Math 2710

Oct 14-18

Mathematical Induction

The axiom of induction says the following. Let $\mathbb{P}$ denote the positive integers, and let S be a subset of $\mathbb{P}$. If:

- $1 \in S$
- $n \in S \implies n+1 \in S$ for all $n \in \mathbb{P}$

then $S = P$.

This is applied to propositions in the following way. Suppose for each n we have a proposition $P(n)$. Suppose $P(1)$ is true, and, for all $n \in \mathbb{P}$, $P(n) \implies P(n+1)$. Then $P(n)$ is true for all n. To prove this, let S be the set of n for which $P(n)$ is true and use the axiom of induction to prove that $S = \mathbb{P}$.

Induction and the well-ordering principle

The axiom of induction and the well-ordering principle are equivalent. To see this, first suppose that the well ordering principle holds, so that *every non-empty set of positive integers has a least element.*

Now suppose S is a subset of the positive integers that satisfies $1 \in S$ and if $n \in S$ then $n+1 \in S$. Let U be the set of positive integers that are NOT in S; note that $1 \notin U$ since $1 \in S$. If U is non-empty then by well ordering it has a least element, say m, and $m > 1$. Therefore $m-1 \in S$. By the assumption, $m-1 \in S \implies m \in S$, which is a contradiction. We conclude that U must have been empty so S contains all positive integers.

Now suppose the *axiom of induction holds* and let U be a non-empty set of positive integers. Suppose U does not have a least element. Let $P(n)$ be the proposition that $\{1, 2, \ldots, n\} \not\subset U$. Now $P(1)$ is true since if $1 \in U$, 1 is clearly the least element in U. Suppose $P(n)$ is true. Then $n+1 \notin U$, since otherwise $n+1$ would be a least element of U. By the axiom of induction, $P(n)$ is true for all n. But since every positive integer k belongs to $P(k)$, this means that no integer k belongs to U, so U is empty.

Standard Examples

- $1 + 2 + 3 + \ldots + n = \frac{n(n+1)}{2}$
- $n! \geq 2^n$ for all n.
- $1 + 3 + 5 + \ldots + (2N - 1) = N^2$

A look back

The text makes the following remark on page 91:

> This principle of induction has already been implicitly used in the Euclidean Algorithm 2.22, the Extended Euclidean algorithm 2.25, Theorem 2.41 on base b representations, twice in the Unique Factorization Theorem 2.54, and in the generalized Chinese Remainder Theorem 3.66.

In the proof of the Fundamental Theorem of algebra, the following step is important. Suppose N has two factorizations into primes:

$$N = p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_n.$$

Then since p_1 divides the product $q_1 q_2 \cdots q_n$, we must have p_1 equal to one of the q_i for $i = 1, \ldots n$. In the book, this is done by a "and so on" argument but you really need induction.

Proposition: If a prime p divides a product $q_1 \cdots q_m$ of m primes, then $p = q_i$ for some $i = 1, \ldots, m$.

Proof: By induction. If $m = 1$, then $p|q_1$ and therefore $p = q_1$ since the only divisor of q_1 greater than 1 is q_1 itself. Now suppose the result is true for m primes. Suppose $p|q_1 \cdots q_{m+1}$. Then $p|(q_1 \cdots q_m)q_{m+1}$. When a prime divides a product, it divides one or the other factor, so either $p|(q_1 \cdots q_m)$ or $p|q_{m_1}$. In the second case, $p = q_{m+1}$, while in the first, by the inductive hypothesis, $p = q_i$ for $i = 1, \ldots, m$. Thus the result holds for all m by induction.

Recursion

Let's call the three poles of the Towers of Hanoi puzzle A, B, and C, and suppose that N disks start out stacked properly on disk A.

If there is only one disk, the Towers of Hanoi have an obvious solution – just move that one disk from A to B.

If there are N disks, solve the puzzle by first moving the top N-1 disks to pole C, then move the bottom (big) disk to pole B, then move the N-1 disks from C back to B.

If $f(n)$ is the number of steps needed to move n disks, then $f(n+1) = 2f(n)+1$ and $f(1) = 1$. This is called a *recursive* definition.

Proposition: $f(n) = 2^n - 1$.

Proof: By induction. Since $f(1) = 2 - 1 = 1$, the base case is true. Suppose $f(n) = 2^n - 1$. Then $f(n+1) = 2(2^n - 1) + 1 = 2^{n+1} + 1$. So the formula holds in all cases.

Other recursive definitions

Fibonacci Numbers: $a_0 = 0$, $a_1 = 1$, and $a_{n+1} = a_n + a_{n-1}$.

Differential equations: $f'(x) = f(x)$. If

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots$$

then $na_n = a_{n-1}$. So $a_n = a_{n-1}/n$. If $a_0 = 1$, this gives $a_n = 1/n!$.

Maximum: Define the maximum of $a_1, \ldots, a_n$ to be $\max(\max(a_1, \ldots, a_{n-1}), a_n))$

Newton's method: $x_{n+1} = x_n - f(x_n)/f'(x_n)$.

Things to work on

Fibonacci numbers: Show that consecutive fibonacci numbers have gcd equal to 1.

Finite geometric series: Prove that $\sum_{i=0}^{N} r^N = (r^{N+1} - 1)/(r-1)$.