Nonstandard Models of Number Theory:
Why not expect an iPhone app for them?

Victoria Gitman

City University of New York

vgitman@nylogic.org
http://websupport1.citytech.cuny.edu/faculty/vgitman

March 16, 2010
Euclid and the Axiomatic Method

Around 300 BC, Euclid revolutionized how mathematics is done with the introduction of the axiomatic method.

- In his treatise on geometry, *Elements*, propositions are proved using rules of logical inference from a small collection of “obviously true” statements - axioms.
- Euclid’s crucial assumption was that the axioms capture ALL geometrical truths: every true geometrical statement must follow logically from the axioms.

Was Euclid right about this?
The Axioms of Number Theory

Ancient Greek mathematicians, including Euclid, made the earliest contributions to number theory: the study of the properties of natural numbers \( \mathbb{N} = \{0, 1, 2, \ldots\} \) with

- operations: \(+, \cdot\)
- ordering \(\lt\)

Many of the greatest contributions followed nearly 2 millennia later in the period 16 – 19th century (Fermat, Euler, Gauss, etc.).

But not until the 19th century did mathematicians become concerned with explicitly formulating the axioms of number theory.

The 19th century saw a strong revival of formal mathematics that would continue well into the beginning of the 20th century.

In 1889, Giuseppe Peano (1858-1932) proposed the Peano Axioms (PA) for number theory. The Peano Axioms summarized:

- fundamental properties of \(+, \cdot, \lt\)
- induction
The Peano Axioms: modern formulation

Peano Axioms

Addition and Multiplication

- \( \forall x \forall y \forall z \ (x + y) + z = x + (y + z) \) (associativity of addition)
- \( \forall x \forall y \ x + y = y + x \) (commutativity of addition)
- \( \forall x \forall y \forall z \ (x \cdot y) \cdot z = x \cdot (y \cdot z) \) (associativity of multiplication)
- \( \forall x \forall y \ x \cdot y = y \cdot x \) (commutativity of multiplication)
- \( \forall x \forall y \forall z \ x \cdot (y + z) = x \cdot y + x \cdot z \) (distributive law)
- \( \forall x \ (x + 0 = x \land x \cdot 1 = x) \) (additive and multiplicative identity)
Peano Axioms (continued)

**Order**
- $\forall x \forall y \forall z ((x < y \land y < z) \rightarrow x < z)$ (the order is transitive)
- $\forall x \lnot x < x$ (the order is anti-reflexive)
- $\forall x \forall y ((x < y \lor y = x) \lor y < x)$ (any two elements are comparable)
- $\forall x \forall y \forall z (x < y \rightarrow x + z < y + z)$ (order respects addition)
- $\forall x \forall y \forall z ((0 < z \land x < y) \rightarrow x \cdot z < x \cdot z)$ (order respects multiplication)
- $\forall x \forall y (x < y \leftrightarrow \exists z (z > 0 \land x + z = y))$
- $\forall x (x \geq 0 \land (x > 0 \rightarrow x \geq 1))$ (the order is discrete)

**Induction Scheme**

For every statement $\varphi(x)$ we have
- $(\varphi(0) \land \forall x (\varphi(x) \rightarrow \varphi(x + 1))) \rightarrow \forall x \varphi(x)$
The Peano Axioms: key points and questions

- The Peano Axioms are formalized in the system of **first order logic**:
  - language of formal mathematics
  - rules of logical inference

- There are infinitely many induction axioms:
  - one for every number theoretic statement
  - first order logic allows quantification only over members of the structure
  - a number theoretic statement can quantify only over elements of \( \mathbb{N} \)

- Peano Axioms are **computable**:
  - we can write a computer program to recognize whether a string of symbols is a Peano axiom
  - this is an inherent property of any axiom system defined by human beings

- Do the Peano Axioms satisfy Euclid’s “crucial assumption”?
  Can every true statement about the natural numbers be proved by logical inference from the Peano Axioms?
Tarski and Euclid’s Axioms

Alfred Tarski (1901-1983) reformulated Euclid’s axioms in first order logic.

**Theorem (Tarski, 1930?)**

- *Every true geometric statement can be proved from Euclid’s axioms.*
- *The proof procedure is algorithmic: we can write a computer program to decide whether a given geometric statement is true or false (caveat: the program might take a couple billion years to answer!).*

So Euclid is vindicated!

But what about the axiomatic method in general?
Gödel and the Peano Axioms

Kurt Gödel (1906-1978) proved that number theory is too informationally rich to be captured algorithmically: by a computable collection of axioms.

Theorem (Gödel’s First Incompleteness Theorem, 1931)

- There is a true number theoretic statement that cannot be proved from PA.
- Every consistent computable collection of axioms extending PA is incomplete: there is a statement that can be neither proved nor disproved from the axioms.

Gödel’s theorem forces a philosophical reformulation of the axiomatic method.

This leads to the modern view of axioms as “constraints” rather than “obvious truths” from which all other truths follow.
Nonstandard models of the Peano Axioms

- A model of PA is a set with:
  - the operations: +, ·
  - ordering <
  satisfying the Peano Axioms.
- The natural numbers: \((\mathbb{N}, +, \cdot, <, 0, 1)\) is called the standard model of PA.
- A nonstandard model of PA is any model of PA other than \((\mathbb{N}, +, \cdot, <, 0, 1)\).

By Gödel’s incompleteness theorem, there is a true number theoretic statement \(\varphi\) that cannot be proved from PA.

**Theorem:** If a statement \(\psi\) can be neither proved nor disproved from a collection of axioms \(T\), then \(T\) together with \(\psi\) is consistent.

**Theorem:** Every consistent collection of axioms has a model of every infinite cardinality.

**Conclusion:** There is a countable model \(M\) of PA in which \(\neg \varphi\) is true.

Clearly \(M\) is nonstandard!

What does \(M\) look like?
The ordering on a countable nonstandard model of PA

- $\mathbb{N}$ is the initial segment $M$ (any model of PA).
The ordering on a countable nonstandard model of PA

\[ \mathbb{N} \text{ is the initial segment } M \text{ (any model of PA).} \]
The ordering on a countable nonstandard model of PA

- \( \mathbb{N} \) is the initial segment \( M \) (any model of PA).
- \( M \) must have an element \( c > \mathbb{N} \).
The ordering on a countable nonstandard model of PA

- \( \mathbb{N} \) is the initial segment \( M \) (any model of PA).
- \( M \) must have an element \( c > \mathbb{N} \).
The ordering on a countable nonstandard model of PA

- $\mathbb{N}$ is the initial segment $M$ (any model of PA).
- $M$ must have an element $c > \mathbb{N}$.
- $M$ must have $c + 1, c + 2, c + 3, \ldots$ as well as $c - 1, c - 2, c - 3, \ldots$.
The ordering on a countable nonstandard model of PA

- \( \mathbb{N} \) is the initial segment \( M \) (any model of PA).
- \( M \) must have an element \( c > \mathbb{N} \).
- \( M \) must have \( c + 1, c + 2, c + 3, \ldots \) as well as \( c - 1, c - 2, c - 3, \ldots \).
The ordering on a countable nonstandard model of PA

- \( \mathbb{N} \) is the initial segment \( M \) (any model of PA).
- \( M \) must have an element \( c > \mathbb{N} \).
- \( M \) must have \( c + 1, c + 2, c + 3, \ldots \) as well as \( c - 1, c - 2, c - 3, \ldots \).
- \( M \) must have \( 2c: 2c > c + n \) for all \( n \in \mathbb{N} \).

\[ \underbrace{\cdots}_{\text{\( c \)}} \quad \underbrace{\cdots}_{\text{\( \mathbb{N} \)}} \]
The ordering on a countable nonstandard model of PA

- $\mathbb{N}$ is the initial segment $M$ (any model of PA).
- $M$ must have an element $c > \mathbb{N}$.
- $M$ must have $c + 1, c + 2, c + 3, \ldots$ as well as $c - 1, c - 2, c - 3, \ldots$.
- $M$ must have $2c$: $2c > c + n$ for all $n \in \mathbb{N}$.
The ordering on a countable nonstandard model of PA

- \( \mathbb{N} \) is the initial segment \( M \) (any model of PA).
- \( M \) must have an element \( c > \mathbb{N} \).
- \( M \) must have \( c + 1, c + 2, c + 3, \ldots \) as well as \( c - 1, c - 2, c - 3, \ldots \).
- \( M \) must have \( 2c: 2c > c + n \) for all \( n \in \mathbb{N} \).
- If we assume \( c \) is even, then \( M \) must have \( \frac{c}{2} : \frac{c}{2} < c - n \) for all \( n \in \mathbb{N} \).
The ordering on a countable nonstandard model of PA

- \( \mathbb{N} \) is the initial segment \( M \) (any model of PA).
- \( M \) must have an element \( c > \mathbb{N} \).
- \( M \) must have \( c + 1, c + 2, c + 3, \ldots \) as well as \( c - 1, c - 2, c - 3, \ldots \).
- \( M \) must have \( 2c: 2c > c + n \) for all \( n \in \mathbb{N} \).
- If we assume \( c \) is even, then \( M \) must have \( \frac{c}{2}: \frac{c}{2} < c - n \) for all \( n \in \mathbb{N} \).
The ordering on a countable nonstandard model of PA

- \( \mathbb{N} \) is the initial segment \( M \) (any model of PA).
- \( M \) must have an element \( c > \mathbb{N} \).
- \( M \) must have \( c + 1, c + 2, c + 3, \ldots \) as well as \( c - 1, c - 2, c - 3, \ldots \).
- \( M \) must have \( 2c: 2c > c + n \) for all \( n \in \mathbb{N} \).
- If we assume \( c \) is even, then \( M \) must have \( \frac{c}{2}: \frac{c}{2} < c - n \) for all \( n \in \mathbb{N} \).
- If we assume \( c \) is even, then \( M \) must have \( \frac{3c}{2}: \frac{3c}{2} > c + n \) for all \( n \in \mathbb{N} \) and \( \frac{3c}{2} < 2c - n \) for all \( n \in \mathbb{N} \).
The ordering on a countable nonstandard model of PA

- \( \mathbb{N} \) is the initial segment \( M \) (any model of PA).
- \( M \) must have an element \( c > \mathbb{N} \).
- \( M \) must have \( c + 1, c + 2, c + 3, \ldots \) as well as \( c - 1, c - 2, c - 3, \ldots \).
- \( M \) must have \( 2c: 2c > c + n \) for all \( n \in \mathbb{N} \).
- If we assume \( c \) is even, then \( M \) must have \( \frac{c}{2}: \frac{c}{2} < c - n \) for all \( n \in \mathbb{N} \).
- If we assume \( c \) is even, then \( M \) must have \( \frac{3c}{2} \):
  - \( \frac{3c}{2} > c + n \) for all \( n \in \mathbb{N} \) and \( \frac{3c}{2} < 2c - n \) for all \( n \in \mathbb{N} \).

\[
\begin{align*}
\cdots & \quad \left( \underbrace{\cdots}_{\frac{c}{2}} \right) \quad \left( \underbrace{\cdots}_{c} \right) \quad \left( \underbrace{\cdots}_{\frac{3c}{2}} \right) \quad \left( \underbrace{\cdots}_{2c} \right) \\
\end{align*}
\]
The ordering on a countable nonstandard model of PA

- \( \mathbb{N} \) is the initial segment \( M \) (any model of PA).
- \( M \) must have an element \( c > \mathbb{N} \).
- \( M \) must have \( c + 1, c + 2, c + 3, \ldots \) as well as \( c - 1, c - 2, c - 3, \ldots \).
- \( M \) must have \( 2c: 2c > c + n \) for all \( n \in \mathbb{N} \).
- If we assume \( c \) is even, then \( M \) must have \( \frac{c}{2}: \frac{c}{2} < c - n \) for all \( n \in \mathbb{N} \).
- If we assume \( c \) is even, then \( M \) must have \( \frac{3c}{2}: \frac{3c}{2} > c + n \) for all \( n \in \mathbb{N} \) and \( \frac{3c}{2} < 2c - n \) for all \( n \in \mathbb{N} \).

\[
\begin{array}{cccccc}
\cdots & \cdots & \cdots & \cdots & \cdots \\
\frac{c}{2} & c & \frac{3c}{2} & 2c & \cdots \\
\mathbb{N} & \cdots & \mathbb{Z} & \cdots & \mathbb{Z} & \cdots \\
\end{array}
\]

\[ \mathbb{Q} \text{ many copies of } \mathbb{Z} \]
The ordering on a countable nonstandard model of PA

- $\mathbb{N}$ is the initial segment $M$ (any model of PA).
- $M$ must have an element $c > \mathbb{N}$.
- $M$ must have $c + 1, c + 2, c + 3, \ldots$ as well as $c - 1, c - 2, c - 3, \ldots$.
- $M$ must have $2c$: $2c > c + n$ for all $n \in \mathbb{N}$.
- If we assume $c$ is even, then $M$ must have $\frac{c}{2}$: $\frac{c}{2} < c - n$ for all $n \in \mathbb{N}$.
- If we assume $c$ is even, then $M$ must have $\frac{3c}{2}$: $\frac{3c}{2} > c + n$ for all $n \in \mathbb{N}$ and $\frac{3c}{2} < 2c - n$ for all $n \in \mathbb{N}$.

\[ \begin{array}{cccc}
\ldots & (\ldots & \ldots & \ldots) \\
\frac{c}{2} & c & \frac{3c}{2} & 2c \\
\ldots & (\ldots & \ldots & \ldots) \\
\end{array} \]

\[ \begin{array}{cccc}
\ldots & \ldots & \ldots & \ldots \\
\mathbb{N} & \mathbb{Z} & \mathbb{Z} & \mathbb{Z} \\
\end{array} \]

**Brain Teaser:** The Peano Axioms imply that every subset has a least element but clearly this is not true!
An iphone app for nonstandard models of PA

Fundamentally a computer algorithm manipulates natural numbers. In order for a computer to manipulate other objects (letters, pictures), they have to be coded by natural numbers.

Can we assign a number to every element of a countable nonstandard model of PA in a way that preserves information about its structure?

Can we have a computing device adding and multiplying nonstandard numbers?
The ordering is computable

**Fact:** Cantor’s pairing function \( f(x, y) = \frac{(x + y)(x + y + 1)}{2} + y \) is a bijection between \( \mathbb{N} \) and \( \mathbb{N} \times \mathbb{N} \).

- Each \( \mathbb{Z} \)-copy is indexed by a rational number.
- Index each \( \mathbb{Z} \)-copy by a natural number using Cantor’s pairing function.
- Index \( \mathbb{N} \) with one of the left-over numbers.
- If \( p_n \) is the \( n \)th prime number, index \( n \)th \( \mathbb{Z} \)-copy using powers of \( p_n \):
  - \( p_n \) is 0, \( p_n^{2a} \) index the positive part, and \( p_n^{2a+1} \) index the negative part.

We can write a computer program to decide when \( p_n^a \leq p_m^b \) in the ordering of the nonstandard model:

- If \( n = m \), compare powers \( a \) and \( b \).
- Else find \( f(x, y) = n \) and \( f(v, w) = m \).
- Check whether \( \frac{x}{y} < \frac{v}{w} \).

The ordering of a nonstandard model of PA is **computable**.

Is there a nonstandard model of PA for which the operations \(+\) and \(\cdot\) are computable?
Stanley Tennenbaum (1927-2005) proved that the addition and multiplication of a nonstandard model of PA codes information that cannot be accessed algorithmically!

**Theorem (Tennenbaum, 1959)**

The addition and multiplication of a nonstandard model of PA are NEVER computable.
Standard systems of nonstandard models of PA

- Every natural number codes a finite subset of \( \mathbb{N} \) through its binary expansion: 
  \[
  1288_{10} = 2^3 + 2^8 + 2^{10} = 10100001000_2 
  \]
codes the set \( \{3, 8, 10\} \).

- Every element of a nonstandard model of PA codes a possibly infinite subset of \( \mathbb{N} \) through the restriction of its binary expansion to powers in \( \mathbb{N} \):
  \[
  c = 2^1 + 2^3 + 2^5 + \ldots + 2^{2^b} = 101010\ldots)(\ldots1010101\ldots)(\ldots1010102.
  \]

**Definition (Friedman, 1973)**

The standard system of a nonstandard model of PA consists of all the subsets of \( \mathbb{N} \) coded by elements of the model.
**Standard systems: key points and questions**

- **Different** nonstandard models of PA have **different** elements and therefore **different** standard systems.
- Certain subsets of $\mathbb{N}$ are in the standard system of **every** nonstandard model of PA.
  - A standard system is a collection of subsets of the natural numbers.
  - $\mathbb{N}$ is in every standard system:
    - every nonstandard model of PA has an element $a$ whose binary expansion contains $2^n$ for every $n \in \mathbb{N}$.
    - Use induction on the statement:
      - $\varphi(x)$ - there is $y$ whose binary expansion has all powers of 2 less than $x$.
  - The **set of all even numbers** is in every standard system:
    - every nonstandard model of PA has an element $a$ whose binary expansion contains $2^{2n}$ but not $2^{2n+1}$ for every $n \in \mathbb{N}$.
    - Use induction on the statement:
      - $\varphi(x)$ - there is $y$ whose binary expansion contains exactly the even powers of 2 less than $x$.

What general properties do standard systems possess?
Boolean algebras and computable sets

Definitions:

- A collection of subsets of $\mathbb{N}$ is a **Boolean algebra** if it is closed under union, intersection, and complement.
- A set $A \subseteq \mathbb{N}$ is **computable** if there is an algorithm that returns 1 whenever $n \in A$ and 0 otherwise.
- A set $A \subseteq \mathbb{N}$ is **computable relative to** another set $B \subseteq \mathbb{N}$ if it is computable with an **oracle** for $B$.
  - Idea: there is an algorithm to retrieve $A$ from $B$.
  - Example: the complement of $B$ is always computable relative to $B$.
- A collection $\mathcal{I}$ of subsets of $\mathbb{N}$ is **closed under relative computability** if whenever $B \in \mathcal{I}$ and $A$ is computable relative to $B$, then $A \in \mathcal{I}$.

Examples:

- The collection $\mathcal{C}$ of all computable subsets of $\mathbb{N}$ is
  - a Boolean algebra
  - closed under relative computability
- Any nonempty collection $\mathcal{I}$ closed under relative computability must contain all the computable sets.
Binary trees

- The collection of all finite binary sequences ordered by end extension is a full binary tree.
The collection of all finite binary sequences ordered by end extension is a **full binary tree**.
Binary trees

- The collection of all finite binary sequences ordered by end extension is a **full binary tree**.
- A **binary tree** is a subset of the full binary tree that is closed downwards.
Binary trees

- The collection of all finite binary sequences ordered by end extension is a **full binary tree**.
- A **binary tree** is a subset of the full binary tree that is closed downwards.
Binary trees

- The collection of all finite binary sequences ordered by end extension is a full binary tree.
- A binary tree is a subset of the full binary tree that is closed downwards.

**Theorem (König’s Lemma, 1936)**

*Every infinite binary tree has an infinite branch.*

- A binary tree can be coded by a subset of \( \mathbb{N} \).
- A collection of subsets of \( \mathbb{N} \) has the tree property if whenever it contains a set coding a binary tree, it also contains a set coding one of its branches.

Does the collection \( \mathcal{C} \) of all computable sets have the tree property?
Properties of standard systems

**Theorem (Scott, 1962)**

The standard system of a nonstandard model of PA

- is a Boolean algebra
- is closed under relative computability
- has the tree property

**Theorem (Scott, 1962)**

Any countable collection of subsets of $\mathbb{N}$ satisfying the three properties above is realized as the standard system of a nonstandard model of PA.

**Summary:**

- It follows that the standard system of a nonstandard model of PA contains all computable sets.
- Is the collection $\mathcal{C}$ of all computable sets the standard system of a nonstandard model of PA?
- It comes down to: Does $\mathcal{C}$ have the tree property?
A computable tree with no computable branches

Here is an algorithm to build a binary tree $T$

- **Computably** index all number theoretic statements of first order logic:
  $\varphi_0, \varphi_1, \varphi_2, \ldots$

- **Computably** index all the Peano Axioms:
  $\psi_0, \psi_1, \psi_2, \ldots$

- define $\varphi^i_n = \begin{cases} \varphi_n & \text{if } i = 1 \\ \neg \varphi_n & \text{if } i = 0 \end{cases}$

- for every binary sequence $s$ of length $l$, associate the sequence of number theoretic statements $\varphi^{s(0)}_0, \varphi^{s(1)}_1, \ldots, \varphi^{s(l-1)}_{l-1}$

- a binary sequence $s$ of length $l$ is good if there is no proof of a contradiction from the sequence $\varphi^{s(0)}_0, \varphi^{s(1)}_1, \ldots, \varphi^{s(l-1)}_{l-1}$ together with $\psi_0, \ldots, \psi_{l-1}$ of length $\leq l$

- $T$ consists of all good sequences $s$

Every branch of the tree $T$ gives a consistent collection of number theoretic statements extending PA and containing every statement or its negation!

By Gödel’s incompleteness theorem, $T$ cannot have a computable branch!
Proof of Tennenbaum’s Theorem

● Every standard system has a **non-computable** set!

● If we could index elements of a nonstandard model of PA, $M$, with numbers and compute its $+$ and $\cdot$, then every set in the standard system of $M$ would be computable!

   ▶ If $A$ is in the standard system of $M$, then there is $a \in M$ whose binary expansion contains $2^n$ exactly for $n \in A$.

   ▶ To determine if $0 \in A$, check whether $a$ is odd or even:
      search for an element $b$ such that either $2b = a$ or $2b + 1 = a$.

   ▶ Let $a_1 = \begin{cases} 
   a & \text{if } a \text{ is even} \\
   a - 1 & \text{if } a \text{ is odd} 
   \end{cases}$

   ▶ To determine if $1 \in A$, check whether $a_1$ is divisible by $2^2$.

   ▶ Let $a_2 = \begin{cases} 
   a_1 & \text{if } a \text{ is not divisible by } 2^2 \\
   a_1 - 2^2 & \text{if } a \text{ is divisible by } 2^2 
   \end{cases}$

   ▶ To determine if $2 \in A$, check whether $a_2$ is divisible by $2^3$.

   ▶ Let $a_3 = \begin{cases} 
   a_2 & \text{if } a \text{ is not divisible by } 2^3 \\
   a_2 - 2^3 & \text{if } a \text{ is divisible by } 2^3 
   \end{cases}$

   $\vdots$