Here There Be Monsters

Martin Davis

Courant Institute, NYU

August 20, 2020

Weierstrass's Monster

$$\sum_{n=0}^{\infty} \frac{\cos(3^n \pi x)}{2^n}$$

Weierstrass's Monster

$$\sum_{n=0}^{\infty} \frac{\cos(3^n \pi x)}{2^n}$$

- Everywhere continuous

Weierstrass's Monster

$$\sum_{n=0}^{\infty} \frac{\cos(3^n \pi x)}{2^n}$$

- Everywhere continuous
- Nowhere differentiable

Weierstrass's Monster

$$\sum_{n=0}^{\infty} \frac{\cos(3^n \pi x)}{2^n}$$

- Everywhere continuous
- Nowhere differentiable

Hermite 1893: Je me détourne avec horreur et effroi de cette plaie lamentable des fonctions continues qui n'ont pas de dérivées.

I turn away with horror and dread from this lamentable plague of continuous functions that have no derivatives.

Two related consequences of the work of Gödel,Church,Kleene,Post,and Turing in the 1930s.

Two related consequences of the work of
Gödel,Church,Kleene,Post,and Turing in the 1930s.

Examples of algorithmic unsolvability are widespread, found in many branches of mathematics,

Algorithmic Unsolvability and Formal Undecidability

Two related consequences of the work of Gödel,Church,Kleene,Post,and Turing in the 1930s.

Examples of algorithmic unsolvability are widespread, found in many branches of mathematics,

Gödel formal undecidability has had no impact on mathematical practice.

Algorithmic Unsolvability and Formal Undecidability

Two related consequences of the work of Gödel,Church,Kleene,Post,and Turing in the 1930s.

Examples of algorithmic unsolvability are widespread, found in many branches of mathematics,

Gödel formal undecidability has had no impact on mathematical practice.

Are formally undecidable propositions necessarily monsters?

Gödel in 1933

We set out to find a formal system [of axioms] for mathematics and instead of that found an infinity of systems, and whichever system you choose . . . there is one . . . whose axioms are stronger,

Gödel in 1933

We set out to find a formal system [of axioms] for mathematics and instead of that found an infinity of systems, and whichever system you choose . . . there is one . . . whose axioms are stronger,

For any formal system you can construct a proposition – in fact a proposition of the arithmetic of integers – which is certainly true if the given system is free from contradictions but cannot be proved in the given system.

Gödel in 1933

We set out to find a formal system [of axioms] for mathematics and instead of that found an infinity of systems, and whichever system you choose . . . there is one . . . whose axioms are stronger,

For any formal system you can construct a proposition – in fact a proposition of the arithmetic of integers – which is certainly true if the given system is free from contradictions but cannot be proved in the given system.

. . . if the system under consideration (call it S) is based on the theory of types, . . . this proposition becomes a provable theorem if you add to S the next higher type and the axioms concerning it.

Gödel in 1933

We set out to find a formal system [of axioms] for mathematics and instead of that found an infinity of systems, and whichever system you choose . . . there is one . . . whose axioms are stronger,

For any formal system you can construct a proposition – in fact a proposition of the arithmetic of integers – which is certainly true if the given system is free from contradictions but cannot be proved in the given system.

. . . if the system under consideration (call it S) is based on the theory of types, . . . this proposition becomes a provable theorem if you add to S the next higher type and the axioms concerning it.

the construction of higher and higher types . . . is necessary for proving theorems even of a relatively simple structure.

The Gödel Hierarchy

|

Measurable Cardinals

|

Inacccessable Cardinals

|

Zermelo-Fraenkel

|

ω-Order Number theory

|

Third-Order Number Theory

|

Second-Order Number Theory

|

Peano Arithmetic

|

Primitive Recursive Arithmetic

Π^0_1 Propositions

Π^0_1 propositions assert that some computable property of the natural numbers is true of all natural numbers.

Π_1^0 Propositions

Π_1^0 propositions assert that some computable property of the natural numbers is true of all natural numbers.

Here is a list of familiar propositions that have this "relatively simple structure" of which Gödel spoke.

- Fermat's Last Theorem
- The Goldbach conjecture
- The Riemann Hypothesis
- There are no odd perfect numbers

Π^0_1 Propositions

Π^0_1 propositions assert that some computable property of the natural numbers is true of all natural numbers.

Here is a list of familiar propositions that have this "relatively simple structure" of which Gödel spoke.

- Fermat's Last Theorem
- The Goldbach conjecture
- The Riemann Hypothesis
- There are no odd perfect numbers

By the MRDP Theorem, each Π^0_1 proposition is equivalent to some polynomial equation with integer coeficients having no natural number solutions.

Π^0_1 Propositions

Π^0_1 propositions assert that some computable property of the natural numbers is true of all natural numbers.

Here is a list of familiar propositions that have this "relatively simple structure" of which Gödel spoke.

- Fermat's Last Theorem
- The Goldbach conjecture
- The Riemann Hypothesis
- There are no odd perfect numbers

By the MRDP Theorem, each Π^0_1 proposition is equivalent to some polynomial equation with integer coeficients having no natural number solutions.

So any counter-example could, in principle, be verified by a finite number of additions and multiplications of integers.

The Case of Fermat's Last Theorem

The published proof uses Grothendieck universes which can be formalized in the lower transfinite level of the Gödel hierarchy.

The Case of Fermat's Last Theorem

The published proof uses Grothendieck universes which can be formalized in the lower transfinite level of the Gödel hierarchy.

Nevertheless, the proof was generally accepted.

The Case of Fermat's Last Theorem

The published proof uses Grothendieck universes which can be formalized in the lower transfinite level of the Gödel hierarchy.

Nevertheless, the proof was generally accepted.

Colin McLarty has shown how to formalize the proof in third-order arithmetic.

The Case of Fermat's Last Theorem

The published proof uses Grothendieck universes which can be formalized in the lower transfinite level of the Gödel hierarchy.

Nevertheless, the proof was generally accepted.

Colin McLarty has shown how to formalize the proof in third-order arithmetic.

Is it provable in PA?

The Case of Fermat's Last Theorem

The published proof uses Grothendieck universes which can be formalized in the lower transfinite level of the Gödel hierarchy.

Nevertheless, the proof was generally accepted.

Colin McLarty has shown how to formalize the proof in third-order arithmetic.

Is it provable in PA?

Might one be able to obtain a model of PA in which FLT is false?

An Example from Harvey Friedman: (indepennce from ZFC)

Proposition HF: If S is an order invariant subset of Q_r^{2n}, then there is a rigid maximal square in S.

An Example from Harvey Friedman

Definition

Q_r is the set of rational numbers q such that $| q | \leq r$. This discussion is in terms of elements and subsets of Q_r^{2n}. For $x \in Q_r^{2n}$ the i-th component of x is written x_i.

Definition

Q_r is the set of rational numbers q such that $\mid q \mid \leq r$. This discussion is in terms of elements and subsets of Q_r^{2n}. For $x \in Q_r^{2n}$ the i-th component of x is written x_i.

S is a square if $S = A \times A$ where $A \subseteq Q_r^n$.

An Example from Harvey Friedman

Definition

Q_r is the set of rational numbers q such that $\mid q \mid \leq r$. This discussion is in terms of elements and subsets of Q_r^{2n}. For $x \in Q_r^{2n}$ the i-th component of x is written x_i.

S is a square if $S = A \times A$ where $A \subseteq Q_r^n$. A square S is a maximal square in U if $S \subseteq U$ and there is no square T for which $S \subset T \subseteq U$.

An Example from Harvey Friedman

Definition

Q_r is the set of rational numbers q such that $|\, q \,| \leq r$. This discussion is in terms of elements and subsets of Q_r^{2n}. For $x \in Q_r^{2n}$ the i-th component of x is written x_i.

S is a square if $S = A \times A$ where $A \subseteq Q_r^n$. A square S is a maximal square in U if $S \subseteq U$ and there is no square T for which $S \subset T \subseteq U$.

$x \approx y$ if $x_i < x_j \Leftrightarrow y_i < y_j$ for $i, j = 1, 2, \ldots, 2n$.

An Example from Harvey Friedman

Definition

Q_r is the set of rational numbers q such that $|\, q \,| \leq r$. This discussion is in terms of elements and subsets of Q_r^{2n}. For $x \in Q_r^{2n}$ the i-th component of x is written x_i.

S is a square if $S = A \times A$ where $A \subseteq Q_r^n$. A square S is a maximal square in U if $S \subseteq U$ and there is no square T for which $S \subset T \subseteq U$.

$x \approx y$ if $x_i < x_j \Leftrightarrow y_i < y_j$ for $i, j = 1, 2, \ldots, 2n$.
S is order invariant if $x, y \in S$ and $x \approx y$ implies $y \in S$.

An Example from Harvey Friedman

Definition

Q_r is the set of rational numbers q such that $|\, q \,| \leq r$. This discussion is in terms of elements and subsets of Q_r^{2n}. For $x \in Q_r^{2n}$ the i-th component of x is written x_i.

S is a square if $S = A \times A$ where $A \subseteq Q_r^n$. A square S is a maximal square in U if $S \subseteq U$ and there is no square T for which $S \subset T \subseteq U$.

$x \approx y$ if $x_i < x_j \Leftrightarrow y_i < y_j$ for $i, j = 1, 2, \ldots, 2n$.
S is order invariant if $x, y \in S$ and $x \approx y$ implies $y \in S$.

x is pointy if each x_i for which $x_i \geq 0$ is an integer.

An Example from Harvey Friedman

Definition

Q_r is the set of rational numbers q such that $\mid q \mid \leq r$. This discussion is in terms of elements and subsets of Q_r^{2n}. For $x \in Q_r^{2n}$ the i-th component of x is written x_i.

S is a square if $S = A \times A$ where $A \subseteq Q_r^n$. A square S is a maximal square in U if $S \subseteq U$ and there is no square T for which $S \subset T \subseteq U$.

$x \approx y$ if $x_i < x_j \Leftrightarrow y_i < y_j$ for $i, j = 1, 2, \ldots, 2n$.
S is order invariant if $x, y \in S$ and $x \approx y$ implies $y \in S$.

x is pointy if each x_i for which $x_i \geq 0$ is an integer.
$x \sim y$ if x, y are pointy, $x_i < 0 \Leftrightarrow y_i < 0$, if $x_i < 0$ then $x_i = y_i$, and if $x_i, x_j \geq 0$ then $x_i \leq x_j \Leftrightarrow y_i \leq y_j$

An Example from Harvey Friedman

Definition

Q_r is the set of rational numbers q such that $| q | \leq r$. This discussion is in terms of elements and subsets of Q_r^{2n}. For $x \in Q_r^{2n}$ the i-th component of x is written x_i.

S is a square if $S = A \times A$ where $A \subseteq Q_r^n$. A square S is a maximal square in U if $S \subseteq U$ and there is no square T for which $S \subset T \subseteq U$.

$x \approx y$ if $x_i < x_j \Leftrightarrow y_i < y_j$ for $i, j = 1, 2, \ldots, 2n$.
S is order invariant if $x, y \in S$ and $x \approx y$ implies $y \in S$.

x is pointy if each x_i for which $x_i \geq 0$ is an integer.
$x \sim y$ if x, y are pointy, $x_i < 0 \Leftrightarrow y_i < 0$, if $x_i < 0$ then $x_i = y_i$, and if $x_i, x_j \geq 0$ then $x_i \leq x_j \Leftrightarrow y_i \leq y_j$

S is rigid if $x \in S$ and $x \sim y$ implies $y \in S$

An Example from Harvey Friedman (continued)

Proposition HF: If S is an order invariant subset of Q_r^{2n}, then there is a rigid maximal square in S.

An Example from Harvey Friedman (continued)

Proposition HF: If S is an order invariant subset of Q_r^{2n}, then there is a rigid maximal square in S.

SRP((Stationary Ramsey Property) names a particular cardinal number that is much too large for its existence to be provable in ZFC, but such that the existence of a measurable cardinal proves the consistency of ZFC + Existence of SRP.

An Example from Harvey Friedman (continued)

Proposition HF: If S is an order invariant subset of Q_r^{2n}, then there is a rigid maximal square in S.

SRP((Stationary Ramsey Property) names a particular cardinal number that is much too large for its existence to be provable in ZFC, but such that the existence of a measurable cardinal proves the consistency of ZFC + Existence of SRP.

con(SRP) is the Π_1^0 sentence obtained fron Gödel arithmetization of the statement "[ZFC + Existence of SRP] is consistent".

An Example from Harvey Friedman (continued)

Proposition HF: If S is an order invariant subset of Q_r^{2n}, then there is a rigid maximal square in S.

SRP((Stationary Ramsey Property) names a particular cardinal number that is much too large for its existence to be provable in ZFC, but such that the existence of a measurable cardinal proves the consistency of ZFC + Existence of SRP.

con(SRP) is the Π_1^0 sentence obtained fron Gödel arithmetization of the statement "[ZFC + Existence of SRP] is consistent".

Theorem: If [ZFC + Existence of SRP] is consistent, then HF $\iff$ con(SRP).

An Example from Harvey Friedman (continued)

Proposition HF: If S is an order invariant subset of Q_r^{2n}, then there is a rigid maximal square in S.

SRP((Stationary Ramsey Property) names a particular cardinal number that is much too large for its existence to be provable in ZFC, but such that the existence of a measurable cardinal proves the consistency of ZFC + Existence of SRP.

con(SRP) is the Π_1^0 sentence obtained fron Gödel arithmetization of the statement "[ZFC + Existence of SRP] is consistent".

Theorem: If [ZFC + Existence of SRP] is consistent, then HF $\Longleftrightarrow$ con(SRP).

Corollary: If [ZFC + Existence of SRP] is consistent, then, HF is not provable in ZFC, but is provable from ZFC + existence of a measurable cardinal.

An Example from Harvey Friedman (continued)

Proposition HF: If S is an order invariant subset of Q_r^{2n}, then there is a rigid maximal square in S.

SRP((Stationary Ramsey Property) names a particular cardinal number that is much too large for its existence to be provable in ZFC, but such that the existence of a measurable cardinal proves the consistency of ZFC + Existence of SRP.

con(SRP) is the Π_1^0 sentence obtained fron Gödel arithmetization of the statement "[ZFC + Existence of SRP] is consistent".

Theorem: If [ZFC + Existence of SRP] is consistent, then HF $\iff$ con(SRP).

Corollary: If [ZFC + Existence of SRP] is consistent, then, HF is not provable in ZFC, but is provable from ZFC + existence of a measurable cardinal.

Note: Much more can be said about the place of SRP in the large cardinal hierarchy.

The Riemann Hypothesis

$$\zeta(z) = \sum_{n=1}^{\infty} \frac{1}{n^z} \quad \text{for} \quad \mathcal{R}z > 1$$

$$\zeta(z) = \sum_{n=1}^{\infty} \frac{1}{n^z} \quad \text{for} \quad \mathcal{R}z > 1$$

The functional equation:

$$\zeta(1-z) = 2^{1-z}\pi^{-z}\cos(\pi z/2)\Gamma(z)\zeta(z)$$

$$\zeta(z) = \sum_{n=1}^{\infty} \frac{1}{n^z} \quad \text{for} \quad \mathcal{R}z > 1$$

The functional equation:

$$\zeta(1-z) = 2^{1-z}\pi^{-z}\cos(\pi z/2)\Gamma(z)\zeta(z)$$

The Riemann Hypothesis:

If $0 < \mathcal{R}z < 1$ and $\zeta(z) = 0$ then $\mathcal{R}z = 1/2$.

The Riemann Hypothesis

$$\zeta(z) = \sum_{n=1}^{\infty} \frac{1}{n^z} \text{ for } \mathcal{R}z > 1$$

The functional equation:

$$\zeta(1-z) = 2^{1-z}\pi^{-z}\cos(\pi z/2)\Gamma(z)\zeta(z)$$

The Riemann Hypothesis:

$$\text{If } 0 < \mathcal{R}z < 1 \text{ and } \zeta(z) = 0 \text{ then } \mathcal{R}z = 1/2.$$

The Riemann Hypothesis is provably equivalent to a Π_1^0 statement.

$$\zeta(z) = \sum_{n=1}^{\infty} \frac{1}{n^z} \text{ for } \mathcal{R}z > 1$$

The functional equation:

$$\zeta(1-z) = 2^{1-z}\pi^{-z}\cos(\pi z/2)\Gamma(z)\zeta(z)$$

The Riemann Hypothesis:

$$\text{If } 0 < \mathcal{R}z < 1 \text{ and } \zeta(z) = 0 \text{ then } \mathcal{R}z = 1/2.$$

The Riemann Hypothesis is provably equivalent to a Π^0_1 statement.

Gödel in 1951 on contemporary mathematics using only the lowest levels of what I am calling the Gödel Hierarchy: "this . . . may have something to do with . . . [the] inability to prove . . . for example Riemann's hypothesis despite many years of effort."