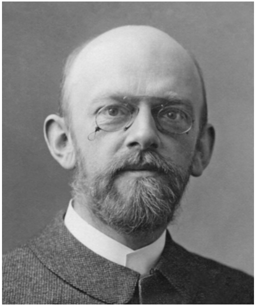
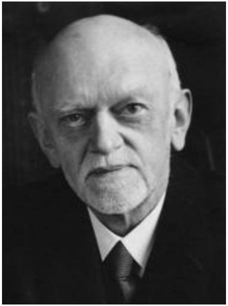
The Hilbert Problems

Keith Conrad

September 4, 2019

David Hilbert (1862-1943)





One of the preeminent mathematicians of his generation:

- analysis and mathematical physics (Hilbert spaces)
- algebra and algebraic geometry (Hilbert basis theorem)
- number theory (Hilbert reciprocity law)
- logic (Hilbert proof system)

Worked in Königsberg (1886-1895) and Göttingen (1895-1930).

The Paris ICM in 1900

On August 8, 1900, Hilbert gave a lecture on "Mathematical Problems" at the 2nd International Congress of Mathematicians (ICM) in Paris.

"*Who of us would not be glad to lift the veil behind which the future lies hidden; to cast a glance at the next advances of our science and at the secrets of its development during future centuries*?"

"*It is by the solution of problems that the investigator* [. . .] *finds new methods and new outlooks.*"

Examples of how work towards solving a problem leads to new areas of mathematics:

- Newton's work on gravity led him to create calculus.
- Showing there is *no* analogue of the quadratic formula for general polynomials of degree ≥ 5 led Lagrange, Galois, *et al.* to study permutation groups.

The scope of Hilbert's problems

"*Permit me* [...] *to mention particular definite problems, drawn from various branches of mathematics, from the discussion of which an advancement of science may be expected.*"

Hilbert proposed 23 problems.

Abstract algebra: 14, 17
Analysis: 13, 16, 22, 23
Differential equations: 19, 20, 21
Geometry: 3, 4, 5, 14, 15, 16, 18
Logic: 1, 2, 10, 24
Number theory: 7, 8, 9, 10, 11, 12
Mathematical Physics: 6

Note: Hilbert viewed 1st and 2nd problems as part of analysis.

Some of these problems were solved affirmatively, some negatively, and some are still not settled or are too vague ever to be settled.

Each math club talk this semester will be about a Hilbert problem.

Hilbert's first problem

Problem: is every infinite subset of $\mathbf{R}$ *in one-to-one correspondence with either* $\mathbf{Z}^+ = \{1, 2, 3, \ldots\}$ *or with* $\mathbf{R}$?

Background: infinite sets have counterintuitive properties.

Example. (Galileo) There are as many positive even numbers as positive integers since we can list out the evens like this:

$$\begin{array}{cccccccccccccc} 2 & 4 & 6 & 8 & 10 & 12 & 14 & 16 & 18 & 20 & \ldots & 2n & \ldots \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & \ldots & n & \ldots \end{array}$$

In the sense of "density" half the positive integers are even, but in the sense of pure counting, the positive even numbers are just as numerous as the positive integers: we can use the positive integers to count each positive even number exactly once.

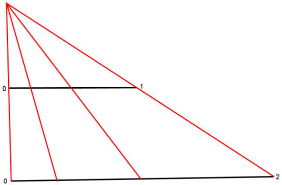
For similar reasons, the set of squares $1, 4, 9, 16, \ldots$ is "just as big" as the set of positive integers despite having density 0 in $\mathbf{Z}^+$.

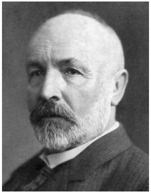
Hilbert's first problem

Does a line segment of length 1 contain more, less, or as many points as a line segment of length 2?

Hilbert's first problem

Does a line segment of length 1 contain more, less, or as many points as a line segment of length 2?



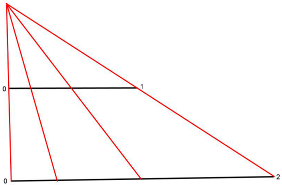


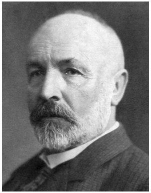
Cantor said two sets A and B are *in one-to-one correspondence* if there is a function from A to B that (i) sends different elements of A to different elements of B and (ii) has all of B as values: there is some way to use A to "count" the elements of B exactly.

Example. Two line segments of different length are in one-to-one correspondence with each other.

Hilbert's first problem

Does a line segment of length 1 contain more, less, or as many points as a line segment of length 2?





Cantor said two sets A and B are *in one-to-one correspondence* if there is a function from A to B that (i) sends different elements of A to different elements of B and (ii) has all of B as values: there is some way to use A to "count" the elements of B exactly.

Example. Two line segments of different length are in one-to-one correspondence with each other.

Example. A line segment is in one-to-one correspondence with $\mathbf{R}$, and $\mathbf{R}$ is in one-to-one correspondence with $\mathbf{R}^2$ (?!?).

Hilbert's first problem

An infinite set is not finite, so it has elements that we can list as $a_1, a_2, a_3, \ldots$ (may miss some). This subset is in a one-to-one correspondence with $\mathbf{Z}^+$, so $\mathbf{Z}^+$ is the "smallest" type of infinity.

Some infinite subsets of $\mathbf{R}$ are in one-to-one correspondence with $\mathbf{Z}^+$ (*e.g.*, $\mathbf{Z}$ and $\mathbf{Q}$) and some with $\mathbf{R}$.

Hilbert's first problem

An infinite set is not finite, so it has elements that we can list as $a_1, a_2, a_3, \ldots$ (may miss some). This subset is in a one-to-one correspondence with $\mathbf{Z}^+$, so $\mathbf{Z}^+$ is the "smallest" type of infinity.

Some infinite subsets of $\mathbf{R}$ are in one-to-one correspondence with $\mathbf{Z}^+$ (*e.g.*, $\mathbf{Z}$ and $\mathbf{Q}$) and some with $\mathbf{R}$.

Theorem. (Cantor, 1874) *There is no one-to-one correspondence between* $\mathbf{Z}^+$ *and* $\mathbf{R}$.

In a sense, $\mathbf{Q}$ and $\mathbf{Z}$ are "just as large" as $\mathbf{Z}^+$, but $\mathbf{R}$ is "larger".

Every infinite set in $\mathbf{R}$ that Cantor could think of was in one-to-one correspondence with either $\mathbf{Z}^+$ or $\mathbf{R}$. He asked if this is true for every infinite subset of $\mathbf{R}$, and that is Hilbert's first problem.

Hilbert's first problem

An infinite set is not finite, so it has elements that we can list as $a_1, a_2, a_3, \ldots$ (may miss some). This subset is in a one-to-one correspondence with $\mathbf{Z}^+$, so $\mathbf{Z}^+$ is the "smallest" type of infinity.

Some infinite subsets of $\mathbf{R}$ are in one-to-one correspondence with $\mathbf{Z}^+$ (*e.g.*, $\mathbf{Z}$ and $\mathbf{Q}$) and some with $\mathbf{R}$.

Theorem. (Cantor, 1874) *There is no one-to-one correspondence between* $\mathbf{Z}^+$ *and* $\mathbf{R}$.

In a sense, $\mathbf{Q}$ and $\mathbf{Z}$ are "just as large" as $\mathbf{Z}^+$, but $\mathbf{R}$ is "larger".

Every infinite set in $\mathbf{R}$ that Cantor could think of was in one-to-one correspondence with either $\mathbf{Z}^+$ or $\mathbf{R}$. He asked if this is true for every infinite subset of $\mathbf{R}$, and that is Hilbert's first problem.

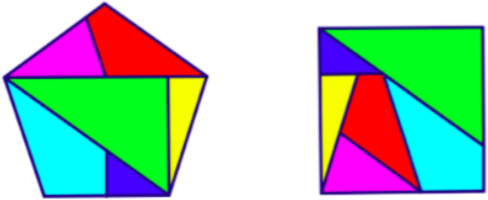
By work of Gödel (1940) and Cohen (1963), this problem has no definite answer! It's undecidable within usual axioms of set theory.

Hilbert had written in 1900: "*Every definite mathematical problem must necessarily be susceptible of an exact settlement*." ¯_(ツ)_/¯

Hilbert's third problem

Problem: could two polyhedra have the same volume but not be decomposable into finitely many congruent polyhedra?

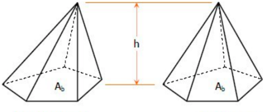
Background: This is a problem about 3-dimensional geometry. A 2-dimensional analogue for polygons is that having equal area is always explained by being equidecomposable. That is a theorem of Bolyai, Gerwien, and Wallace from the early 1800s.



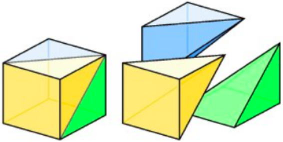
For polygons, "equal area" is the same as "equidecomposable". So we can define "equal area" for polygons purely by geometric decompositions (using translations and rotations).

Hilbert's third problem

Pyramids have an elementary-looking volume formula $\frac{1}{3}Ah$, but all known derivations of that formula are based on calculus.



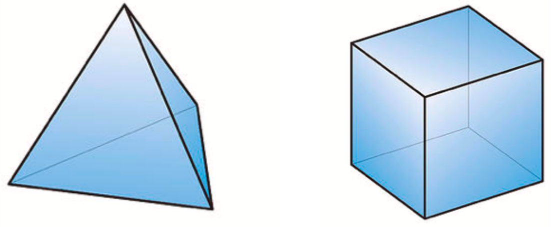
Some pyramids don't need calculus to find their volume.



Gauss (1844) thought it unfortunate that the simple volume formula $\frac{1}{3}Ah$ relies on limits (calculus). Hilbert asked for an example of two polyhedra with the same volume that *can't* be decomposed into congruent polyhedra.

Hilbert's third problem

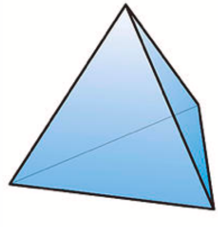
This was the first Hilbert problem to be solved: in 1901 by Max Dehn (before Hilbert's lecture was published).

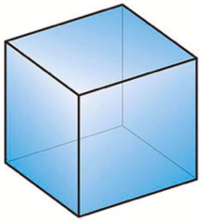


He found a *numerical invariant*, now called the Dehn invariant, that has the same value on any two equidecomposable polyhedra but has different values on a regular tetrahedron and a cube.

Hilbert's third problem

This was the first Hilbert problem to be solved: in 1901 by Max Dehn (before Hilbert's lecture was published).





He found a *numerical invariant*, now called the Dehn invariant, that has the same value on any two equidecomposable polyhedra but has different values on a regular tetrahedron and a cube.

This problem was already proposed and solved in the 1880s in Poland, but the solution was unpublished and rediscovered quite recently!

Hilbert's sixth problem

Problem: give a mathematical treatment of the axioms of physics, especially the theory of probabilities and mechanics.

In 1900, probability was not viewed as part of math, but as part of physics or philosophy. Since the 1930s, probability has had an axiomatic foundation (*e.g.*, what is a "random variable"?).

In 1900, relativity and quantum mechanics were unknown, so "mechanics" then meant classical mechanics and statistical mechanics. Hilbert specifically wanted an explanation of the transition from atomic physics to models of continuous matter.

Hilbert wrote: "*The desired proof of the compatibility of all assumptions seems to me also of importance.*" This issue is one of the great unsolved problems in modern physics: general relativity and quantum mechanics are not compatible physical theories (continuity vs. discreteness).

Hilbert's seventh problem

Problem: if a is algebraic and $a \neq 0, 1$ and b is algebraic irrational, is a^b transcendental?

Example. Is $2^{\sqrt{2}}$ transcendental?

Background: algebraic vs. transcendental numbers.

A number t is *algebraic* if it's the root of a polynomial equation with rational coefficients:

$$c_n x^n + c_{n-1} t^{n-1} + \cdots + c_1 t + c_0 = 0$$

where c_i are rational and not all zero. For instance, $1/2$ and $\sqrt[5]{2}$ are algebraic (roots of $2x - 1$ and $x^5 - 2$). A number that is not algebraic is *transcendental*. This refines irrationality (why?)

Irrationality of e and π was proved in 1700s: for e in 1737 (Euler) and for π in 1760 (Lambert). Transcendence took 100 more years: e in 1873 (Hermite) and π in 1882 (Lindemann, Hilbert's Ph.D. advisor). Hilbert (1893) simplified both transcendence proofs.

Hilbert's seventh problem

Lindemann really showed that e^α *is transcendental for algebraic* $\alpha \neq 0$. This implies transcendence of $e = e^1$. It also implies from $e^{i\pi} = -1$ that $i\pi$ can't be algebraic, so π isn't algebraic: π is transcendental.

Lindemann's theorem on transcendental values of e^α for algebraic $\alpha \neq 0$ inspired Hilbert's question about transcendence of a^b for algebraic $a \neq 0, 1$ and algebraic irrational b.

- Kuzmin (1930) showed a^b is transcendental if $a \neq 0, 1$ is algebraic and b is a *quadratic irrational*. In particular, $2^{\sqrt{2}}$ is transcendental.
- Gelfond and Schneider (1934) independently settled the general question posed by Hilbert.

Hilbert's seventh problem

Lindemann really showed that e^α *is transcendental for algebraic* $\alpha \neq 0$. This implies transcendence of $e = e^1$. It also implies from $e^{i\pi} = -1$ that $i\pi$ can't be algebraic, so π isn't algebraic: π is transcendental.

Lindemann's theorem on transcendental values of e^α for algebraic $\alpha \neq 0$ inspired Hilbert's question about transcendence of a^b for algebraic $a \neq 0, 1$ and algebraic irrational b.

- Kuzmin (1930) showed a^b is transcendental if $a \neq 0, 1$ is algebraic and b is a *quadratic irrational*. In particular, $2^{\sqrt{2}}$ is transcendental.
- Gelfond and Schneider (1934) independently settled the general question posed by Hilbert.

It is expected that $e + \pi$ and $e\pi$ are both transcendental, but this is still unproved. Even the irrationality of both is an open problem. Would follow from a special case of Schanuel's conjecture (1966).

Hilbert's eighth problem

Problem: some problems about prime numbers. Solve the Riemann hypothesis, Goldbach's conjecture, and the twin prime problem.

The Riemann hypothesis is about the location of numbers where the Riemann zeta-function is 0.

For $s > 1$, and complex s with $\mathrm{Re}(s) > 1$, the infinite series

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

converges (*e.g.*, $\zeta(2) = \pi^2/6$, $\zeta(3) \approx 1.202$). Analogy: for $|x| < 1$,

$$\sum_{n \geq 0} x^n = 1 + x + x^2 + x^3 + x^4 + \cdots = \frac{1}{1 - x}$$

and the formula $1/(1 - x)$ has meaning for all $x \neq 1$. There is also a (hard) formula for $\zeta(s)$ that has meaning for all $s \neq 1$.

Hilbert's eighth problem

Problem: some problems about prime numbers. Solve the Riemann hypothesis, Goldbach's conjecture, and the twin prime problem.

The Riemann hypothesis is about the location of numbers where the Riemann zeta-function is 0.

For $s > 1$, and complex s with $\mathrm{Re}(s) > 1$, the infinite series

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

converges (*e.g.*, $\zeta(2) = \pi^2/6$, $\zeta(3) \approx 1.202$). Analogy: for $|x| < 1$,

$$\sum_{n \geq 0} x^n = 1 + x + x^2 + x^3 + x^4 + \cdots = \frac{1}{1-x}$$

and the formula $1/(1-x)$ has meaning for all $x \neq 1$. There is also a (hard) formula for $\zeta(s)$ that has meaning for all $s \neq 1$.

Riemann hypothesis: $\zeta(s) = 0$ and $0 < \mathrm{Re}(s) < 1 \Rightarrow \mathrm{Re}(s) = \frac{1}{2}$.
Example: The first solution of $\zeta(s) = 0$ is $s \approx \frac{1}{2} + 14.1347i$.

Hilbert's eighth problem

The Riemann hypothesis (RH) doesn't sound important or related to prime numbers! The connection is through *multiplication*.

Connection to prime numbers: for $s > 1$, and also $\mathrm{Re}(s) > 1$,

$$\zeta(s) = \frac{1}{1-1/2^s}\frac{1}{1-1/3^s}\frac{1}{1-1/5^s}\frac{1}{1-1/7^s}\frac{1}{1-1/11^s}\cdots$$

At the time of Hilbert's lecture, it had recently been shown that RH is equivalent to a sharp bound on the error term in the prime number theorem ($|\{p \leq x\}| \sim x/\log x$), which itself had been proved just a few years earlier (1896).

Evidence (without a proof) in favor of RH:

- Has been checked numerically very far (first 10 trillion zeros).
- There are analogues of RH in other settings in math that can be proved.
- Some theorems first proved using RH were later proved by other methods (never turned out to be wrong).

Hilbert's eighth problem

Goldbach conjecture: each even number ≥ 4 is sum of two primes. Some examples:

$$4 = 2 + 2,\ 6 = 3 + 3,\ 8 = 3 + 5,\ 10 = 3 + 7 = 5 + 5,\ 12 = 5 + 7.$$

While small even numbers ≥ 4 may be expressible in essentially just one way as a sum of two primes, what we *really* expect is that the number of representations grows (erratically).

Evidence (without a proof) in favor of Goldbach's conjecture:

- It has been checked numerically very far (up to 10^{18}).
- Chen (1966) proved every sufficiently large even number is either $p + q$ or $p + q_1q_2$.
- The proportion of even numbers $\leq x$ not expressible as a sum of two primes tends to 0 as $x \to \infty$.
- In 2013 Helfgott showed every odd number ≥ 7 is a sum of three primes. This would follow from Goldbach's conjecture.

Hilbert's eighth problem

Twin prime problem: show that infinitely many primes differ by 2 (called twin primes): (3,5), (5,7), (11,13), (17,19), (29,31), (41, 43), (59, 61), (71, 73), (101, 103), (107, 109), (137, 139), . . .

Evidence (without a proof) in favor of the infinitude of twin primes.

- There are heuristic formulas for the number of twin primes up to x for large x and the data fit this.
- Chen (1966) proved there are infinitely many prime p such that $p + 2$ is prime or a product of two primes.
- For each even $k \geq 2$, nearly everything we expect about twin primes $p, p + 2$ (*e.g.*, Chen's theorem) has an analogue for prime pairs $p, p + k$ and this is supported numerically and by what's been proved.
- In 2013 Zhang and Maynard–Tao proved the set of prime gaps are infinitely often bounded (by at most 246).

Hilbert's tenth problem

Problem: find a procedure that can decide in finitely many steps whether each polynomial equation $P(x_1, \ldots, x_n) = 0$ *with integer coefficients has an integer solution*.

We are allowing any number of variables and any degree in the equation, and want a *single* algorithm to determine when *each* $P = 0$ is solvable in $\mathbf{Z}$. (Are two algorithms a single algorithm?)

Example. $x^2 - 3y^2 = 1$ vs. $x^2 - 3y^2 = 2$. The real solutions look the same: both are hyperbolas. First one has the integral solution $(1, 0)$ (and there are more). Second one has no integral solution.

Example. Does $y^2 = x^3 + 11$ have an integral solution? That it has a rational solution $(-7/4, 19/8)$ does not answer the question.

Hilbert's tenth problem

Problem: find a procedure that can decide in finitely many steps whether each polynomial equation $P(x_1, \ldots, x_n) = 0$ *with integer coefficients has an integer solution*.

We are allowing any number of variables and any degree in the equation, and want a *single* algorithm to determine when *each* $P = 0$ is solvable in $\mathbf{Z}$. (Are two algorithms a single algorithm?)

Example. $x^2 - 3y^2 = 1$ vs. $x^2 - 3y^2 = 2$. The real solutions look the same: both are hyperbolas. First one has the integral solution $(1, 0)$ (and there are more). Second one has no integral solution.

Example. Does $y^2 = x^3 + 11$ have an integral solution? That it has a rational solution $(-7/4, 19/8)$ does not answer the question.

Hilbert is asking not how to find an integral solution, but how to determine if such a solution *exists*. (Analogue: it is known that $2^{2^{14}} + 1$ is composite but a nontrivial factorization is unknown.) His problem was posed before the general notion of an algorithm was defined, without which it couldn't be *disproved*.

Hilbert's tenth problem

Answer: for Hilbert's tenth problem there is *no* algorithm. This is based on work of Davis, Putnam, Robinson, and Matiyasevich during 1949–1970. Matiyasevich's work in 1970 was based on a previously unnoticed property of *Fibonacci numbers*.

By DPRM theorem, statements like Fermat's Last Theorem (FLT), Goldbach conjecture, and RH are each *equivalent* to a polynomial equation with **Z**-coefficients *not* having **Z**-solution.

DPRM theorem did *not* end the study of integral solutions to polynomial equations! There are still unsolved problems about **Z**-solutions of cubic polynomials in two variables.

Hilbert's eighteenth problem

Problem: Three questions about ways of filling up space. For example, what is the densest way to pack spheres in $\mathbf{R}^3$?

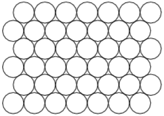
Use non-overlapping spheres of equal radius. Density is taken in a limiting sense over large regions of space.

Kepler (1611) conjectured that the"grocery store" packing has the largest density: $\pi/\sqrt{18} \approx .74$.

- Other arrangements may have the same density. Problem is to show no arrangement has a larger density.
- Rule out all other possibilities, including those that might not involve a regular pattern of spheres.
- Similar question in other spaces is important in coding theory.

Hilbert's eighteenth problem

In 2 dimensions, Thue (1890) proved most dense sphere-packing (really circle-packing) is the hexagonal one, as shown below.



Thomas Hales announced a proof of Kepler's conjecture in 1998 using computers to check about 5000 cases (each one being a nonlinear optimization problem). In 2014, Hales announced a formal version of the proof had been checked by an automated theorem prover.

Do we get insight from such a proof? Similarly, is there insight in knowing Goldbach's conjecture is true up to 10^{18}?

Most dense sphere-packing in $\mathbf{R}^n$ known for $n = 1$, 2, 3, 8, and 24. The 8 and 24-dimensional cases were proved in 2016 by Maryna Viazovska and collaborators without massive computer help.

Millennium prize problems

In 2000, the Clay Math Institute offered a $1 million prize for the solution of any of the following 7 unsolved problems:

- Poincaré conjecture (topology)
- P vs. NP (computer science)
- Navier–Stokes existence and smoothness (physics, PDE)
- Yang–Mills existence and mass gap (physics)
- Riemann hypothesis (number theory)
- Birch and Swinnnerton-Dyer conjecture (number theory)
- Hodge conjecture (algebraic geometry)

Informal description of P vs. NP: *if a problem can have its solutions checked quickly, can the problem be solved quickly*?

Example: factoring appears to be difficult in general, but it's easy to check if an explicitly proposed factorization is correct or not.

Millennium prize problems

In 2000, the Clay Math Institute offered a $1 million prize for the solution of any of the following 7 unsolved problems:

- Poincaré conjecture (topology)
- P vs. NP (computer science)
- Navier–Stokes existence and smoothness (physics, PDE)
- Yang–Mills existence and mass gap (physics)
- Riemann hypothesis (number theory)
- Birch and Swinnnerton-Dyer conjecture (number theory)
- Hodge conjecture (algebraic geometry)

Informal description of P vs. NP: *if a problem can have its solutions checked quickly, can the problem be solved quickly*?

Example: factoring appears to be difficult in general, but it's easy to check if an explicitly proposed factorization is correct or not.

The Poincaré conjecture was settled by Perelman in 2002. He proved something more general (Thurston's Geometrization conjecture) and turned down the Clay prize and the Fields medal.

Questions?

References

- F. Browder (ed.), *Mathematical Developments Arising from Hilbert Problems*, Amer. Math. Soc., 1976.
- J. Gray, *The Hilbert Challenge*, Oxford Univ. Press, 2000.
- D. Hilbert, “Mathematical Problems,” Bulletin Amer. Math. Soc. **8** (1902), 437–479.
- B. Yandell, *The Honors Class: Hilbert's Problems and Their Solvers*, A. K. Peters, 2001.