality test

Fermat's Theorem suggests the following algorithm to test if a number  $N$  is prime.

# A probabilistic primality test

Fermat's Theorem suggests the following algorithm to test if a number  $N$  is prime.

Step 1: Choose a random number  $a$  and compute the remainder of  $a^N - a$  upon dividing by  $N$ .

# A probabilistic primality test

Fermat's Theorem suggests the following algorithm to test if a number  $N$  is prime.

Step 1: Choose a random number  $a$  and compute the remainder of  $a^N - a$  upon dividing by  $N$ .

Step 2: If the remainder is not zero, then STOP:  $N$  is not prime.

# A probabilistic primality test

Fermat's Theorem suggests the following algorithm to test if a number  $N$  is prime.

Step 1: Choose a random number  $a$  and compute the remainder of  $a^N - a$  upon dividing by  $N$ .

Step 2: If the remainder is not zero, then STOP:  $N$  is not prime.

Step 3: If the remainder is zero, repeat Step 1 with a new random number  $a$ .

# A probabilistic primality test

Fermat's Theorem suggests the following algorithm to test if a number  $N$  is prime.

Step 1: Choose a random number  $a$  and compute the remainder of  $a^N - a$  upon dividing by  $N$ .

Step 2: If the remainder is not zero, then STOP:  $N$  is not prime.

Step 3: If the remainder is zero, repeat Step 1 with a new random number  $a$ .

Continue the loop until, with increasing probability, you conclude that  $N$  is either prime or (if you are really unlucky) a Carmichael number.

# A polynomial time algorithm

**Question:** Is there a "fast" algorithm for determining whether a number is prime *with certainty*?

# A polynomial time algorithm

**Question:** Is there a "fast" algorithm for determining whether a number is prime *with certainty*?

Here, "fast" is given a precise meaning: The number of divisions in the algorithm should be bounded by a **polynomial** function of the number of digits ( $n$ ) of the number being tested.

# A polynomial time algorithm

**Question:** Is there a "fast" algorithm for determining whether a number is prime *with certainty*?

Here, "fast" is given a precise meaning: The number of divisions in the algorithm should be bounded by a **polynomial** function of the number of digits ( $n$ ) of the number being tested.

For example,  $5n^3 + 3n^2 - 20n + 7$  is a polynomial function in  $n$ .

# A polynomial time algorithm

**Question:** Is there a "fast" algorithm for determining whether a number is prime *with certainty*?

Here, "fast" is given a precise meaning: The number of divisions in the algorithm should be bounded by a **polynomial** function of the number of digits ( $n$ ) of the number being tested.

For example,  $5n^3 + 3n^2 - 20n + 7$  is a polynomial function in  $n$ .

However, the function

$$\frac{(3.16)^n}{(1.15)^n}$$

is **not** bounded by a polynomial function of  $n$ .

# A polynomial time algorithm

Remarkably, the first polynomial time algorithm for primality testing was only just discovered in 2002 by three mathematicians in India: [Manindra Agrawal](#), [Neeraj Kayal](#), and [Nitin Saxena](#).

# A polynomial time algorithm

Remarkably, the first polynomial time algorithm for primality testing was only just discovered in 2002 by three mathematicians in India: [Manindra Agrawal](#), [Neeraj Kayal](#), and [Nitin Saxena](#).

In fact, Kayal and Saxena were undergraduates!!

# A polynomial time algorithm

Remarkably, the first polynomial time algorithm for primality testing was only just discovered in 2002 by three mathematicians in India: [Manindra Agrawal](#), [Neeraj Kayal](#), and [Nitin Saxena](#).

In fact, Kayal and Saxena were undergraduates!!

Their algorithm, now known as the AKS primality test, determines with certainty whether an  $n$ -digit number. The number of divisions needed in their algorithm is bounded by a polynomial function in  $n$  of degree 12.

This has now been improved to a polynomial of degree 6.

# Prime factorization

We now know there are "fast" algorithms for finding very large primes. (Currently, the largest known prime number has about 17 million digits.)

# Prime factorization

We now know there are "fast" algorithms for finding very large primes. (Currently, the largest known prime number has about 17 million digits.)

However, there is no known polynomial time algorithm for finding prime factors of numbers which are not prime.

# Prime factorization

We now know there are "fast" algorithms for finding very large primes. (Currently, the largest known prime number has about 17 million digits.)

However, there is no known polynomial time algorithm for finding prime factors of numbers which are not prime.

In fact, suppose  $n$  is a 400-digit number which is the product of two prime numbers,  $p$  and  $q$ . Using the best known algorithms, it would take a supercomputer thousands of years to find  $p$  and  $q$ !

# Prime factorization

We now know there are "fast" algorithms for finding very large primes. (Currently, the largest known prime number has about 17 million digits.)

However, there is no known polynomial time algorithm for finding prime factors of numbers which are not prime.

In fact, suppose  $n$  is a 400-digit number which is the product of two prime numbers,  $p$  and  $q$ . Using the best known algorithms, it would take a supercomputer thousands of years to find  $p$  and  $q$ !

The good news: This phenomenon has practical applications!

# Prime factorization

We now know there are "fast" algorithms for finding very large primes. (Currently, the largest known prime number has about 17 million digits.)

However, there is no known polynomial time algorithm for finding prime factors of numbers which are not prime.

In fact, suppose  $n$  is a 400-digit number which is the product of two prime numbers,  $p$  and  $q$ . Using the best known algorithms, it would take a supercomputer thousands of years to find  $p$  and  $q$ !

The good news: This phenomenon has practical applications!

It forms the basis for *public key cryptography*, which was discovered by three mathematicians at M.I.T.: [Ron Rivest](#), [Adi Shamir](#), and [Leonard Adleman](#) in 1977. It is now known as the [RSA cryptosystem](#).

# RSA cryptosystem

Here is roughly the idea behind RSA:

# RSA cryptosystem

Here is roughly the idea behind RSA:

I first find two large prime numbers  $p$  and  $q$  and multiply them together to get  $N = pq$ .

# RSA cryptosystem

Here is roughly the idea behind RSA:

I first find two large prime numbers  $p$  and  $q$  and multiply them together to get  $N = pq$ .

Now I choose any number  $e$  which has no common divisor with  $p - 1$  or  $q - 1$ .

# RSA cryptosystem

Here is roughly the idea behind RSA:

I first find two large prime numbers  $p$  and  $q$  and multiply them together to get  $N = pq$ .

Now I choose any number  $e$  which has no common divisor with  $p - 1$  or  $q - 1$ .

I tell anyone (say, Bob) who wants to send me a secure message to first convert the message into a number  $m$ .

# RSA cryptosystem

Here is roughly the idea behind RSA:

I first find two large prime numbers  $p$  and  $q$  and multiply them together to get  $N = pq$ .

Now I choose any number  $e$  which has no common divisor with  $p - 1$  or  $q - 1$ .

I tell anyone (say, Bob) who wants to send me a secure message to first convert the message into a number  $m$ .

Then Bob should compute the remainder of  $m^e$  divided by  $N$ . Call this remainder  $r$ .

# RSA cryptosystem

Here is roughly the idea behind RSA:

I first find two large prime numbers  $p$  and  $q$  and multiply them together to get  $N = pq$ .

Now I choose any number  $e$  which has no common divisor with  $p - 1$  or  $q - 1$ .

I tell anyone (say, Bob) who wants to send me a secure message to first convert the message into a number  $m$ .

Then Bob should compute the remainder of  $m^e$  divided by  $N$ . Call this remainder  $r$ .

Bob then sends  $r$  to me using any public channel he wishes (e.g., the internet).

# RSA - decryption

So I receive from Bob the number  $r$ . How do I recover the original message  $m$ ?

# RSA - decryption

So I receive from Bob the number  $r$ . How do I recover the original message  $m$ ?

Since I know  $p$  and  $q$ , I can compute a number  $d$  such that the remainder of  $ed$  divided by  $(p - 1)(q - 1)$  is 1.

# RSA - decryption

So I receive from Bob the number  $r$ . How do I recover the original message  $m$ ?

Since I know  $p$  and  $q$ , I can compute a number  $d$  such that the remainder of  $ed$  divided by  $(p-1)(q-1)$  is 1.

By the magic of Fermat's Theorem, one can show that the remainder of  $r^d$  divided by  $N$  is  $m$ !

# RSA - decryption

So I receive from Bob the number  $r$ . How do I recover the original message  $m$ ?

Since I know  $p$  and  $q$ , I can compute a number  $d$  such that the remainder of  $ed$  divided by  $(p-1)(q-1)$  is 1.

By the magic of Fermat's Theorem, one can show that the remainder of  $r^d$  divided by  $N$  is  $m$ !

Why is this secure? Because there is no known way to find  $d$  without first knowing  $p$  and  $q$ . So the security depends on the factorization problem being "hard".

# Fermat Primes

A prime number of the form  $2^n + 1$  is called a **Fermat prime**.

# Fermat Primes

A prime number of the form  $2^n + 1$  is called a **Fermat prime**.

Some Fermat primes:

$$3 = 2^1 + 1$$

$$5 = 2^2 + 1$$

$$17 = 2^4 + 1$$

$$257 = 2^8 + 1$$

$$65,537 = 2^{16} + 1$$

# Fermat Primes

A prime number of the form  $2^n + 1$  is called a **Fermat prime**.

Some Fermat primes:

$$3 = 2^1 + 1$$

$$5 = 2^2 + 1$$

$$17 = 2^4 + 1$$

$$257 = 2^8 + 1$$

$$65,537 = 2^{16} + 1$$

Fact: If  $2^n + 1$  is prime then  $n$  must be a power of 2.

# Fermat Primes

A prime number of the form  $2^n + 1$  is called a **Fermat prime**.

Some Fermat primes:

$$3 = 2^1 + 1$$

$$5 = 2^2 + 1$$

$$17 = 2^4 + 1$$

$$257 = 2^8 + 1$$

$$65,537 = 2^{16} + 1$$

Fact: If  $2^n + 1$  is prime then  $n$  must be a power of 2.

It is unknown if any other Fermat primes exist.

# Mersenne primes

A prime number of the form  $2^n - 1$  is called a **Mersenne prime**.  
(Mersenne was a French monk who lived in the 17th century.)

Some Mersenne primes:

$$3 = 2^2 - 1$$

$$7 = 2^3 - 1$$

$$31 = 2^5 - 1$$

$$127 = 2^7 - 1$$

# Mersenne primes

A prime number of the form  $2^n - 1$  is called a **Mersenne prime**.  
(Mersenne was a French monk who lived in the 17th century.)

Some Mersenne primes:

$$3 = 2^2 - 1$$

$$7 = 2^3 - 1$$

$$31 = 2^5 - 1$$

$$127 = 2^7 - 1$$

Fact: If  $2^n - 1$  is prime then  $n$  must be prime.

# Mersenne primes

A prime number of the form  $2^n - 1$  is called a **Mersenne prime**.  
(Mersenne was a French monk who lived in the 17th century.)

Some Mersenne primes:

$$3 = 2^2 - 1$$

$$7 = 2^3 - 1$$

$$31 = 2^5 - 1$$

$$127 = 2^7 - 1$$

Fact: If  $2^n - 1$  is prime then  $n$  must be prime.

There are 48 known Mersenne primes. (In fact, these are the largest known prime numbers.)

# Mersenne primes

A prime number of the form  $2^n - 1$  is called a **Mersenne prime**. (Mersenne was a French monk who lived in the 17th century.)

Some Mersenne primes:

$$3 = 2^2 - 1$$

$$7 = 2^3 - 1$$

$$31 = 2^5 - 1$$

$$127 = 2^7 - 1$$

Fact: If  $2^n - 1$  is prime then  $n$  must be prime.

There are 48 known Mersenne primes. (In fact, these are the largest known prime numbers.)

It is unknown if there are infinitely many Mersenne primes.



# Perfect numbers

A number is called **perfect** if it is equal to the sum of all its divisors (except itself).

# Perfect numbers

A number is called **perfect** if it is equal to the sum of all its divisors (except itself).

- The divisors of 6 are 1, 2, and 3. Since  $1 + 2 + 3 = 6$ , 6 is a perfect number.

# Perfect numbers

A number is called **perfect** if it is equal to the sum of all its divisors (except itself).

- The divisors of 6 are 1, 2, and 3. Since  $1 + 2 + 3 = 6$ , 6 is a perfect number.
- The divisors of 28 are 1, 2, 4, 7, and 14. Since  $1 + 2 + 4 + 7 + 14 = 28$ , 28 is a perfect number.

# Perfect numbers

A number is called **perfect** if it is equal to the sum of all its divisors (except itself).

- The divisors of 6 are 1, 2, and 3. Since  $1 + 2 + 3 = 6$ , 6 is a perfect number.
- The divisors of 28 are 1, 2, 4, 7, and 14. Since  $1 + 2 + 4 + 7 + 14 = 28$ , 28 is a perfect number.

It is unknown if there are any odd perfect numbers.

# Perfect numbers

A number is called **perfect** if it is equal to the sum of all its divisors (except itself).

- The divisors of 6 are 1, 2, and 3. Since  $1 + 2 + 3 = 6$ , 6 is a perfect number.
- The divisors of 28 are 1, 2, 4, 7, and 14. Since  $1 + 2 + 4 + 7 + 14 = 28$ , 28 is a perfect number.

It is unknown if there are any odd perfect numbers.

It can be shown (with a little arithmetic) that if  $N$  is a Mersenne prime, then  $\frac{N(N+1)}{2}$  is a perfect number.

# Perfect numbers

A number is called **perfect** if it is equal to the sum of all its divisors (except itself).

- The divisors of 6 are 1, 2, and 3. Since  $1 + 2 + 3 = 6$ , 6 is a perfect number.
- The divisors of 28 are 1, 2, 4, 7, and 14. Since  $1 + 2 + 4 + 7 + 14 = 28$ , 28 is a perfect number.

It is unknown if there are any odd perfect numbers.

It can be shown (with a little arithmetic) that if  $N$  is a Mersenne prime, then  $\frac{N(N+1)}{2}$  is a perfect number.

Moreover, every even perfect number has this form. So there are exactly as many even perfect numbers as there are Mersenne primes!

# Goldbach's Conjecture

There are many unsolved problems concerning prime numbers.  
Here are two favorites:

# Goldbach's Conjecture

There are many unsolved problems concerning prime numbers. Here are two favorites:

**Goldbach's Conjecture**, proposed in 1742, asserts that every even number greater than 2 is the sum of two primes.

# Goldbach's Conjecture

There are many unsolved problems concerning prime numbers. Here are two favorites:

**Goldbach's Conjecture**, proposed in 1742, asserts that every even number greater than 2 is the sum of two primes.

For example:

- $10=7+3$
- $32=19+13$
- $68=61+7$
- $100=47+53$

# Goldbach's Conjecture

There are many unsolved problems concerning prime numbers. Here are two favorites:

**Goldbach's Conjecture**, proposed in 1742, asserts that every even number greater than 2 is the sum of two primes.

For example:

- $10=7+3$
- $32=19+13$
- $68=61+7$
- $100=47+53$

This problem has been unsolved for over 350 years!

# The Twin Prime Conjecture

Two prime numbers which differ by two are called **twin primes**.

# The Twin Prime Conjecture

Two prime numbers which differ by two are called **twin primes**.

Here are some examples of twin primes:

- 11, 13
- 29, 31
- 41, 43
- 71, 73

The Twin Prime Conjecture asserts that there are infinitely many twin prime pairs.

# The Twin Prime Conjecture

Two prime numbers which differ by two are called **twin primes**.

Here are some examples of twin primes:

- 11, 13
- 29, 31
- 41, 43
- 71, 73

The Twin Prime Conjecture asserts that there are infinitely many twin prime pairs.

This problem has remained unsolved for centuries (perhaps even millenia).

# A recent breakthrough

One could ask an even weaker question:

# A recent breakthrough

One could ask an even weaker question:

**Question:** Does there exist any number  $N$  such that there are infinitely many prime pairs which are exactly  $N$  units apart?

(The case  $N = 2$  is the twin prime conjecture.)

# A recent breakthrough

One could ask an even weaker question:

**Question:** Does there exist any number  $N$  such that there are infinitely many prime pairs which are exactly  $N$  units apart?

(The case  $N = 2$  is the twin prime conjecture.)

Even the answer to this question was unknown

# A recent breakthrough

One could ask an even weaker question:

**Question:** Does there exist any number  $N$  such that there are infinitely many prime pairs which are exactly  $N$  units apart?

(The case  $N = 2$  is the twin prime conjecture.)

Even the answer to this question was unknown .....until 2013!

# A recent breakthrough

One could ask an even weaker question:

**Question:** Does there exist any number  $N$  such that there are infinitely many prime pairs which are exactly  $N$  units apart?

(The case  $N = 2$  is the twin prime conjecture.)

Even the answer to this question was unknown .....until 2013!

[Yitang Zhang](#), a mathematician at the University of New Hampshire, proved that there exists an  $N \leq 70,000,000$  such that there are infinitely many prime pairs exactly  $N$  units apart.

# A recent breakthrough

One could ask an even weaker question:

**Question:** Does there exist any number  $N$  such that there are infinitely many prime pairs which are exactly  $N$  units apart?

(The case  $N = 2$  is the twin prime conjecture.)

Even the answer to this question was unknown .....until 2013!

[Yitang Zhang](#), a mathematician at the University of New Hampshire, proved that there exists an  $N \leq 70,000,000$  such that there are infinitely many prime pairs exactly  $N$  units apart.

This bound has since been improved to  $N \leq 246$ .

# A recent breakthrough

One could ask an even weaker question:

**Question:** Does there exist any number  $N$  such that there are infinitely many prime pairs which are exactly  $N$  units apart?

(The case  $N = 2$  is the twin prime conjecture.)

Even the answer to this question was unknown .....until 2013!

[Yitang Zhang](#), a mathematician at the University of New Hampshire, proved that there exists an  $N \leq 70,000,000$  such that there are infinitely many prime pairs exactly  $N$  units apart.

This bound has since been improved to  $N \leq 246$ .

The case  $N = 2$  remains elusive....waiting for YOU to solve it.

# Thank you!