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 $\sum_{i=0}^{N} r^N = (r^{N+1} - 1)/(r - 1)$.

Binomial coefficients

Definition: The binomial coefficient $\binom{n}{r}$ is defined as

$$\binom{n}{r} = \frac{n!}{r!(n-r)!}$$

for integers n and r with $n \geq 1$ and $0 \leq r \leq n$.

Notice that $\binom{n}{n} = \binom{n}{0} = 1$ and $\binom{n}{r} = \binom{n}{n-r}$; also $\binom{n}{1} = \binom{n}{n-1} = n$.

Proposition: $\binom{n}{r-1} + \binom{n}{r} = \binom{n+1}{r}$ if $1 \leq r \leq n$.

Notice that this condition actually determines all of the values of $\binom{n}{r}$ recursively once we set the 'end conditions' $\binom{n}{0} = \binom{n}{n} = 1$.

Conclusions about binomial coefficients

Proposition: The coefficients are all integers. By induction. We know that $\binom{1}{r}$ are integers for $r = 0, 1$.

Proof: Suppose that all of the binomial coefficients $\binom{N}{r}$ are integers for $r = 0, \ldots, N$. (In other words, a row of Pascal's triangle is made up of integers.) Then the next row has integer ends (by definition) and the middle values are sums of values from the previous row, so they are also integers.

Proposition: The binomial coefficient $\binom{n}{r}$ counts the number of r element subsets in an n element set.

Proof: Let S be a set with n elements. Pick one element of S, and call it x. Then we can divide the r element subsets of S into two subsets: those that contain x, and those that don't. The number of subsets of S with r elements that don't contain x is precisely the number of r element subsets of $S - \{x\}$, which by induction is $\binom{n-1}{r}$. The number of subsets that do contain x is the same as the number of $r-1$ element subsets of $S - \{x\}$, so it is $\binom{n-1}{r-1}$. Thus the number of subsets obeys the same recursion relation as the binomial coefficients so they are equal.

The binomial theorem

Proposition: The binomial theorem:

$$(a+b)^n = \sum_{r=0}^{n} \binom{n}{r} a^r b^{n-r}$$

For $n = 1$ this says that $a + b = \binom{1}{0}a + \binom{0}{1}b$ which is true since these binomial coefficients are both 1.

Suppose this is true for the n^{th}-power. We compute

$$(a+b)^n = a(a+b)^{n-1} + b(a+b)^{n-1} = \sum_{r=0}^{n-1} \binom{n-1}{r} a^{r+1} b^{n-1-r} + \sum_{r=0}^{n-1} \binom{n-1}{r} a^r b^{n-r}.$$

binomial theorem continued

Using $s = r + 1$ in the first sum, it becomes

$$\sum_{s=1}^{n} \binom{n-1}{s-1} a^s b^{N-s}$$

Renaming $r = s$ in the second sum, combining, and separating out the ends, we have

$$(a+b)^n = a^n + \sum_{s=1}^{n-1}(\binom{n-1}{s-1} + \binom{n-1}{s})a^s b^{n-s} + b^n.$$

binomial theorem continued

Finally, using the recursion relation for the binomial coefficients:

$$\binom{n-1}{s-1} + \binom{n-1}{s} = \binom{n}{s}$$

we have the desired formula for n.