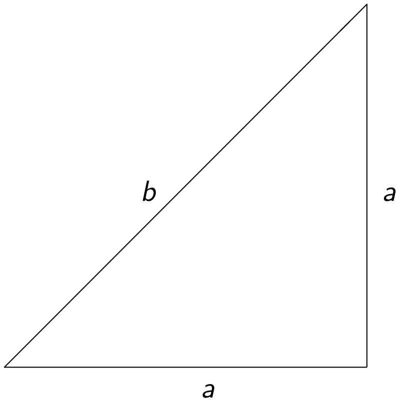
Paradoxes, or The Art of the Impossible

Thomas Jech

Praha, February 2016

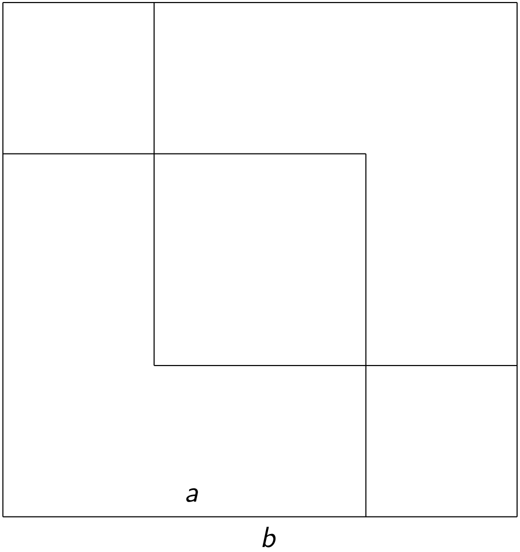
Irrationality of $\sqrt{2}$

Pythagoreans (Hippasus?, Theodorus?) around 400 B.C. contempopraries of Platon



$$b^2 = a^2 + a^2$$

Irrationality of $\sqrt{2}$



Transcendental numbers

A real number is *algebraic* if it is the root of a polynomial with integer coefficients. A number is *transcendental* if it is not algebraic.

Squaring the circle

Given a circle, construct (using a ruler and a compass) a square that has the same area.

It turns out that if this is possible then the number π has to be an algebraic number.

Liouville 1844: there exist (infinitely many) transcendental numbers.

(Cantor 1873: "Most" real numbers are transcendental.)

Lindemann 1882: π is transcendental

Infinity

Galileo's Paradox Galileo 1638:

$1 \quad 2 \quad 3 \quad 4 \quad \dots n \quad \dots$
$1 \quad 4 \quad 9 \quad 16 \quad \dots n^2 \quad \dots$

(one-to-one correspondence, density 0)

Galileo's Paradox Galileo 1638:

$1 \quad 2 \quad 3 \quad 4 \quad \ldots n \quad \ldots$
$1 \quad 4 \quad 9 \quad 16 \quad \ldots n^2 \quad \ldots$

(one-to-one correspondence, density 0)

Bolzano 1851: "Paradoxien des Unendlichen"
Menge (= set=množina=ensemble=...)

Galileo's Paradox Galileo 1638:

$1 \quad 2 \quad 3 \quad 4 \quad \ldots n \quad \ldots$
$1 \quad 4 \quad 9 \quad 16 \quad \ldots n^2 \quad \ldots$

(one-to-one correspondence, density 0)

Bolzano 1851: "Paradoxien des Unendlichen"
Menge (= set=množina=ensemble=...)

Hilbert: the Grand Hotel (1924)

Galileo's Paradox Galileo 1638:

$1 \quad 2 \quad 3 \quad 4 \quad \ldots n \quad \ldots$
$1 \quad 4 \quad 9 \quad 16 \quad \ldots n^2 \quad \ldots$

(one-to-one correspondence, density 0)

Bolzano 1851: "Paradoxien des Unendlichen"
Menge (= set=množina=ensemble=...)

Hilbert: the Grand Hotel (1924)

Cantor 1873: **cardinal numbers**

Set Theory

Cantor's letter to Dedekind, December 1873:

Countable sets = those for which there is a one-to-one correspondence with the set **N** of all of all natural numbers.

The set of all real numbers **R** is uncountable while the set of all algebraic real numbers is countable, therefore there exist uncountably many transcendental numbers.

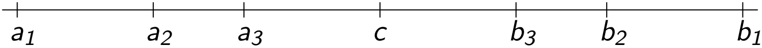
Set Theory

Cantor's letter to Dedekind, December 1873:

Countable sets = those for which there is a one-to-one correspondence with the set **N** of all of all natural numbers.

The set of all real numbers **R** is uncountable while the set of all algebraic real numbers is countable, therefore there exist uncountably many transcendental numbers.

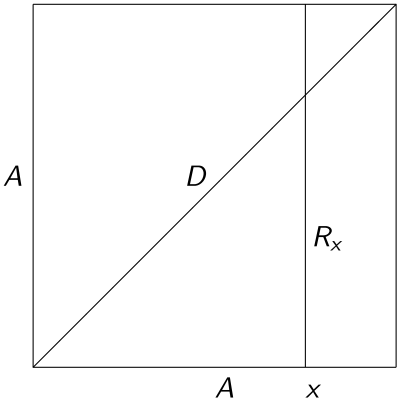
Proof. Let $\{c_1, c_2, c_3, \ldots\}$ be a sequence of real numbers. There exists a real number c not in the sequence.



Let $\{a_1, b_1\}$ be first two members of the sequence $\{c_n\}$. Let $\{a_2, b_2\}$ be first two members of the sequence inside the interval (a_1, b_1) and so on. Let $c = \lim_n a_n$.

The Diagonal Method

Cantor 1891 - another proof of $2^{\aleph_0} > \aleph_0$.



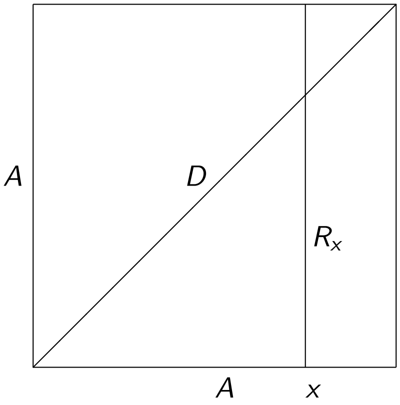
Let $R \subset A \times A$. For $x \in A$ let $R_x = \{y \in A : (x, y) \in R\}$.

The set $D = \{x \in A : (x, x) \notin R\}$ has the property that $D \neq R_x$ for every $x \in A$.

$x \in D$ iff $x \notin R_x$

The Diagonal Method

Cantor 1891 - another proof of $2^{\aleph_0} > \aleph_0$.



Let $R \subset A \times A$. For $x \in A$ let $R_x = \{y \in A : (x, y) \in R\}$.

The set $D = \{x \in A : (x, x) \notin R\}$ has the property that $D \neq R_x$ for every $x \in A$.

$x \in D$ iff $x \notin R_x$

Applications: $|P(A)| > |A|$, therefore $2^{\aleph_\alpha} > \aleph_\alpha$;
There exists no set $\{x : x \notin x\}$ ("Russell's Paradox").

The Axiom of Choice

Zermelo 1904: Every set can be well-ordered.

Axiom of Choice. For every set S of nonempty sets there exists a function F such that $F(X) \in X$ for every $X \in S$.

The Axiom of Choice

Zermelo 1904: Every set can be well-ordered.

Axiom of Choice. For every set S of nonempty sets there exists a function F such that $F(X) \in X$ for every $X \in S$.

Vitali 1905: There exists a nonmeasurable set of reals.
Proof. Using the axiom of choice, there is a set V that contains exactly one element of each coset of the quotient $\mathbf{R}/\mathbf{Q}$.

The Axiom of Choice

Zermelo 1904: Every set can be well-ordered.

Axiom of Choice. For every set S of nonempty sets there exists a function F such that $F(X) \in X$ for every $X \in S$.

Vitali 1905: There exists a nonmeasurable set of reals.
Proof. Using the axiom of choice, there is a set V that contains exactly one element of each coset of the quotient $\mathbf{R}/\mathbf{Q}$.

Hausdorff 1914: A paradoxical decomposition of the sphere:
$A \cup B \cup C \cup Q$ with Q countable and A, B, C, $B \cup C$ all congruent to each other.
(Using the free product of the cyclic groups $\{1, \varphi\}$ and $\{1, \psi, \psi^2\}$ which can easily be decomposed into $A \cup B \cup C$.)

The Axiom of Choice

Zermelo 1904: Every set can be well-ordered.

Axiom of Choice. For every set S of nonempty sets there exists a function F such that $F(X) \in X$ for every $X \in S$.

Vitali 1905: There exists a nonmeasurable set of reals.
Proof. Using the axiom of choice, there is a set V that contains exactly one element of each coset of the quotient $\mathbf{R}/\mathbf{Q}$.

Hausdorff 1914: A paradoxical decomposition of the sphere:
$A \cup B \cup C \cup Q$ with Q countable and A, B, C, $B \cup C$ all congruent to each other.
(Using the free product of the cyclic groups $\{1, \varphi\}$ and $\{1, \psi, \psi^2\}$ which can easily be decomposed into $A \cup B \cup C$.)

Banach-Tarski 1924: The unit ball can be decomposed into a finitely many pieces that can be rearranged to form TWO unit balls. (The Banach-Tarski Paradox.)

The Axiom of Choice

Zermelo 1904: Every set can be well-ordered.

Axiom of Choice. For every set S of nonempty sets there exists a function F such that $F(X) \in X$ for every $X \in S$.

Vitali 1905: There exists a nonmeasurable set of reals.
Proof. Using the axiom of choice, there is a set V that contains exactly one element of each coset of the quotient $\mathbf{R}/\mathbf{Q}$.

Hausdorff 1914: A paradoxical decomposition of the sphere: $A \cup B \cup C \cup Q$ with Q countable and A, B, C, $B \cup C$ all congruent to each other.
(Using the free product of the cyclic groups $\{1, \varphi\}$ and $\{1, \psi, \psi^2\}$ which can easily be decomposed into $A \cup B \cup C$.)

Banach-Tarski 1924: The unit ball can be decomposed into a finitely many pieces that can be rearranged to form TWO unit balls. (The Banach-Tarski Paradox.)

Gödel 1938: The axiom of choice is consistent with the other axioms of set theory.

The Liar Paradox

Epimenides of Crete (around 600 BC, quoted by Apostle Paul):
"The Cretans are liars."

The Liar Paradox

Epimenides of Crete (around 600 BC, quoted by Apostle Paul): "The Cretans are liars."

Eubulides (around 350 BC): "Does a man who says that he is lying speak the truth?"

The Liar Paradox

Epimenides of Crete (around 600 BC, quoted by Apostle Paul): "The Cretans are liars."

Eubulides (around 350 BC): "Does a man who says that he is lying speak the truth?"

The Liar Paradox:

This statement is false.

The Liar Paradox

Epimenides of Crete (around 600 BC, quoted by Apostle Paul):
"The Cretans are liars."

Eubulides (around 350 BC): "Does a man who says that he is lying speak the truth?"

The Liar Paradox:

This statement is false.

An example of *self-reference*. Other examples:

The Liar Paradox

Epimenides of Crete (around 600 BC, quoted by Apostle Paul): "The Cretans are liars."

Eubulides (around 350 BC): "Does a man who says that he is lying speak the truth?"

The Liar Paradox:

This statement is false.

An example of *self-reference*. Other examples:

The barber paradox: A barber is a man who shaves those and only those men who do not shave themselves.

The Liar Paradox

Epimenides of Crete (around 600 BC, quoted by Apostle Paul): "The Cretans are liars."

Eubulides (around 350 BC): "Does a man who says that he is lying speak the truth?"

The Liar Paradox:

This statement is false.

An example of *self-reference*. Other examples:

The barber paradox: A barber is a man who shaves those and only those men who do not shave themselves.

Russell's Paradox:

$$\{x : x \notin x\}$$

Gödel 1931:
Arithmetic is incomplete. (The First Incompleteness Theorem.)
Arithmetic cannot prove its own consistency. (The Second Incompleteness Theorem.)

Gödel's Incompleteness Theorems

Gödel 1931:
Arithmetic is incomplete. (The First Incompleteness Theorem.)
Arithmetic cannot prove its own consistency. (The Second Incompleteness Theorem.)

Recursive functions and relations, arithmetization of the language (Gödel numbers $\#$).

Gödel 1931:
Arithmetic is incomplete. (The First Incompleteness Theorem.)
Arithmetic cannot prove its own consistency. (The Second Incompleteness Theorem.)

Recursive functions and relations, arithmetization of the language (Gödel numbers #).

If T is a recursive set of axioms containing the arithmetic then there exists a sentence σ such that

$$T \vdash [\sigma \leftrightarrow \neg \exists p (p = \#(\text{proof of } \sigma))]$$

It follows that (if T is consistent then) σ is *undecidable* in T.

The Diagonal Lemma. Let φ be a formula of one free variable. Then there is a sentence σ such that

$$T \vdash \sigma \leftrightarrow \varphi(\#\sigma).$$

Letting $\varphi(x)$ be "*x is unprovable*", one gets the Gödel sentence.

The Diagonal Lemma. Let φ be a formula of one free variable. Then there is a sentence σ such that

$$T \vdash \sigma \leftrightarrow \varphi(\#\sigma).$$

Letting $\varphi(x)$ be "x *is unprovable*", one gets the Gödel sentence.

Assuming that $\varphi = \neg\tau$ where τ is a definition of truth, one gets Tarski 1936 : Truth is undefinable in T.

The Diagonal Lemma. Let φ be a formula of one free variable. Then there is a sentence σ such that

$$T \vdash \sigma \leftrightarrow \varphi(\#\sigma).$$

Letting $\varphi(x)$ be "x *is unprovable*", one gets the Gödel sentence.

Assuming that $\varphi = \neg\tau$ where τ is a definition of truth, one gets Tarski 1936 : Truth is undefinable in T.

Undecidable Statements

Turing 1936: The halting problem.
(No algorithm exists to decide whether a given program halts or runs forever.)

The Diagonal Lemma. Let φ be a formula of one free variable. Then there is a sentence σ such that

$$T \vdash \sigma \leftrightarrow \varphi(\#\sigma).$$

Letting $\varphi(x)$ be "x *is unprovable*", one gets the Gödel sentence.

Assuming that $\varphi = \neg\tau$ where τ is a definition of truth, one gets Tarski 1936 : Truth is undefinable in T.

Undecidable Statements

Turing 1936: The halting problem.
(No algorithm exists to decide whether a given program halts or runs forever.)

Gödel 1938, Cohen 1963: The Continuum Hypothesis, the Axiom of Choice.

The Diagonal Lemma. Let φ be a formula of one free variable. Then there is a sentence σ such that

$$T \vdash \sigma \leftrightarrow \varphi(\#\sigma).$$

Letting $\varphi(x)$ be "x *is unprovable*", one gets the Gödel sentence.

Assuming that $\varphi = \neg\tau$ where τ is a definition of truth, one gets Tarski 1936 : Truth is undefinable in T.

Undecidable Statements

Turing 1936: The halting problem.
(No algorithm exists to decide whether a given program halts or runs forever.)

Gödel 1938, Cohen 1963: The Continuum Hypothesis, the Axiom of Choice.

Other examples: Inaccessible cardinals (Zermelo 1930), diophantine equations (Matiyasevich 1970) and many others, in set theory, arithmetic, algebra, topology etc.

A short proof of the Second Incompleteness Theorem

Set theory (if consistent) does not prove its own consistency. It does not prove that there exists a model of set theory.

A short proof of the Second Incompleteness Theorem

Set theory (if consistent) does not prove its own consistency. It does not prove that there exists a model of set theory.

Proof does not use Gödel's First Theorem (rather a version of the Liar Paradox directly). Inspired by Vopěnka's proof (1966) that uses Berry's Paradox (around 1890: "the smallest positive integer not definable in fewer than twelve words").

A short proof of the Second Incompleteness Theorem

Set theory (if consistent) does not prove its own consistency. It does not prove that there exists a model of set theory.

Proof does not use Gödel's First Theorem (rather a version of the Liar Paradox directly). Inspired by Vopěnka's proof (1966) that uses Berry's Paradox (around 1890: "the smallest positive integer not definable in fewer than twelve words").

A **model** is a set M with a binary relation $\in^M$ that satisfies the axioms of set theory.

A short proof of the Second Incompleteness Theorem

Set theory (if consistent) does not prove its own consistency. It does not prove that there exists a model of set theory.

Proof does not use Gödel's First Theorem (rather a version of the Liar Paradox directly). Inspired by Vopěnka's proof (1966) that uses Berry's Paradox (around 1890: "the smallest positive integer not definable in fewer than twelve words").

A **model** is a set M with a binary relation $\in^M$ that satisfies the axioms of set theory.

If M and N are models, we define

$$M < N \text{ if there exists some } m \in N \text{ such that } \in^M = (\in^m)^*$$

where $(\in^m)^*$ is the set of all pairs (x, y) such that $N \models x \in^m y$.

The relation $<$ is transitive: if $M_1 < M_2$ and $M_2 < M_3$ then $M_1 < M_3$.

A short proof of the Second Incompleteness Theorem

A *property* is a formula with one free variable. Consider the property p (of properties q)

$$\exists M \; M \models \neg q(q)$$

and let A be the sentence $p(p)$. Then (provably in set theory)

$$A \;\leftrightarrow\; \exists M \, (M \models \neg A)$$

A short proof of the Second Incompleteness Theorem

A *property* is a formula with one free variable. Consider the property p (of properties q)

$$\exists M \, M \models \neg q(q)$$

and let A be the sentence $p(p)$. Then (provably in set theory)

$$A \; \leftrightarrow \; \exists M \, (M \models \neg A)$$

and if M is a model then

$$M \models A \; \leftrightarrow \; \exists N < M \, (N \models \neg A).$$

A short proof of the Second Incompleteness Theorem

A *property* is a formula with one free variable. Consider the property p (of properties q)

$$\exists M\, M \models \neg q(q)$$

and let A be the sentence $p(p)$. Then (provably in set theory)

$$A \;\leftrightarrow\; \exists M\,(M \models \neg A)$$

and if M is a model then

$$M \models A \;\leftrightarrow\; \exists N < M\,(N \models \neg A).$$

We say that M is *positive* if $M \models A$, and *negative* otherwise. As a consequence of the last equivalence, if M is negative then all $N < M$ are positive.

A short proof of the Second Incompleteness Theorem

Now, assuming that set theory proves that there exists a model, it also proves that for every model M there exists a model $N < M$. From this we prove a contradiction.

A short proof of the Second Incompleteness Theorem

Now, assuming that set theory proves that there exists a model, it also proves that for every model M there exists a model $N < M$. From this we prove a contradiction.

Let M_1 be a model. If M_1 is positive, there exists a negative model $M_2 < M_1$; otherwise let $M_2 = M_1$. Then let $M_3 < M_2$. Since M_2 is negative, M_3 is positive. Therefore there exists a negative $M_4 < M_3$ and we have $M_4 < M_2$ by transitivity. Hence M_4 is positive, a contradiction.

[Proceedings Amer. Math. Society 121 (1994), 311-313.]