Great Solved Problems

MUIC Seminar

31 January 2018

PROBLEMS

- (0) Axiom of Choice
- (1) Continuum Hypothesis
- (2) Basis Problem, Approximation Problem
- (3) Apèry Theorem
- (4) Four Color Problem
- (5) Bieberbach Conjecture
- (6) Mordell Conjecture
- (7) Invariant Subspace Problem
- (8) Fermat Last Theorem
- (9) Unconditional Basic Sequence
- (10) Maharam Problem
- (11) Poincaré Hypothesis
- (12) Primes in Arithmetic Progression

Problems in Progress

- (13) Goldbach Hypothesis
- (14) Twin Primes Conjecture

Continuum Hypothesis

Problem (Cantor, 1878; Hilbert, 1900)

Every infinite set of real numbers is either countable or has the same cardinality as $\mathbb{R}$.

Fact

- (*AC*) $\Longrightarrow$ *every set (in particular, every infinite set of real numbers) can be put into* $1-1$ *correspondence with a cardinal number.*
- *(CH)* $\Longleftrightarrow$ *card* $\mathbb{R} = \aleph_1 \Longleftrightarrow 2^{\aleph_0} = \aleph_1$.

Fact (Gödel, 1938)

(CH) (and (AC)) is consistent with the (ZF) Axioms.

Theorem (Paul Cohen, 1963; Fields Medal 1966)

(CH) is undecidable in (ZFC).

Cohen constructed by a new technique of **forcing** a model M of (ZFC) (= forcing extension of $M(G)$) that is also a model of (ZFC). In this model (CH) is false, i.e. showing that $(CH)$is **independent** of (ZFC).

Corollary

There exists a model of set theory without (AC) where all sets are measurable $\Rightarrow$ (AC) is necessary for existence of non–measurable sets.

Basis Problem

Definition

Let X be a separable Banach space. A sequence $\{x_n\}_{n=1}^{\infty}$ is called a (Schauder) basis of X if every element $x \in X$ can be uniquely represented as

$$x = \sum_{n=1}^{\infty} a_n x_n \,,$$

with $a_n \in \mathbb{R}$, $n = 1, 2, \ldots$.

Problem (Mazur, Scottish Book 1936)

Does every separable Banach space have a Schauder basis ?

Theorem (Per Enflö 1973)

There exists a separable Banach space without a Schauder basis.

Approximation Problem

Definition

A Banach space X has the ApproximationProperty if, for every Banach space Y the set of finite–rank members of $B(X, Y)$ is dense in $K(X, Y)$ (= compact operators $K : X \to Y$).

Problem (Alexandre Grothendieck, Fields Medal 1966)

Does every separable Banach space have the Approximation Property ?

Theorem (Per Enflö 1973)

There exists a separable Banach space without the Approximation Property.

Four Color Problem

Problem (Four Color Problem, 1852)

Given any separation of a plane into contiguous regions (a map), the regions can be colored using at most four colors so that no two adjacent regions have the same color.

- all corners belonging to three or more countries must be ignored
- every ”country” must be a connected region, or contiguous

Problem (Four Color Problem, Graph Version)

Is every planar graph four colorable ?

History

- asked by a botanist Francis Guthrie
- considered by Augustus de Morgan
- William Rowan Hamilton
- Arthur Cayley, 1878
- Alfred Kempe "proof", 1879
- Percy Heawood found gap in Kempe's proof, 1889
- Heinrich Heesch, 1948 - unavoidable and irreducible configurations
- Wolfgang Haken and Kenneth Appel, 1976 - computer proof

Theorem (Haken–Appel, 1976)

Every planar graph is four colorable.

Apèry Theorem

Theorem (Apèry,1978)

The number

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

is irrational.

Theorem (Euler)

If n is a positive integer then

$$\zeta(2n) = \frac{1}{1^{2n}} + \frac{1}{2^{2n}} + \frac{1}{3^{2n}} + \cdots = \frac{p}{q}\pi^{2n}$$

for some integers p and q.

Euler showed that, in fact,

$$\zeta(2n) = (-1)^{n+1}\frac{B_{2n}(2\pi)^{2n}}{2(2n!)}$$

where the B_{2n} are the rational Bernoulli numbers.

Theorem (Rivoal, 2000)

The sequence

$$\zeta(3), \zeta(5), \zeta(7), \zeta(9), \ldots$$

contains infinitely many irrational numbers.

This theorem has been extended by V.V.Zudilin in 2002. It is believed (but not proved) that all values of $\zeta(n)$ are **irrational**, in fact, **transcendental**.

Bieberbach Conjecture

Problem (Bieberbach Conjecture,1916)

Let $f(z)$ be a univalent function, i.e. one–to–one holomorphic function that maps the open unit disk $\Delta = \{z \in \mathbb{C} : |z| < 1\}$ into the complex plane $\mathbb{C}$ with $f(0) = 0$ and $f'(0) = 1$. Then $f(z)$ has a Taylor series

$$f(z) = z + \sum_{n \geq 2} a_n z^n.$$

Ludwig Bieberbach conjectured in 1916 that for such functions $|a_n| \leq n$ for $n = 2, 3, \ldots$.

Theorem (L. de Branges, 1984)

Bieberbach Conjecture is true.

Mordell Conjecture

Problem (Mordell Conjecture, 1922)

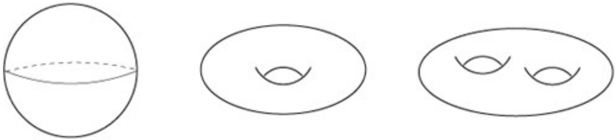
Any Diophantine equation with genus at least 2 has only finitely many (rational) solutions.

Theorem (Gerd Faltings, 1983; Fields Medal, 1986)

Mordell Conjecture is True.

The Mordell Conjecture/Faltings Theorem says roughly that if K is an algebraic number field and X is an algebraic curve defined over K of genus $g > 1$ then the set of K - rational points $X(K)$ is finite.
Mordell objected to it being called "Mordell's conjecture", saying it was more of a question, not even a wild guess, and that he had little or no intuition to base it on.

The genus of a plane algebraic curve of degree *n* is the integer $\frac{(n-1)(n-2)}{2}$ minus the orders of multiplicity of singular points of the curve in the complex projective plane.
It is the genus of this curve considered as a surface (i.e. a manifold of dimension 2) of the complex projective plane, which itself is a manifold of dimension 4 .
A real curve of genus g is therefore the section of a torus with g holes by a plane, and, as a result, has, in general and at most $g+1$ connected components in the real projective plane.



By the Harnack theorem (1878), we can find curves of any degree having $g+1$ real connected components (and the 16th problem of Hilbert consisted in classifying these curves).
The curves of genus zero are the rational curves, that can be parametrized by rational functions, and the curves of genus 1, the elliptic curves, that can be parametrized by elliptic functions; the curves of maximal genus $\frac{(n-1)(n-2)}{2}$ are the smooth curves.

History

- Poincaré conjectured that the group of rational points on an elliptic curve is finitely generated
- proved by Louis Mordell in 1922
- Falting's proof in 1983
- Simplified proof by Enrico Bombieri (1990) and Pavel Vojta (1991)
- Cosequences for the proof of the Fermat Last Theorem

Invariant Subspace Problem

Definition

Let $T : X \to X$ be a bounded linear operator on a Banach space X and let V be a proper subspace of X (*i.e.* $\emptyset \neq V \neq X$). We say that V is invariant under T if $T(V) \subseteq V$.

Problem

When does a bounded linear operator on an infinite dimensional Banach space have a non–trivial closed invariant subspace ?

- P. Enflö (1987) showed an example of a bounded linear operator on a real or complex separable non–reflexive space Banach space without non–trivial invariant subspaces;
- C. J. Read (1984) showed an example of a bounded linear operator on the space ℓ_1 without non–trivial closed invariant subspaces.

Fermat Last Theorem

Theorem (Pierre de Fermat)

It is impossible to divide a cube into two cubes, or a four power into two four powers, or in general, any power higher than the second, into two like powers.

Proof.

I have discovered a truly marvellous proof of this, which this margin is too narrow to contain. □

NOTE : Fermat does have a complete proof of the *FLT* for the case $n = 4$ by *reductio ad absurdum* through the use of Mathematical Induction.

Early Steps in the Solution of the *FLT*

- $n = 3$ Euler 1770
- Gauss 1816 – too isolated problem to be interesting
- $n = 5$ Legendre, Dirichlet 1825
- $n = 7$ Lamé 1834
- Sophie Germain, two cases : $p|xyz$, $p \not| xyz$
- cyclotomic integers, Lamé 1847
- unique factorization, Liouville
- Ideals, Class Number, Dedekind, Kummer

Final Steps in the Solution of the *FLT*

Problem (Taniyama – Shimura Conjecture)

Every elliptic curve is modular.

- Weil–Taniyama–Shimura Conjecture
- Faltings Theorem $\Rightarrow$ there are at most finitely many solutions of the *FLT*
- Frey : $TS \Longrightarrow FLT$
- Serre (Fields Medal, 1954), Ribet
- Laglands Correspondence

FINALLY !!!, AFTER 350 YEARS

Summer of 1993, Andrew Wiles' Cambridge Lecture
"Elliptic Curves, Modular Forms, and Galois Theory"

Corollary

Given $x, y, z \in \mathbb{Z}_+$ *and* $\in \mathbb{N}, n \geq 3$*, the equation*

$$x^n + y^n = z^n$$

has a solution if and only if $xyz = 0$*.*

Final proof April 1995 – Andrew Wiles with Richard Taylor.

Unconditional Basic Sequence

Definition

Let X be a Banach space . A sequence $\{x_n\}_{n=1}^{\infty}$ of elements of X is a basic sequence of X if it is a Schauder basis for its closed linear span. The basis is unconditional if the series $\sum_{\pi(n)} a_n x_n$ converges for any permutation of indices $\pi(n)$.

Fact

Every Banach space has a basic sequence.

Problem

Does every Banach space have an unconditional basic sequence ?

The question of unconditional basic sequence is fundamental in many applications of Banach spaces, e.g. in the probability theory.

Theorem (Timothy Gowers, Bernard Maurey 1993)

There exists a Banach space without any unconditional basic sequence.

This important discovery allowed Gowers to answer many important longstanding problems about structure of Banach spaces. For these important discoveries Timothy Gowers was awarded Fields Medal in 1994.

Sample consequences of the Gowers – Maurey Theorem
:

- there exists an infinite–dimensional Banach space noy isomorphic to any of its proper subspaces
- there exist two nonisomorphic Banach spaces such that each is isomorphic to a subspace of the other
- a Banach space which is isomorphic to all of its infinite–dimensional subspaces is isomorphic to ℓ_2
- there exists a Banach space X such that the only linear operators $L(X, X)$ are the identity and compact operators

Maharam Problem

Definition

Let $\mathfrak{B}$ be a Boolean algebra. A function $\mu : \mathfrak{B} \to [0, 1]$ is called a submeasure on $\mathfrak{B}$ if $\mu(0) = 0$ and $\mu(A \cup B) \leq \mu(A) + \mu(B)$ for $A, B \in \mathfrak{B}$.
A submeasure is called order continuous if $A_n \downarrow 0$ implies that $\mu(A_n) \to 0$.

Problem (Dorothy Maharam 1947)

If a Boolean algebra $\mathfrak{B}$ admits a continuous submeasure, does it admit a measure ?

Theorem (M.Talagrand 1996)

There exists a Boolean submeasure algebra with no non–trivial measure.

Poincaré Conjecture

Problem (Poincaré,1904)

Every compact, simply connected, three–dimensional manifold is (homeomorphic to) the three–dimensional sphere.

Definition

A manifold with the property that any closed loop in it can be continuously contracted to a point is called simply connected.

Fact

Every two-dimensional manifold has a geometric structure that is either spherical, Euclidean, or hyperbolic. Moreover, if it has a structure of one of these types, it cannot have one of a different type.

Problem (Geometrization Conjecture, William Thurston 1982 ; Fields Medal 1983)

Every smooth three-dimensional manifold can be cut in a canonical fashion along a predetermined spheres and one–holed tori so that each of resulting parts has precisely one of the list of eight possible geometric structures.

Theorem (Grigori Perelman,2003; Fields Medal 2006)

The Geometrization Conjecture is True.

- Poincaré himself solved the problem for $n = 2$ early in the XX-th century by completely classifying all compact 2–manifolds and noting that in the list of all possible such manifolds only the sphere was simply connected.
- For a time he believed that he solved the three–dimensional case as well, but then he discovered a counterexample to one of his main assertions.
- 1961 – Stephen Smale (Fields Medal 1966) proved the conjecture for $n \geq 5$, and Michael Freedman (Fields Medal 1986) proved the $n = 4$ case in 1982.

The Geometrization Conjecture implies the Poincaré Conjecture.

- 1981 Richard Hamilton set up a program to address both conjectures. The main idea of this program was to solve the problems by analyzing Ricci Flow.
- Ricci Flow is a technique that allows one to take an arbitrary Riemannian manifold and smooth out the geometry of the manifold to make it look more symmetric
- Ricci flow converts an arbitrary manifold into a finite union of very symmetric pieces (GEOMETRIZATION THEOREM).

Primes in Arithmetic Progression

Problem (Erdös–Tùran Conjecture)

Does every infinite sequence of integers $\{n_i\}_{n=1}^{\infty}$ *such that*

$$\sum \frac{1}{n_i}$$

contain an arbitrary arithmetic progression ?

Theorem (Green–Tao, Terence Tao; Fields Medal 2010)

For every $k \in \mathbb{N}$ *there are infinitely many* k*–term arithmetic progressions of primes, i.e. pairs of integers* a, d *such that* $a, a+d, a+2d, \ldots, a+(k-1)d$ *are all primes.*

Goldbach Conjecture

Problem (Even Goldbach Conjecture 1742)

Every even integer greater than 2 is the sum of two primes.

Problem (Odd Goldbach Conjecture 1742)

Every odd integer greater than 5 is the sum of 3 primes.

- The even conjecture implies the odd one but not conversely.

Odd Goldbach Conjecture

- 1937 Vinogradov – all "sufficiently large" odd integers can be expressed as a sum of three primes
- 2002 Liu Ming Chit and Wang Tien Ze : $n > e^{3100} \approx 2 \times 10^{1346}$
- 2012 Tao – every odd integer is a sum of at most 5 primes
- 2012, 2013 Harald Helfgot - proves the odd Goldbach Conjecture (?)

Even Goldbach Conjecture

- Chen Jingru 1973 – every sufficiently large even integer can be written as either a sum of two primes or a sum of a prime and a semiprime (the product of two primes)
- T. Oliveira da Silva computer verified the even case for all $n \leq 4 \times 10^{18}$

Twin Prime Conjecture

Theorem (Vigo Brun, 1915)

The series

$$\sum \frac{1}{p}$$

taken over all twin primes p, is convergent

Theorem (Erdös 1940)

There exists a constant $c < 1$ and infinitely many primes p such that $(p' - p) < c \ln p$, where p' is the next prime.

In 2005 Goldston, Prinz and Yilddirim showed that the constant in the Theorem can be arbitrarily small

$$\liminf_{p \to \infty} \frac{p_{n+1} - p_n}{\log p_n} = 0.$$

Theorem (Yitzang Zhang 2013)

There is a constant $N\,(= 7 \times 10^7)$ *and infinitely many primes* p_n *such that*

$$\liminf_{n\to+\infty}(p_{n+1} - p_n) < N.$$

- Tao and Maynard reduced N to 246, and in some cases to 12, or even to 6 (under additional assumptions).