MATH 2170 Introduction to Number Theory

January 17, 2017

Summary of Mathematical Induction

The *natural numbers* 0, 1, 2, 3, ... are the heart and the core of this course. The set of all natural numbers is denoted by $\mathbb{N}$ or by ω. I tend to use $\mathbb{N}$ when I am thinking mostly of arithmetic (addition and multiplication) and to use ω when I am thinking mostly of order $0 < 1 < 2 < 3 < \ldots$. The key fact about the natural numbers is that they come *in order*: there is a *first* natural number 0; and given any natural number n there is a "next" natural number $n+1$. This is the foundation of the important techniques of *proof by mathematical induction* and *definition by recursion*.

The natural numbers are a subset of the set of integers $\mathbb{Z}$, which includes all the negatives of the natural numbers. The set of *positive integers* is $\mathbb{Z}^+ = 1, 2, 3, \ldots$.

Simple Induction: Suppose $P(-)$ is some statement about natural numbers.
If

1. $P(0)$ is true, and
2. whenever $P(n)$ is true, then $P(n+1)$ is also true,

then
$P(n)$ is true for all natural numbers n.

There are several other properties of natural numbers that are equivalent to "simple induction"

Complete Induction: Suppose $P(-)$ is some statement about natural numbers.
Suppose that $P(-)$ has the following property:

If $P(k)$ is true for all $k < n$, then $P(n)$ is also true.

Then $P(n)$ is true for all natural numbers n.

Well-ordering Principle: Let X be a non-empty set of natural numbers. Then X has a smallest element.

In particular, suppose that $P(-)$ is some statement about natural numbers, which is true of at least one natural number. Then there is a least natural number k such that $P(k)$ is true.

Shifting the origin We can "start at" any integer a. For instance, Simple Induction starting at a reads:

Suppose $P(-)$ is some statement about integers.

If

1. $P(a)$ is true, and
2. whenever $P(z)$ is true, then $P(z+1)$ is also true,

then

$P(z)$ is true for all integers z with $z \geq a$.

Parallel to the process of Proof by Induction there is a process of *Definition by Recursion*. (Here A^k is the set of all k-tuples of elements of A, and $\vec{a}$ represents such a k-tuple.)

Recursion Theorem (simple form): Let A be any non-empty set.

Let g be any function $A^k \to A$.

Let h be any function $A^k \times \mathbb{N} \times A \to A$.

Then there is a unique function $F : A^k \times \mathbb{N} \to A$ satisfying

$$\begin{aligned} F(\vec{a}, 0) &= g(\vec{a}) \\ F(\vec{a}, n+1) &= h(\vec{a}, n, F(\vec{a}, n)) \end{aligned}$$

For example, how do we usually define natural number exponents in terms of multiplication? We write

$$\begin{aligned} x^0 &= 1 \\ x^{n+1} &= x^n x \end{aligned}$$

We define the exponent function $F(x, n) = x^n$ by using the scheme of the Recursion Theorem with A being any of the usual number systems where multiplication makes sense (such as $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{R}$, etc.), $k = 1$, $g(x) = 1$ and $h(x, n, z) = zx$.

In this course, A is almost always $\mathbb{Z}$ or $\mathbb{N}$ or $\mathbb{Z}^+$, and k is usually 1 or even 0, in which case the definition by recursion looks like:

$$\begin{aligned} F(0) &= a \\ F(n+1) &= h(n, F(n)) \end{aligned}$$

(where the *initial value* a is just some element of A).