An iPhone app for a nonstandard model of number theory?

Victoria Gitman

City University of New York

vgitman@nylogic.org
http://boolesrings.org/victoriagitman

February 14, 2012

Euclid and the Axiomatic Method

Around 300 BC, Euclid revolutionized mathematics 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 from the axioms.

Did Euclid get it right?

Axiomatizing Number Theory

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

- operations: $+$, $\cdot$,
- ordering: $<$.

Many of the greatest contributions followed nearly 2 millennia later in the period 16-19$^{\text{th}}$ century (Fermat, Euler, Gauss, etc.).

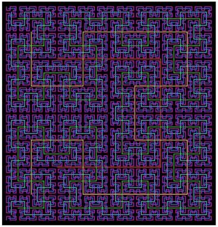
But not until the 19th century did mathematicians become concerned with explicitly formulating the axioms of number theory.

The 19$^{\text{th}}$ century saw a strong revival of formal mathematics that would continue well into the beginning of the 20$^{\text{th}}$ century.

In 1889, Giuseppe Peano (1858-1932) proposed the Peano Axioms (PA):

- fundamental properties of $+$, $\cdot$, $<$,
- 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)
- $\forall x\ (x+0 = x \wedge x \cdot 1 = x)$ (additive and multiplicative identity)

Peano Axioms (continued)

Order

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

Induction Scheme

For every statement $\varphi(x)$:

- $(\varphi(0) \wedge \forall x\ (\varphi(x) \rightarrow \varphi(x+1))) \rightarrow \forall x \varphi(x)$

The Peano Axioms: comments and questions

- The Peano Axioms are formalized in first-order logic:
  - formulated by Thoralf Skolem in the early 20^{th} century
  - alphabet+grammer of formal mathematics
  - rules of logical inference
- The induction scheme consists of infinitely many axioms:
  - one for every number theoretic statement
  - first-order logic does not allow quantification over subsets of the model (equivalently, over number theoretic statements)
- The Peano Axioms are computable:
  - there is an algorithm to recognize whether a string of symbols is a Peano axiom
  - this is an inherent property of any axiom system defined by human beings
- Every familiar theorem of number theory follows from the Peano Axioms, e.g.,
  - divisibility
  - infinitude of prime numbers
- Do the Peano Axioms satisfy Euclid's "crucial assumption"?
  Does every true number theoretic statement follow from the Peano Axioms?

Tarski and Euclid's Axioms

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

Theorem (Tarski, 1930's)

- *Every true geometric statement follows from Euclid's axioms.*
- *There is an algorithm to decide whether a given geometric statement is true or false (caveat: the algorithm might take a couple billion years to answer!).*

So Euclid is vindicated!

But what about Peano?

Gödel and the Peano Axioms

Kurt Gödel (1906-1978) proved that number theory is too informationally rich to be captured 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 statements extending PA is incomplete: there is a statement that can be neither proved nor disproved from this collection.*

- 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 *M* with:
  - the operations: $+^M$, $\cdot^M$
  - ordering $<^M$

  satisfying the Peano Axioms.
- The natural numbers: $(\mathbb{N}, +, \cdot, <)$ is the standard model of PA.
- All others are nonstandard.

By Gödel's incompleteness theorem, there is a true number theoretic statement φ that cannot be proved from PA.

Theorem: (fol) If a statement ψ can be neither proved nor disproved from a collection of statements *T*, then *T* together with $\neg\psi$ is consistent.
Theorem: (fol) Every consistent collection of statements 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!

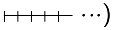
What does *M* look like?

The order on a countable nonstandard model of PA

- $\mathbb{N}$ is the initial segment of M.

The order on a countable nonstandard model of PA

- $\mathbb{N}$ is the initial segment of M.



The order on a countable nonstandard model of PA

- $\mathbb{N}$ is the initial segment of *M*.
- *M* must have an element $c > \mathbb{N}$.

$\vdash\!\!+\!\!+\!\!+\!\!+\!\!- \cdots)$

The order on a countable nonstandard model of PA

- $\mathbb{N}$ is the initial segment of *M*.
- *M* must have an element $c > \mathbb{N}$.

$\vdash\!\!+\!\!+\!\!+\!\!+\!\!- \cdots)$ $\qquad\qquad\qquad\qquad \underset{c}{|}$

The order on a countable nonstandard model of PA

- $\mathbb{N}$ is the initial segment of M.
- 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 order on a countable nonstandard model of PA

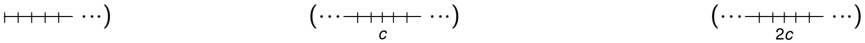
- $\mathbb{N}$ is the initial segment of M.
- M must have an element $c > \mathbb{N}$.
- M must have $c+1, c+2, c+3, \ldots$ as well as $c-1, c-2, c-3, \ldots$.

The order on a countable nonstandard model of PA

- $\mathbb{N}$ is the initial segment of M.
- 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 $n \in \mathbb{N}$.

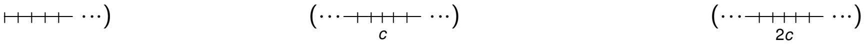
The order on a countable nonstandard model of PA

- $\mathbb{N}$ is the initial segment of M.
- 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 $n \in \mathbb{N}$.



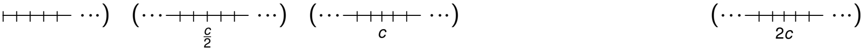
The order on a countable nonstandard model of PA

- $\mathbb{N}$ is the initial segment of M.
- 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 $n \in \mathbb{N}$



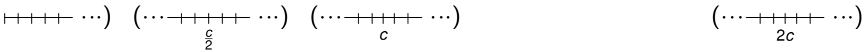
The order on a countable nonstandard model of PA

- $\mathbb{N}$ is the initial segment of M.
- 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 $n \in \mathbb{N}$



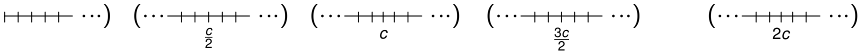
The order on a countable nonstandard model of PA

- $\mathbb{N}$ is the initial segment of M.
- 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 $n \in \mathbb{N}$.



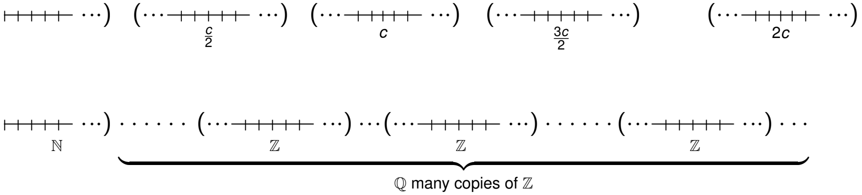
The order on a countable nonstandard model of PA

- $\mathbb{N}$ is the initial segment of M.
- 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 $n \in \mathbb{N}$.



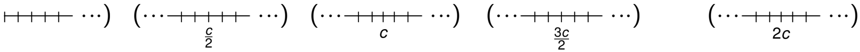
The order on a countable nonstandard model of PA

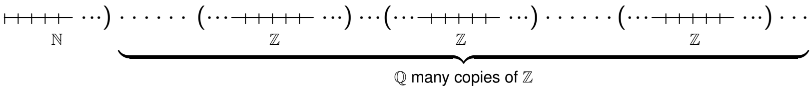
- $\mathbb{N}$ is the initial segment of M.
- M must have an element $c > \mathbb{N}$.
- M must have $c+1, c+2, c+3, \ldots$ as well as $c-1, c-2, c-3, \ldots$.
- M must have $2c$: $2c > c+n$ for all $n \in \mathbb{N}$.
- If we assume c is even, then M must have $\frac{c}{2}$: $\frac{c}{2} < c-n$ for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

- $\mathbb{N}$ is the initial segment of M.
- 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 $n \in \mathbb{N}$.





Brain Teaser: The Peano Axioms imply that every subset has a least element but clearly this is not true!

An iphone app for a nonstandard model of PA

Fundamentally, an algorithm manipulates natural numbers. In order for a computer to manipulate other objects (text, images), they must be coded by natural numbers.

Can we code elements of a countable nonstandard model of PA by natural numbers? Theoretically YES, since the model is countable.

Can we have a computing device adding and multiplying nonstandard numbers?

Coding a nonstandard model by natural numbers: a sensible approach

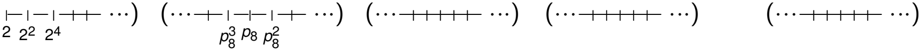
Step 1: Assign a natural number to every block of M ($\mathbb{N}$ or $\mathbb{Z}$).

- Assign 0 to the $\mathbb{N}$ block
- Assign a rational number in $(0,1)$ to every $\mathbb{Z}$ block (there are $\mathbb{Q}$ many)
- Assign a natural number to every $\mathbb{Z}$ block using Cantor's pairing function:

$$f(x,y) = \frac{(x+y)(x+y+1)}{2} + y$$

Step 2: Assign a natural number to every element of M.

- Consider a block indexed by the number n
- Let p_n be the n^{th} prime number.
- View the block as $\mathbb{Z}$ ($\mathbb{N}$)
- Assign the natural number p_n to 0 (of the block)
- Assign the natural number p_n^{2a} to a (of the block)
- Assign the natural number p_n^{2a-1} to $-a$ (of the block)



An app for the ordering?

The algorithm to decide when $p_n^a <_M p_m^b$:

- 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 M is computable!

Is there a nonstandard model of PA for which the operations $+^M$ and $\cdot^M$ are computable?

An app for addition and multiplication?

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 $\mathbb{N}$: $c = 2^1 + 2^3 + 2^5 + \ldots + 2^{2b+1} = 101010\ldots)\ldots(\ldots 1010101\ldots)\ldots(\ldots 101010_2$.

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: comments 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:

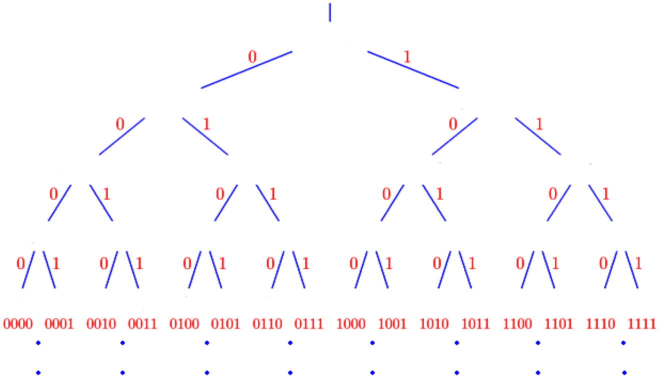
- A collection of subsets of $\mathbb{N}$ is a Boolean algebra if it is closed under union, intersection, and complement.
- A set $A \subseteq \mathbb{N}$ is computable if there is an algorithm that returns YES whenever $n \in A$ and NO otherwise.
- A set $A \subseteq \mathbb{N}$ is computable relative to another set $B \subseteq \mathbb{N}$ if it is computable with an 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 $\mathscr{S}$ of subsets of $\mathbb{N}$ is closed under relative computability if whenever $B \in \mathscr{S}$ and A is computable relative to B, then $A \in \mathscr{S}$.
- Any nonempty collection $\mathscr{S}$ 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.

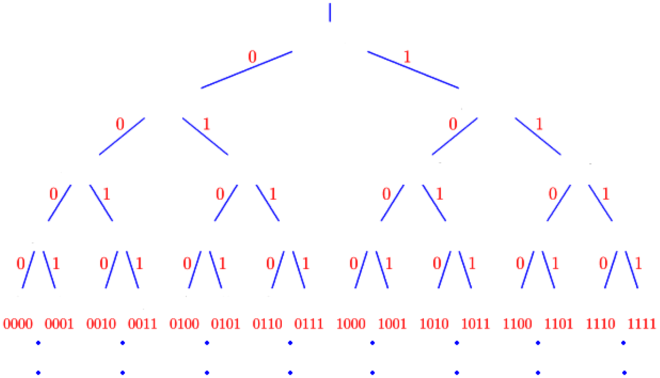
Binary trees

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



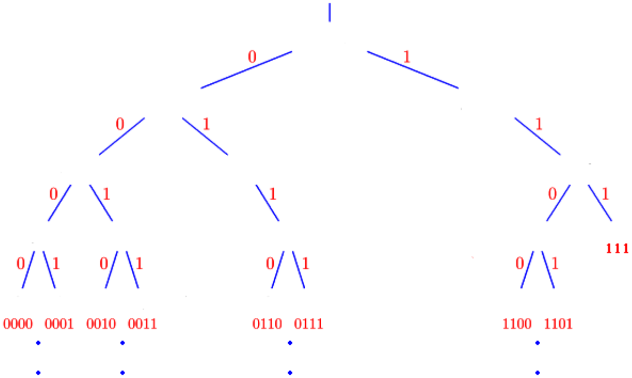
Binary trees

- 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 binary tree, it also an infinite branch of that tree.

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.*

Corollary

The standard system of a nonstandard model of PA contains all the computable sets.

What about non-computable sets?

A computable tree with no computable branches

Here is an algorithm to build a binary tree $\mathscr{T}$:

- Order all number theoretic statements of first-order logic: $\varphi_0, \varphi_1, \varphi_2, \ldots$
- Order all the Peano Axioms: $\psi_0, \psi_1, \psi_2, \ldots$
- define $\varphi_n^i = \begin{cases} \varphi_n & \text{if } i = 1 \\ \neg\varphi_n & \text{if } i = 0 \end{cases}$
- for every binary sequence s of length l, associate the sequence of number theoretic statements:
$$\varphi_0^{s(0)}, \varphi_1^{s(1)}, \ldots, \varphi_{l-1}^{s(l-1)}$$
- a binary sequence s of length l is good if there is no proof of a contradiction from the sequence
$$\varphi_0^{s(0)}, \varphi_1^{s(1)}, \ldots, \varphi_{l-1}^{s(l-1)} \text{ together with } \psi_0, \ldots, \psi_{l-1}$$
that uses at most l many symbols
- $\mathscr{T}$ consists of all good sequences s

Every branch of the tree $\mathscr{T}$ gives a consistent collection of number theoretic statements extending PA and containing every statement or its negation!
By Gödel's incompleteness theorem, $\mathscr{T}$ cannot have a computable branch!

Proof of Tennenbaum's Theorem

- Every standard system has a non-computable set!
- But, if we could code elements of a nonstandard model M of PA by natural numbers so that we could compute $+^M$ and $\cdot^M$, then every set in the standard system of M would be computable!
  - There is a divisibility algorithm: given a and b, it returns c, d such that $a = c \cdot^M b +^M d$ (perform a brute force search)
  - Using divisibility, there is an algorithm for determining binary expansions
  - Suppose A is in the standard system of M and fix a in M whose binary expansion contains 2^n exactly for $n \in A$.
  - Is $0 \in A$? Check whether a is odd or even!
  - Let $a_1 = \begin{cases} a & \text{if } a \text{ is even} \\ a-1 & \text{if } a \text{ is odd} \end{cases}$
  - Is $1 \in A$? Check whether a_1 is divisible by 2^2!
  - Let $a_2 = \begin{cases} a_1 & \text{if } a \text{ is not divisible by } 2^2 \\ a_1 - 2^2 & \text{if } a \text{ is divisible by } 2^2 \end{cases}$
  - Is $2 \in A$? Check whether a_2 is divisible by 2^3!
  - Let $a_3 = \begin{cases} a_2 & \text{if } a \text{ is not divisible by } 2^3 \\ a_2 - 2^3 & \text{if } a \text{ is divisible by } 2^3 \end{cases}$

  $\vdots$