The Millennium Prize Problems For Dummies

A UTM Math Club Presentation

Brandon Papandrea

Department of Mathematical and Computational Sciences
University of Toronto - Mississauga

February 24, 2025

Introduction

What is the most difficult way to earn a million dollars?

What Are The Millennium Prize Problems?

Announced on May 24, 2000, the Millennium Prize Problems are a collection of 7 problems chosen by the Clay Mathematical Institute in order to both celebrate mathematics in the third millennium, and to "record some of the most difficult problems with which mathematicians were grappling at the turn of the second millennium."

The problems come from a wide range of mathematical subjects, like number theory, mathematical physics, geometry, PDEs, and topology.

Solving one of these problems will earn you \$1 million dollars.

The Problems

1. Birch and Swinnerton-Dyer Conjecture
2. Hodge Conjecture
3. Navier-Stokes Equation
4. P vs. NP
5. Riemann Hypothesis
6. Yang-Mills & The Mass Gap
7. Poincare Conjecture

Elliptic Curves

Elliptic curves, equations of the form

$$y^2 = x^3 + ax + b$$

are an important area of number theory and have had a key part in modern mathematical research, including the proof of Fermat's Last Theorem, Elliptic Curve Cryptography, and integer factorization.

Elliptic Curves

Elliptic curves, equations of the form

$$y^2 = x^3 + ax + b$$

are an important area of number theory and have had a key part in modern mathematical research, including the proof of Fermat's Last Theorem, Elliptic Curve Cryptography, and integer factorization.

A particular area of interest is whether or not an elliptic curve has **rational solutions**.

Algebraic and Analytic Rank

It is known that the set of rational solutions of any elliptic curve C is a group, $C(\mathbb{Q})$, and has a finite generating set. If the number of solutions is infinite, then there must be an element in this generating set of infinite order. The number of such elements is called the **algebraic rank** of the elliptic curve, denoted r. We know that $r = 0$ if and only if $C(\mathbb{Q})$ if finite.

Algebraic and Analytic Rank

It is known that the set of rational solutions of any elliptic curve C is a group, $C(\mathbb{Q})$, and has a finite generating set. If the number of solutions is infinite, then there must be an element in this generating set of infinite order. The number of such elements is called the **algebraic rank** of the elliptic curve, denoted r. We know that $r = 0$ if and only if $C(\mathbb{Q})$ if finite.

Analytic rank is defined differently. We first consider our elliptic curve modulo a prime p, and denote its set of solution modulo p $C(\mathbb{F}_p)$.

Algebraic and Analytic Rank

It is known that the set of rational solutions of any elliptic curve C is a group, $C(\mathbb{Q})$, and has a finite generating set. If the number of solutions is infinite, then there must be an element in this generating set of infinite order. The number of such elements is called the **algebraic rank** of the elliptic curve, denoted r. We know that $r = 0$ if and only if $C(\mathbb{Q})$ if finite.

Analytic rank is defined differently. We first consider our elliptic curve modulo a prime p, and denote its set of solution modulo p $C(\mathbb{F}_p)$. A theorem of Hasse tells us that

$$|C(\mathbb{F}_p) - p - 1| \leq 2\sqrt{p}$$

We'll let $C(\mathbb{F}_p) - p - 1 = a_p$.

Analytic Rank Continued

From here we can define an L-series using an Euler product that will allow us to collect the a_p values in a good way:

Analytic Rank Continued

From here we can define an L-series using an Euler product that will allow us to collect the a_p values in a good way: Given an elliptic curve C we have

$$L(C,s) = \prod_{p|\Delta}(1 - a_p p^{-s} + p^{1-2s})^{-1} \cdot \prod_{p|\Delta}(1 - a_p p^{-s})^{-1}$$

Analytic Rank Continued

From here we can define an L-series using an Euler product that will allow us to collect the a_p values in a good way: Given an elliptic curve C we have

$$L(C,s) = \prod_{p|\Delta}(1 - a_p p^{-s} + p^{1-2s})^{-1} \cdot \prod_{p|\Delta}(1 - a_p p^{-s})^{-1}$$

Then we define the **analytic rank** of C as

$$r_{an} = \text{ord}_{s=1} L(C,s)$$

Birch and Swinnerton-Dyer Conjecture (1965)

Bryan John Birch and Peter Swinnerton-Dyer studied the properties of L for $\Re(s) = 1$. They observed that for an elliptic curve C

$$L(C, 1) = \prod_p \frac{p}{|C(\mathbb{F}_p)|}$$

Upon further inspection, they noticed that the order of $L(C, 1)$ coincided with the number of generators of infinite order in $C(\mathbb{Q})$.

Birch and Swinnerton-Dyer Conjecture (1965)

Bryan John Birch and Peter Swinnerton-Dyer studied the properties of L for $\Re(s) = 1$. They observed that for an elliptic curve C

$$L(C, 1) = \prod_p \frac{p}{|C(\mathbb{F}_p)|}$$

Upon further inspection, they noticed that the order of $L(C, 1)$ coincided with the number of generators of infinite order in $C(\mathbb{Q})$. This led to the following conjecture:

Birch and Swinnerton-Dyer Conjecture

Let C be an elliptic curve over $\mathbb{Q}$. Then

$$r(C) = r_{an}(C)$$

Why Should I Care?

If this conjecture is true, we can easily compute if an elliptic curve has finite or infinite solutions over $\mathbb{Q}$ by computing $L(C, 1)$.

This means we can study local properties of an elliptic curve to decduce some of its global properties.

Why Should I Care?

If this conjecture is true, we can easily compute if an elliptic curve has finite or infinite solutions over $\mathbb{Q}$ by computing $L(C, 1)$.

This means we can study local properties of an elliptic curve to decduce some of its global properties.

It would also mean many arithmetic properties that have yet to be proven in general will hold true. For example:

- Every positive integer congruent to 5, 6, or 7, mod 8, is a congruent number.

Why Should I Care?

If this conjecture is true, we can easily compute if an elliptic curve has finite or infinite solutions over $\mathbb{Q}$ by computing $L(C, 1)$.

This means we can study local properties of an elliptic curve to decduce some of its global properties.

It would also mean many arithmetic properties that have yet to be proven in general will hold true. For example:

- Every positive integer congruent to 5, 6, or 7, mod 8, is a congruent number.
- Every positive integer can be written as $s^2(t^3 - 91t - 182)$ for some $s, t \in \mathbb{Q}$.

Hodge Theory

Hodge Theory is a subfield of algebraic topology that studies the cohomology groups of smooth manifolds using PDEs.

It was conceived in the 1930s by Sir William Vallance Douglas Hodge for use in algebraic geometry, more specifically to study complex projective manifolds.

It is a very useful part of algebraic geometry, but also has applications in number theory.

Kahler Manifolds & Hodge Classes

Definition

A **Kahler manifold** is a manifold which has complex, Riemannian, and symplectic structures that are compatible with each other.

Kahler Manifolds & Hodge Classes

Definition

A **Kahler manifold** is a manifold which has complex, Riemannian, and symplectic structures that are compatible with each other.

Definition

A homology class x in a homology group

$$H_k(X, \mathbb{C}) = H$$

where X is a Kahler manifold, is called a **Hodge class** if $k = 2p$, x is of type (p, p) in the decomposition of H, and lies in the image of the abelian group homomorphism

$$H_k(X, \mathbb{Q}) \to H$$

Algebraic Cycles and Classes

Let X be a Kahler manifold and Z a subvariety (subset) of X. An **algebraic cycle** on X is a formal sum of its subvarieties

$$\sum_i c_i Z_i$$

where the c_i's are rational.

Algebraic Cycles and Classes

Let X be a Kahler manifold and Z a subvariety (subset) of X. An **algebraic cycle** on X is a formal sum of its subvarieties

$$\sum_i c_i Z_i$$

where the c_i's are rational. The cohomology class of an algebraic cycle is just the sum of the cohomology classes of the subvarieties:

$$\sum_i c_i [Z_i]$$

we call this cohomology class **algebraic**.

Hodge Conjecture (1952)

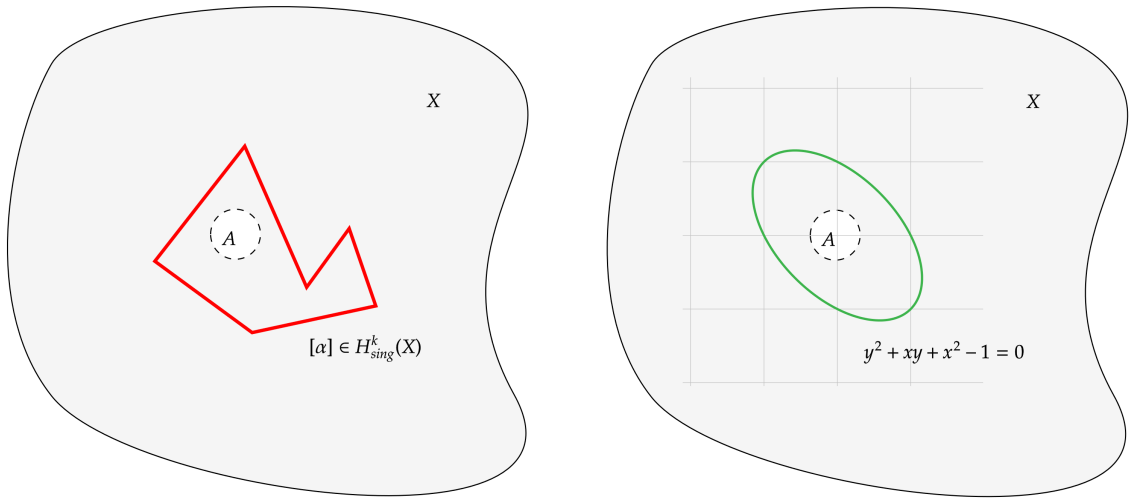
Hodge Conjecture

Let X be a Kahler manifold (projective complex manifold). Then every Hodge class on X is algebraic.

While special cases of the Hodge conjecture have been proven, a general proof remains elusive.

Why Should I Care?

If true, the Hodge conjecture would ensure that certain topological properties can be understood by studying much simpler shapes, like the zero set of a polynomial, inside of the space we're working on. These nicer structures can be studied using calculus or algebra, which make understanding the broader structure of these objects much easier.



The Navier-Stokes Equations (1800s)

The Navier-Stokes Equations are a collection of partial differential equations designed to model the movement of fluids using continuum mechanics. They were developed by Claude-Louis Navier and George Stokes between the 1820s and 1850s.

The Navier-Stokes Equations (1800s)

The Navier-Stokes Equations are a collection of partial differential equations designed to model the movement of fluids using continuum mechanics. They were developed by Claude-Louis Navier and George Stokes between the 1820s and 1850s.

The Navier-Stokes Equations

$$\nabla \cdot \vec{u} = 0 \tag{1}$$

$$\rho \frac{D\vec{u}}{Dt} = -\nabla p + \mu \nabla^2 \vec{u} + \rho \vec{F} \tag{2}$$

The Navier-Stokes Equations (1800s)

The Navier-Stokes Equations are a collection of partial differential equations designed to model the movement of fluids using continuum mechanics. They were developed by Claude-Louis Navier and George Stokes between the 1820s and 1850s.

The Navier-Stokes Equations

$$\nabla \cdot \vec{u} = 0 \tag{1}$$

$$\rho \frac{D\vec{u}}{Dt} = -\nabla p + \mu \nabla^2 \vec{u} + \rho \vec{F} \tag{2}$$

(1) is just the Conservation of Mass, while (2) is Newton's Second Law.

The Navier-Stokes Equations (1800s)

While these equations have been used to model fluids for hundreds of years, there is one slight problem: we don't have a good understanding of them mathematically in $\mathbb{R}^3$.

The Navier-Stokes Equations (1800s)

While these equations have been used to model fluids for hundreds of years, there is one slight problem: we don't have a good understanding of them mathematically in $\mathbb{R}^3$. In particular, we don't know three things: Given a set of initial conditions,

1. Does a solution exist?

The Navier-Stokes Equations (1800s)

While these equations have been used to model fluids for hundreds of years, there is one slight problem: we don't have a good understanding of them mathematically in $\mathbb{R}^3$. In particular, we don't know three things: Given a set of initial conditions,

1. Does a solution exist? If so,
2. Is that solution unique?

The Navier-Stokes Equations (1800s)

While these equations have been used to model fluids for hundreds of years, there is one slight problem: we don't have a good understanding of them mathematically in $\mathbb{R}^3$. In particular, we don't know three things: Given a set of initial conditions,

1. Does a solution exist? If so,
2. Is that solution unique? If so,
3. Is that solution smooth and defined globally?

Time Complexity

In the realm of theoretical computer science, **time complexity** represents the amount of computer time it would take to run a particular algorithm.

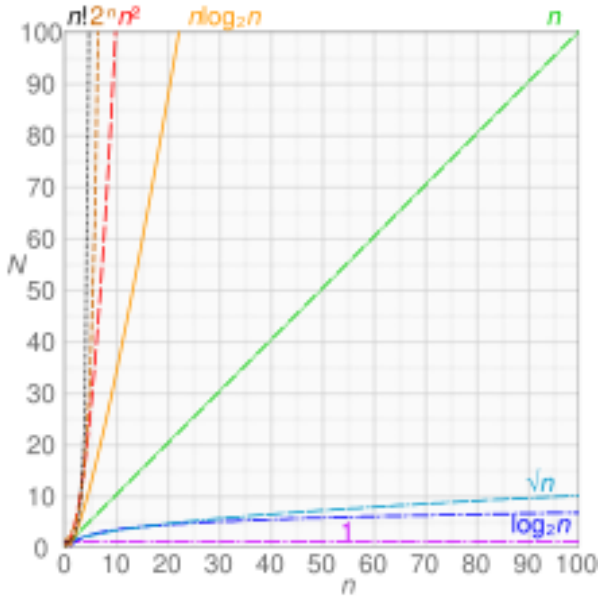
Time complexity is often used to determine how the runtime of an algorithm increases as the amount of inputs increases. It is often represented by **Big-O Notation**.

Time Complexity

In the realm of theoretical computer science, **time complexity** represents the amount of computer time it would take to run a particular algorithm.

Time complexity is often used to determine how the runtime of an algorithm increases as the amount of inputs increases. It is often represented by **Big-O Notation**. Examples include

- Constant time $O(1)$
- Logarithmic time $O(\log n)$
- Linear time $O(n)$
- Quadratic time $O(n^2)$
- Polynomial time $O(2^{\log n})$
- Factorial time $O(n!)$



P and NP

Problems and algorithms can be classified into many different groups depending on their time complexity. Two of them are particularly important:

P and NP

Problems and algorithms can be classified into many different groups depending on their time complexity. Two of them are particularly important:

Definition

We say that a problem is in the set P if there is an algorithm that can **solve** the problem in polynomial time.

P and NP

Problems and algorithms can be classified into many different groups depending on their time complexity. Two of them are particularly important:

Definition

We say that a problem is in the set P if there is an algorithm that can **solve** the problem in polynomial time.

We say that a problem is in the set NP if there is an algorithm that can **verify** a possible solution in polynomial time.

P and NP

Problems and algorithms can be classified into many different groups depending on their time complexity. Two of them are particularly important:

Definition

We say that a problem is in the set P if there is an algorithm that can **solve** the problem in polynomial time.

We say that a problem is in the set NP if there is an algorithm that can **verify** a possible solution in polynomial time.

Examples

Sorting a list using merge sort is a problem in P.

Finding a solution to a sudoku puzzle is a problem in NP.

P vs. NP (1971)

It is obvious that any problem in P is also in NP, hence $P \subseteq NP$. However, the other inclusion is not known.

P vs. NP (1971)

It is obvious that any problem in P is also in NP, hence $P \subseteq NP$. However, the other inclusion is not known. This led Stephen Cook to formally ask about the relationship between the two sets in a 1971 paper.

P vs. NP

What is the relationship between P and NP? Is $P = NP$?

Why Should I Care?

Proving that $P \neq NP$, or more shockingly, $P = NP$, would have massive implications for computer science and its applications.

Why Should I Care?

Proving that $P \neq NP$, or more shockingly, $P = NP$, would have massive implications for computer science and its applications.

Assuming $P = NP$, many difficult problems to solve would theoretically be solvable in polynomial time, including

- Any computer encryption method

Why Should I Care?

Proving that $P \neq NP$, or more shockingly, $P = NP$, would have massive implications for computer science and its applications.

Assuming $P = NP$, many difficult problems to solve would theoretically be solvable in polynomial time, including

- Any computer encryption method
- The Traveling Salesman Problem

Why Should I Care?

Proving that $P \neq NP$, or more shockingly, $P = NP$, would have massive implications for computer science and its applications.

Assuming $P = NP$, many difficult problems to solve would theoretically be solvable in polynomial time, including

- Any computer encryption method
- The Traveling Salesman Problem
- Protein structure prediction

Why Should I Care?

Proving that $P \neq NP$, or more shockingly, $P = NP$, would have massive implications for computer science and its applications.

Assuming $P = NP$, many difficult problems to solve would theoretically be solvable in polynomial time, including

- Any computer encryption method
- The Traveling Salesman Problem
- Protein structure prediction

With that said, it is widely accepted that $P \neq NP$, and many computer scientists have noted that if $P = NP$, there would still be issues with finding solutions to problems.

The Riemann-Zeta Function

Definition

The **Riemann-Zeta Function** $\zeta : \mathbb{C} \to \mathbb{C}$ is defined for all $s \in \mathbb{C}$ with $\Re(s) > 1$ and is given by

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \cdots$$

The Riemann-Zeta Function

Definition

The **Riemann-Zeta Function** $\zeta : \mathbb{C} \to \mathbb{C}$ is defined for all $s \in \mathbb{C}$ with $\Re(s) > 1$ and is given by

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \cdots$$

Examples

- $\zeta(2) = 1 + \frac{1}{2^2} + \frac{1}{3^2} + \cdots = \frac{\pi^2}{6}$

The Riemann-Zeta Function

Definition

The **Riemann-Zeta Function** $\zeta : \mathbb{C} \to \mathbb{C}$ is defined for all $s \in \mathbb{C}$ with $\Re(s) > 1$ and is given by

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \cdots$$

Examples

- $\zeta(2) = 1 + \frac{1}{2^2} + \frac{1}{3^2} + \cdots = \frac{\pi^2}{6}$
- $\zeta(i) \approx 0.00330 - 0.41816i$
- $\zeta(10 + 5i) = 5i + \frac{\pi^{10}}{93555}$

The Riemann-Zeta Function

Definition

The **Riemann-Zeta Function** $\zeta : \mathbb{C} \to \mathbb{C}$ is defined for all $s \in \mathbb{C}$ with $\Re(s) > 1$ and is given by

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \cdots$$

Examples

- $\zeta(2) = 1 + \frac{1}{2^2} + \frac{1}{3^2} + \cdots = \frac{\pi^2}{6}$
- $\zeta(i) \approx 0.00330 - 0.41816i$
- $\zeta(10 + 5i) = 5i + \frac{\pi^{10}}{93555}$
- $\zeta(-1) = 1 + 2 + 3 + \ldots$

The Riemann-Zeta Function

ζ converges only for complex numbers with real part greater than 1. However, Riemann (1859) showed that ζ is a mereomorphic function, and thus has a unique analytic continuation to all of $\mathbb{C}$. This continuation is given by the equation

$$\zeta(s) = 2^s \pi^{s-1} \sin\left(\frac{\pi s}{2}\right) \Gamma(1-s)\zeta(1-s)$$

The Riemann-Zeta Function

ζ converges only for complex numbers with real part greater than 1. However, Riemann (1859) showed that ζ is a mereomorphic function, and thus has a unique analytic continuation to all of $\mathbb{C}$. This continuation is given by the equation

$$\zeta(s) = 2^s \pi^{s-1} \sin\left(\frac{\pi s}{2}\right) \Gamma(1-s)\zeta(1-s)$$

Using this equation we can show that $\zeta(-1) = \dfrac{-1}{12}$

The Zeroes of ζ

If $s = -2n$ is a negative even integer, we have that

$$\zeta(s) = 2^{-2n}\pi^{-2n-1}\sin(-n\pi)\Gamma(1+2n)\zeta(1+2n) = 0$$

These are called the **trivial zeroes** of ζ.

The Zeroes of ζ

If $s = -2n$ is a negative even integer, we have that

$$\zeta(s) = 2^{-2n}\pi^{-2n-1}\sin(-n\pi)\Gamma(1+2n)\zeta(1+2n) = 0$$

These are called the **trivial zeroes** of ζ.

ζ does not vanish for any other values of s with a real component that is negative or greater than 1. Thus the non-trivial zeroes of ζ must be in the set

$$\{s \in \mathbb{C} : 0 < \Re(s) < 1\}$$

This is a special region called the **Critical Strip**.

The Riemann Hypothesis (1859)

Riemann knew that the zeroes inside the Critical Strip had to be symmetric around the line $s = \frac{1}{2} + it$. Explicit computations showed that many zeroes lied exactly on this line.

The Riemann Hypothesis (1859)

Riemann knew that the zeroes inside the Critical Strip had to be symmetric around the line $s = \frac{1}{2} + it$. Explicit computations showed that many zeroes lied exactly on this line. This led Riemann to make the following conjecture:

The Riemann Hypothesis

Every non-trivial zero of the Riemann-Zeta function is of the form

$$s = \frac{1}{2} + it$$

for some $t \in \mathbb{R}$.

The Riemann Hypothesis (1859)

Riemann knew that the zeroes inside the Critical Strip had to be symmetric around the line $s = \frac{1}{2} + it$. Explicit computations showed that many zeroes lied exactly on this line. This led Riemann to make the following conjecture:

The Riemann Hypothesis

Every non-trivial zero of the Riemann-Zeta function is of the form

$$s = \frac{1}{2} + it$$

for some $t \in \mathbb{R}$.

George Hardy and John Littlewood (1914, 1921) showed that there an infinite number of such zeroes, and as of 2020, we know that at least 41% of non-trivial zeroes lie on this line.

Why Should I Care?

The Riemann-Zeta Function plays an important role in number theory, particularly with respect to the distribution of prime numbers.

Why Should I Care?

The Riemann-Zeta Function plays an important role in number theory, particularly with respect to the distribution of prime numbers.

The Prime Number Theorem tells us that the function $\pi(x)$ can be approximated by the logarithmic integral $\mathrm{Li}(x)$. What's interesting is that the difference between $\pi(x)$ and the apporximation by Li is related to the non-trivial zeroes of ζ.

Why Should I Care?

The Riemann-Zeta Function plays an important role in number theory, particularly with respect to the distribution of prime numbers.

The Prime Number Theorem tells us that the function $\pi(x)$ can be approximated by the logarithmic integral $\mathrm{Li}(x)$. What's interesting is that the difference between $\pi(x)$ and the apporximation by Li is related to the non-trivial zeroes of ζ.

If the Riemann Hypothesis is true, then

$$\pi(x) = \mathrm{Li}(x) + O(\sqrt{x}\ln(x))$$

which gives us the best possible bound for the error in the Prime Number Theorem.

Why Should I Care?

Another interesting consequence is related to calculating gaps between the primes. Harald Cramer (1919), showed that if p_k is the k-th prime number, then if the Riemann Hypothesis is true,

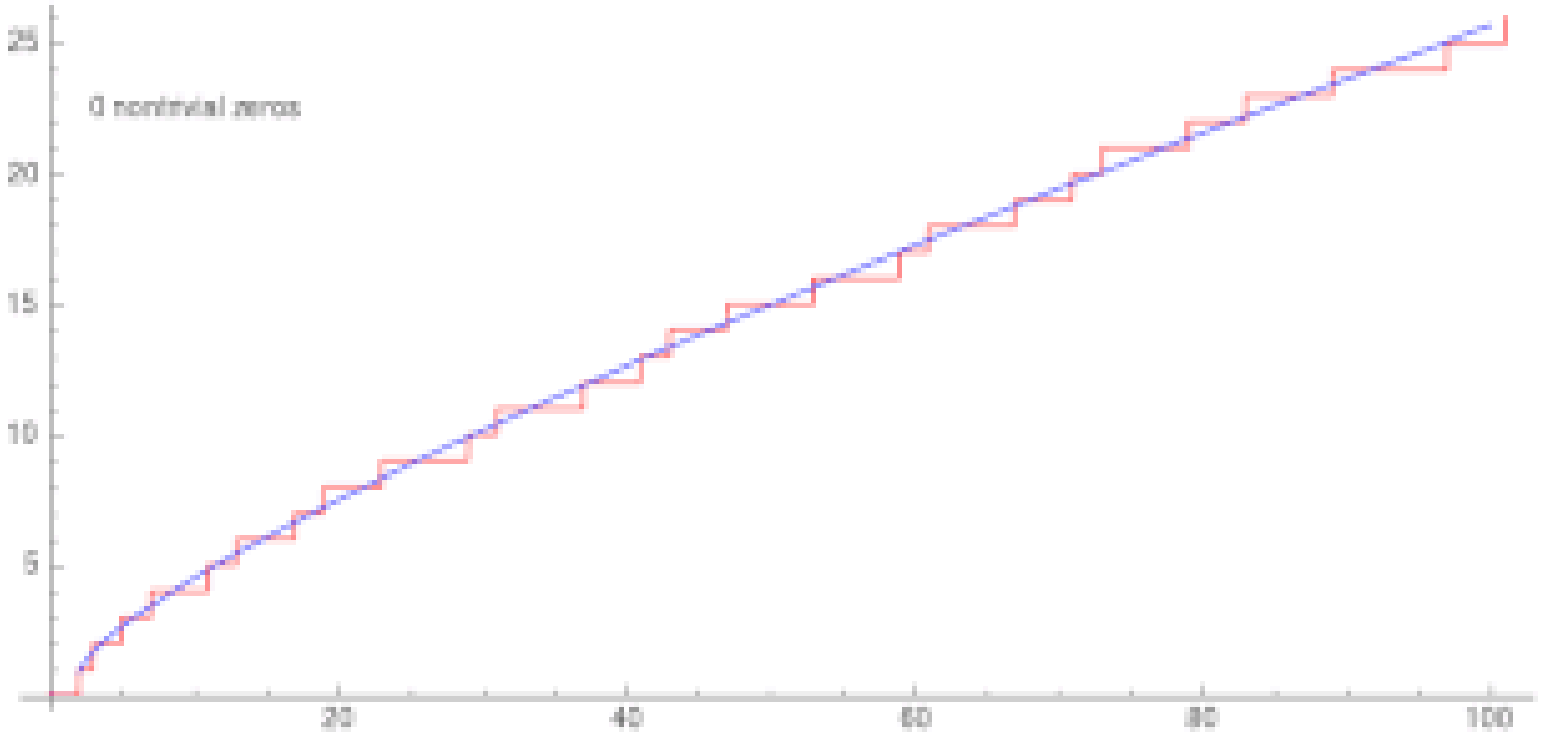
$$p_{k+1} - p_k = O(\sqrt{p_k}\ln(p_k))$$

Why Should I Care?

Another interesting consequence is related to calculating gaps between the primes. Harald Cramer (1919), showed that if p_k is the k-th prime number, then if the Riemann Hypothesis is true,

$$p_{k+1} - p_k = O(\sqrt{p_k}\ln(p_k))$$

In short, if the Riemann Hypothesis is true, we get a lot of interesting information about the bounds on the gaps between primes, and their distribution.

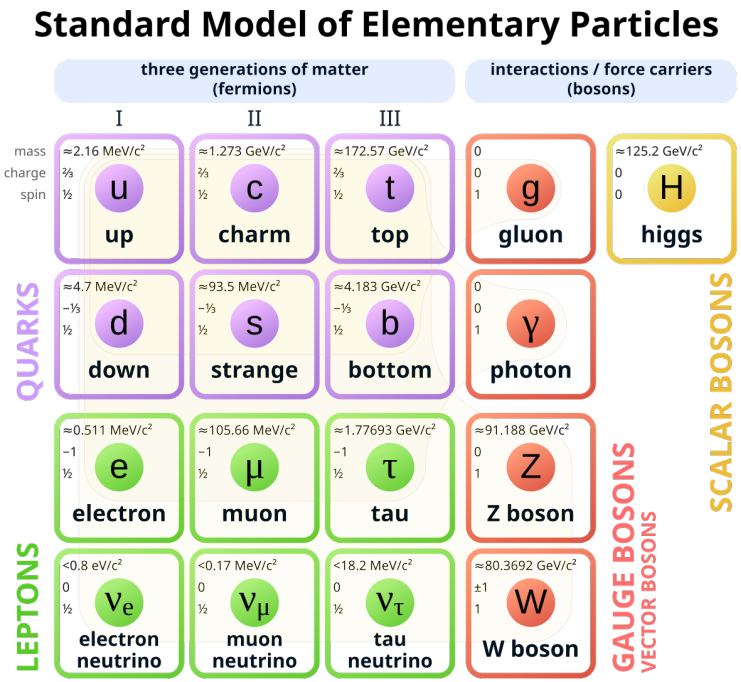

0 nontrivial zeros
25
20
15
10
5
20
40
60
80
100

Quantum Field Theory

Developed throughout the 20th century, **quantum field theory** is a part of mathematical physics that combines field theory, relativity, group theory, and quantum mechanics, into one singular theoretical framework. It has been used to construct models for subatomic particles and quasiparticles.

Quantum Field Theory

Developed throughout the 20th century, **quantum field theory** is a part of mathematical physics that combines field theory, relativity, group theory, and quantum mechanics, into one singular theoretical framework. It has been used to construct models for subatomic particles and quasiparticles.



Yang-Mills Theory

Yang-Mills Theory is a specific type of quantum field theory that attempts to use non-abelian Lie groups like $SU(n)$ to describe the behaviour of elementary particles. It was developed in the 1950s by Chen Ning Yang and Robert Mills.

Yang-Mills Theory

Yang-Mills Theory is a specific type of quantum field theory that attempts to use non-abelian Lie groups like $SU(n)$ to describe the behaviour of elementary particles. It was developed in the 1950s by Chen Ning Yang and Robert Mills.

It is at the core of the unification of electromagnetic and weak forces, as well as our understanding of the strong forces, called quantum chromodynamics (QCD). It also provides the basis for our understanding of the Standard Model.

Yang-Mills Theory

Yang-Mills Theory is a specific type of quantum field theory that attempts to use non-abelian Lie groups like $SU(n)$ to describe the behaviour of elementary particles. It was developed in the 1950s by Chen Ning Yang and Robert Mills.

It is at the core of the unification of electromagnetic and weak forces, as well as our understanding of the strong forces, called quantum chromodynamics (QCD). It also provides the basis for our understanding of the Standard Model.

Problem: We don't have a great theoretical (mathematical) understanding of Yang-Mills Theory in 4D spacetime.

Wightman Axioms & The Mass Gap

The **Wightman Axioms**, developed by Arthur Wightman in the early 1950s, is a rigorous mathematical formulation of quantum field theory that provides a basis for rigorous study of quantum fields. They are:

1. W0: assumptions of relativistic quantum mechanics
2. W1: assumptions on the domain and continuity of the field
3. W2: transformation law of the field
4. W3: local commutativity or microscopic causality

Wightman Axioms & The Mass Gap

The **Wightman Axioms**, developed by Arthur Wightman in the early 1950s, is a rigorous mathematical formulation of quantum field theory that provides a basis for rigorous study of quantum fields. They are:

1. W0: assumptions of relativistic quantum mechanics
2. W1: assumptions on the domain and continuity of the field
3. W2: transformation law of the field
4. W3: local commutativity or microscopic causality

In a quantum system, there are many different energy states, the lowest of which is called the vacuum. The **mass gap** Δ_0 is the difference in energy between the vacuum and the next lowest energy state.

Yang-Mills Existence & Mass Gap (1950s)

Yang-Mills Existence & Mass Gap

For a gauge group G, there is a non-trivial Yang-Mills theory on $\mathbb{R}^4$ such that the theory

1. satisfies axiomatic properties as strong as the Wightman Axioms, and
2. there exists a mass gap $\Delta_0 > 0$.

While experimental and computational results have shown that a mass gap is likely to exist, no rigorous theoretical proof of 1 or 2 has been published.

Why Should I Care?

It has been shown that special types of Yang-Mills theory exhibit a special type of property call confinement; finding a proof of the above problem would give a more rigorous proof of confinement, and lead to the theoretical existence of objects called *glueballs*.

Why Should I Care?

It has been shown that special types of Yang-Mills theory exhibit a special type of property call confinement; finding a proof of the above problem would give a more rigorous proof of confinement, and lead to the theoretical existence of objects called *glueballs*.

Furthermore, if Yang-Mills theory does indeed satisfy the necessary axiomatic properties and have a mass gap, it would be the smallest non-trivial constructive quantum field theory in 4 dimensions.

Properties of Spheres

Spheres are cool.

Properties of Spheres

Spheres are cool.

In addition to being closed and connected as topological objects, they have another special property:

If we pick any point along a sphere, and then draw any path that starts and ends at the chosen point, we can continuously deform this path and shrink it down to the point without the need to cut our path or the sphere.

Simply Connected

If two paths can be continuously deformed into one another, we say they're *equivalent*. The set of all non-equivalent paths which start and end at a point p in a space X is called the **Fundamental Group of X at p**, denoted $\pi(X, p)$.

Simply Connected

If two paths can be continuously deformed into one another, we say they're *equivalent*. The set of all non-equivalent paths which start and end at a point p in a space X is called the **Fundamental Group of X at p**, denoted $\pi(X, p)$.

We say that X is **simply-connected** if any path that starts and ends at any point can be continuously deformed down to that point. More rigorously, for any $p \in X$,

$$\pi(X, p) = \{\mathrm{id}_p\}$$

Classifying Simply-Connected Spaces

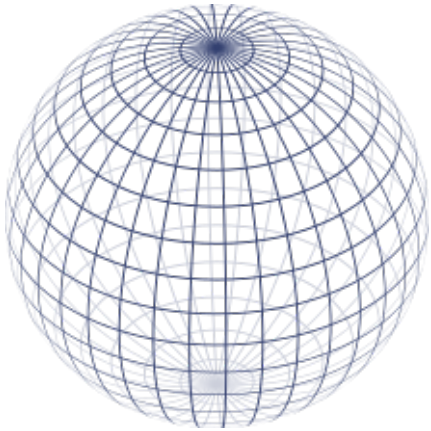
Fact

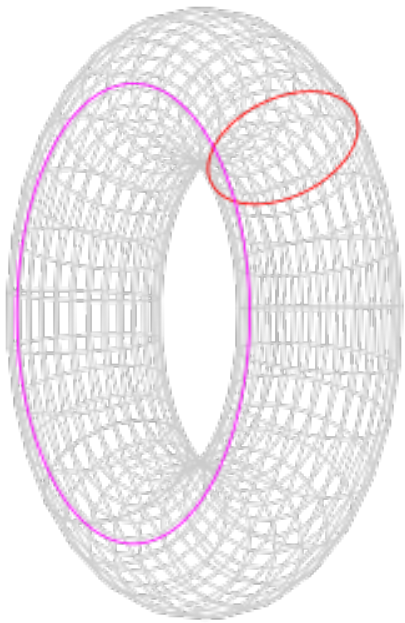
Any compact 2-dimensional topological manifold without boundary that is simply connected is homeomorphic to the 2-sphere.

Classifying Simply-Connected Spaces

Fact

Any compact 2-dimensional topological manifold without boundary that is simply connected is homeomorphic to the 2-sphere.





The Poincare Conjecture (1904)

Henri Poincare introduced the fundamental group to show that a similar claim does not hold in higher dimensions. Later works by him tried to find conditions that hold in higher dimensions but he was unsuccessful.

The Poincare Conjecture (1904)

Henri Poincare introduced the fundamental group to show that a similar claim does not hold in higher dimensions. Later works by him tried to find conditions that hold in higher dimensions but he was unsuccessful. Eventually he posed an open-ended question on the matter that would eventually lead to this following conjecture:

The Poincare Conjecture

Any compact 3-dimensional topological manifold without boundary that is simply connected is homeomorphic to the 3-sphere.

The Poincare Conjecture (1904)

Henri Poincare introduced the fundamental group to show that a similar claim does not hold in higher dimensions. Later works by him tried to find conditions that hold in higher dimensions but he was unsuccessful. Eventually he posed an open-ended question on the matter that would eventually lead to this following conjecture:

The Poincare Conjecture

Any compact 3-dimensional topological manifold without boundary that is simply connected is homeomorphic to the 3-sphere.

A proof of a more generalized version of The Poincare Conjecture was proved for 4-dimensions and higher by Stephen Smale (1961), and Michael Freedman (1982), but a proof for 3-dimensions remained elusive.

Ricci Flow

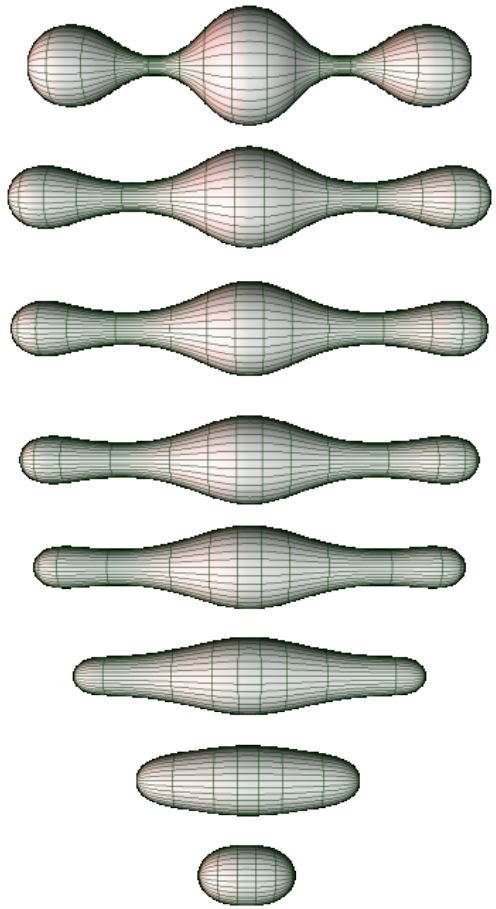
In 1982, Richard Hamilton introduced the concept of **Ricci Flow** and used it to prove many special cases on the Poincare Conjecture.

Ricci Flow

In 1982, Richard Hamilton introduced the concept of **Ricci Flow** and used it to prove many special cases on the Poincare Conjecture.

In essence, Ricci Flow is a process that acts like the Heat Equation, and tries to "smoothen" the surface we're working on so it has constant positive curvature; then it must be homeomophic to the 3-sphere.

The only problem is that Ricci Flow can create singularities.



The Solution

Between 2002 and 2003, Grigori Perelman published a solution to the Poincare Conjecture using Ricci Flow. While his solution was a rough sketch, the gaps were later filled in by others and a full proof was published by 2006.

Perelman was awarded the $1 million by CMI and was offered the Fields Medal, but he *declined both of them*.