Hilbert's Mistake

Edward Nelson

Department of Mathematics

Princeton University

Abstract

Hilbert was at heart a Platonist. ("No one shall expel us from the paradise that Cantor has created for us.") His formalism was primarily a tactic in his battle against Brouwer's intuitionism.

His mistake was to pose the problem of *showing that* mathematics, beginning with Peano Arithmetic, is consistent, rather than to ask *whether* it is consistent.

In this talk I give reasons for taking seriously the possibility that contemporary mathematics, including Peano Arithmetic, may indeed be inconsistent.

Potential vs. Completed Infinity

Let us distinguish between the *genetic*, in the dictionary sense of pertaining to origins, and the *formal*. Numerals (terms containing only the unary function symbol S and the constant 0) are genetic; they are formed by human activity. All of mathematical activity is genetic, though the subject matter is formal.

Numerals constitute a *potential infinity*. Given any numeral, we can construct a new numeral by prefixing it with S.

Now imagine this potential infinity to be completed. Imagine the inexhaustible process of constructing numerals somehow to have been finished, and call the result *the set of all numbers*, denoted by $\mathbb{N}$.

Thus $\mathbb{N}$ is thought to be an *actual infinity* or a *completed infinity*. This is curious terminology, since the etymology of “infinite” is “not finished”.

We were warned.

Aristotle: Infinity is always potential, never actual.

Gauss: I protest against the use of infinite magnitude as something completed, which is never permissible in mathematics.

We ignored the warnings.

With the work of Dedekind, Peano, and Cantor above all, completed infinity was accepted into mainstream mathematics.

Mathematics became a faith-based initiative.

Try to imagine $\mathbb{N}$ as if it were real.

A friend of mine came across the following on the Web:

www.completedinfinity.com

Buy a copy of $\mathbb{N}$!

Contains zero—contains the successor of everything it contains—contains only these.

Just $100.

Do the math! What is the price per number?

Satisfaction guaranteed!

Use our secure form to enter your credit card number and its security number, zip code, social security number, bank's routing number, checking account number, date of birth, and mother's maiden name.

The product will be shipped to you within two business days in a plain wrapper.

My friend answered this ad and proudly showed his copy of $\mathbb{N}$ to me. I noticed that zero was green, and that the successor of every green number was green, but that his model contained a red number. I told my friend that he had been cheated, and had bought a nonstandard model, but he is color blind and could not see my point.

I bought a model from another dealer and am quite pleased with it. My friend maintains that it contains an ineffable number, although zero is effable and the successor of every effable number is effable, but I don't know what he is talking about. I think he is just jealous.

The point of this conceit is that it is impossible to characterize $\mathbb{N}$ unambiguously, as we shall argue in detail.

As a genetic concept, the notion of numeral is clear. The attempt to formalize the concept usually proceeds as follows:

(i) zero is a number;

(ii) the successor of a number is a number;

(iii) zero is not the successor of any number;

(iv) different numbers have different successors;

(v) something is a number only if it is so by virtue of (i) and (ii).

We shall refer to this as the *usual definition.* Sometimes (iii) and (iv) are not stated explicitly, but it is the extremal clause (v) that is unclear.

What is the meaning of "by virtue of"? It is obviously circular to define a number as something constructible by applying (i) and (ii) any number of times.

We cannot characterize numbers from below, so we attempt to characterize them from above.

The study of the foundations of arithmetic began in earnest with the work of Dedekind and Peano. Both of these authors gave what today would be called set-theoretic foundations for arithmetic. In ZFC (and extensions by definitions thereof) let us write 0 for the empty set and define the successor by

$$\mathrm{S}x = x \cup \{\, x \,\}$$

We define

$$x \text{ is inductive} \quad \leftrightarrow \quad 0 \in x \quad \& \quad \forall y\,[\, y \in x \quad \rightarrow \quad \mathrm{S}y \in x \,].$$

Then the axiom of infinity of ZFC is

$$\exists x\,[\, x \text{ is inductive} \,]$$

and one easily proves in ZFC that there exists a unique smallest inductive set; i.e.,

$$\exists! x\,\big[\, x \text{ is inductive} \quad \& \quad \forall y\,[\, y \text{ is inductive} \rightarrow x \subseteq y \,]\big]$$

We define the constant $\mathbb{N}$ to be this smallest inductive set:

$$\mathbb{N} = x \quad \leftrightarrow \quad x \text{ is inductive} \quad \& \quad \forall y\,[\,y \text{ is inductive} \rightarrow x \subseteq y\,]$$

and we define

$$x \text{ is a number} \quad \leftrightarrow \quad x \in \mathbb{N}.$$

Then the following are theorems:

(1) $\quad 0$ is a number

(2) $\quad x$ is a number $\quad\rightarrow\quad \mathrm{S}x$ is a number

(3) $\quad x$ is a number $\quad\rightarrow\quad \mathrm{S}x \neq 0$

(4) $\quad x$ is a number $\quad\&\quad y$ is a number $\quad\&\quad x \neq y \quad\rightarrow\quad \mathrm{S}x \neq \mathrm{S}y$.

These theorems are a direct expression of (i)–(iv) of the usual definition. But can we express the extremal clause (v)? The induction theorem

$$x \text{ is a number} \quad \& \quad y \text{ is inductive} \quad \to \quad x \in y$$

merely asserts that for any property that can be expressed in ZFC, if 0 has the property, and if the successor of every element that has the property also has the property, then every number has the property.

We cannot say, “For all numbers x there exists a numeral d such that $x = \mathrm{d}$” since this is a category mistake conflating the formal with the genetic.

Using all the power of modern mathematics, let us try to formalize the concept of number.

Let T be any theory whose language contains the constant 0, the unary function symbol S, and the unary predicate symbol “is a number”, such that (1)–(4) are theorems of T.

For example, T could be the extension by definitions of ZFC described above or it could be Peano Arithmetic P with the definition:
x is a number $\leftrightarrow x = x$.

Have we captured the intended meaning of the extremal clause (v)?

To study this question, construct T^{φ} by adjoining a new unary predicate symbol φ and the axioms

$$(5) \quad \varphi(0)$$

$$(6) \quad \varphi(x) \quad \rightarrow \quad \varphi(\mathrm{S}x).$$

Notice that φ is an undefined symbol.

If T is ZFC, we cannot form the set $\{\, x \in \mathbb{N} : \varphi(x) \,\}$ because the subset axioms of ZFC refer only to formulas of ZFC and $\varphi(x)$ is not such a formula. Sets are not genetic objects, and to ask whether a set with a certain property exists is to ask whether a certain formula beginning with $\exists$ can be proved in the theory.

Similarly, if T is P we cannot apply induction to $\varphi(x)$ since this is not a formula of P. Induction is not a truth; it is an axiom scheme of a formal theory.

If T is consistent then so is T^{φ}, because we can interpret $\varphi(x)$ by $x = x$. (And conversely, of course, if T is inconsistent then so is T^{φ}.) For any numeral S…S0 we can prove $\varphi(\mathrm{S}\ldots\mathrm{S}0)$ in S…S0 steps using these two axioms and detachment (modus ponens).

Let d be a variable-free term.

Proving $\varphi(\mathrm{d})$ in T^{φ} perfectly expresses the extremal clause, that d is a number by virtue of (i) and (ii) of the usual definition. We can read $\varphi(x)$ as "x is a number by virtue of (i) and (ii)".

Therefore we ask: can

$$(7) \quad x \text{ is a number} \quad \rightarrow \quad \varphi(x)$$

be proved in T^{φ}?

That is, can we prove that our formalization "x is a number" captures the intended meaning of the extremal clause?

Trivially yes if T is inconsistent, so assume that T is consistent.

Then the answer is no. Here is a semantic argument for this assertion.

By (1)–(4), none of the formulas

$$x \text{ is a number} \quad\rightarrow\quad x = 0 \;\vee\; x = \mathrm{S}0 \;\vee\; \cdots \;\vee\; x = \mathrm{S}\ldots\mathrm{S}0$$

is a theorem of T. Hence the theory T_1 obtained from T by adjoining a new constant e and the axioms

$$\mathrm{e} \text{ is a number}, \ \mathrm{e} \neq 0, \ \mathrm{e} \neq \mathrm{S}0, \ldots, \mathrm{e} \neq \mathrm{S}\ldots\mathrm{S}0, \ldots$$

is consistent.

By the Gödel completeness theorem, T_1 has a model $\mathcal{A}$. Let $\mathcal{X}$ be the smallest subset of the universe $|\mathcal{A}|$ of the model containing $0_{\mathcal{A}}$ and closed under the function $\mathrm{S}_{\mathcal{A}}$. Then $\mathrm{e}_{\mathcal{A}}$ is not in $\mathcal{X}$. Expand $\mathcal{A}$ to be a model $\mathcal{A}\varphi$ of T^{φ} by letting $\varphi_{\mathcal{A}\varphi}$ be $\mathcal{X}$. Then (7) is not valid in this model, and so is not a theorem of T^{φ}.

The conclusion to be drawn from this argument is that it is impossible to formalize the notion of number in such a way that the extremal clause holds.

Despite all the accumulated evidence to the contrary, mathematicians persist in believing in $\mathbb{N}$ as a real object existing independently of any formal human construction.

In a way this is not surprising. Mathematics as a deductive discipline was invented by Pythagoras, possibly with some influence from Thales. The Pythagorean religion held that all is number, that the numbers are pre-existing and independent of human thought. Plato was strongly influenced by Pythagoras and has been called the greatest of the Pythagoreans.

Over two and a half millennia after Pythagoras, most mathematicians continue to hold a religious belief in $\mathbb{N}$ as an object existing independently of formal human construction.

Against Finitism

There is obviously something inelegant about making arithmetic depend on set theory. What today is called *Peano Arithmetic* (P) is the theory whose nonlogical symbols are the constant 0, the unary function symbol S, and the binary function symbols + and $\cdot$, and whose nonlogical axioms are

$$\mathrm{S}x \neq 0 \tag{8}$$

$$\mathrm{S}x = \mathrm{S}y \quad \rightarrow \quad x = y \tag{9}$$

$$x + 0 = x \tag{10}$$

$$x + \mathrm{S}y = \mathrm{S}(x + y) \tag{11}$$

$$x \cdot 0 = 0 \tag{12}$$

$$x \cdot \mathrm{S}y = (x \cdot y) + x \tag{13}$$

and all *induction formulas*

$$\mathrm{A}_{\mathrm{x}}(0) \quad \& \quad \forall \mathrm{x}\,[\,\mathrm{A} \rightarrow \mathrm{A}_{\mathrm{x}}(\mathrm{Sx})\,] \quad \rightarrow \quad \mathrm{A} \tag{14}$$

where A is any formula in the language of P.

How is the induction axiom scheme (14) justified?

Assume the *basis* $\mathrm{A}_{\mathrm{x}}(0)$ and the *induction step* $\forall \mathrm{x}\,[\,\mathrm{A} \rightarrow \mathrm{A}_{\mathrm{x}}(\mathrm{Sx})\,]$. Then for any numeral $\mathrm{S}\ldots\mathrm{S}0$ we can prove $\mathrm{A}_{\mathrm{x}}(\mathrm{S}\ldots\mathrm{S}0)$ in $\mathrm{S}\ldots\mathrm{S}0$ steps without using induction.

The usual belief is that any number is denoted by a numeral, so that induction applies to any number, but as we saw in the preceding section this belief is inexpressible or meaningless. And if this were all that there is to induction, why bother to postulate it?

But the use of induction goes far beyond the application to numerals. If there were a completed infinity $\mathbb{N}$ consisting of all numbers, then the axioms of P would be true assertions about numbers and P would be consistent.

It is not a priori obvious that P can express combinatorics, but this is well known thanks to Gödel's great paper on incompleteness. As a consequence, exponentiation $\uparrow$ and superexponentiation $\Uparrow$ can be defined in P so that we have

(15) $x \uparrow 0 = \mathrm{S}0$

(16) $x \uparrow \mathrm{S}y = x \cdot (x \uparrow y)$

(17) $x \Uparrow 0 = \mathrm{S}0$

(18) $x \Uparrow \mathrm{S}y = x \uparrow (x \Uparrow y)$

and similarly for primitive-recursive functions in general.

Finitists believe that primitive recursions always terminate; for example, that applying (10)–(13) and (15)–(18) a sufficient number of times,

$$\mathrm{SS0} \Uparrow \mathrm{SS0} \Uparrow \mathrm{SS0} \Uparrow \mathrm{SS0} \Uparrow \mathrm{SS0} \Uparrow \mathrm{SS0} \Uparrow \mathrm{SS0} \Uparrow \mathrm{SS0} \Uparrow \mathrm{SS0} \Uparrow \mathrm{SS0} \Uparrow \mathrm{SS0} \Uparrow \mathrm{SS0} \Uparrow \mathrm{SS0} \Uparrow \mathrm{SS0} \Uparrow \mathrm{SS0} \Uparrow \mathrm{SS0}$$

reduces to a numeral. (Infix symbols are associated from right to left.)

But the putative number of times these rules must be applied can only be expressed by means of a superexponential expression—the argument is circular.

The objection to regarding variable-free superexponential terms as denoting numbers is not a naive feeling that they are too big. Rather, there is a *structural* problem with them.

Recapitulation:

We take the extremal clause seriously: something is a number only if it can be proved to be a number by (i) zero is a number, and (ii) the successor of a number is a number.

We cannot formalize this within any theory. Instead, we adjoin a unary predicate symbol φ and the axioms

(5) $\varphi(0)$

(6) $\varphi(x) \quad \rightarrow \quad \varphi(\mathrm{S}x).$

and if we have proved $\varphi(\mathrm{d})$ we say that d is a number. In this way we express the extremal clause by a combination of the formal and the genetic.

We cannot prove

$$\varphi(x_1) \quad \& \quad \varphi(x_2) \quad \rightarrow \quad \varphi(x_1 + x_2).$$

That is, if we take the extremal clause at face value, we cannot prove that the sum of two numbers is a number.

To see this, we again argue semantically. Consider again the non-standard number e in our structure $\mathcal{A}$, but now let $\mathcal{X}$ be the set of all individuals of the form $\mathrm{e}_{\mathcal{A}} + \xi$ where ξ is standard—that is, of the form $\mathcal{A}(\mathrm{S} \ldots \mathrm{S}0)$—and let $\varphi_{\mathcal{A}_\varphi}$ be $\mathcal{X}$. Then $\varphi(\mathrm{e})$ is true in the structure but $\varphi(\mathrm{e} + \mathrm{e})$ is not.

But we can do something almost as good.

Assuming the associative, distributive, and commutative laws and the usual properties of $\leq$, we can establish the following *relativization scheme.* Introduce

$$(19) \quad \varphi^0(x) \quad \leftrightarrow \quad \forall y\,[\, y \leq x \rightarrow \varphi(y)\,]$$

$$(20) \quad \varphi^1(x) \quad \leftrightarrow \quad \forall y\,[\, \varphi^0(x) \rightarrow \varphi^0(y + x)\,]$$

$$(21) \quad \varphi^2(x) \quad \leftrightarrow \quad \forall y\,[\, \varphi^1(y) \rightarrow \varphi^1(y \cdot x)\,].$$

Then φ^2 is not only inductive but respects $+$ and $\cdot$ and is hereditary, and it is stronger than φ. That is, we have the following theorem (proved without using induction, of course, which is not available for φ).

$$(22) \quad \varphi^2(0) \quad \& \quad [\,\varphi^2(x) \rightarrow \varphi^2(\mathrm{S}x)\,] \quad \&$$

$$[\,\varphi^2(x_1)\ \&\ \varphi^2(x_2) \rightarrow \varphi^2(x_1 + x_2)\ \&\ \varphi^2(x_1 \cdot x_2)\,] \ \ \&$$

$$[\,\varphi^2(x)\ \&\ y \leq x \rightarrow \varphi^2(y)\,] \quad \&$$

$$[\,\varphi^2(x) \rightarrow \varphi(x)\,].$$

The use of relativization schemes permits an extensive development of arithmetic staying within the world of numbers—numbers x satisfying $\varphi(x)$.

Associativity is essential to the relativization scheme. For example, suppose that
$\varphi^2(x_1)$ & $\varphi^2(x_2)$; we want to prove $\varphi^2(x_1 \cdot x_2)$.

Suppose that $\varphi^1(y)$; by (21), we need to prove that

$$\varphi^1\big(y \cdot (x_1 \cdot x_2)\big).$$

But we have $\varphi^1(y \cdot x_1)$ by (21) and so
$\varphi^1\big((y \cdot x_1) \cdot x_2\big)$, again by (21). By the associativity of multiplication we have the desired result.

Exponentiation is not associative, so we cannot extend the relativization scheme, in the first way one would think of, to include exponentiation. In fact, one can prove the following theorem:

Let T *be any consistent theory containing the axioms* (8)–(13) *and* (15)–(18) *(the usual axioms for* 0 S $+$ $\cdot$ $\uparrow$ *and* $\Uparrow$*) and the usual defining axiom for* $\leq$*. Then there is no unary predicate symbol* φ^3 *in an extension by definitions* T' *of* T^φ *such that*

$$(23) \quad \vdash_{\mathrm{T}'} \ \varphi^3(0) \quad \& \quad [\,\varphi^3(x) \rightarrow \varphi^3(\mathrm{S}x)\,] \quad \&$$

$$[\,\varphi^3(x_1) \mathbin{\&} \varphi^3(x_2) \rightarrow \varphi^3(x_1 + x_2) \mathbin{\&} \varphi^3(x_1 \cdot x_2) \mathbin{\&}$$

$$\varphi^3(x_1 \uparrow x_2)\,] \quad \&$$

$$[\,\varphi^3(x) \mathbin{\&} y \leq x \rightarrow \varphi^3(y)\,] \quad \&$$

$$[\,\varphi^3(x) \rightarrow \varphi(x)\,].$$

That is, we cannot construct a world of numbers, within the world of those satisfying the extremal clause (those satisfying φ), that is closed under exponentiation. If the extremal clause is taken seriously, the conclusion is that exponentiation is not total.

The proof is based on a study of the algorithm for eliminating special constants in the proof of the Hilbert-Ackermann Consistency Theorem. This algorithm is essentially a quantifier-elimination procedure, and it is superexponentially long but only superexponentially long.

The method of proof also yields this:

With the same hypotheses, there is no unary φ^4 *such that*

(24) $\vdash_{\mathrm{T}'}$ $\varphi^4(0)$ & $[\,\varphi^4(x) \rightarrow \varphi^4(\mathrm{S}x)\,]$ & $[\,\varphi^4(x) \rightarrow \varphi(\mathrm{SS0} \Uparrow x)\,]$.

If we take the extremal clause seriously, the conclusion is that even if $2 \Uparrow \mathrm{d}$ happens to be a number, satisfying $\varphi(2 \Uparrow \mathrm{d})$, there is no general method for proving that the same holds for $2 \Uparrow \mathrm{Sd}$. That is, there is no reason to believe that every explicit superexponential recursion terminates.

The Goal

The goal is to produce an explicit superexponentially long recursion and prove that it does not terminate, thereby disproving Church's Thesis from below, demonstrating that finitism is untenable, and proving that Peano Arithmetic is inconsistent.

Do you wish me luck?

Material relevant to this talk is in *Predicative Arithmetic*, posted online at

www.math.princeton.edu/~nelson/books/pa.pdf

This talk is posted at

`www.math.princeton.edu/~nelson/papers/hm.pdf`