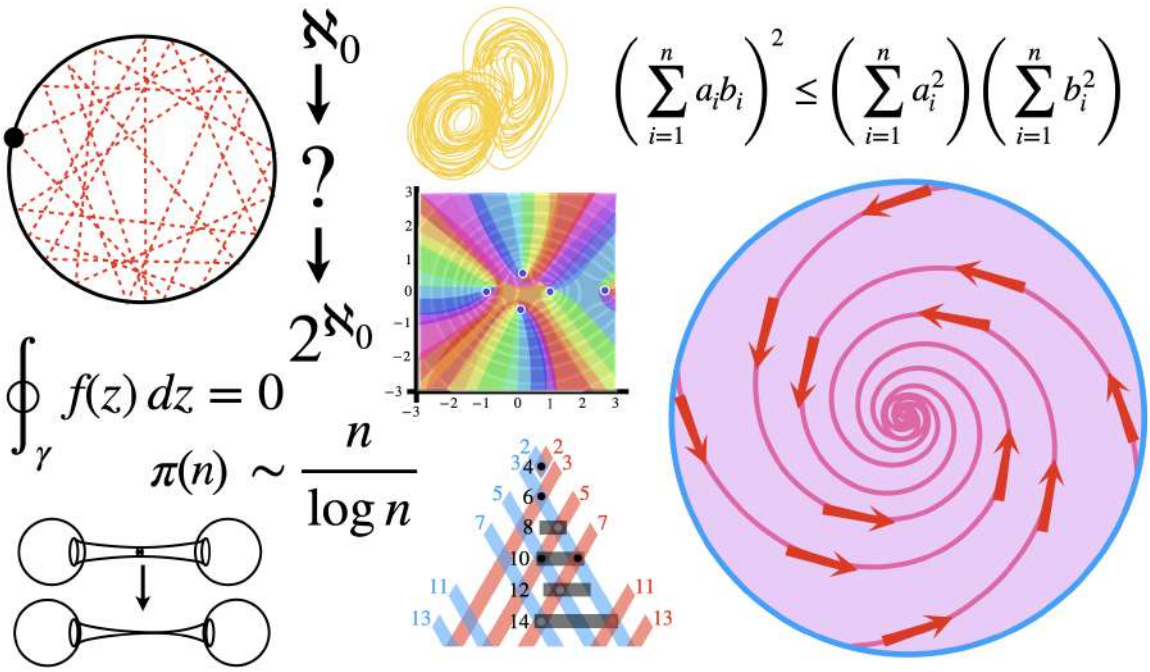
The Most Important Results & Open Problems In Math

by DiBeos

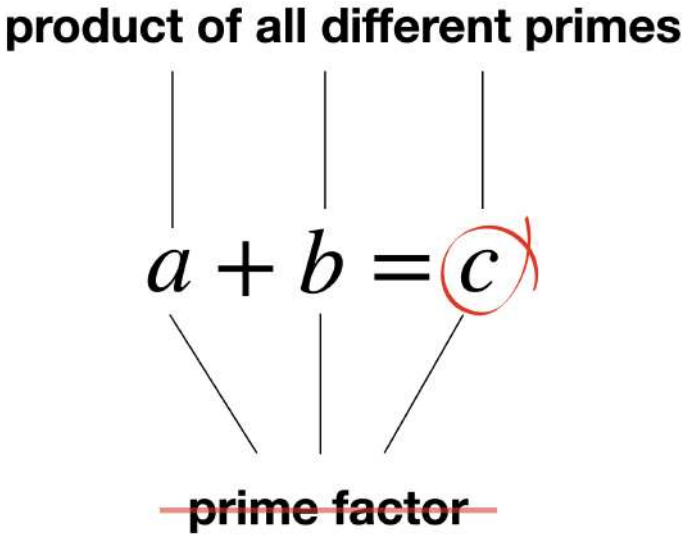


Introduction

Mathematics has thousands of theorems and conjectures, but there are just a few that are essential and foundational. Some of them have been proven, others are still waiting for their solution. The goal here is not to deeply understand all the intricacies of each result, but to acquire a general idea of what mathematicians work on in their daily lives. This approach will help you to learn what interests you the most and how to start your journey on becoming an expert in it. Let's see what they are.

The ABC Conjecture

The *ABC conjecture*, introduced in 1985, roughly speaking says that it is impossible for one number to be the sum of two others if all three numbers have many repeated prime factors, and no two have a prime factor in common.



Ok, said this way it is really confusing. Instead, suppose you add two numbers: $a + b = c$, and none of the three numbers a, b, c, share any *prime factors* (i.e., no prime number divides more than one of them). Then the ABC Conjecture says: usually, the number c isn't much bigger than the product of all the different primes found in a, b and c. This product is called the *radical* of abc:

$$\text{rad}(abc) = \text{the product of all distinct prime factors of } a, b \text{ and } c$$

A radical just multiplies each distinct prime together, ignoring exponents, like this for example:

$$3960 = 2^3 \cdot 3^2 \cdot 5 \cdot 11 \quad \Rightarrow \quad \text{rad}(3960) = 2 \cdot 3 \cdot 5 \cdot 11 = 330$$

The conjecture says that:

$$c < K_\varepsilon \cdot \text{rad}(abc)^{1+\varepsilon}$$

for any tiny positive number $\varepsilon > 0$, and some constant K_ε depending on epsilon.

Let's see a concrete example:

Let $a = 4,\ b = 27,\ c = 31$, then the hypothesis of the ABC Conjecture is verified, since:

$$a + b = c$$

and

$$a = 2^2,\ b = 3^3,\ c = 31$$

$$\implies \operatorname{rad}(abc) = 2 \cdot 3 \cdot 31 = 186 > 31 = c$$

This helps explain why equations like: $x^r + y^r = z^r$ usually don't have many solutions with all numbers coprime.

The conjecture is still officially unproven, despite claims from the mathematician Shinichi Mochizuki to have proved the ABC conjecture using a new and extremely complex theory called *Inter-universal Teichmüller Theory* (IUT). But it still hasn't been confirmed or well understood.

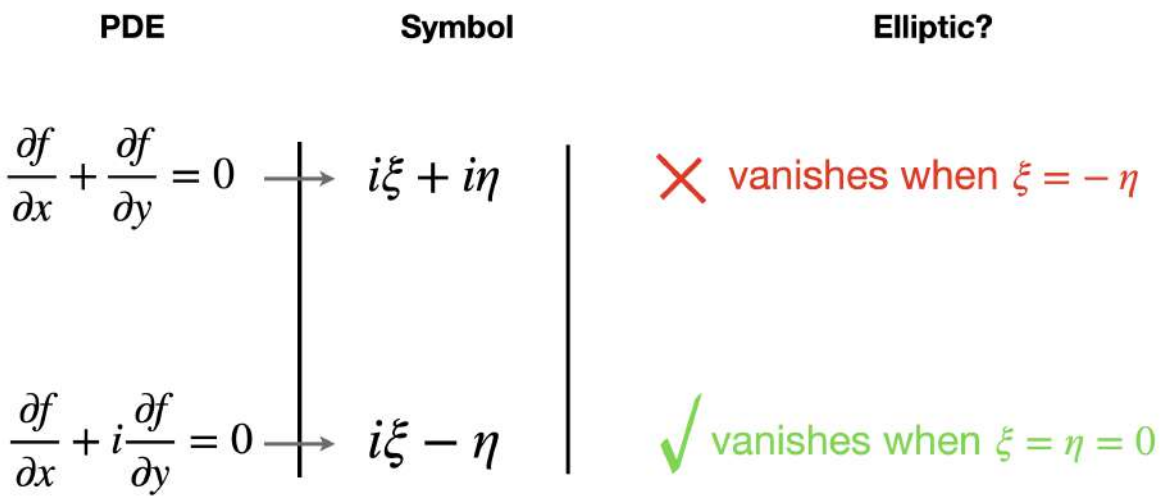
The Atiyah–Singer index theorem

This theorem is concerned with the existence and uniqueness of solutions to linear partial differential equations of the elliptic type.

Take a look at these two very similar equations:

$$\frac{\partial f}{\partial x} + \frac{\partial f}{\partial y} = 0 \quad \text{and} \quad \frac{\partial f}{\partial x} + i\frac{\partial f}{\partial y} = 0$$

Even though they differ by just a factor of $i = \sqrt{-1}$, they behave very differently. Any function of the form $f(x, y) = g(x - y)$ is a solution to the first equation, but the second only admits *constant bounded solutions*, as shown by *Liouville's theorem*.



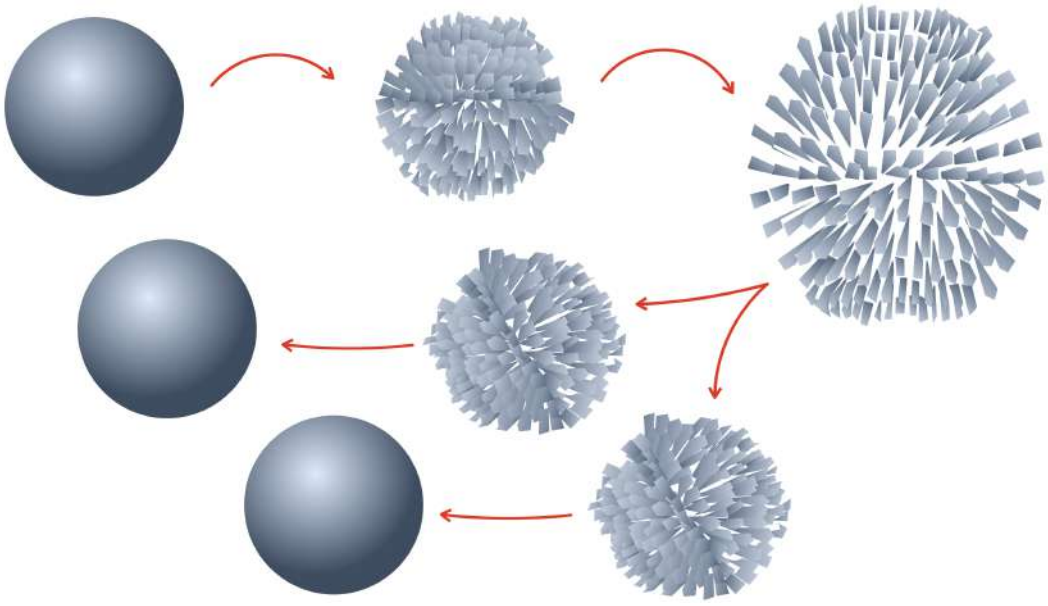
This distinction comes from the symbols of the equations, which are polynomials formed by replacing derivatives with variables $i\xi$, and $i\eta$. The symbols of the two equations become $i\xi + i\eta$ and $i\xi - \eta$.

A PDE is called *elliptic* if its symbol vanishes only when all variables do. So, in other words, $\xi = \eta = 0$. The second equation meets this condition and is elliptic. The first doesn't.

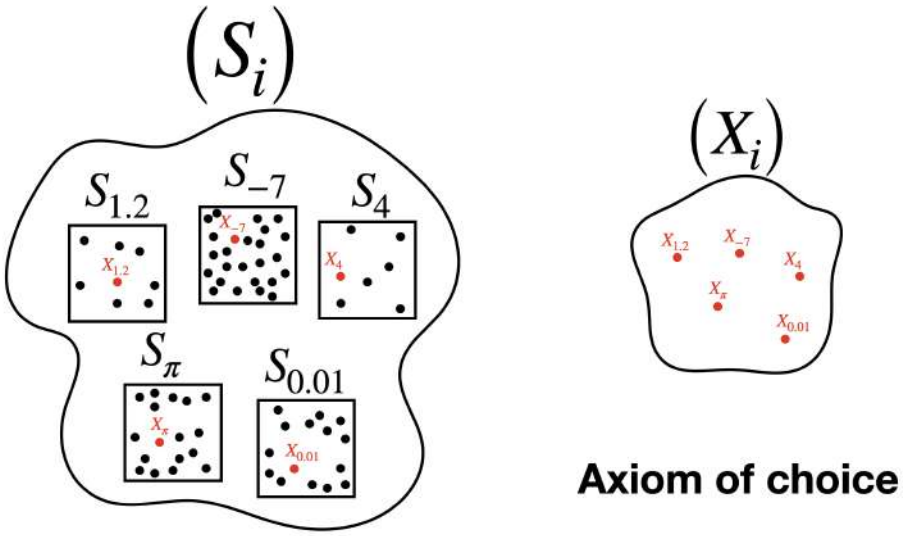
This theorem was proven in the 1960s by Michael Atiyah and Isadore Singer.

Banach–Tarski Paradox

The Banach–Tarski Paradox states that a solid ball in 3-dimensional space can be split into a finite number of non-overlapping pieces, which can then be reassembled using only *rotations* and *translations* into two identical copies of the original ball. There's of course a lot of math to it, but that's the essence of the paradox.



This paradox is mathematically proven, but it relies on the *Axiom of Choice*. The pieces involved are highly non-constructive: they are so fragmented that they can't be explicitly described or realized physically.



Birch–Swinnerton-Dyer Conjecture

The Conjecture deals with understanding the set of rational solutions to certain types of equations called *elliptic curves* $y^2 = x^3 + ax + b$.

The question is: how many rational solutions (fractions or whole numbers) do they have?

The conjecture states that this number is deeply connected to the L-function of the elliptic curve, which roughly speaking looks like this:

$$L(E,s) = \prod_{p \nmid N} \left(1 - a_p p^{-s} + p^{1-2s}\right)^{-1}$$

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

how many **rational solutions** (fractions or whole numbers) do they have?

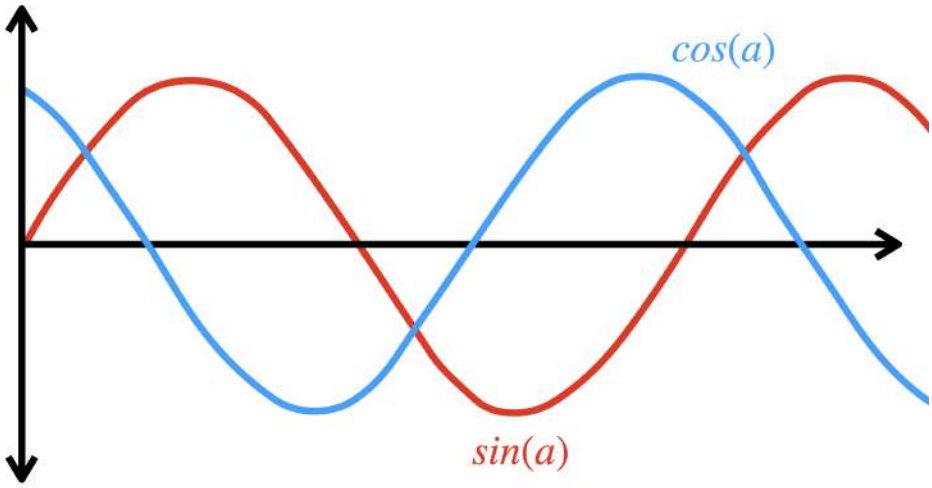
$$L(E,s) = \prod_{p \nmid N} \left(1 - a_p p^{-s} + p^{1-2s}\right)^{-1}$$

Take the equation $y^2 = x^3 - x$. This curve has infinitely many rational solutions, like $(0,0)$, $(1,0)$, $(2, \pm\sqrt{6})$, and more. According to the conjecture, this is because its L-function $L(E,s)$ vanishes at a key point $s = 1$.

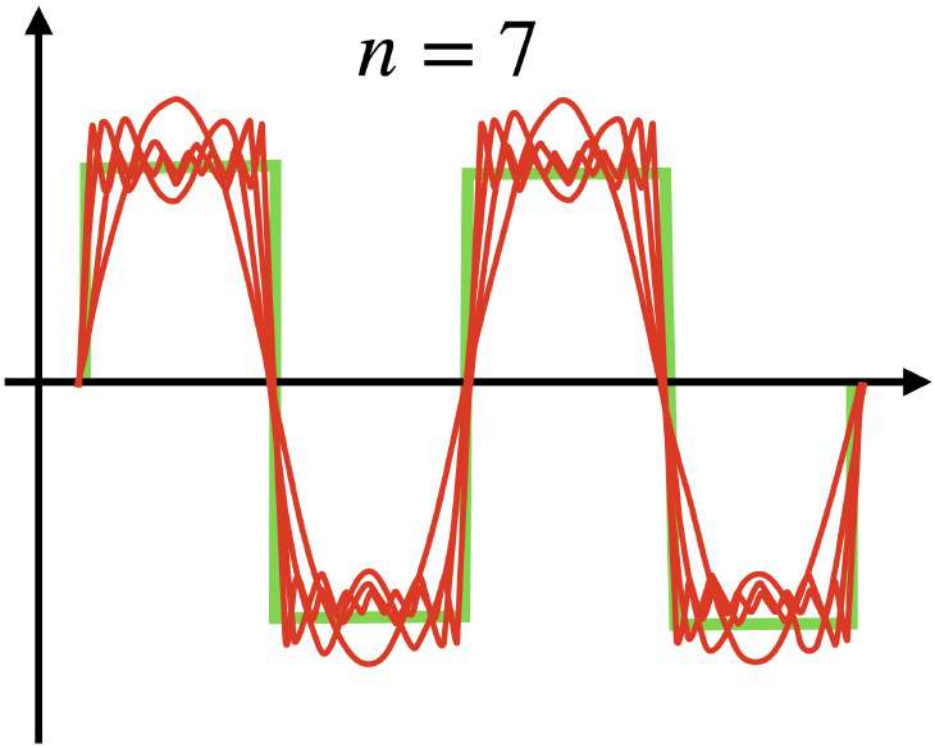
$$L(E,1) = 0$$

In other words, the L-function "vanishing" at $s = 1$ is the conjectural reason why this curve has so many rational solutions. Despite the fact that it's supported by a lot of evidence, it still remains unproven, and is one of the seven *Millennium Prize Problems*, with one million dollars offered for a correct proof.

Carleson's Theorem



Carleson's Theorem answers a fundamental question about *Fourier series*, which are used to represent functions as sums of *sine* and *cosine* waves.



The question is: If you take a function that's *square-integrable* (i.e. in L^2), will its Fourier series converge to the function itself *almost everywhere*?

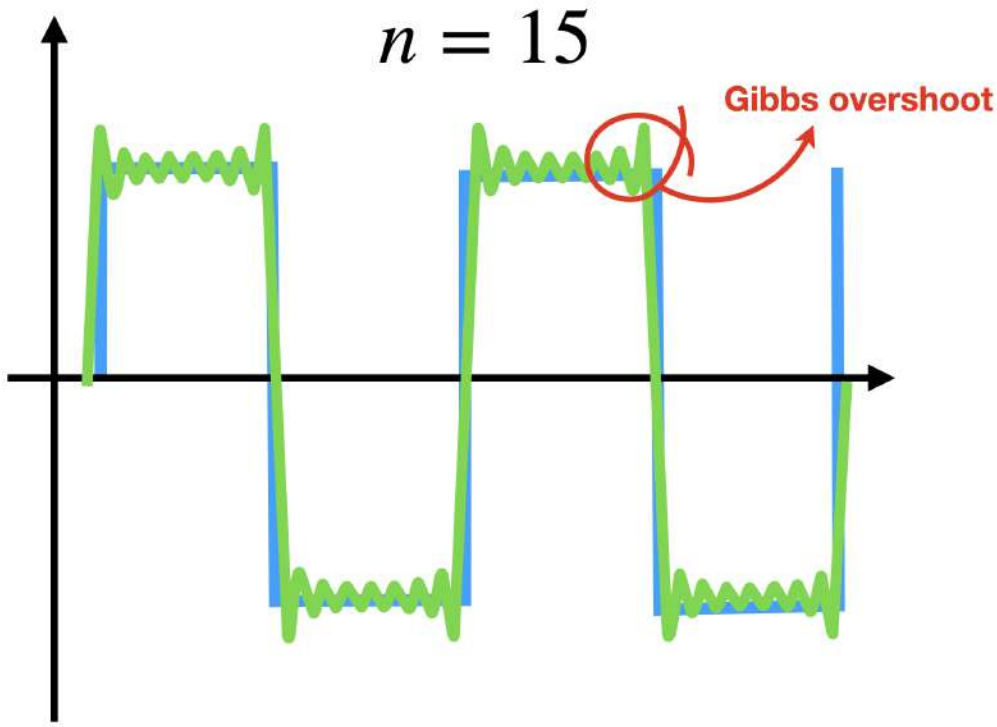
'Almost everywhere' means the Fourier series might not match the function at some points, but those exceptions are so rare that they don't matter for most practical purposes–they make up a set of *measure zero* (like having "zero length" on $\mathbb{R}$).

This was an open problem for nearly a century, but was proved in 1966 and says that: yes, the Fourier series of any L^2-function does indeed converge to the function almost everywhere.

$$\lim_{N\to\infty} S_N f(x) = f(x) \quad \text{for almost every } x \in [0, 2\pi]$$

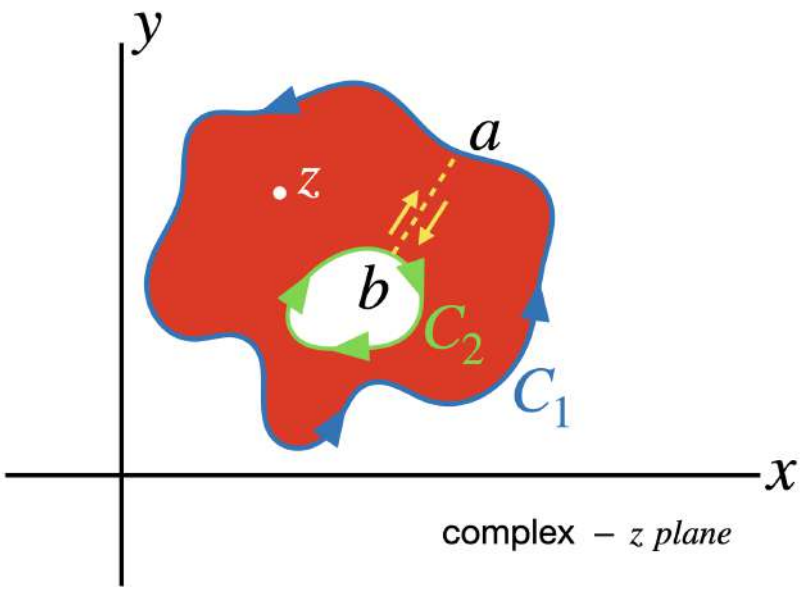
What ends up happening is that despite Gibbs overshoots (i.e. the little

spikes that you see in the image below) and other complications, the approximation still converges pointwise almost everywhere.



Cauchy's Theorem

$$\oint_\gamma f(z)\,dz = 0$$



The theorem, in Complex Analysis, states that if a function is *complex-differentiable* (i.e., *holomorphic*) inside and along a closed curve, then the integral of that function around the curve is zero.

$$\oint_\gamma f(z)\,dz = 0$$

This might sound abstract, but here's the core idea behind this formula:

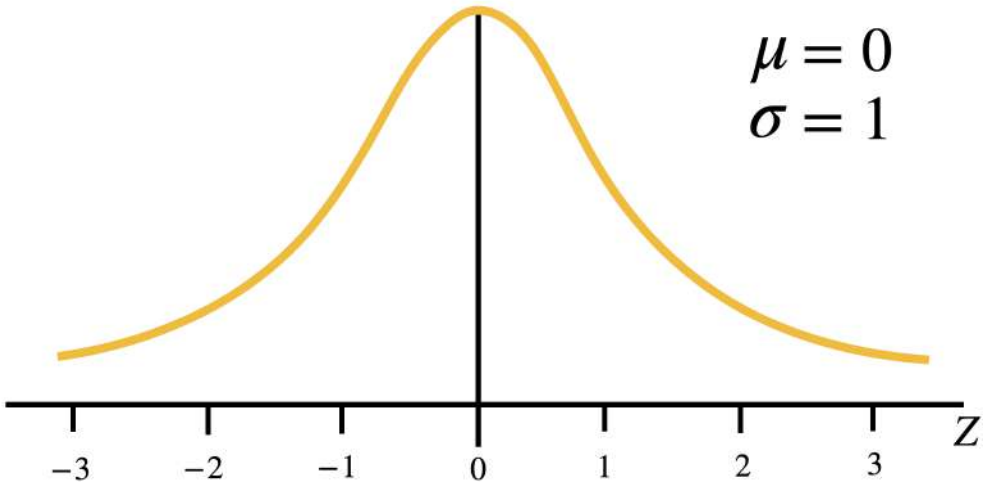
Imagine you're walking along a loop in the complex plane, which can be viewed as a sort of $2D$ space where numbers have both a real and an imaginary part. If the function you're evaluating is "well-behaved" (so, smooth and differentiable) all along your path and in everything enclosed by that path, then adding up its values as you go around the loop brings you right back to where you started, and thus the total net change is *zero*.

Central Limit Theorem (CLT)

The Theorem states that if you take a sequence of independent and identically distributed random variables $X_1, X_2, \ldots, X_n$ with finite *mean* μ and finite *variance* σ^2, then the *normalized sum*

$$Z_n = \frac{1}{\sqrt{n}} \sum_{i=1}^{n} \left(\frac{X_i - \mu}{\sigma} \right)$$

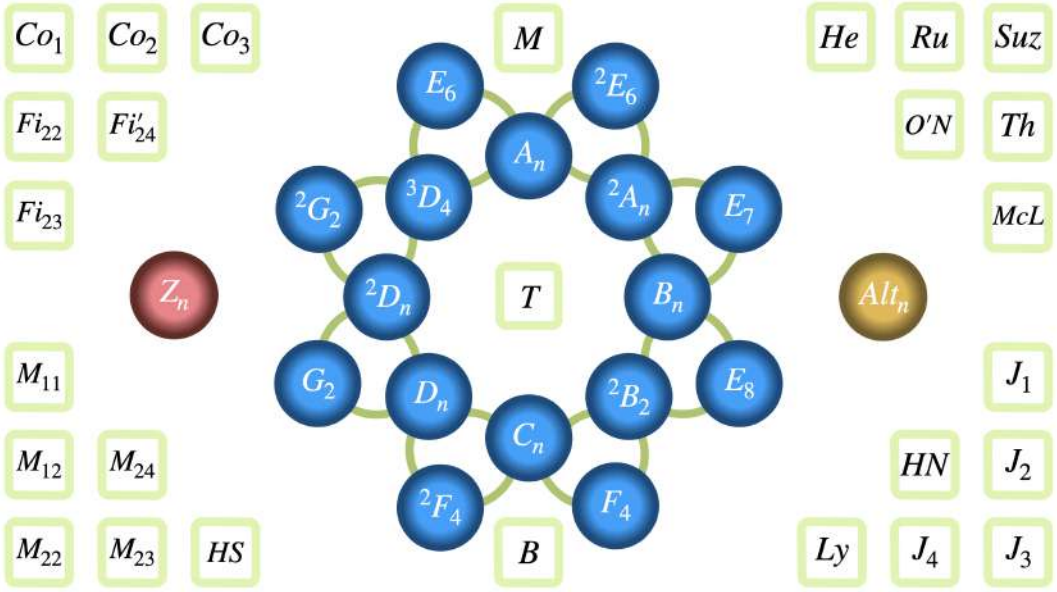
converges in distribution to the *standard normal distribution* as $n \to \infty$. In other words, even if the original data doesn't follow a bell curve, the sum or average of many such values will start to look like a bell curve when the sample size is large enough.



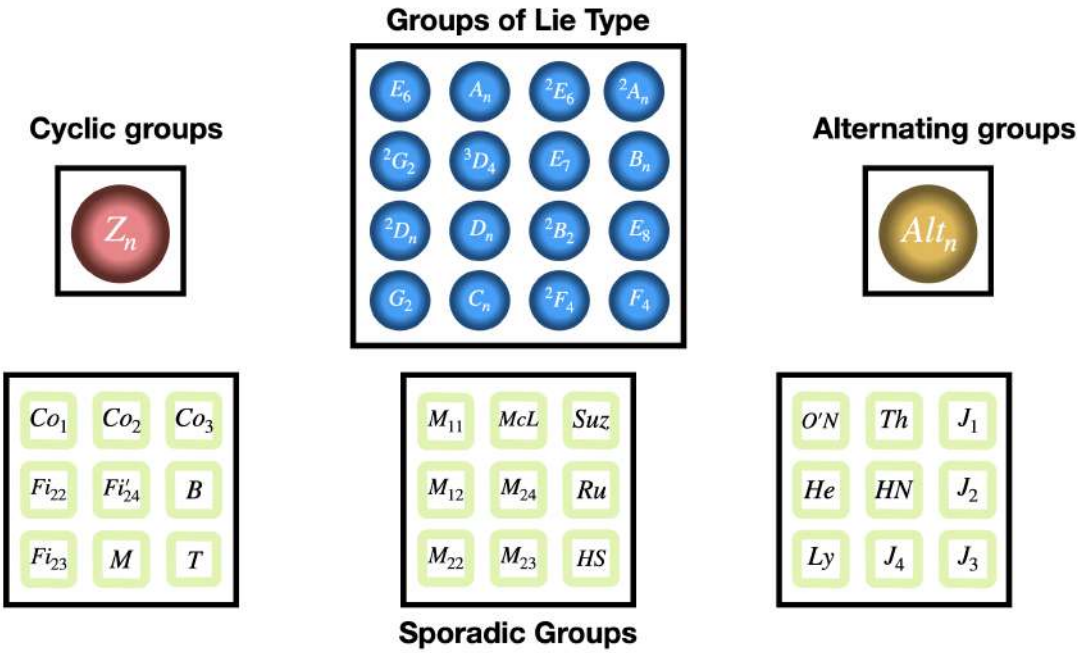
The Classification of Finite Simple Groups

The *Classification Theorem* refers to the result in Group Theory that classifies all finite simple groups, which are considered to be the "building blocks" of all finite groups, analogous to what prime numbers are for

integers.



The theorem states that every finite simple group belongs to one of four categories: *cyclic groups of prime order*, *alternating groups*, *groups of Lie type*, and 26 exceptional groups known as the *sporadic groups*.



The proof is huge,it was completed over decades, involved hundreds of mathematicians and overall required tens of thousands of pages of work.

The Enormous Theorem

The classification of the finite, simple groups is unprecedented in the history of mathematics, for its proof is 15,000 pages long. The exotic solution has stimulated interest far beyond the field

by Daniel Gorenstein

How could a single mathematical theorem require 15,000 pages to prove? Who could read such a proof? Who could pass judgment on its validity? Yet there it is: the proof that all finite, simple groups have been found has run to between 10,000 and 15,000 pages. Of course, no one person is responsible for the achievement, nor is the size of the proof attributable to lengthy computer calculations (although computers are used at one place in the analysis). The work is instead the combined effort of more

forms a group; indeed, the rules for combining the members of a group are simply borrowed, in more general form, from some of the rules of ordinary arithmetic. Given the striking applicability of arithmetic in daily life, it is hardly surprising that the same concepts in a more abstract setting have become powerful tools for the understanding of the universe.

The fundamental building blocks for all groups are the simple groups. Such groups bind together like the atoms in a molecule to generate ever

is called closure. Furthermore, to be a group the operation $*$ must satisfy three rules. First, the set must include a so-called identity element, designated e, such that for any element a in the set the products $a * e$ and $e * a$ are equal to a. Second, for each element a in the set there must be some element in the set called the inverse of a and designated a^{-1}, such that the products $a * a^{-1}$ and $a^{-1} * a$ are equal to e. Finally, the operation $*$ must be associative. In other words, for every three members a, b and c in the set the sequence in which

Dirichlet's Theorem

Dirichlet's Theorem on Arithmetic Progressions states that if a and d are positive integers with no common factors $\gcd(a, d) = 1$, then the arithmetic sequence $a\,,\ a + d\,,\ a + 2d\,,\ \ldots$ contains infinitely many prime numbers. It was proved by Dirichlet in the 19th century.

$$\gcd(a, d) = 1$$

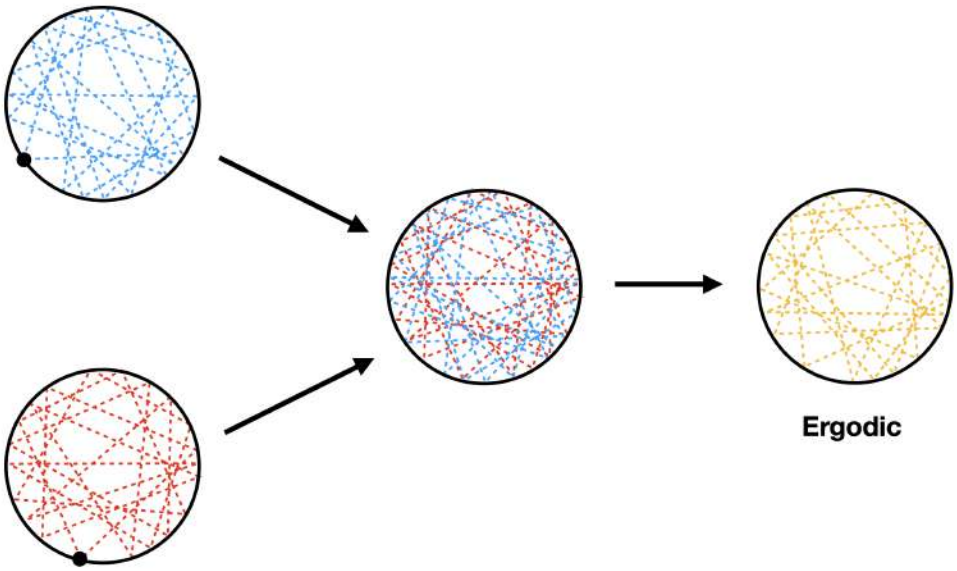
$$\downarrow$$

$$\underbrace{a, a + d, a + 2d, \ldots}_{\text{infinitely many prime numbers}}$$

Ergodic Theorems

The Theorems, developed in the early 20th century, concern themselves with the long-term behavior of Dynamical Systems.

The basic idea is that if you watch a system evolve over time (like gas particles moving in a box), and then compare that to averaging over all possible positions of the system at a fixed moment, the two averages are equal under certain conditions.



This is formalized in *Birkhoff's Ergodic Theorem*, which states that for an ergodic system, the time average of a function along a trajectory equals the space average almost everywhere.

Let $(X, \mathcal{B}, \mu)$ be a probability space, $T : X \to X$ be a measure-preserving transformation, $f \in L^1(\mu)$ be an integrable function, then:

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=0}^{N-1} f(T^n x)$$

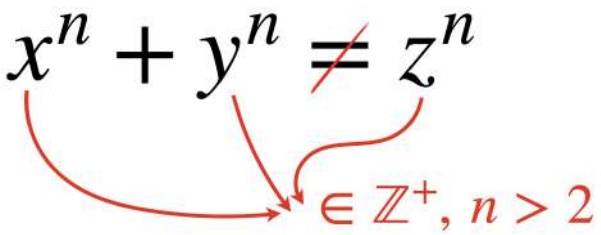
Time average exists for almost every $x \in X$, and is equal to the space average:

$$\int_X f \, d\mu$$

if T is ergodic.

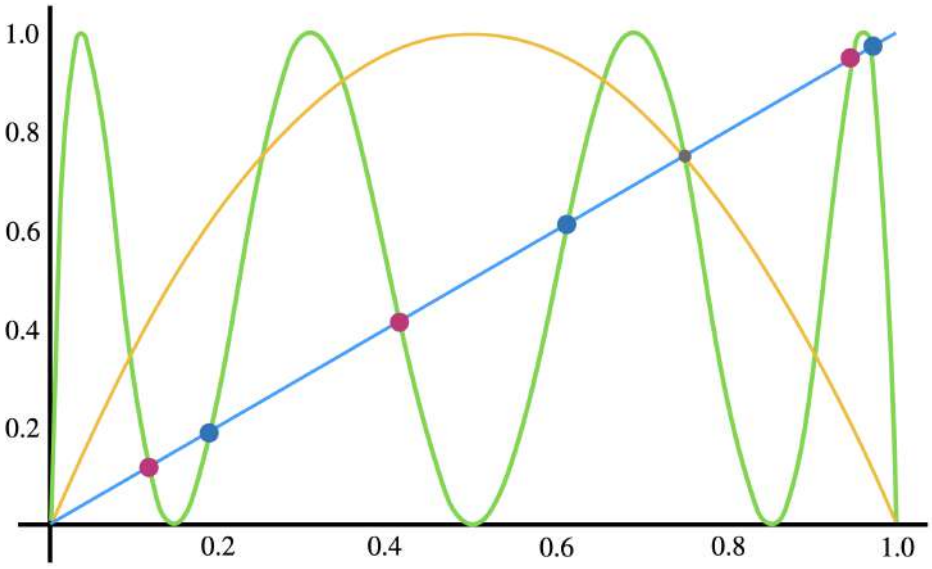
Fermat's Last Theorem

Fermat's Last Theorem states that there are no positive integer solutions to the equation $x^n + y^n = z^n$, for integers $n > 2$.



Even though Fermat claimed he had proved it, his proof was never found anywhere in his writings, and it remained unsolved for 350 years until it was finally proven in 1994 by Andrew Wiles, using concepts that were definitely beyond Fermat's time.

Fixed Point Theorems

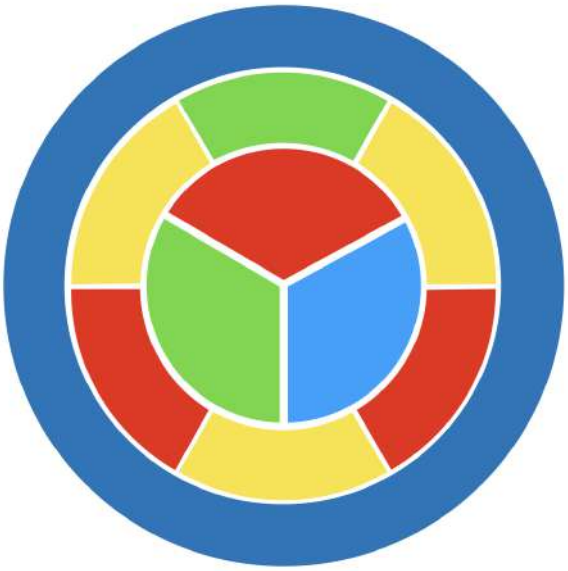


The *Fixed Point Theorems* assert that under certain conditions, a function will always have at least one fixed point, which is a value that is mapped to itself.

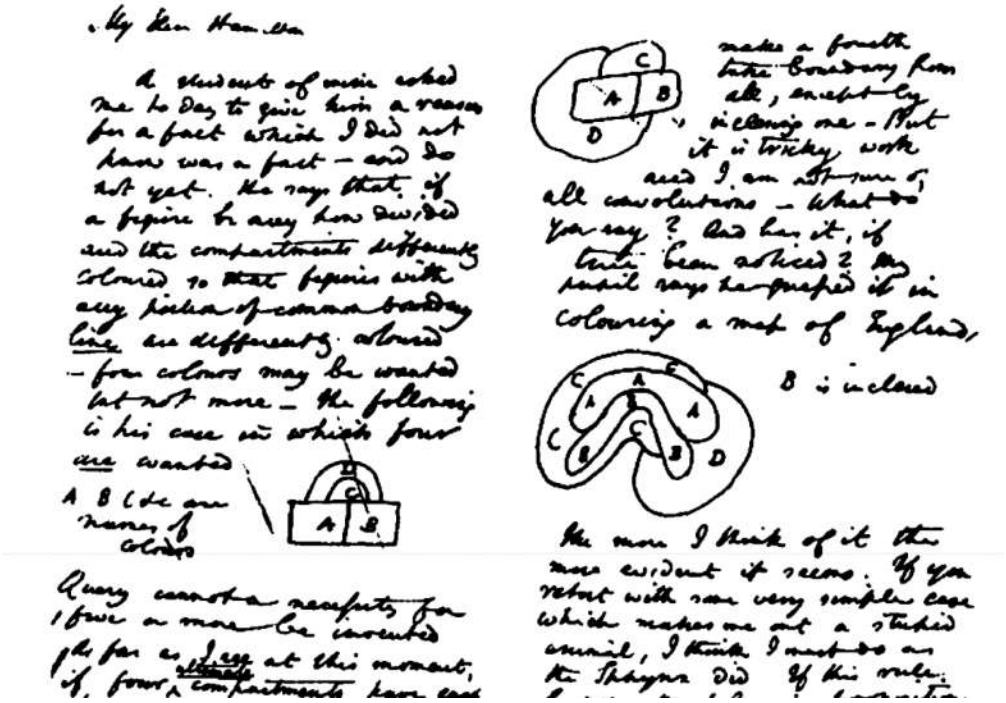
The most famous version is *Brouwer's Fixed Point Theorem*, which states that any continuous function from a closed disk (or ball) to itself must have a *fixed point*. That means, for example, if you stir a cup of coffee, there is always at least one point in the liquid that ends up in exactly the same place that it started at.

The Four Color Theorem

The Theorem states that any map drawn on a plane or on a sphere can be colored using at most four colors so that no two adjacent regions share the same color.

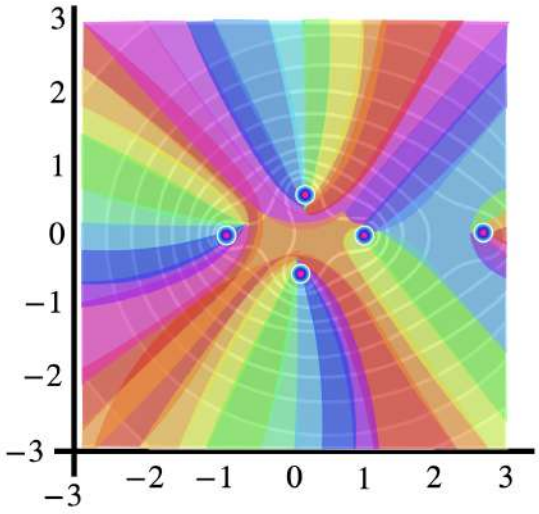


It was originally conjectured in the 19th century, but oddly enough it resisted proof for over a century. The breakthrough came only in 1976, when Kenneth Appel and Wolfgang Haken proved it using a method that was assisted by a computer, since over a thousand special cases had to be checked. It was actually one of the first major theorems to rely on computation to verify it.



Fundamental Theorem of Algebra

$$f(z) = a_5z^5 + a_4z^4 + a_3z^3 + a_2z^2 + a_1z + a_0$$



The Theorem states that a degree-n polynomial equation always has exactly n complex roots.

$$\boxed{p(z) = a_nz^n + a_{n-1}z^{n-1} + \cdots + a_1z + a_0} \quad a_n \neq 0\,, \quad a_i \in \mathbb{C}$$

There exist $\ldots, z_n \in \mathbb{C}$ such that $p(z) = a_n(z - z_1)(z - z_2)\cdots(z - z_n)$.

Let's take a simple polynomial:

$$p(z) = z^2 + 1$$

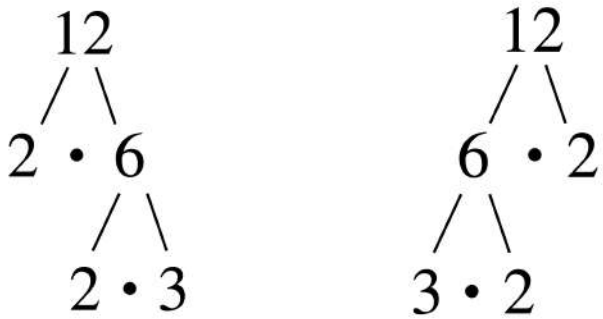
Over the real numbers, it has no real roots, but over the complex numbers:

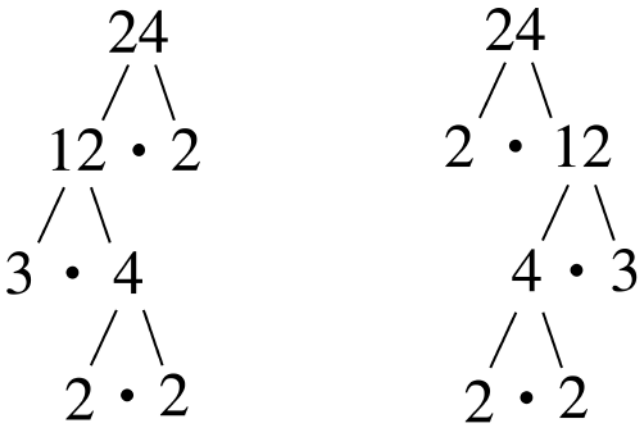
$$z^2 + 1 = 0 \Rightarrow z = \pm i$$

Both roots are in $\mathbb{C}$, demonstrating that we don't need to go beyond the complex numbers to solve this equation.

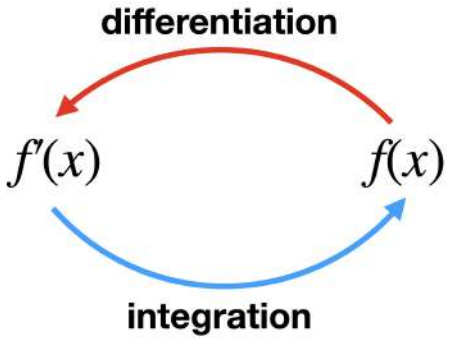
The Fundamental Theorem of Arithmetic

The Theorem states that every positive integer, with the exception of 1, can be represented in exactly one way, the only thing which can be different is the order in which the primes are written.





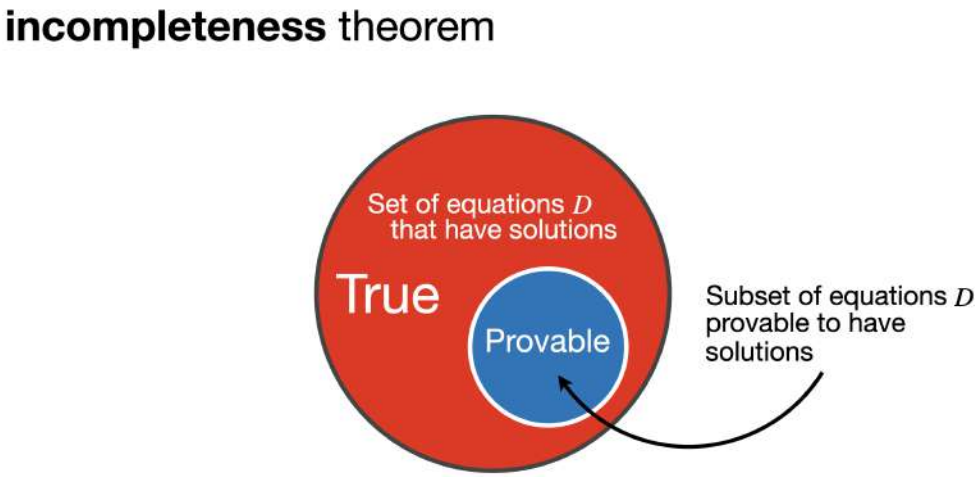
The Fundamental Theorem of Calculus



Roughly speaking, it states that *integration* and *differentiation* are inverse processes. More precisely:

$$\text{if } F(x) = \int_a^x f(t)\,dt, \text{ then } F'(x) = f(x)\,; \text{ and } \int_a^b f(x)\,dx = F(b) - F(a)$$

Gödel's Theorem



Gödel's First Incompleteness Theorem states that in any consistent formal system powerful enough to express basic arithmetic, there are true mathematical statements that cannot be proven within the system.

The Goldbach Conjecture

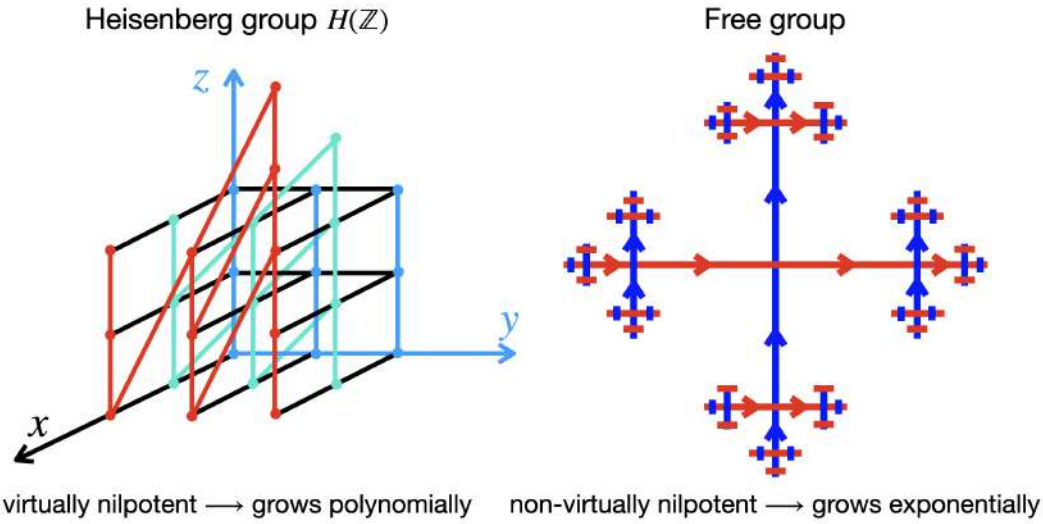
The *Goldbach Conjecture* is one of the oldest unsolved problems in number theory. It says that every even number greater than 2 can be written as the sum of two prime numbers.

$$4 = 2 + 2\ ,\quad 6 = 3 + 3\ ,\quad 8 = 3 + 5\ ,\quad 10 = 5 + 5\ ,\ \text{etc.}$$

Although no one has found a counterexample, and it's been verified by computers for even numbers up to huge sizes, no general proof exists.

Gromov's Polynomial-Growth Theorem

It says that if a group has *polynomial growth* (meaning the number of distinct elements you can reach using up to n generators grows like a polynomial in n) then the group is virtually nilpotent.



A *group* is a mathematical structure where you can combine elements according to certain rules – like symmetries or moves in a puzzle. A *generator* is an element that helps build others by repeated combinations. For example, in the integers $\mathbb{Z}$, the number 1 is a generator because you can reach any integer by adding or subtracting 1 enough times.

If we count how many elements of the group we can reach using at most n steps from the generators, we get a *growth function*. If this number grows like a polynomial, say:

$$\#(\text{elements reachable in } \leq n \text{ steps}) \leq Cn^d$$

for constants C and d, then the group has polynomial growth.

A group is called *virtually nilpotent* if it has a nilpotent subgroup of finite index. In simple terms, it contains a "nice" subgroup (nilpotent)

that makes up most of the group, except for possibly a finite number of extra pieces.

A *nilpotent* group is one in which the elements eventually "settle down" under repeated commutators. Meaning that its structure becomes more and more commutative (i.e., the order of operations matters less and less). This makes nilpotent groups well-behaved and algebraically simple.

So, *Gromov's theorem* says: if a group grows slowly (like a polynomial), it must have this kind of underlying simple structure.

Many groups (like free groups) grow exponentially.

Hilbert's Nullstellensatz

In German it stands for "zero-locus theorem", and says that if a set of polynomials has no common solution in an algebraically closed field like $\mathbb{C}$, then 1 belongs to the ideal they generate.

Suppose you have a bunch of polynomials $f_1(x,y), f_2(x,y), \ldots, f_k(x,y)$. If there exist other polynomials $g_1, g_2, \ldots, g_k$ such that:

$$g_1 f_1 + g_2 f_2 + \cdots + g_k f_k = 1$$

then we say that the ideal generated by the f_i contains 1. Or simply: they "generate 1".

The common zero set of the f_i is the set of all points (x,y) that make all the polynomials vanish:

$$f_1(x,y) = f_2(x,y) = \cdots = f_k(x,y) = 0.$$

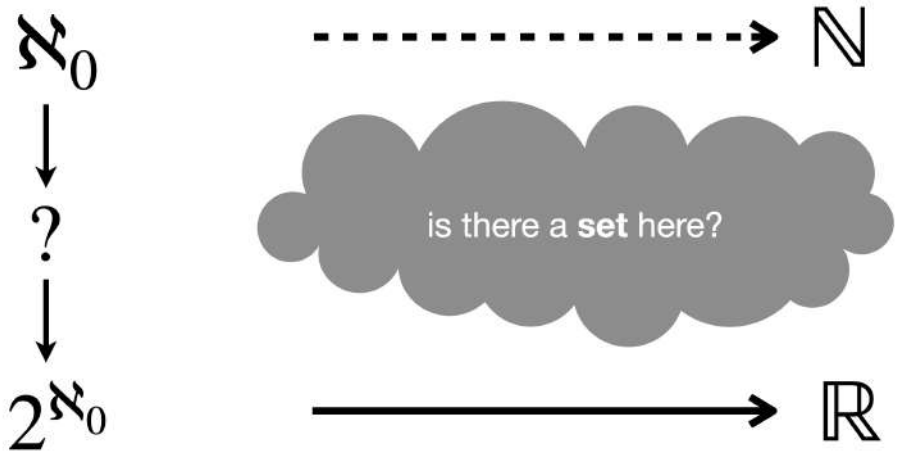
If there is no such point, then the polynomials have no common solution.

Nullstellensatz says that the two facts are equivalent: the polynomials have no common zero, and that you can combine them (with other polynomials) to get 1. This is interesting because if the polynomials vanish together to nowhere, then we can say they're so incompatible that we can literally "force" 1 from them algebraically. And if they vanish to somewhere, then there's no way to algebraically combine them to produce 1.

The Independence of the Continuum Hypothesis

The *Continuum Hypothesis* asks whether there is a set whose size is strictly between that of the natural numbers $\mathbb{N}$ and the real numbers $\mathbb{R}$.

In terms of *cardinality*: is there a set with cardinality strictly between $\aleph_0$ (the size of the natural numbers $\mathbb{N}$) and $2^{\aleph_0}$ (the size of real numbers $\mathbb{R}$)?



The *Independence of the Continuum Hypothesis* means that the standard *axioms of Zermelo-Fraenkel* set theory with the *axiom of choice* (ZFC) can neither prove nor disprove it. Its truth depends on which model of set theory you work in.

Inequalities

Some of the most interesting and frequently used inequalities in mathematics include *Cauchy-Schwarz*, *Hölder's*, *Jensen's*, and *Chebyshev's inequalities*. These allow one to estimate or bound quantities when exact answers are too hard, or even impossible, to compute.

Hölder's

$$\sum_{i=1}^{n} |a_i b_i| \leq \left(\sum_{i=1}^{n} |a_i|^p \right)^{1/p} \left(\sum_{i=1}^{n} |b_i|^q \right)^{1/q}$$

Cauchy-Schwarz

$$\left(\sum_{i=1}^{n} a_i b_i \right)^2 \leq \left(\sum_{i=1}^{n} a_i^2 \right) \left(\sum_{i=1}^{n} b_i^2 \right)$$

Jensen's

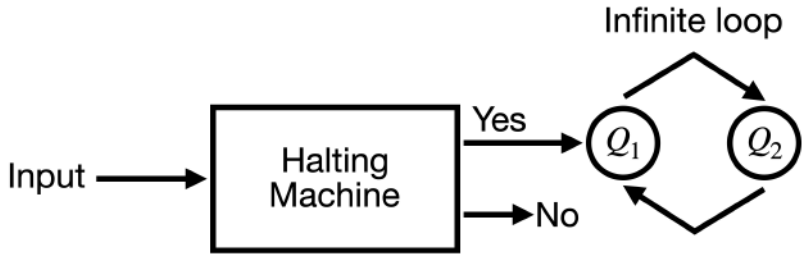
$$\phi \left(\sum_{i=1}^{n} \lambda_i x_i \right) \leq \sum_{i=1}^{n} \lambda_i \phi(x_i)$$

Chebyshev's Inequalities

$$\mathbb{P}(|X - \mu| \geq k\sigma) \leq \frac{1}{k^2}$$

The Insolubility of the Halting Problem

The *Halting Problem* asks whether there exists a general algorithm that can determine, for any computer program and any input, whether that program will eventually stop running or if it will continue to run forever.



Alan Turing proved in 1936 that no such algorithm exists, that the problem is undecidable. That is, that no finite and consistent method can answer this question correctly in all cases.

The Insolubility of the Quintic

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

$$\downarrow$$

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

Quadratic, cubic, and quartic polynomial equations all have formulas that give their solutions, but there is no such general formula by radicals for all quintic equations.

$$ax^3 + bx^2 + cx + d$$

$$\downarrow$$

$$\frac{\sqrt[3]{-27a^2d + 9abc - 2b^3 + 3a\sqrt{3(27a^2d^2 - 18abcd + 4ac^3 + 4b^3d - b^2c^2)}} + \sqrt[3]{-27a^2d + 9abc - ab^3 - 3a\sqrt{3(27a^2d^2 - 18abcd + 4ac^3 + 4b^3d - b^2c^2)}}}{3\sqrt[3]{2a}}$$

In the 19th century, mathematicians like Ruffini, Abel, and Galois proved that the general quintic is not solvable by radicals, using new ideas from what would become Galois theory.

$$ax^4 + bx^3 + cx^2 + dx + f = 0$$

$$\downarrow$$

$$r_1 = \frac{-a}{4} - \frac{1}{2}\sqrt{\frac{a^2}{4} - \frac{2b}{3} + \frac{2^{\frac{1}{3}}(b^2 - 3ac + 12d)}{3\left(2b^3 - 9abc + 27c^2 + 27a^2d - 72bd + \sqrt{-4(b^2 - 3ac + 12d)^3 + (2b^3 - 9abc + 27c^2}\right.}}$$

$$r_2 = \frac{-a}{4} - \frac{1}{2}\sqrt{\frac{a^2}{4} - \frac{2b}{3} + \frac{2^{\frac{1}{3}}(b^2 - 3ac + 12d)}{3\left(2b^3 - 9abc + 27c^2 + 27a^2d - 72bd + \sqrt{-4(b^2 - 3ac + 12d)^3 + (2b^3 - 9abc + 27c^2}\right.}}$$

$$r_3 = \frac{-a}{4} + \frac{1}{2}\sqrt{\frac{a^2}{4} - \frac{2b}{3} + \frac{2^{\frac{1}{3}}(b^2 - 3ac + 12d)}{3\left(2b^3 - 9abc + 27c^2 + 27a^2d - 72bd + \sqrt{-4(b^2 - 3ac + 12d)^3 + (2b^3 - 9abc + 27c^2}\right.}}$$

Liouville's Theorem and Roth's Theorem

Liouville's Theorem was the first result to show that certain real numbers cannot be well-approximated by rationals. Specifically, if α is an algebraic number of degree $d \geq 2$, then there exists a constant $c > 0$ such that:

$$\left| \alpha - \frac{p}{q} \right| > \frac{c}{q^d}$$

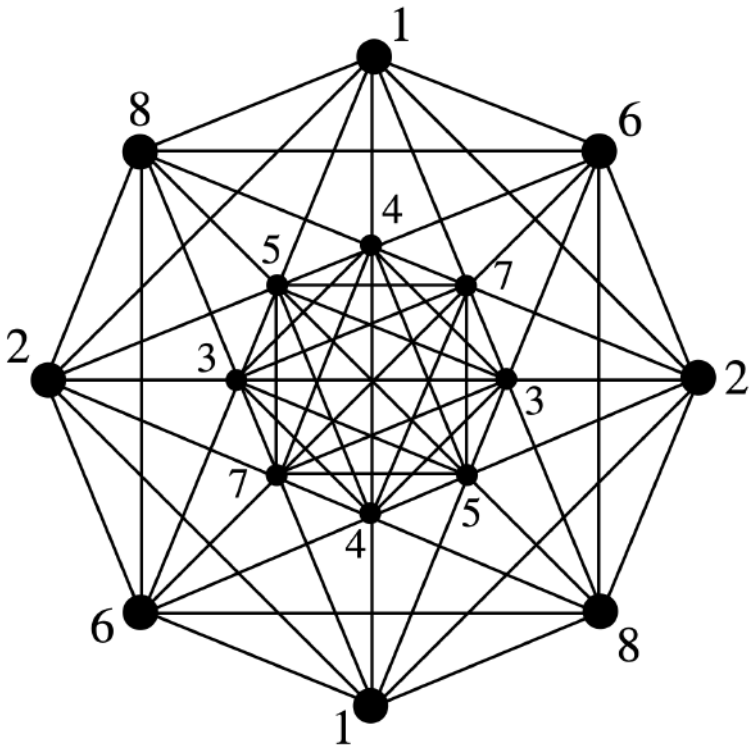
for all rational $\frac{p}{q}$. It gave the first examples of transcendental numbers. But Roth improved this result, by proving that for any irrational algebraic number α, and for any $\varepsilon > 0$, there are only finitely many rational numbers $\frac{p}{q}$ such that:

$$\left| \alpha - \frac{p}{q} \right| < \frac{1}{q^{2+\varepsilon}}$$

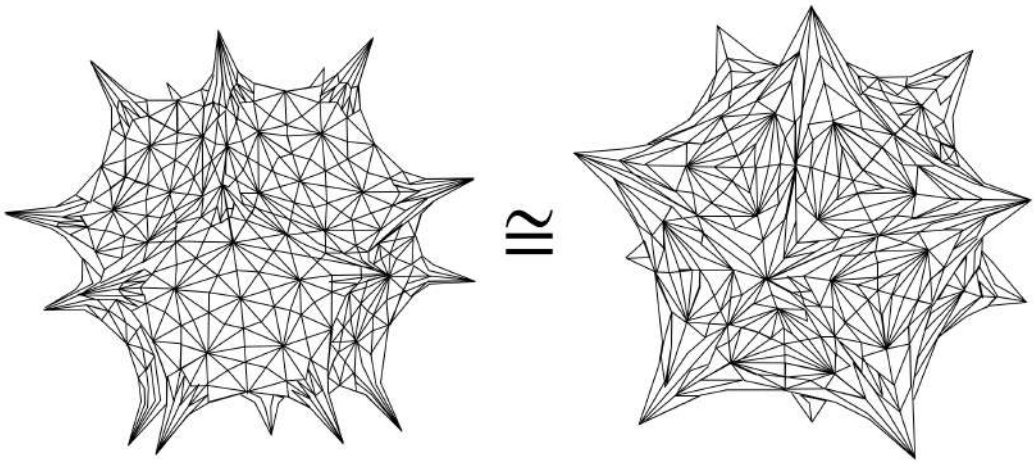
This means algebraic numbers cannot be approximated "too well" by rationals, and it's essentially the best possible result he could've found. Roth's theorem is fully proven, and it earned him the *Fields Medal*.

Mostow's Strong Rigidity Theorem

Mostow's Strong Rigidity Theorem says that in dimensions that are greater than 2, the geometry of a space is determined by its *fundamental group*, at least when it comes to certain negatively curved spaces (like hyperbolic manifolds).

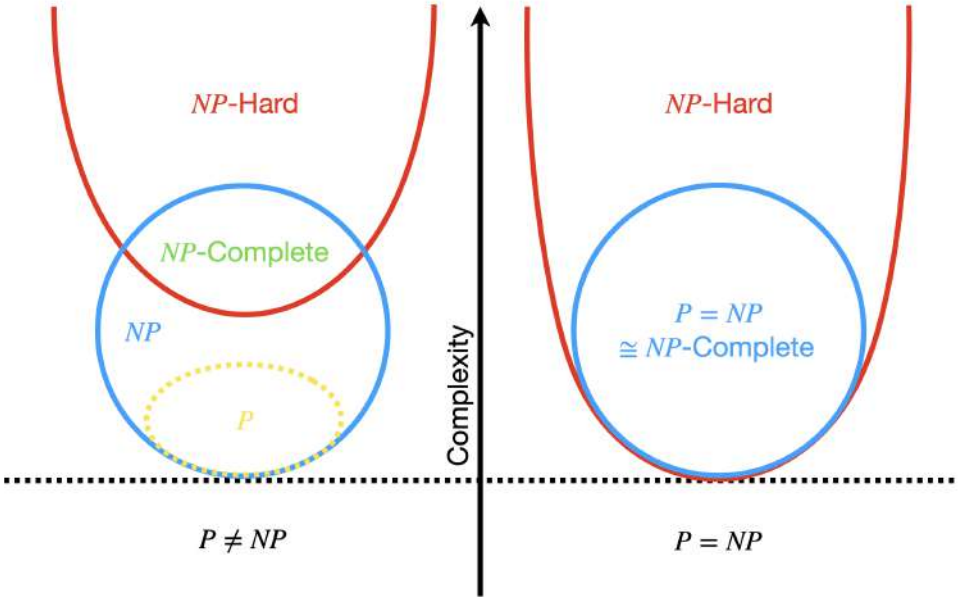


More precisely speaking, if two compact hyperbolic manifolds of dimension $n \geq 3$ have *isomorphic* fundamental groups, then they are isometric. This means there's a distance-preserving map between them.



This is surprising because in two dimensions, like with *Riemann surfaces*, there are many different geometric structures (or moduli) with the same topology.

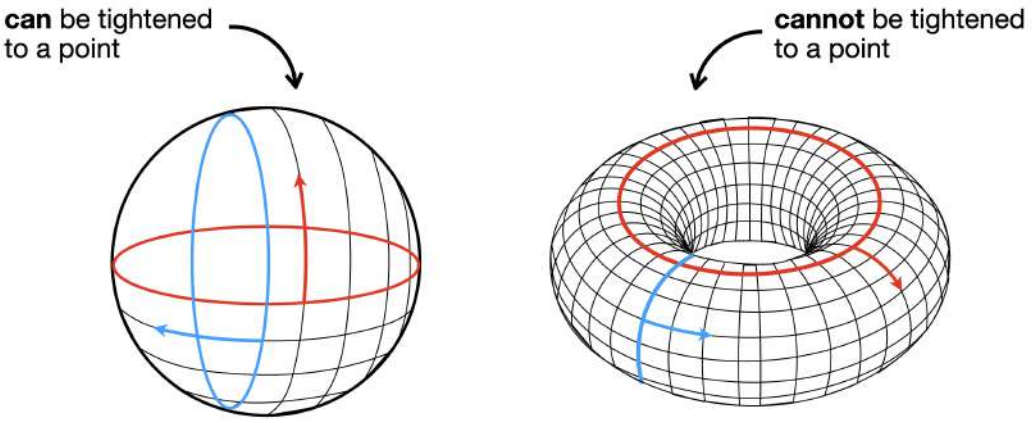
The P versus NP Problem



The *P vs NP problem* asks whether every problem whose solution can be verified quickly, in polynomial time, can also be solved quickly, also in polynomial time. The central question is: does $P = NP$? That is, is verifying a solution no easier than finding one? This is a major open question in theoretical computer science and mathematics that hasn't been solved yet.

The Poincaré Conjecture

Roughly speaking, if a $3D$ space has no holes and every loop in the space can be continuously shrunk to a point, then the space must be essentially the 3-sphere.



Formally speaking, that any closed 3-dimensional manifold that is simply connected is *homeomorphic* to the 3-sphere $\mathbb{S}^3$.

It was proposed by Henri Poincaré in 1904 and remained one of the most famous unsolved problems in mathematics until Grigori Perelman solved it using Richard Hamilton's *Ricci flow technique*. He famously declined the Fields Medal and the Clay Millennium Prize.

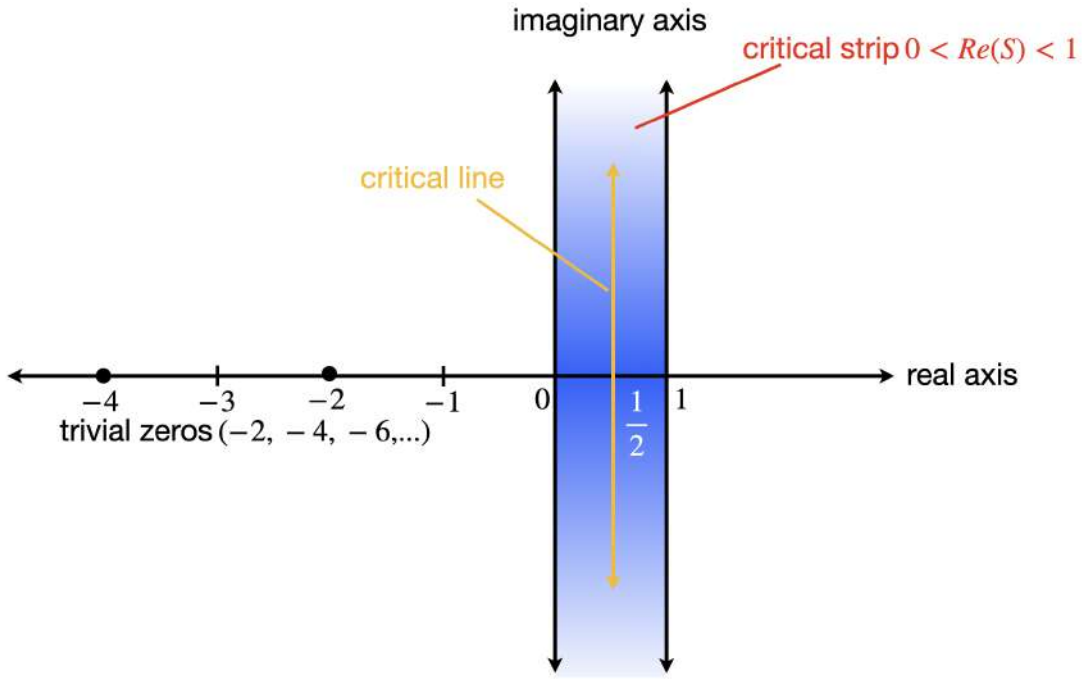
The Prime Number Theorem and the Riemann Hypothesis

How many prime numbers are there between 1 and n? A natural first reaction to this question is to define $\pi(n)$ to be the number of prime numbers between 1 and n and to search for a formula for $\pi(n)$. But, we know that primes do not have any obvious pattern to them and we don't even know if such a formula exists (unless we count really artificial formulas that do not actually help one to calculate $\pi(n)$).

The standard reaction of mathematicians to this kind of situation is to look instead for good estimates. The *Prime Number Theorem* tells us just that: as n grows large, the number of primes less than n, written as $\pi(n)$, is approximately:

$$\pi(n) \sim \frac{n}{\log n}$$

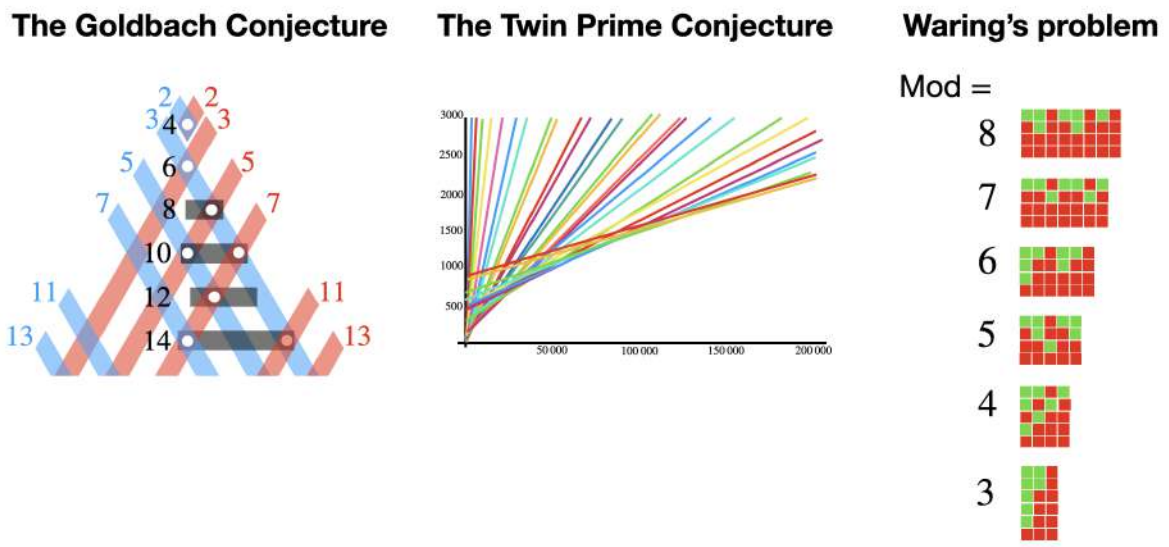
That is, primes become less frequent as numbers get larger, but they do so in a way that's closely ruled by logarithmic decay. This naturally leads to a deeper question: how precise is this estimate? This is where the *Riemann Hypothesis* comes in. It proposes that all the nontrivial zeros of the zeta function lie exactly on this vertical line $\mathrm{Re}(s) = \frac{1}{2}$ in the complex plane.



If it will ever be proven to be true, it will place bounds on the error in the approximations given by the *Prime Number Theorem*, but it remains one of the most important open problems in mathematics.

Problems and Results in Additive Number Theory

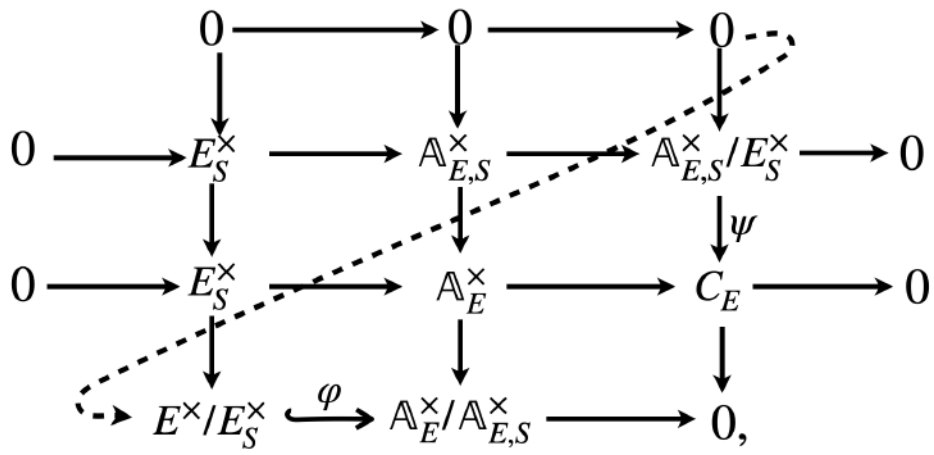
Is every even number greater than 4 the sum of two odd primes? Are there infinitely many primes p such that $p + 2$ is also a prime? Is every sufficiently large positive integer the sum of four cubes?



These three questions are all famous unsolved problems in Number Theory: the first is called the *Goldbach Conjecture*, the second is the *Twin Prime Conjecture* and the third is a special case of *Waring's problem*.

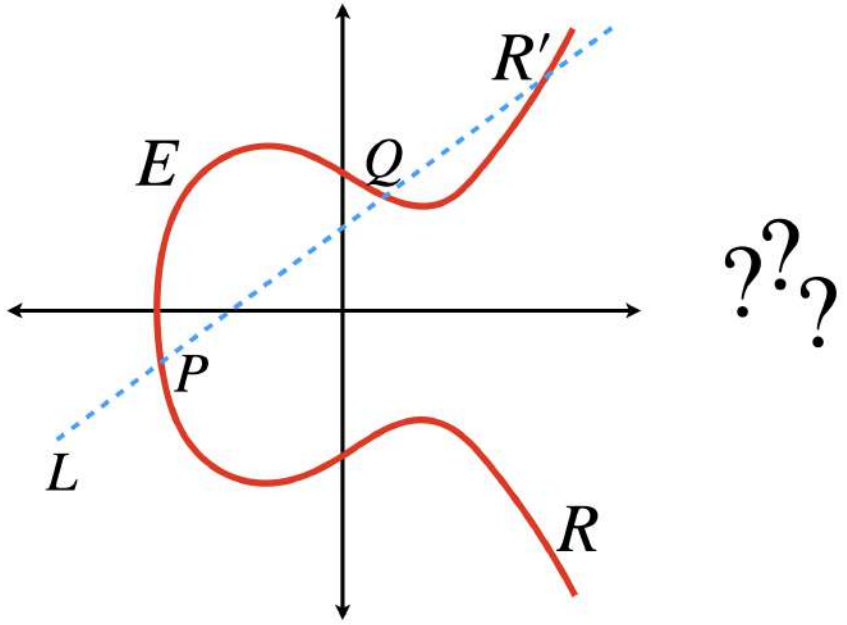
From Quadratic Reciprocity to Class Field Theory

The *law of quadratic reciprocity*, discovered by Gauss, tells us when a quadratic equation $x^2 \equiv p \mod q$ has a solution, in terms of a symmetric relationship between p and q. Mathematicians then started to explore higher-degree congruences ($x^n \equiv a \mod p$) and they found that similar laws could be formulated, but they became more complex and abstract.

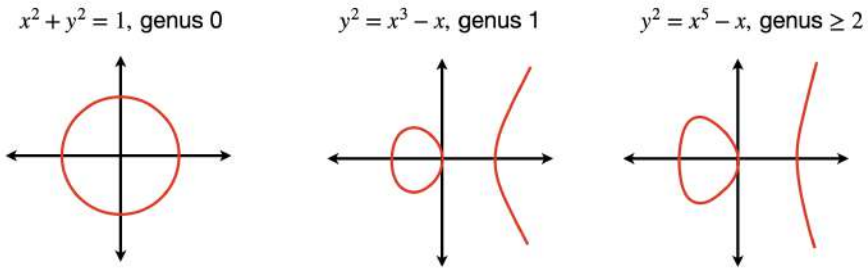


This led to the development of *Class Field Theory*, which studies Abelian (i.e., commutative) extensions of number fields. Class field theory generalizes reciprocity laws, showing them not in terms of individual numbers, but in terms of ideal classes and Galois groups of field extensions.

Rational Points on Curves and the Mordell Conjecture



When we study solutions to polynomial equations in two variables, we can often think of them as defining curves. A central question is: how many rational points (or solutions where both x and y are rational numbers) lie on such curves?

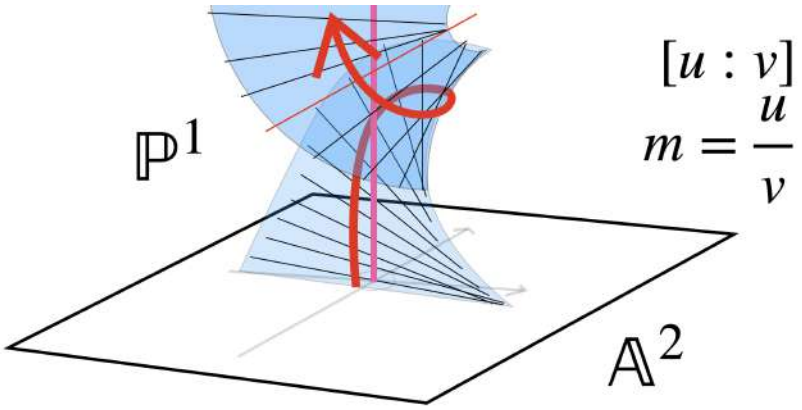


The answer depends strongly on the genus of the curve (or a measure of its complexity, like the number of "holes"). For genus 0, curves either have no rational points or infinitely many. For genus 1 (like elliptic curves), the rational points form a finitely generated abelian group. But for genus ≥ 2, something interesting happens: there are

only finitely many rational points on such curves. This result is formerly known as the *Mordell Conjecture*.

The Resolution of Singularities

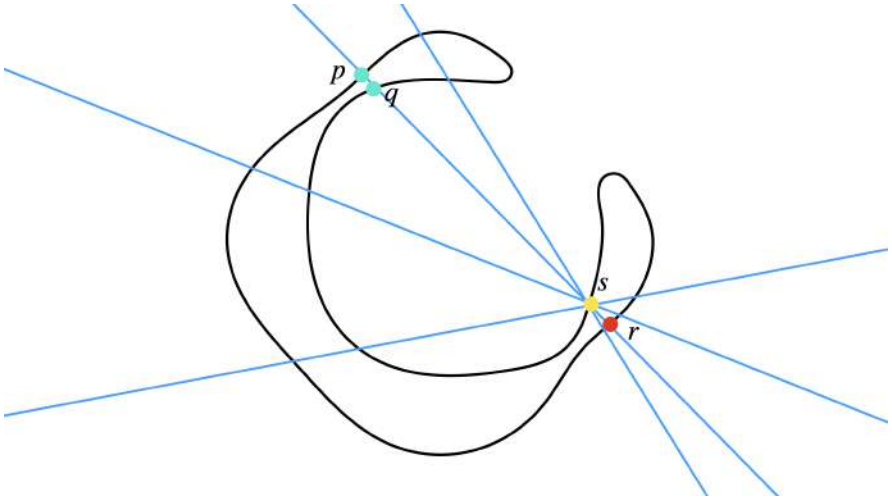
In *Algebraic Geometry*, a singularity is a point on an *algebraic variety* where the object is not "smooth", like where it might have a cusp or a self-intersection. The resolution of singularities is the process of transforming them into something smooth by applying a series of well-defined geometric operations.



The main theorem for varieties over fields of characteristic zero (like the real or complex numbers), says that:

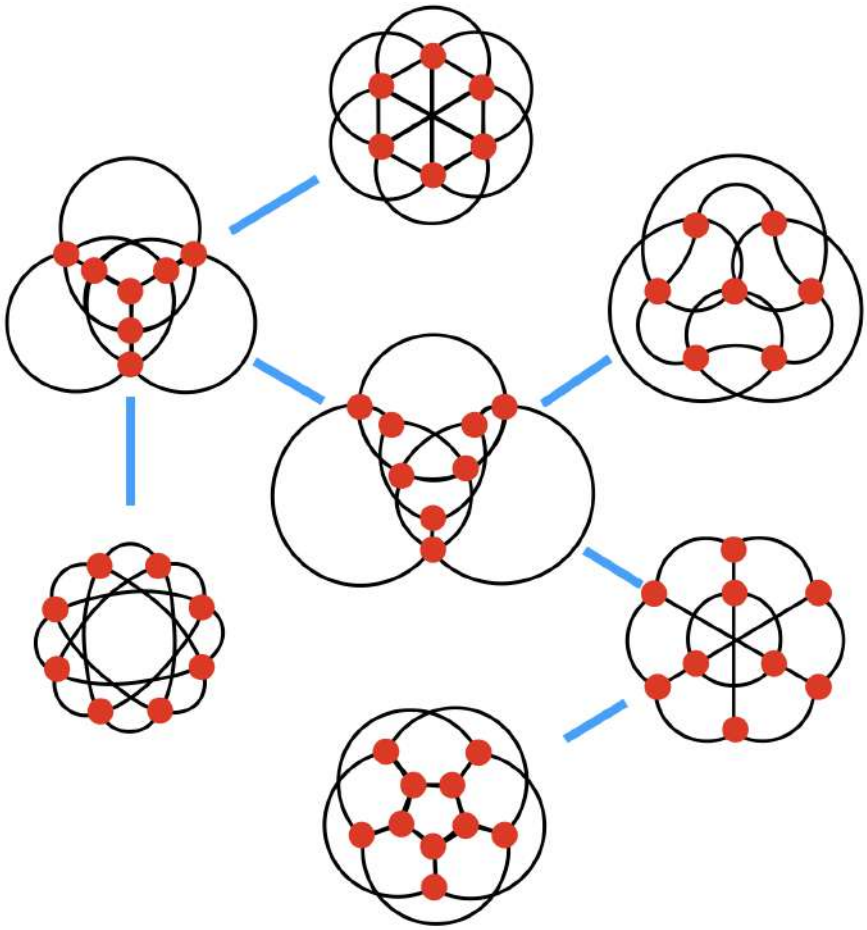
"Every algebraic variety over a field of characteristic 0 admits a resolution of singularities."

The Riemann–Roch Theorem



The Theorem tells you how many *meromorphic functions* (also known as *sections*) with prescribed zeros and poles exist on a curve, using only the genus of the curve and the total number of zeros and poles (also known as the degree of the divisor).

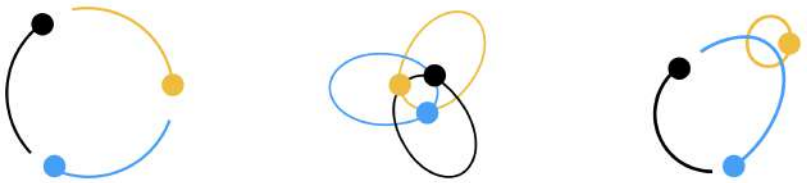
The Robertson–Seymour Theorem



The Theorem states that the set of all finite graphs is well-quasi-ordered under the minor relation: basically that in any infinite sequence of graphs, one is a minor of a later one.

The Three-Body Problem

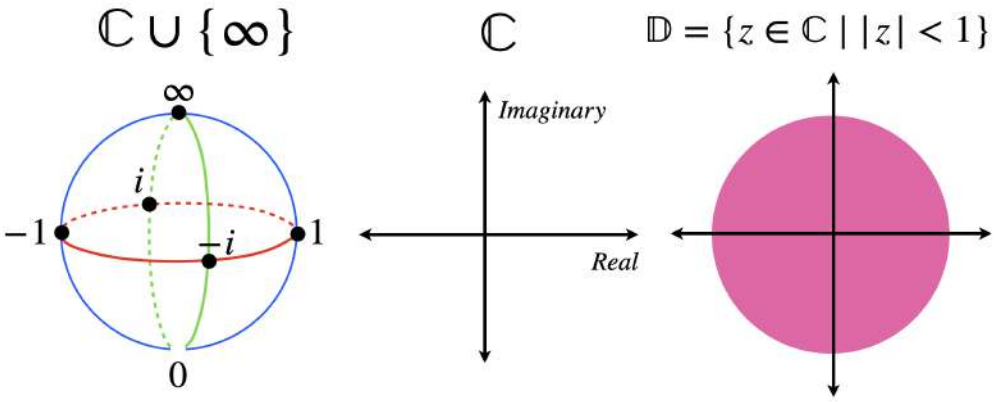
The *Three-Body Problem* asks: given the initial positions and velocities of three celestial bodies, how will they move under their mutual gravitational attraction?



The problem is simple to say but incredibly complex to solve. Generally speaking, Newton's laws give exact equations for how bodies influence each other through gravity. For two bodies, we get elliptical orbits. But once a third body is introduced, the situation becomes a lot messier. Their paths can swing around, exchange energy, and become impossible to predict long-term using only formulas.

Henri Poincaré proved in the 1890s that there's no general solution in terms of simple formulas. This was one of the first signs of what would later be known as chaos theory. The motion of the three bodies can be extremely sensitive to initial conditions.
Thurston's Geometrization Conjecture proposed that every closed 3-manifold can be decomposed into pieces that each have one of eight geometric structures which are well understood.

The Uniformization Theorem



It says that every simply connected Riemann surface is conformally equivalent to exactly one of these three:
1. The Riemann sphere $\mathbb{C} \cup \{\infty\}$, **2.** The complex plane $\mathbb{C}$, **3.** The unit disk $\mathbb{D} = \{z \in \mathbb{C} \mid |z| < 1\}$.

The Weil Conjectures

It's something really complicated to summarize in a paragraph, but basically speaking the *Weil Conjectures* were a set of predictions made by André Weil in the 1940s about the number of solutions to equations over finite fields.

For a given variety V defined over a finite field $\mathbb{F}_q$, the zeta function $Z(V,t)$ is defined as this:

$$Z(V,t) = \exp\left(\sum_{n=1}^{\infty} \frac{|V(\mathbb{F}_{q^n})|}{n} t^n\right)$$

where $|V(\mathbb{F}_{q^n})|$ denotes the number of solutions over the field extension $\mathbb{F}_{q^n}$.

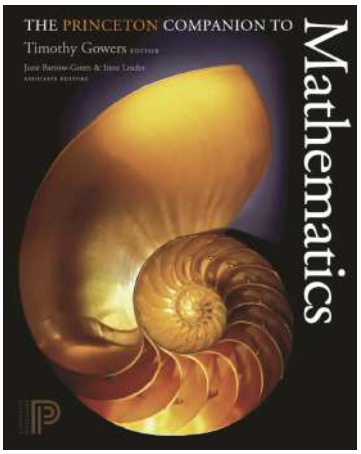
André Weil conjectured that this zeta function satisfies these interesting properties:

1. $Z(V,t)$ is a rational function.
2. It satisfies a symmetry relating t and $1/q^d t$, where d is the dimension of V.
3. The zeta function can be expressed as a product involving polynomials whose degrees relate to the Betti numbers of V.
4. The zeros and poles of $Z(V,t)$ lie on specific "critical lines" in the complex plane—analogous to the classical Riemann Hypothesis.

These conjectures were proven across several decades. The Weil Conjectures were foundational in developing *Modern Étale Cohomology* and *Algebraic Geometry*.

Of course, I am sure there are some foundational theorems for other fields we've missed, so let us know in the comments if you know of any, but this was hopefully a pretty comprehensive list to give you guys an idea of each theorem and conjecture.

This file was based on the book "*The Princeton Companion to Mathematics*"



If you found this document useful let us know. If you found typos and things to improve, let us know as well. Your feedback is very important to us. We're working hard to deliver the best material possible. Contact us at: dibeos.contact@gmail.com