Induction and the Well-Ordering Property

The Well-Ordering Property is probably the least familiar of our axioms for $\mathbb{Z}$, but it is extremely powerful. In this note we will develop some of the basic consequences of WOP. These will be standard tools for working with the integers.

Theorem 1 (Principle of Mathematical Induction)**.** *Let $B \subseteq \mathbb{N}$. If B satisfies the following two properties:*

1. $0 \in B$, *and*
2. *If $n \in B$, then $n+1 \in B$;*

then $B = \mathbb{N}$.

Proof. We will prove this result by contradiction. Let $S = \{n \in \mathbb{N} \mid n \notin B\}$, and suppose S is not empty. Then by the Well-Ordering Principle, S has a least element; say t. Since $t \in \mathbb{N}$, either $t = 0$ or $t = u + 1$ for some $u \in \mathbb{N}$. Since $0 \in B$, it must be the case that $t = u + 1$. Note that since $u < t$, and t is minimal among the natural numbers which are not in B, we have $u \in B$. But then $t = u + 1 \in B$, a contradiction. So in fact S is empty and we have $B = \mathbb{N}$. $\square$

The Principle of Mathematical Induction (also called just "induction" or PMI) gives us a straightforward way to show that a given statement is true for all natural numbers. Proofs using PMI require two steps: the Base Case ($0 \in B$) and the Inductive Step (if $n \in B$ then $n + 1 \in B$). Most importantly, constructive proofs by induction can be turned into *recursive algorithms* which actually compute things.

The following slight variation on PMI is known as Strong Induction; it is equivalent to PMI, but frequently more convenient to use.

Corollary 2 (Strong Induction)**.** *Let $B \subseteq \mathbb{N}$. If B satisfies the following two properties:*

1. $0 \in B$, *and*
2. *If $n \in \mathbb{N}$ such that $a \in B$ for all $0 \le a \le n$, then $n + 1 \in B$;*

then $B = \mathbb{N}$.

Bounded Sets

Definition 1. *Let $B \subseteq \mathbb{Z}$ be a set of integers, and let $m \in \mathbb{Z}$. We say that m is an* upper bound *of B if $t \le m$ for every $t \in B$. Similarly, we say m is a* lower bound *of B if $m \le t$ for every $t \in B$.*

Theorem 3. *Let $B \subseteq \mathbb{Z}$ be a nonempty set of integers.*

1. *If B has an upper bound, then B has a largest element.*

2. If B has a lower bound, then B has a smallest element.

Proof. Let $S = \{m - t \mid t \in B\}$, where m is an upper bound of B. Note that if $t \in B$, then $m - t \geq 0$, so that $S \subseteq \mathbb{N}$. Since B is not empty, S is not empty. By WOP, then, S has a minimal element, say $m - u$. If $t \in B$, then $m - t \in S$, so $m - u \leq m - t$, and thus $t \leq u$. So u is the largest element of B. $\square$