Math 126 Number Theory

Prof. D. Joyce, Clark University

25 Jan 2006

Due Today. From page 14, Misc. exercises: 1, 2, 3, 4.

Last meeting. We discussed most of *An Innocent Investigation*. We discovered some axioms for number theory. For that discussion, we took 'number' to mean positive integer. One of the axioms said that 1 was not the successor of any number, that is, there does not exist a number k such that $1 = k+1$.

For the next axiom, we could take any of three logically equivalent statements. The first said that there is no infinite decreasing sequence of numbers, the second was the principle of mathematical induction (if a property of numbers holds for $n = 1$, and if it holds for any number n it also holds for $n+1$, then it holds for all numbers), and the third was the principle of minimization (if a property of numbers holds for a least one number, then it holds for a smallest number).

There's still more axioms that we'll have to find. We assumed in our discussion that we knew all about addition, but more axioms are required to justify that knowledge.

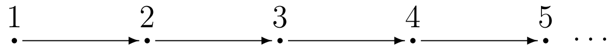
Today. What are numbers? We'll discuss the nature of numbers.

The term *natural numbers* refers to positive integers, and the set of natural numbers is usually denoted $\mathbf{N}$.

Just what are natural numbers? By this question I mean what kind of mathematical object is $\mathbf{N}$, not what kind physical thing, since numbers certainly are matter or energy.

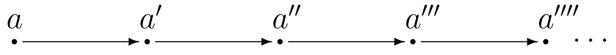
Richard Dedekind (1831–1916) published in 1888 a paper entitled *Was sind und was sollen die Zahlen?* variously translated as *What are numbers and what should they be?* or *The Nature of Meaning of Numbers.* We'll look at his answer to this question.

Dedekind defined the set of natural numbers $\mathbf{N}$ in terms of chains. We can illustrate the intent of his definitions with a diagram.



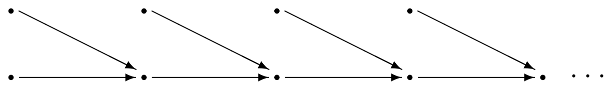
Associated with each number is a successor, and that's indicated by an arrow from the number to its successor. Although this diagram stops with 5, it should go on forever.

Dedekind realized that the names of the numbers aren't relevant to defining them, so let's do as he did and use arbitrary symbols. He also used a prime to indicate the successor of a number, so if n is the number, then n' is its successor. Our diagram now looks like this.



We have the beginnings of a definition for the set of numbers. It is a set $\mathbf{N}$ equipped with a function $\mathbf{N} \xrightarrow{\prime} \mathbf{N}$ which sends an element n to an element n', called the *successor* of n. Whenever we have that situation, we can illustrate it with a diagram with arrows as above.

Now, there are lots of things of this sort that aren't at all like the set of numbers. Here's an example of a set with a successor function that doesn't look right.



The problem is that two different elements have the same successor. So, we'll add the condition that two different elements can't have the same successor. In other words, the function $\mathbf{N} \xrightarrow{\prime} \mathbf{N}$ is required to be a one-to-one function. (There are other names for one-to-one functions. Sometimes they're called injective functions; sometimes monic functions.) With this requirement, no two arrows in the diagram can end at the same point.

That requirement helps, but it's not enough. There has to be a starting point, that is, some element in the set that's not the successor of any element. That's easy to do. Just make that a requirement—there exists an element, called the *initial element*, that is not the successor of any element. We'll denote that initial element 1.

That's still not enough. We need to make sure that every element in the set can be reached from 1. Dedekind's solution was to add one more requirement, and that is that the only subset of $\mathbf{N}$ containing 1 that is closed under the successor function is all of $\mathbf{N}$. That means that if S is a subset of $\mathbf{N}$, and the initial element is in S, and whenever $n \in S$ then $n' \in S$, then S is all of $\mathbf{N}$.

That does it. We can summarize all that as a definition.

Definition. (Dedekind) A set $\mathbf{N}$ is said to be *simply infinite* when there exists a one-to-one function $\mathbf{N} \xrightarrow{\prime} \mathbf{N}$ called the *successor function*, such that there is an element, called the *initial element* and denoted 1, that is not the successor of any element, and if a subset S of $\mathbf{N}$ contains 1 and is closed under the successor function, then $S = \mathbf{N}$.

Such a simply infinite set $\mathbf{N}$ is characterized by an element 1 and a transformation $\mathbf{N} \xrightarrow{\prime} \mathbf{N}$ satisfying the following conditions:

(1). $\forall n, m, n \neq m$ implies $n' \neq m'$.

(2). $\forall n, 1 \neq n'$.

(3). If $S \subseteq \mathbf{N}$, $1 \in S$, and $(\forall n, n \in S$ implies $n' \in S)$, then $\forall n, n \in S$.

The Dedekind/Peano axioms are this last characterization involving 1, the successor function, and the three conditions.

Dedekind then shows, given any simply infinite set $\mathbf{N}$, how to define the usual arithmetic operations, how to prove they all have the expected properties, and most important, that any two simply infinite sets are the same in the following sense. If $\mathbf{N}_1$ and $\mathbf{N}_2$ are two simply infinite sets, then there is a unique function $\mathbf{N}_1 \xrightarrow{f} \mathbf{N}_2$ such that $f(1) = 1$ and $\forall n \in \mathbf{N}_1, f(n') = (f(n))'$. Furthermore, this f is a one-to-one correspondence, that is, has an inverse function. That means the structures of $\mathbf{N}_1$ and $\mathbf{N}_2$ are identical; only the names of their elements are different.

That's enough justification to conclude that *any* simply infinite set may be taken to be the natural numbers $\mathbf{N}$.