It's the last class

(and it's sunny out)

Who cares about the syllabus?

CS 2800: Discrete Structures, Spring 2015

Sid Chaudhuri

https://youtu.be/OFjgPGPQ0NA

ADVANCES IN APPLIED MATHEMATICS 4, 175–196 (1983)

The Mathematics of Perfect Shuffles

PERSI DIACONIS

Stanford University, Stanford, California 94305 and Harvard University, Cambridge, Massachusetts 02138

R. L. GRAHAM

Bell Laboratories, Murray Hill, New Jersey 07974 and Stanford University, Stanford, California 94305

WILLIAM M. KANTOR

University of Oregon, Eugene, Oregon 97403 and Bell Laboratories, Murray Hill, New Jersey 07974

There are two ways to perfectly shuffle a deck of $2n$ cards. Both methods cut the deck in half and interlace perfectly. The out shuffle O leaves the original top card on top. The in shuffle I leaves the original top card second from the top. Applications to the design of computer networks and card tricks are reviewed. The main result is the determination of the group $\langle I, O \rangle$ generated by the two shuffles, for all n. If $2n$ is not a power of 2, and if $2n \neq 12, 24$, then $\langle I, O \rangle$ has index 1, 2, or 4 in the Weyl group B_n (the group of all $2^n n!$ signed $n \times n$ permutation matrices). If $2n = 2^k$, then $\langle I, O \rangle$ is isomorphic to a semi-direct product of Z_2^k and Z_k. When $2n = 24$, $\langle I, O \rangle$ is isomorphic to a semi-direct product of Z_2^{11} and M_{12}, the Mathieu group of degree 12. When $2n = 12$, $\langle I, O \rangle$ is isomorphic to a semi-direct product of Z_2^6 and the group $PGL(2, 5)$ of all linear fractional transformations over $GF(5)$.

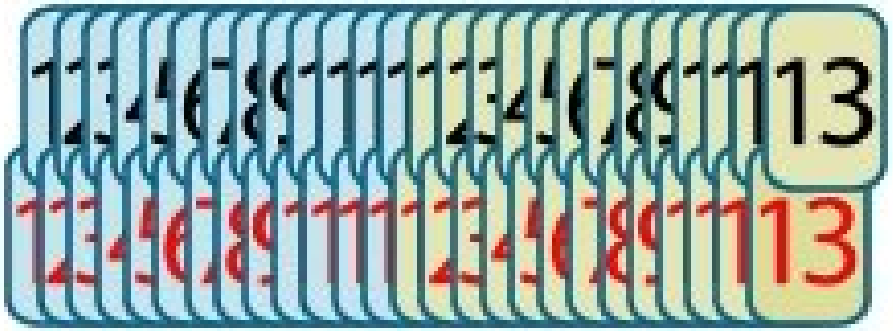
Persi Diaconis, Professor of Statistics and Mathematics, Stanford University

Admitted to Harvard PhD program for his abilities as a cardsharp

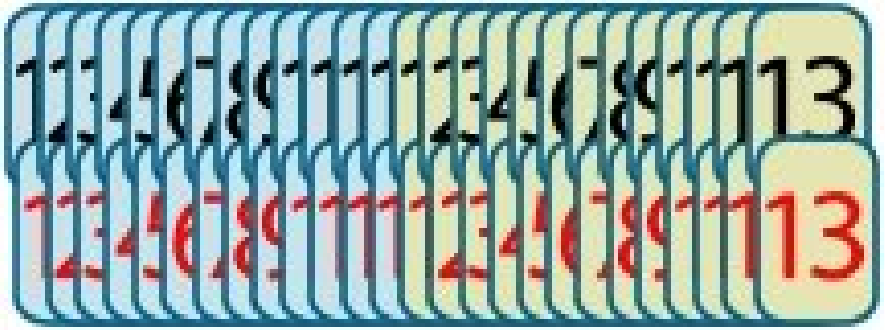
Can do eight consecutive perfect shuffles

Original order

Out shuffle



In shuffle



Perfect Shuffles

- A shuffle is a permutation of n cards
  - A permutation is a bijection from a set to itself
  - … it is a *function*
  - … and functions can be *composed* (do one shuffle after another)
- The set of all permutations (shuffles) forms a group under composition
  - Recall from HW6, a group is a set G plus operation * s.t.
    - **Closure:** $a * b \in G$ for all $a, b \in G$
    - **Associativity:** $(a * b) * c = a * (b * c)$
    - **Identity:** $\exists\, e \in G$ s.t. $a * e = e * a = a$ for all $a \in G$
    - **Inverse:** For all $a \in G$, $\exists\, a^{-1} \in G$ s.t. $a * a^{-1} = a^{-1} * a = e$

Perfect Shuffles

- The set of all permutations (shuffles) forms a group under composition
  - This is called the *symmetric group*
- Two types of perfect shuffles: **IN** and **OUT**
  - Here are some combinations:

    IIIII, OO, IOIO, OOIIOOII
  - The set of all such combinations forms a subgroup of the symmetric group
    - It's denoted <I, O> (“the group generated by I and O”)

Order of a perfect shuffle

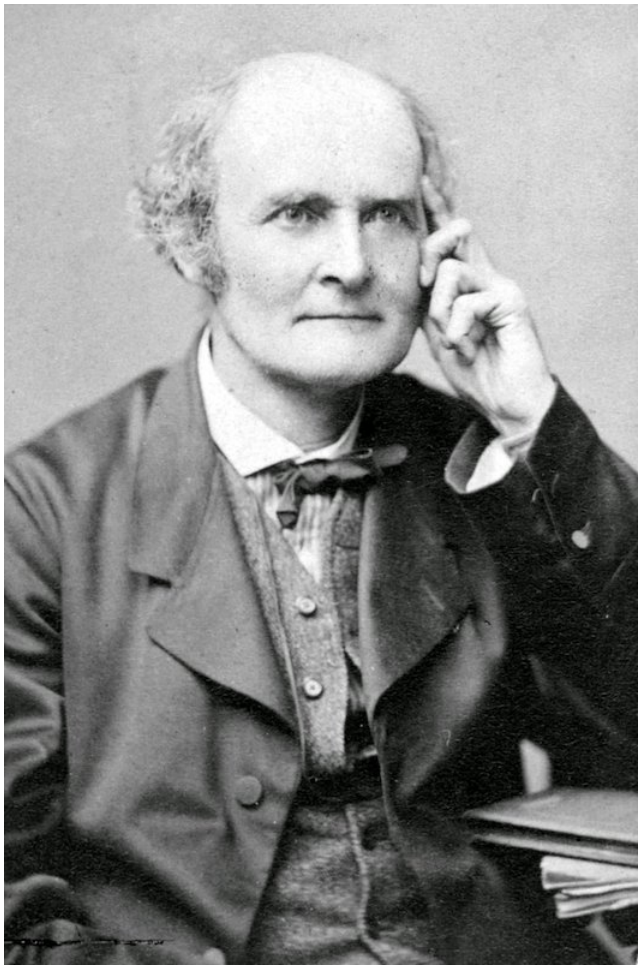
- The order of an element a in a group (or, the length of its cycle) is the smallest integer m such that $a^m = e$

  $a \;\; a^2 \;\; a^3 \;\; a^4 \;\; \ldots \;\; a^{m-1} \;\; e$

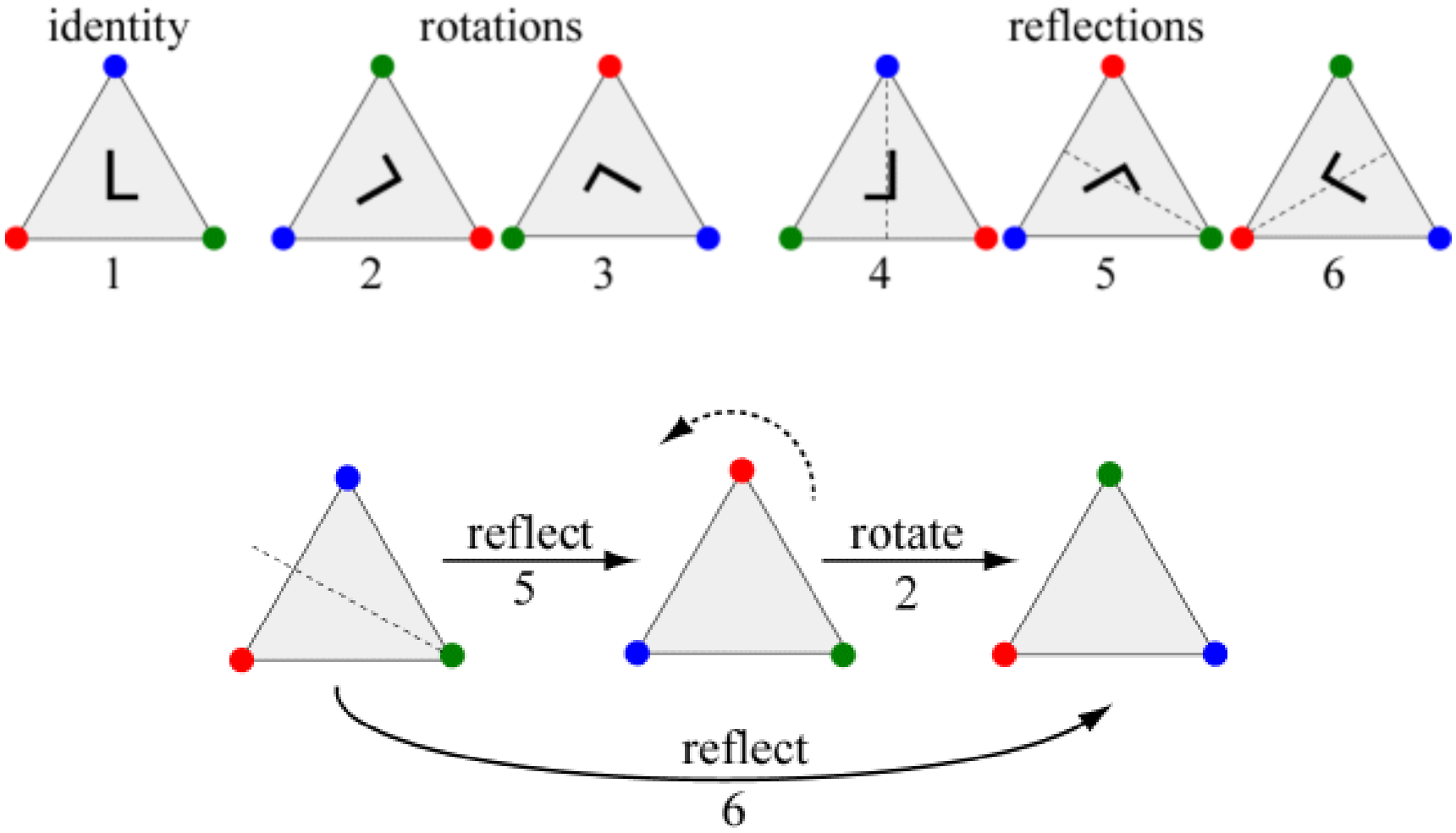
- In group <I, O> on $2n$ cards
  - the order of I is the smallest k s.t. $2^k \equiv 1 \pmod{2n+1}$
  - the order of O is the smallest k s.t. $2^k \equiv 1 \pmod{2n-1}$
- 8 perfect out-shuffles restore order in a 52-card deck!
  - ... since $2^8 \equiv 1 \pmod{51}$
- $2n-1$ out-shuffles or $2n+1$ in-shuffles also restore the deck (Fermat's Little Theorem!)

Permutation groups are fundamental

- Every group is isomorphic to a group of permutations [*Cayley's Theorem*]
- Arthur Cayley (1821-95) took group theory beyond permutations. His theorem is the link.
  - Cayley's formula for number of trees on a labeled graph is also named after him

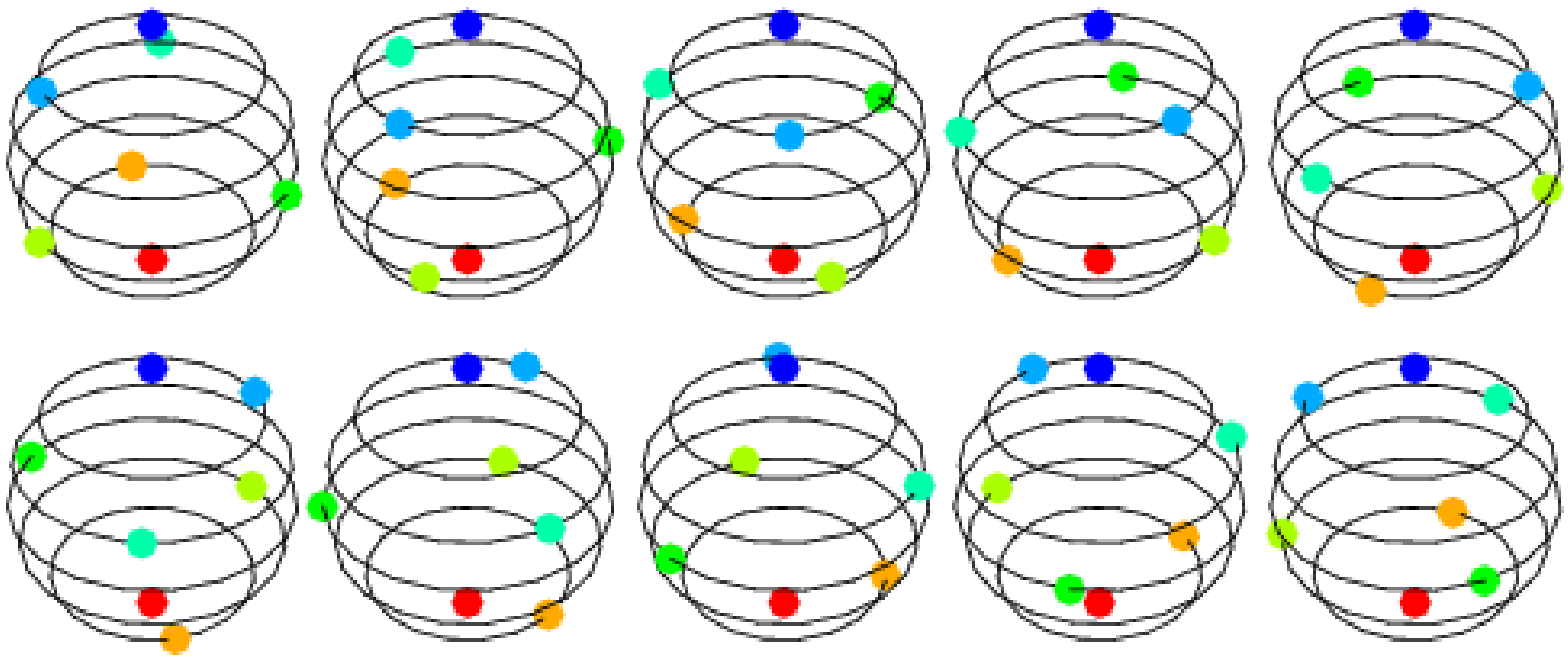


Groups encode symmetries



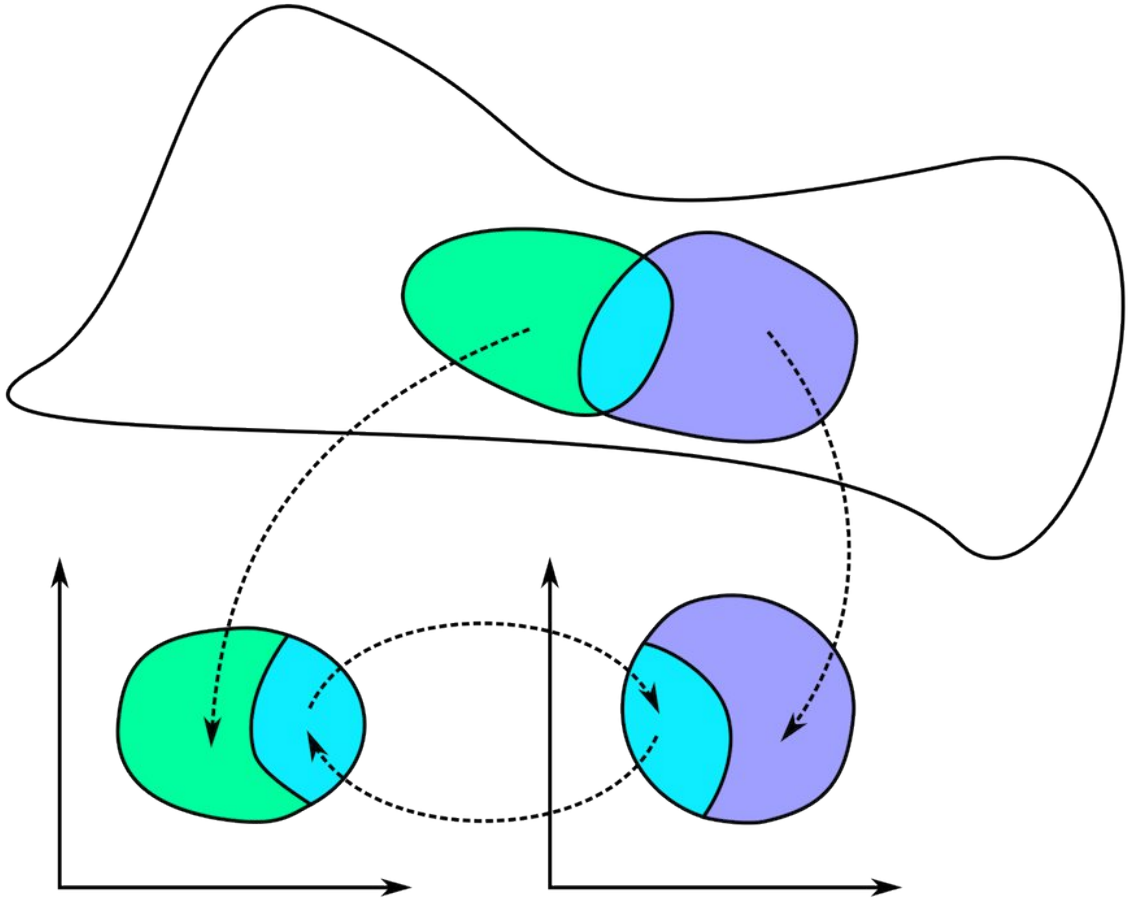
Dihedral group of an equilateral triangle

Symmetries can be continuous!



The 1D rotation group SO(2) acting on the sphere
The points trace out orbits under rotation

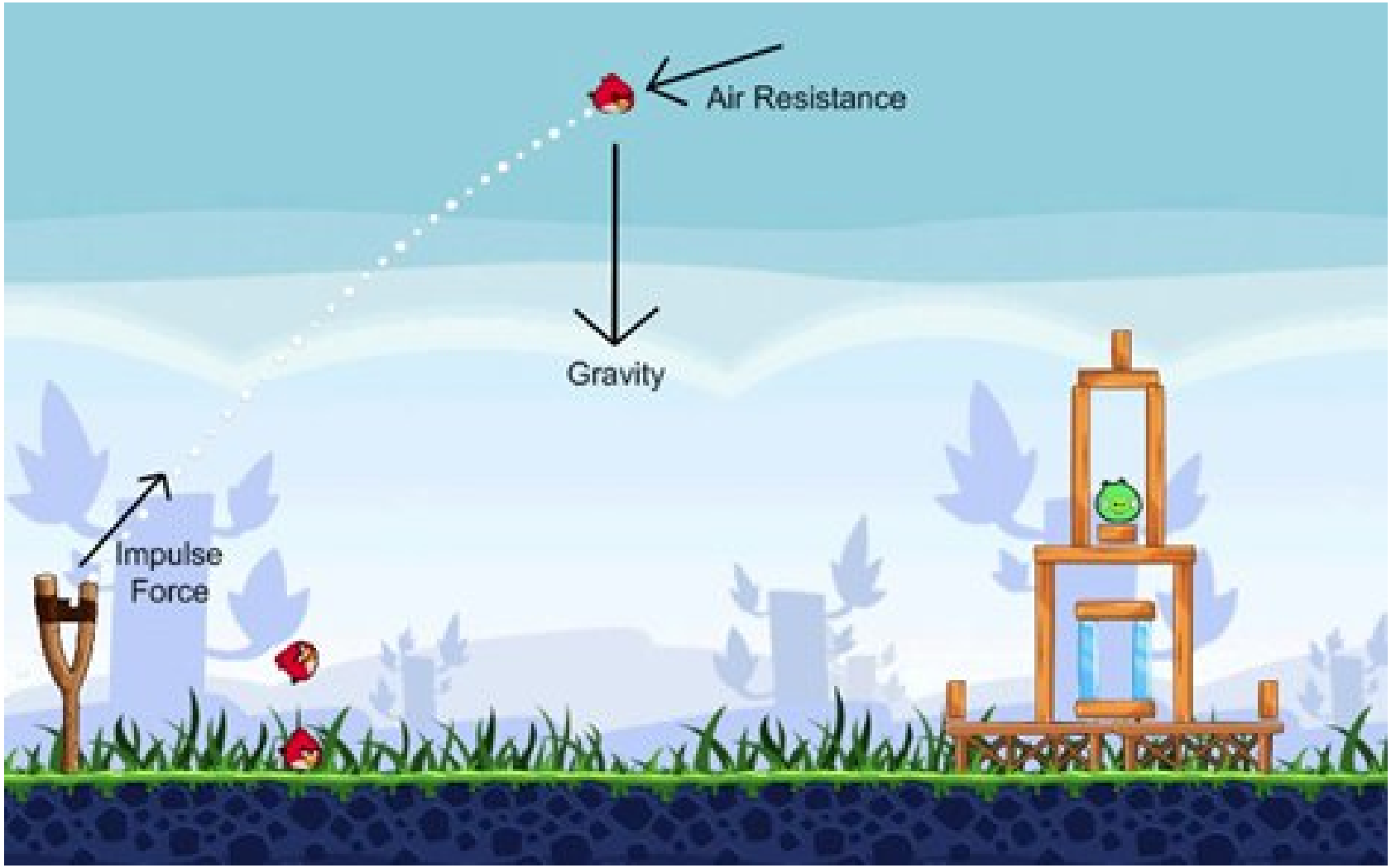
A Lie group of continuous symmetries is a differentiable manifold

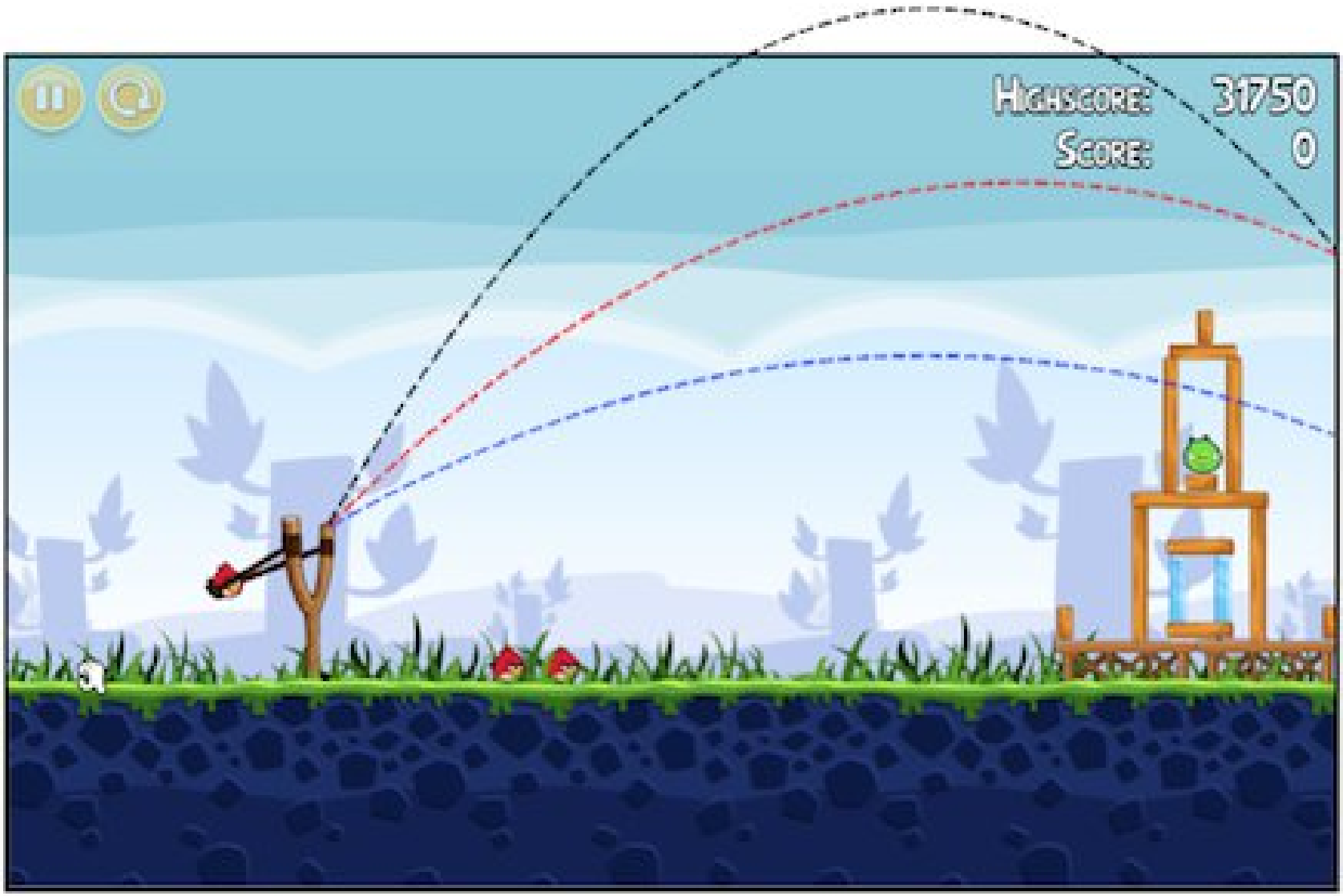


Some Lie groups:

- Euclidean space (under vector addition)
- SO(2), SO(3), SO(n)
- Heisenberg group
- Lorentz group

Stomatapoll@wikipedia





http://sites.davidson.edu/mathmovement/algebra-of-angry-birds/

The Lagrangian of a system

- The action of a physical system with parameters $\mathbf{q}$ is

$$I = \int L\left(\boldsymbol{q}, \dot{\boldsymbol{q}}, t\right) dt$$

... where L is the Lagrangian of the system

- The path taken by the system is given by the principle of least action, as expressed by the Euler-Lagrange equation

$$\frac{\partial L}{\partial \boldsymbol{q}} - \frac{d}{dt}\left(\frac{\partial L}{\partial \dot{\boldsymbol{q}}}\right) = 0$$

A symmetry of the Lagrangian

- The Lagrangian of a free particle is its kinetic energy $\frac{1}{2} mv^2$
- This is the same regardless of the particle's absolute position, so it has translational symmetry (Lie group is Euclidean space)
- Substituting into Euler-Lagrange equation,

$$\frac{d}{dt}\left(\frac{\partial L}{\partial \dot{\boldsymbol{x}}}\right) = \frac{\partial L}{\partial \boldsymbol{x}} = 0$$

... so the momentum of the system $\frac{\partial L}{\partial \dot{\boldsymbol{x}}}$ or mv is constant

Noether's Theorem

- *Any* global differentiable symmetry of the action of the Lagrangian corresponds to a conserved quantity
  - Translational invariance ↔ Momentum
  - Time invariance ↔ Energy
  - Rotational invariance ↔ Angular momentum

    ...
- Noether's Second Theorem: local symmetries
  - Local energy conservation in general relativity

Emmy Noether, 1882-1935

THE LATE EMMY NOETHER.

To the Editor of The New York Times:

The efforts of most human beings are consumed in the struggle for their daily bread, but most of those who are, either through fortune or some special gift, relieved of this struggle are largely absorbed in further improving their worldly lot. Beneath the effort directed toward the accumulation of worldly goods lies all too frequently the illusion that this is the most substantial and desirable end to be achieved; but there is, fortunately, a minority composed of those who recognize early in their lives that the most beautiful and satisfying experiences open to humankind are not derived from the outside, but are bound up with the development of the individual's own feeling, thinking and acting. The genuine artists, investigators and thinkers have always been persons of this kind. However inconspicuously the life of these individuals runs its course, none the less the fruits of their endeavors are the most valuable contributions which one generation can make to its successors.

Within the past few days a distinguished mathematician, Professor Emmy Noether, formerly connected with the University of Goettingen and for the past two years at Bryn Mawr College, died in her fifty-third year. In the judgment of the most competent living mathematicians, Fraeulein Noether was the most significant creative mathematical genius thus far produced since the higher education of women began. In the realm of algebra, in which the most gifted mathematicians have been busy for centuries, she discovered methods which have proved of enormous importance in the development of the present-day younger generation of mathematicians. Pure mathematics is, in its way, the poetry of logical ideas. One seeks the most general ideas of operation which will bring together in simple, logical and unified form the largest possible circle of formal relationships. In this effort toward logical beauty spiritual formulae are discovered necessary for the deeper penetration into the laws of nature.

Born in a Jewish family distinguished for the love of learning, Emmy Noether, who, in spite of the efforts of the great Goettingen mathematician, Hilbert, never reached the academic standing due her in her own country, none the less surrounded herself with a group of students and investigators at Goettingen, who have already become distinguished as teachers and investigators. Her unselfish, significant work over a period of many years was rewarded by the new rulers of Germany with a dismissal, which cost her the means of maintaining her simple life and the opportunity to carry on her mathematical studies. Farsighted friends of science in this country were fortunately able to make such arrangements at Bryn Mawr College and at Princeton that she found in America up to the day of her death not only colleagues who esteemed her friendship but grateful pupils whose enthusiasm made her last years the happiest and perhaps the most fruitful of her entire career.

ALBERT EINSTEIN.

Princeton University, May 1, 1935.

THE LATE EMMY NOETHER.

To the Editor of The New York Times:

The efforts of most human beings are consumed in the struggle for their daily bread, but most of those who are, either through fortune or some special gift, relieved of this struggle are largely absorbed in further improving their worldly lot. Beneath the effort directed toward the accumulation of worldly goods lies all too frequently the illusion that this is the most substantial and desirable and to be achieved; but there is, fo
those
that
experi
derive
up wi
ual's
The
thinkers have always been persons of this kind. However inconspicuously the life of these individuals runs its course, none the less the fruits of their endeavors are the most valuable contributions which one generation can make to its successors.

Pure mathematics is, in its way, the poetry of logical ideas.

Within the past few days a distinguished mathematician, Professor Emmy Noether, formerly connected with the University of Goettingen and for the past two years at Bryn Mawr College, died in her fifty-third year. In the judgment of the most competent living mathematicians, Fraeulein Noether was the most significant creative mathematical genius thus far produced since the higher education of women began. In the realm of algebra, in which the most gifted mathematicians have been busy for centuries, she discovered methods which have proved of enormous importance in the development of the present-day younger generation of mathematicians. Pure mathematics is, in its way, the poetry of logical ideas. One seeks the most general ideas of operation which will bring together in simple, logical and unified form the largest possible circle of formal relationships. In this effort toward logical beauty spiritual formulae are discovered necessary for the deeper penetration into the laws of nature.

guished as teachers and investigators. Her unselfish, significant work over a period of many years was rewarded by the new rulers of Germany with a dismissal, which cost her the means of maintaining her simple life and the opportunity to carry on her mathematical studies. Farsighted friends of science in this country were fortunately able to make such arrangements at Bryn Mawr College and at Princeton that she found in America up to the day of her death not only colleagues who esteemed her friendship but grateful pupils whose enthusiasm made her last years the happiest and perhaps the most fruitful of her entire career.

ALBERT EINSTEIN.

Princeton University, May 1, 1935.

Galois Theory

- A polynomial of degree 5 or higher is not always solvable by radicals
  - E.g. roots of $x^5 - x - 1 = 0$ can't be found by radicals
- Proved by Niels Abel (1802-29)
- Re-proved, and the conditions for unsolvability-by-radicals characterized, by Évariste Galois (1811-32)
  - Galois group of a polynomial: set of permutations of its roots s.t. any algebraic equation satisfied by the roots is still satisfied after the permutation
  - ^^^ Symmetries of the roots

Niels Henrik Abel, 1802-29

Évariste Galois, 1811-32

$$1 + 2 + 3 + 4 + 5 + \ldots = ???$$

$$1 + 2 + 3 + 4 + 5 + \ldots = -\frac{1}{12}$$

$$1 + 2 + 3 + 4 + 5 + \ldots = -\frac{1}{12}$$

Pull the other one!

A “proof”

- $S_1 = 1 - 1 + 1 - 1 + 1 - 1 + \ldots$
  - $S_1 = 0$ when #terms is even, 1 when it is odd
  - … so $S_1 = (0 + 1) / 2 = ½$
- $S_2 = 1 - 2 + 3 - 4 + 5 - 6 + \ldots$
  - $2S_2 = 1 - 2 + 3 - 4 + 5 - 6 + \ldots$

    $+ 1 - 2 + 3 - 4 + 5 - 6 + \ldots$

    $= 1 - 1 + 1 - 1 + 1 - 1 + \ldots = S_1 = ½$
  - So $S_2 = ¼$
- $S - S_2 = 1 + 2 + 3 + 4 + 5 + 6 + \ldots$

  $- (1 - 2 + 3 - 4 + 5 - 6 + \ldots)$

  $= 4 + 8 + 12 + 16 + \ldots = 4S$
- So $3S = -S_2 = -¼$, or $S = -1/12$

What are the flaws in this “proof”?

But there's more to this result than meets the eye...

another way of finding the constant is as follows — 41
Let us take the series $1+2+3+4+5+\&c$. Let C be its constant. Then $C = 1+2+3+4+\&c$

$\therefore 4C = 4 + 8 + \&c$

$\therefore -3C = 1-2+3-4+\&c = \frac{1}{(1+1)^2} = \frac{1}{4}$

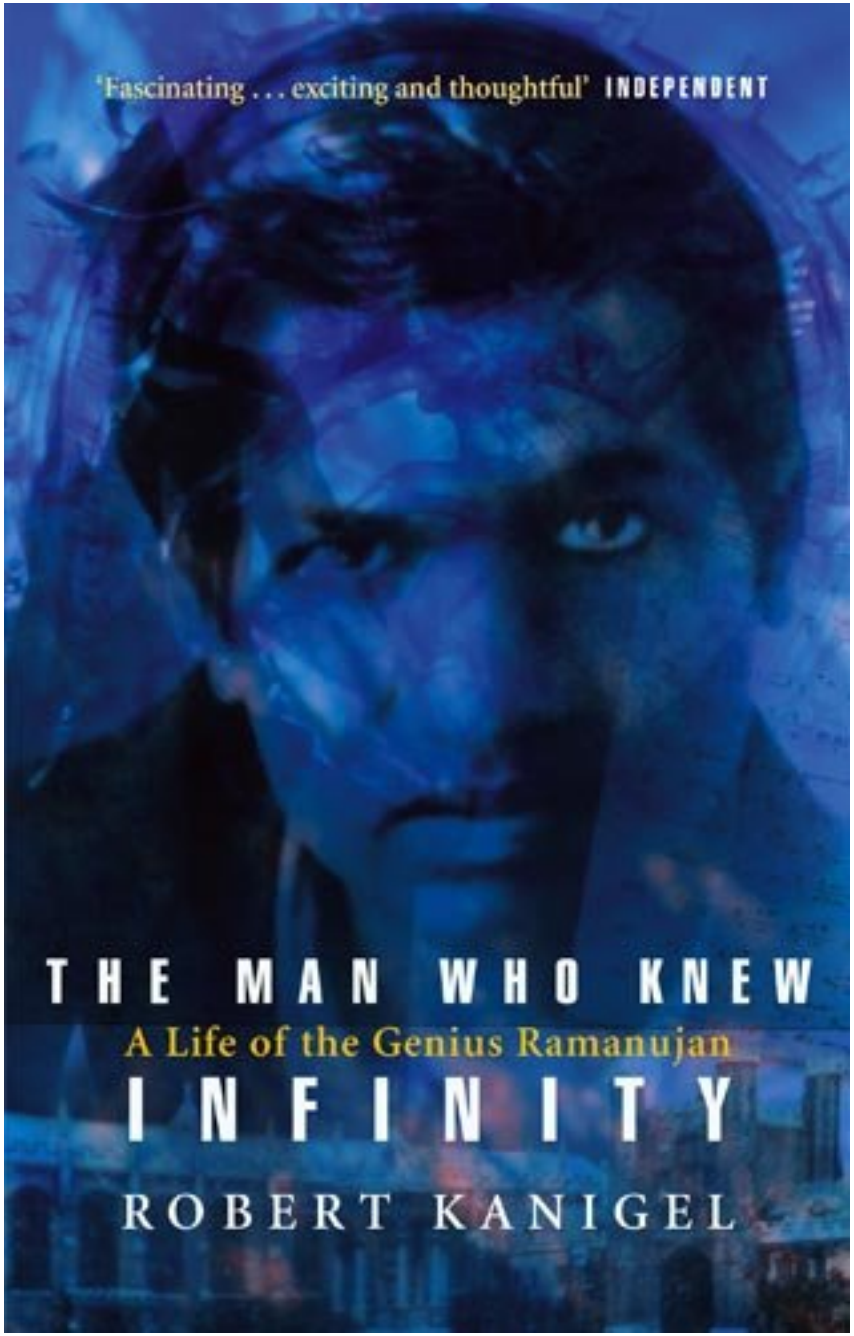
$\therefore C = -\frac{1}{12}$.

Srinivasa Ramanujan, Notebook 1, Chapter 8

“Dear Sir,

I am very much gratified on perusing your letter of the 8th February 1913. I was expecting a reply from you similar to the one which a Mathematics Professor at London wrote asking me to study carefully Bromwich's *Infinite Series* and not fall into the pitfalls of divergent series. ... I told him that the sum of an infinite number of terms of the series: $1 + 2 + 3 + 4 + \cdots = -1/12$ under my theory. If I tell you this you will at once point out to me the lunatic asylum as my goal. I dilate on this simply to convince you that you will not be able to follow my methods of proof if I indicate the lines on which I proceed in a single letter.”

Srinivasa Ramanujan to G. H. Hardy, 27 Feb 1913



Srinivasa Ramanujan, 1887–1920

The Riemann Zeta Function

$$\zeta(s) = \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \frac{1}{5^s} \cdots$$

for complex numbers s with real part > 1

The Riemann Zeta Function

$$\zeta(s) = \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \frac{1}{5^s} \cdots$$

for complex numbers s with real part > 1

For $\mathrm{Re}(s) \leq 1$, the series diverges, but $\zeta(s)$ can be defined by a process called *analytic continuation*.

The Riemann Zeta Function

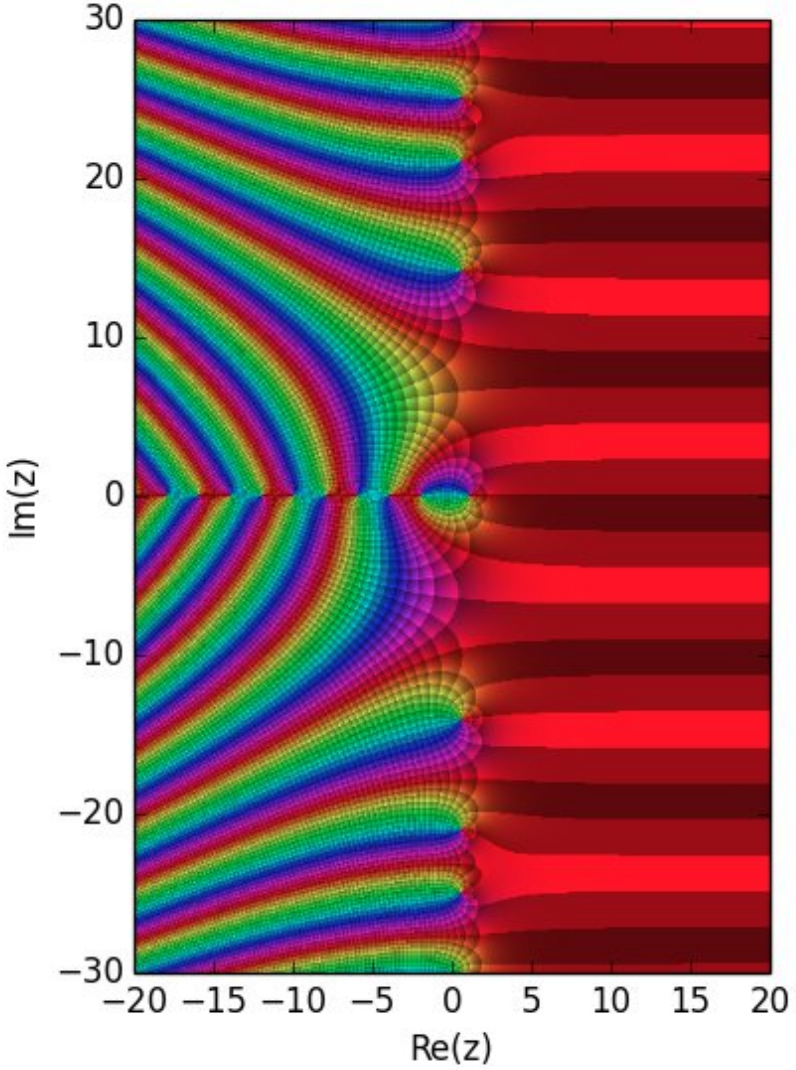
$$\zeta(s) = \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \frac{1}{5^s} \cdots$$

for complex numbers s with real part > 1

For $\mathrm{Re}(s) \leq 1$, the series diverges, but $\zeta(s)$ can be defined by a process called *analytic continuation*.

This also gives $\zeta(-1) = -1/12$!

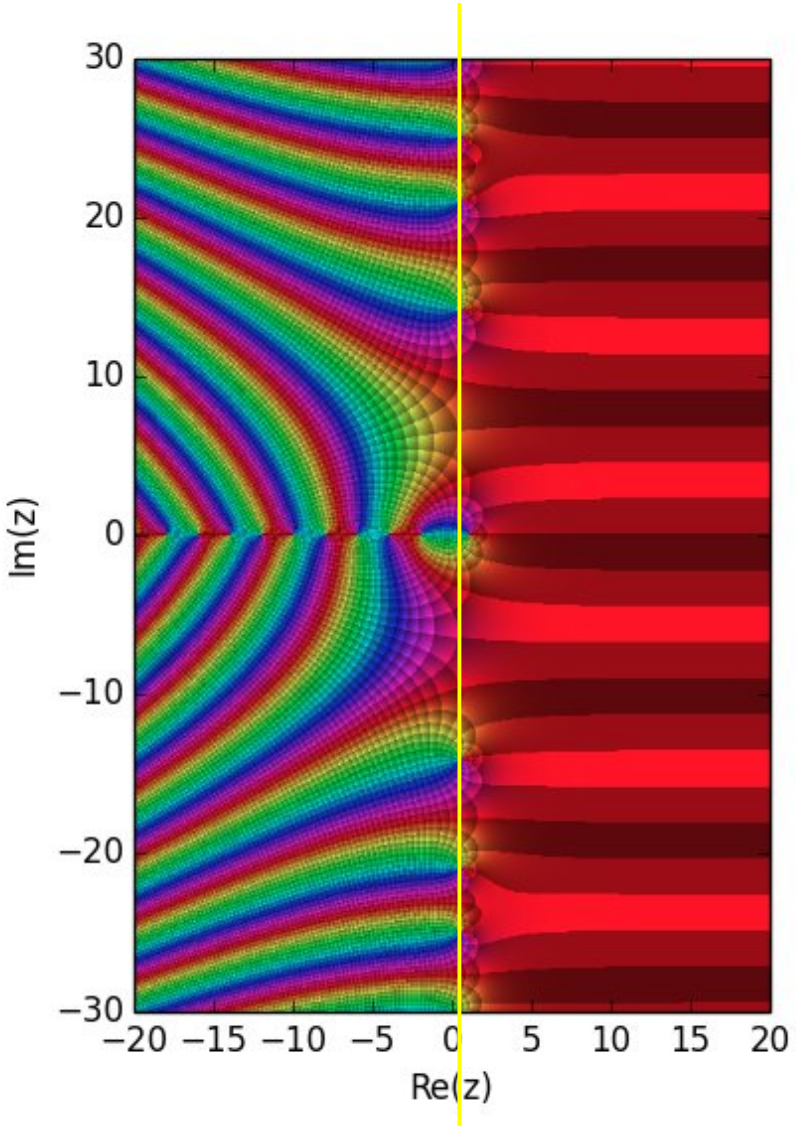
The Riemann Hypothesis



All the “non-trivial” zeros of the Riemann zeta function $\zeta(s)$ have real part ½

Empetrisor@Wikipedia

The Riemann Hypothesis



All the “non-trivial” zeros of the Riemann zeta function $\zeta(s)$ have real part ½

A consequence: characterizes the distribution of the prime numbers (more precisely, gives a tight bound for the error term in the Prime Number Theorem)

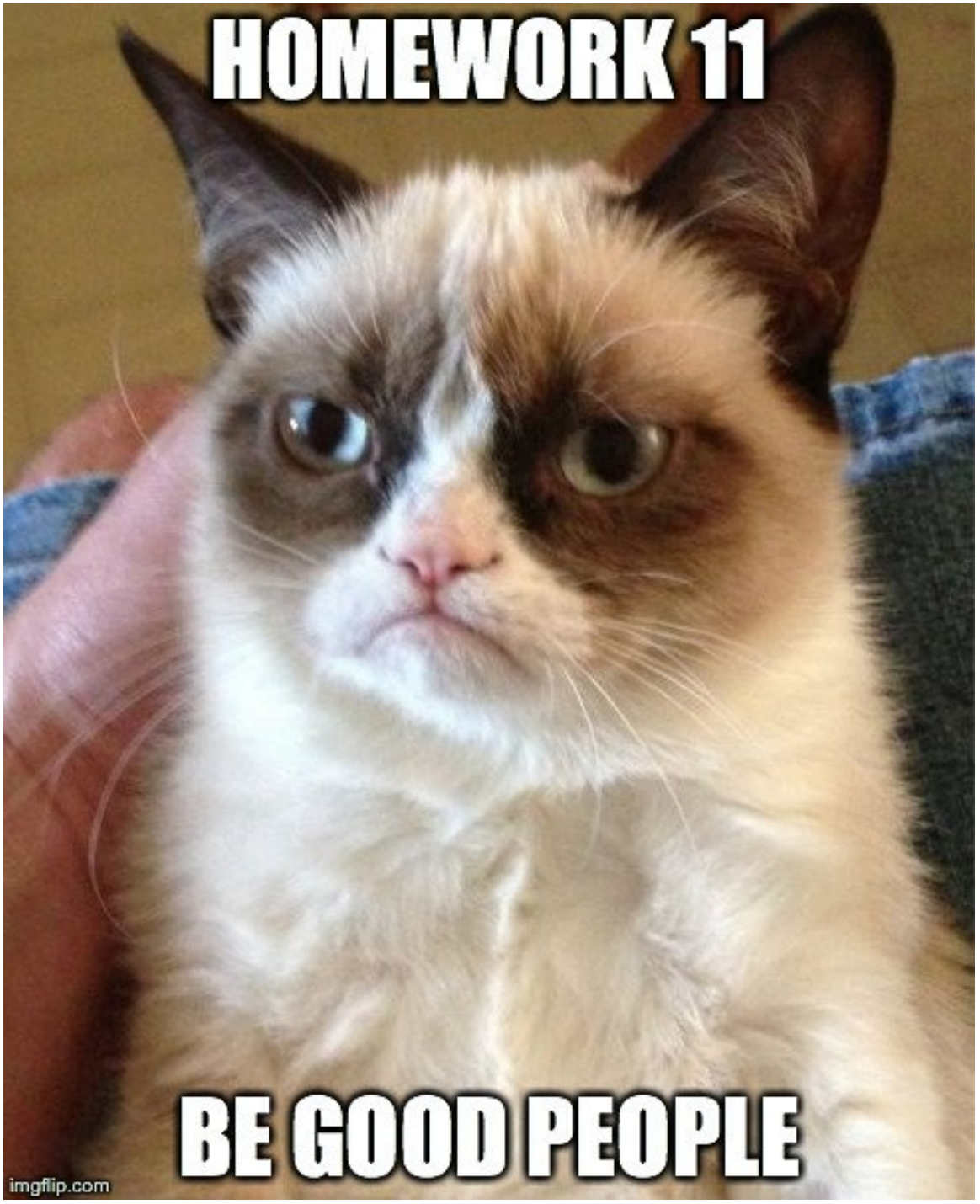
Empetrisor@Wikipedia

WANTED

DEAD OR ALIVE

REWARD $ 1,000,000


HOMEWORK 11
PROVE THE RIEMANN HYPOTHESIS
imgflip.com



(and avoid backwards proofs)