Chapter 2
Induction

This chapter describes the method of proof by induction, in several versions. The last section presents the Binomial Theorem.

A. Induction

Induction is the basic method of proof for facts involving natural numbers. It allows us to obtain, in a finite number of steps, proofs of statements about all the numbers in the infinite set $\mathbb{N}$.

Induction comes in various formulations. Here is the best-known version.

Theorem 1 (Induction). *Fix an integer n_0 and let $P(n)$ be a statement which makes sense for every integer $n \geq n_0$. Then $P(n)$ is true for all $n \geq n_0$, if the following two statements are true:*

(a) $P(n_0)$ is true; and

(b) for all $k \geq n_0$, if $P(k)$ is true then $P(k+1)$ is true.

When using induction to prove a theorem, proving (a) is called the *base case*, and proving (b) is called the *induction step*.

You have almost certainly seen this principle used before, perhaps in calculus, in evaluating sums arising in connection with the definite integral.

Here is a simple example.

Example 1. For all $n \geq 1$,

$$1+3+5+\ldots+(2n-1) = n^2.$$

Proof. Let $P(n)$ be the statement

$$1+3+5+\ldots+(2n-1) = n^2,$$

L.N. Childs, *A Concrete Introduction to Higher Algebra*, Undergraduate Texts in Mathematics, © Springer Science+Business Media LLC 2009

or in words, "the sum of the first n odd numbers is n^2". Thus $P(1)$ is the statement

$$1 = 1^2,$$

$P(2)$ is the statement

$$1+3 = 2^2,$$

$P(5)$ is the statement

$$1+3+5+7+9 = 5^2,$$

and so on. All of these are clearly true, but just looking at $P(n)$ for many specific values of n does not suffice to prove $P(n)$ for *every* natural number $n \geq 1$. So we let $n_0 = 1$ and use induction to prove $P(n)$ for all $n \geq 1$.

The base case $P(1)$ is true, since $1 = 1^2$.

For the induction step, let k be some unspecified number ≥ 1, and assume that $P(k)$ is true, that is,

$$1+3+\ldots+(2k-1) = k^2.$$

We want to show that then $P(k+1)$ is true, that is,

$$1+3+\ldots+(2k-1)+(2k+1) = (k+1)^2.$$

To do so, we can add $(2k+1)$ to both sides of the equation $P(k)$ to get

$$1+3+\ldots+(2k-1)+(2k+1) = k^2+(2k+1). \tag{2.1}$$

The left side of (2.1) is the left side of the statement $P(k+1)$, and, since $k^2+2k+1 = (k+1)^2$, the right side of (2.1) is equal to $(k+1)^2$, the right side of $P(k+1)$. Thus assuming $P(k)$ is true, it follows that $P(k+1)$ is true.

By induction, $P(n)$ is true for all $n \geq 1$. □

The rationale behind induction is that if the base case (a) and the induction step (b) are true, then for any $n > n_0$, one can prove, in $n - n_0$ logical steps, that $P(n)$ is true. For example, if $P(n)$ is the equation of Example 1, above and we wish to prove that $P(5)$ is true, we can argue logically as follows:

$P(1)$ is true, by the base case.

Since $P(1)$ is true, $P(2)$ is true, by the induction step with $k = 1$;

Since $P(2)$ is true, $P(3)$ is true, by the induction step with $k = 2$;

Since $P(3)$ is true, $P(4)$ is true, by the induction step with $k = 3$;

Since $P(4)$ is true, $P(5)$ is true, by the induction step with $k = 4$.

This same reasoning can be used to show that $P(n)$ is true for any given number n. We simply start with the base case, which says that $P(n_0)$ is true, and then successively infer that $P(n_0+1), P(n_0+2), \ldots, P(n)$ is true by $n - n_0$ uses of the induction step. The principle of induction simply asserts that given the validity of the base case and of the induction step for all $n \geq n_0$, then for any $n > n_0$, $P(n)$ can be shown true, and therefore *is* true.

Here are some more examples.

Example 2. For all $n \geq 1$, $2^n \geq 1+n$.

Proof. Here $n_0 = 1$.

The statement

$$P(n) : 2^n \geq 1 + n$$

is clearly true when $n = 1$, so the base case is true.

For the induction step, let k be a number ≥ 1 and assume

$$P(k) : 2^k \geq 1 + k$$

is true. Then multiplying both sides by 2 gives

$$2^k \cdot 2 \geq (1 + k) \cdot 2,$$

so

$$2^{k+1} = 2^k \cdot 2 \geq (1 + k) \cdot 2 = 2 + 2k > (1 + 1) + k = 1 + (k + 1).$$

Thus the statement

$$P(k + 1) : 2^{k+1} \geq 1 + (k + 1)$$

is true. We've shown that for every $k \geq 1$, the induction step is true. Hence the inequality $P(n)$ is true for all $n \geq 1$ by induction. □

Example 3. The number 8 divides $3^{2n} - 1$ for all $n \geq 0$. That is, for every $n \geq 0$, $3^{2n} - 1 = 8m$ for some natural number m.

Proof. The statement $P(n)$: 8 divides $3^{2n} - 1$, is true for $n = 0$ since 8 divides $3^0 - 1 = 0$. The induction step involves a little "trick" of subtracting and adding the same quantity. Suppose 8 divides $3^{2k} - 1$. We examine $3^{2(k+1)} - 1$:

$$\begin{aligned} 3^{2(k+1)} - 1 &= 3^{2k} \cdot 3^2 - 1 \\ &= 3^{2k} \cdot 3^2 - 3^2 + 3^2 - 1 \\ &= 3^2(3^{2k} - 1) + (3^2 - 1). \end{aligned}$$

Since 8 divides $3^{2k} - 1$ and 8 divides $3^2 - 1$, therefore 8 divides $3^2(3^{2k} - 1) + (3^2 - 1) = 3^{2(k+1)} - 1$. Thus the statement $P(n)$ is true for all $n \geq 0$. □

Example 4. The number $2n^3 - 3n^2 + n + 31 \geq 0$ for all $n \geq -2$.

Proof. Let us set $f(n) = 2n^3 - 3n^2 + n + 31$. Then for each $n \geq -2$, the statement $P(n)$ is the inequality

$$P(n) : f(n) \geq 0.$$

In particular, for the base case, $P(-2)$ is the inequality $f(-2) \geq 0$, which is true because $f(-2) = 1$. For the induction step, suppose that for some $k \geq -2$, the statement $P(k)$ is true, that is, $f(k) > 0$. Then expanding $f(k + 1)$ and collecting terms, we find

$$\begin{aligned} f(k+1) &= 2(k+1)^3 - 3(k+1)^2 + (k+1) + 31 \\ &= 2(k^3+3k^2+3k+1) - 3(k^2+2k+1) + (k+1) + 31 \\ &= 2k^3 + 6k^2 + 6k + 2 - 3k^2 - 6k - 3 + k + 1 + 31 \\ &= 2k^3 + 3k^2 + k + 31 \\ &= f(k) + 6k^2 \geq f(k) \geq 0. \end{aligned}$$

So $P(k+1)$ is true. Thus $P(n)$ is true for all $n \geq -2$, that is, $f(n) \geq 0$ for all $n \geq -2$. □

Example 5. In calculus, after the rules for the derivative of a constant and of x, and the product rule are presented, the rule for the derivative of x^n can be proved by induction:

$$\frac{dx^n}{dx} = nx^{n-1}.$$

Proof. Let $P(n)$ be the statement

$$\frac{dx^n}{dx} = nx^{n-1}.$$

Then $P(0)$ is the statement that the derivative of the constant function 1 is 0, and $P(1)$ is the statement that the derivative of x is 1. To prove $P(n)$ by induction, suppose that for some $k \geq 0$,

$$P(k) : \frac{dx^k}{dx} = kx^{k-1}$$

is true. Then consider $\frac{dx^{k+1}}{dx}$. By the product rule, we have

$$\begin{aligned} \frac{dx^{k+1}}{dx} &= \frac{d(x \cdot x^k)}{dx} \\ &= \frac{dx}{dx} \cdot x^k + x \cdot \frac{dx^k}{dx} \\ &= x^k + x \cdot kx^{k-1} \end{aligned}$$

since we know $P(1)$ is true and we have assumed $P(k)$ is true. Collecting terms, we obtain

$$\frac{dx^{k+1}}{dx} = (k+1)x^k$$

and so $P(k+1)$ is true. Thus by induction,

$$P(n) : \frac{dx^n}{dx} = nx^{n-1}$$

is true for all $n \geq 0$. □

Exercises. In the exercises, n is always an integer.

1. Prove that $1+2+3+\ldots+n = n(n+1)/2$ for all $n \geq 1$.

2. Prove that $1^3+2^3+\ldots+n^3 = [n(n+1)/2]^2$ for all $n \geq 1$.

3. Prove that

$$1+2+2^2+\ldots+2^{n-1} = 2^n - 1$$

for every $n > 1$.

4. Prove that for all $n \geq 1$,

$$1^4+2^4+\ldots+n^4 = \frac{n(n+1)(2n+1)(3n^2+3n-1)}{30}$$

5. Prove that for any real number x and for all numbers $n > 1$,

$$x^n - 1 = (x-1)(x^{n-1}+x^{n-2}+\ldots+x^{n-r}+\ldots+x+1).$$

6. Using the last exercise, prove that for all $n > 1$,

$$\lim_{r\to 1} \frac{r^n - 1}{r-1} = n.$$

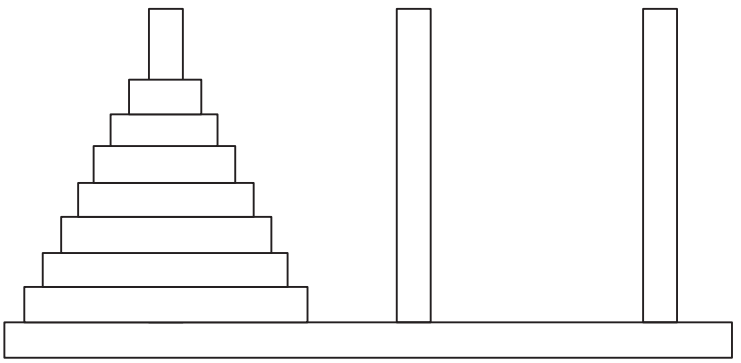
7. (Askey) Show that $\frac{dx^n}{dx} = nx^{n-1}$ as follows: by the definition of the derivative,

$$\frac{dx^n}{dx} = \lim_{y\to x} \frac{y^n - x^n}{y-x}.$$

Set $y = rx$ and compute the limit using the last exercise.

8. Prove that $n! > 2^n$ for all $n \geq 4$.

9. Prove that $2^{2n} > n^4$ for all $n \geq 4$.



10. Let

$$t_n = \frac{n(n+1)}{2} = 1+2+\ldots+n$$

be the n-th triangular number. Define $t_0 = 0$.

(i) Show that the odd square number $(2n+1)^2 = 8t_n + 1$ for all $n \geq 1$.

(ii) Prove that

$$\frac{1}{t_1} + \frac{1}{t_2} + \ldots + \frac{1}{t_n} = 2 - \frac{2}{n+1}.$$

(Hint: observe that $\frac{1}{n(n+1)} = \frac{1}{n} - \frac{1}{n+1}$.)

(iii) Prove that for all $n \geq 1$,

$$\frac{1}{1} + \frac{1}{9} + \frac{1}{25} + \ldots + \frac{1}{(2n+1)^2} \leq \frac{5}{4} - \frac{1}{4(n+1)}$$

in two ways: directly by induction, and by using (i) and (ii).

11. Let a be a natural number >1. Prove that for all integers $r_0, r_1, \ldots, r_{n-1}$ with $0 \leq r_j < a$,

$$r_0 + r_1 a + r_2 a^2 + \ldots + r_{n-1} a^{n-1} < a^n.$$

When $n = 10$ this says that 10^n is larger than any n-digit number.

12. Let b be a number ≥ 2. Prove that for all $n \geq 1$,

$$(b^n - 1)(b^n - b)(b^n - b^2) \cdot \ldots \cdot (b^n - b^{n-2}) \geq b^{n(n-1)} - b^{n(n-1)-1}.$$

13. Prove that for every $n \geq 1$, 24 divides $16^n - 16$.

14. Prove that for every $n \geq 1$, 5 divides $8^n - 3^n$.

15. Prove that for every $n \geq 1$, 5 divides $3^{4n} - 1$.

16. Prove that for every odd number $n \geq 1$, 9 divides $4^n + 5^n$.

17. Prove that for every $n \geq 0$, 3 divides $2^{2n+1} + 1$.

18. Using the addition formulas

$$\cos(a+b) = \cos(a)\cos(b) - \sin(a)\sin(b)$$

and

$$\sin(a+b) = \sin(a)\cos(b) + \cos(a)\sin(b),$$

prove that for each $n > 1$ there are polynomials $f_n(x)$ of degree n and $g_n(x)$ of degree $n-1$ so that

$$\cos(nx) = f_n(\cos(x))$$

and

$$\sin(nx) = g_n(\cos(x))\sin(x).$$

19. For any real number a, define $a^0 = 1$, and for every number $k \geq 0$, define $a^{k+1} = a^k \cdot a$. Using induction, prove that for all natural numbers m and n, $a^{m+n} = a^m \cdot a^n$.

20. Consider the puzzle called the Tower of Hanoi (attributed to the French mathematician Edouard Lucas, 1883). The puzzle consists of n disks of decreasing diameters placed on a pole. There are two other poles. The problem is to move the entire stack of disks to another pole by moving one disk at a time to any other pole, except that no disk may be placed on top of a smaller disk. Find a formula for the least number of moves needed to move a stack of n disks from one pole to another, and prove the formula by induction.

21. (Neal Hill). Suppose in the Tower of Hanoi, the three poles are in a row, and a disc can only be moved from a pole to an adjacent pole. All other rules apply. How many moves does it take to move a stack of n discs from the leftmost pole to the rightmost pole?

22. Show that for every positive integer n, one of the numbers $n, n+1, n+2, \ldots, 2n$ is the square of an integer.

23. What is wrong with the proof of the following (true) theorem?

Theorem 2. *All new 1922 Ford Model T cars had the same exterior color.*

Proof. The case $n = 1$ is obvious.

Suppose that in any set of n new Model T's, all had the same exterior color. Consider a set of $n+1$ new Model T's, lined up from left to right.

We may assume by induction that in the set L of the n Model T's to the left all had the same exterior color, and similarly that in the set R of the n Model T's to the right all had the same exterior color. But then evidently all the $n+1$ Model T's had the same exterior color, for the leftmost and rightmost Model T's had the same exterior color as all the Model T's in between.

By induction, for every number n, in every set of n new Model T's all had the same exterior color. Since the set of all new 1922 Model T's was one such set, the theorem is proved. □

(Henry Ford was reputed to have said of the Model T, "You can paint it any color, so long as it's black.")

24. Show that for $n \geq 1$,

$$1 + 7 + 13 + \ldots (6n - 5) = 3n^2 - 2n.$$

B. Complete Induction

Complete Induction is a reformulation of induction that is often more convenient to use.

Theorem 3 (Complete Induction). *Let n_0 be a fixed integer and let $P(n)$ be a statement which makes sense for every integer $n \geq n_0$. Then $P(n)$ is true for all integers $n > n_0$, if the following two statements are true:*
(a') (base case) $P(n_0)$ is true, and
(b') (induction step) For all $m > n_0$:
if $P(k)$ is true for all k with $n_0 \leq k < m$, then $P(m)$ is true.

Complete induction appears more complicated than ordinary induction, but in fact it is easier to use. Compare the induction step (b') with the induction step (b) for ordinary induction:
(b) *For all $m > n_0$,*
if $P(m-1)$ is true, then $P(m)$ is true.

In attempting to prove the induction step in a proof by induction, complete induction allows us to assume more than we can with ordinary induction. With complete induction, in order to prove $P(m)$, you may assume that $P(k)$ is true for every k, $n_0 \leq k < m$. In ordinary induction you are allowed only to assume that $P(m-1)$ is true. So complete induction is more flexible than ordinary induction.

For certain kinds of results involving multiplication, ordinary induction is awkward to apply, while complete induction is quite natural. The next example is such a result.

Recall that a natural number n is *prime* if $n \geq 2$ and does not factor into the product of two natural numbers each smaller than n. Also, a number q *divides* a number n, or n *is divisible by* q, if $n = qr$ for some natural number r. Thus 3 divides 12, but 3 does not divide 14.

Proposition 4. *Every natural number $n \geq 2$ is divisible by a prime number.*

Proof. Let $P(n)$ be the statement, "n is divisible by a prime number." Then the base case $P(2)$ is true, because 2 is prime and 2 divides itself.

We'll use complete induction for the induction step. Thus we assume that $P(k)$ is true for all k where $2 \leq k < m$: that is, we assume that every natural number ≥ 2 and $< m$ is divisible by a prime number. Now consider m. If m is prime, then m is divisible by a prime number, namely itself, and $P(m)$ is true. If m is not prime, then m factors as $m = ab$, where $2 \leq a < m$ and also $2 \leq b < m$. Since $2 \leq a < m$, by assumption $P(a)$ is true, that is, a is divisible by a prime. Since a is divisible by a prime, and a divides m, m is divisible by the same prime. So $P(m)$ is true.

Thus $P(n)$ is true for all $n \geq 2$ by complete induction. □

Notice that had we tried to use ordinary induction to prove $P(m)$: "m is divisible by a prime" for all $m \geq 2$, then in the induction step we would have been permitted only to assume that $m-1$ is divisible by a prime, in order to try to prove that m is divisible by a prime. But knowing about factors of $m-1$ is of little direct help in finding factors of m, since no factor of $m-1$ other than 1 can possibly be a factor of m. (Why?) Thus if we wanted to prove Proposition 4 by ordinary induction, we would need to change the statement $P(n)$. See the proof of Theorem 6, below.

If we want to prove something using induction, complete induction will work just as well. For suppose we can prove

For all $k \geq n_0$, if $P(k)$ is true, then $P(k+1)$ is true.

Then we can prove

For all $k \geq n_0$, if $P(m)$ is true for all m with $n_0 \leq m < k$, then $P(k+1)$ is true.

For if we can prove $P(k+1)$ assuming only $P(k)$, then we can prove $P(k+1)$ assuming $P(m)$ for all $n_0 \leq m \leq k$.

Hence:

Theorem 5. *If a statement $P(n)$ can be proved for all $n \geq n_0$ by ordinary induction, it can be proved by complete induction.*

It turns out, however, that the two forms of induction are logically equivalent. We prove

Theorem 6. *If a statement $P(n)$ can be proved for all $n \geq n_0$ by complete induction, it can be proved by ordinary induction.*

Proof. Suppose we know that:

(a') $P(n_0)$ is true, and

(b') if $P(k)$ is true for all k, $n_0 \leq k < m$, then $P(m)$ is true.

Then $P(n)$ is true for all $n \geq n_0$ by complete induction. We show how to prove $P(n)$ for all n by ordinary induction. To do so, we consider a new statement

$Q(n)$: $P(m)$ is true for all m, $n_0 \leq m \leq n$.

We prove $Q(n)$ is true for all $n \geq n_0$ by ordinary induction. Note that if $Q(n)$ is true, then $P(n)$ is true.

For the base case, we need to show:

(a) $Q(n_0)$ is true.

But because $Q(n_0)$ is the statement "$P(m)$ is true for all m, $n_0 \leq m \leq n_0$," we have that $Q(n_0)$ is true because by (a), $P(n_0)$ is true.

For the induction step, we need to show:

(b) If $Q(m-1)$ is true then $Q(m)$ is true.

To see this, observe that if $Q(m-1)$ is true, then $P(k)$ is true for all k with $n_0 \leq k \leq m-1$. So since we assumed (b') holds for all $n \geq n_0$, therefore $P(m)$ is true. But then $P(k)$ is true for all k with $n_0 \leq k \leq m$, and so $Q(m)$ is true.

Thus by ordinary induction, $Q(n)$ is true for all $n \geq n_0$. But if $Q(n)$ is true, then $P(n)$ is true. So $P(n)$ is true for all $n \geq n_0$. □

This theorem implies that whenever we want to prove a statement about natural numbers, we can use whichever version of induction is most convenient. Henceforth, when we refer to "induction", we mean either version.

Exercises.

25. Prove "For all $n \geq 2$, every number m with $1 < m \leq n$ is divisible by a prime number" by ordinary induction.

26. Prove that any natural number $n \geq 2$ either is prime or factors into a product of primes.

27. Prove that the sum of the interior angles of an n-sided convex polygon is $180 \times (n-2)$.

28. Let $f : \mathbb{N} \to \mathbb{N}$ be a function with the properties that $f(1) = 1$ and for all numbers $n > 1$, $f(n) < n$. Prove that for every n there is some k so that the function $f^{(k)}$, obtained by composing f with itself $k-1$ times, maps n to 1. (Thus $f^{(1)}(n) = f(n), f^{(2)}(n) = f(f(n)), f^{(3)}(n) = f(f(f(n)))$, etc.)

29. *Russian peasant arithmetic*. Here is a way of multiplying which has been attributed to Russian peasants who could only add, and multiply and divide by 2. In fact this method of multiplying was also used by the ancient Egyptians (2000 B.C.) (see [Gillings (1972)]) and is of interest also to computer programmers (since computers are especially efficient in multiplying and dividing by 2).

To multiply two numbers a and b set up four columns, labeled "left", "right", "sum" and "summand". In the top row place a in the left column, b in the right column, and 0 in the sum column. If b is odd, place a in the summand column. If b is even, place 0 in the summand column.

Then fill in successive rows of the array. If a, b, s and d are the entries in a given row, then fill in the next row as follows:

If b is even, set the entries in the left, right and sum columns of the next row to be $2a$, $b/2$ and $s+d$.

If b is odd, set the entries in the left, right and sum columns of the next row to be $2a$, $(b-1)/2$ and $s+d$.

Then set the entry in the summand column to be 0 if the entry in the right column (either $b/2$ or $(b-1)/2$) in the same row is even; set the entry in the summand column to be the entry in the left column ($2a$) of the new row if the entry in the right column in the new row (either $b/2$ or $(b-1)/2$) is odd.

left	right	sum	summand
		$\vdots$	
a	b	s	d
$2a$	$b/2$ or $(b-1)/2$	$s+d$	$2a$ or 0
		$\vdots$	

Continue until you reach the row in which the entry in the right column is 0. Then the entry in the sum column is $a \cdot b$.

Here is an example, showing that $116 \cdot 311 = 36076$:

left	right	sum	summand
116	311	0	116
232	155	116	232
464	77	348	464
928	38	812	0
1856	19	812	1856
3712	9	2668	3712
7424	4	6380	0
14848	2	6380	0
29696	1	6380	29696
59392	0	36076	

Given two numbers a and b, prove by induction that for each row,

$$(\text{the left entry}) \cdot (\text{the right entry}) + (\text{the sum entry}) = a \cdot b,$$

and therefore $a \cdot b$ is equal to the last entry in the sum column.

30. The Fibonacci sequence is defined by $a_1 = 1, a_2 = 1$ and for all $n \geq 2$, $a_{n+1} = a_n + a_{n-1}$. Thus the sequence begins

$$1, 1, 2, 3, 5, 8, 13, 21, 34, 55, \ldots.$$

Prove that for all $n \geq 1$, $a_n < (\frac{5}{3})^n$.

31. A *composition* of a natural number n is a description of n as an ordered sum of natural numbers. For example, the compositions of 3 are:

$$3, 2+1, 1+2, 1+1+1$$

and the compositions of 4 are

$$4, 3+1, 2+2, 2+1+1, 1+3, 1+2+1, 1+1+2, 1+1+1+1.$$

Let $c(n)$ be the number of compositions of n. Guess a formula for $c(n)$ for all $n \geq 1$ and prove your formula by induction.

C. Well-Ordering

The formulations of induction in the two previous sections were developed in the seventeenth century by Pascal and others. However, some results about natural numbers were obtained many centuries earlier, by the ancient Greek mathematicians whose work was collected in Euclid's Elements (300 B.C.) For example, Proposition 4, above, is found in Euclid, Book IX, Proposition 31. Here is how Euclid proved:

Theorem 7. *Every composite number is divisible by some prime number.*

Proof. Suppose A is a composite number. Then A is divisible by some number B. If B is prime, we're done, so assume B is composite. Then B is divisible by some number C, so C is a divisor of A. If C is prime, we're done, so assume C is composite. Then C is divisible by some number.

"Thus, if the investigation be continued in this way, some prime number will be found which will measure [divide] the number before it, which will also measure A. For if it is not found, an infinite series of numbers will measure the number A, each of which is less than the other: which is impossible in numbers." □

Thus Euclid proves the result by what might be called "infinite descent": there is no infinite descending chain of natural numbers.

The principle of infinite descent can be expressed more affirmatively as the

Theorem 8 (Well-Ordering Principle). *Any nonempty set of natural numbers has a least element.*

We can rephrase Euclid's proof in terms of the well-ordering principle. For any number $A > 2$, let $\mathscr{S}$ be the set of numbers ≥ 2 which divide A. Since A is a positive divisor of itself, $\mathscr{S}$ is nonempty. Euclid's argument using infinite descent is that if we select a strictly decreasing sequence of proper divisors of A, and none is prime, then we get an infinite descending chain of elements of $\mathscr{S}$, impossible. Using well-ordering, we can say: $\mathscr{S}$ has a least element C, that is, A has a least divisor $C \geq 2$. If C is not prime, then C has a smaller divisor $D \geq 2$ which is then a divisor of A, contradicting the assumption that C is least. So C must be prime.

Well-ordering and infinite descent are different forms of induction. We can in fact prove the well-ordering principle using induction. To do so, we prove that if there is a set of natural numbers with no least element, then it must be empty. (This approach uses the standard logical strategy for proving statements of the form "if A then B"-we prove that if B is false, then A must be false. The reason that the strategy works is that the only situation under which the statement "if A then B" is false occurs when A is true and B is false. If we assume B is false and are able to show thereby that A is false, then the situation "A true and B false" cannot occur and so "if A then B" is true.)

Proof of the Well-Ordering Principle. Let $\mathscr{S}$ be a set of natural numbers with no least element. Let $P(n)$ be the statement: "Every number in $\mathscr{S}$ is $>n$." Observe that if $P(m)$ is true, then m is not in $\mathscr{S}$. So by showing that $P(n)$ is true for all n, we will show that $\mathscr{S}$ is empty, which will prove the well-ordering principle.

Evidently $P(1)$ is true, for if not, 1 is in $\mathscr{S}$, and since all natural numbers are ≥ 1, therefore $\mathscr{S}$ would have a least element.

Suppose $P(k)$ is true for some $k > 1$. If $P(k+1)$ is false, then $\mathscr{S}$ contains some number $\leq k+1$. But $P(k)$ is true. So every number in $\mathscr{S}$ is $> k$. But then $k+1$, the only number $\leq k+1$ which is $> k$, would be in $\mathscr{S}$ and would be the least element of $\mathscr{S}$, impossible. Thus if $P(k)$ is true, then $P(k+1)$ is true. By induction, $P(n)$ is true for all $n \geq 1$, and $\mathscr{S}$ is empty. That finishes the proof. □

One important use of the well-ordering principle is that it permits us to define a number by the property that the number is the smallest number in a certain non-empty set.

For example, consider the set $\mathscr{S}$ of numbers that are multiples of both 24 and 90. That set of common multiples of 24 and 90 is non-empty, for it includes $24 \cdot 90 = 2160$. Thus by well-ordering, the set $\mathscr{S}$ has a smallest number, the *least common multiple* of 24 and 90. Some computation verifies that the least common multiple is 360. But with no computation, well-ordering tells us immediately that

Proposition 9. *Any two numbers a and b have a least common multiple, that is, a number m which is a common multiple of a and b and which is $\leq$ any other common multiple of a and b.*

Proof. Since the set $\mathscr{S}$ of common multiples of a and b contains $a \cdot b$, $\mathscr{S}$ is non-empty. So by well-ordering, $\mathscr{S}$ has a smallest element, which is the least common multiple of a and b. □

Exercises.

32. Show that there is no rational number b/a whose square is 2, as follows: if $b^2 = 2a^2$, then b is even, so $b = 2c$, so, substituting and canceling 2, $2c^2 = a^2$. Use that argument and well-ordering to show that there can be no natural number $a > 0$ with $b^2 = 2a^2$ for some natural number b.

33. Prove that the well-ordering principle implies induction, as follows: suppose $P(n)$ is a statement which make sense for every $n \geq n_0$. Suppose (a) $P(n_0)$ is true, and (b) for any $n \geq n_0$, if $P(n)$ is true then $P(n+1)$ is true. Let $\mathscr{S}$ be the set of $n \geq n_0$ for which $P(n)$ is false. Using well-ordering, show that $\mathscr{S}$ must be empty.

34. Show that the well-ordering principle is equivalent to "there is no infinite descending chain of natural numbers".

35. Fix N, some integer, and suppose $\mathscr{S}$ is a nonempty set of integers such that every a in $\mathscr{S}$ is $<N$. Show that $\mathscr{S}$ has a maximal element. (Hint: Let $\mathscr{T} = \{n \text{ in } \mathbb{N} | n \geq a \text{ for all } a \text{ in } \mathscr{S}\}$.)

D. The Binomial Theorem

The Binomial Theorem describes the coefficients when the expression $(x+y)^n$ is multiplied out. Recall that $n!$ ("n factorial") is defined by $n! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot n$ for $n > 0$. We set $0! = 1$.

Theorem 10 (The Binomial Theorem). *For every integer $n \geq 1$,*

$$(x+y)^n = \binom{n}{0} x^n + \ldots + \binom{n}{r} x^{n-r} y^r + \ldots + \binom{n}{n} y^n$$

where

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

for $0 \le r \le n$.

Examples:

$$(x+y)^2 = x^2 + 2xy + y^2;\ (x+y)^3 = x^3 + 3x^2y + 3xy^2 + y^3.$$

The proof is by induction on n. In order to carry through the argument passing from $n-1$ to n (the induction step) we first set up Pascal's triangle,

$$\begin{array}{ccccccc} & & & 1 & & & \\ & & 1 & & 1 & & \\ & 1 & & 2 & & 1 & \\ 1 & & 3 & & 3 & & 1 \\ 1 & 4 & & 6 & & 4 & 1 \\ & & & \vdots & & & \end{array}.$$

We number the elements $c(n,r)$ of Pascal's triangle by the row n and the position r of the element within the row, both indices starting from 0. Thus Pascal's triangle is labeled

$$\begin{array}{ccccccc} & & & c(0,0) & & & \\ & & c(1,0) & & c(1,1) & & \\ & c(2,0) & & c(2,1) & & c(2,2) & \\ c(3,0) & & c(3,1) & & c(3,2) & & c(3,3) \\ & & & \vdots & & & \end{array},$$

where

$$c(0,0) = c(n,0) = c(n,n) = 1$$

for all n, and for $1 \le r \le n-1$,

$$c(n,r) = c(n-1,r-1) + c(n-1,r).$$

That is, $c(n,r)$ is the sum of the terms to the upper left and to the upper right:

$$\begin{array}{ccc} c(n-1,r-1) & + & c(n-1,r) \\ & = c(n,r) & \end{array}$$

The entries $c(n,r)$ have a combinatorial interpretation.

Proposition 11. *Let S be a set with n elements. Then $c(n,r)$ is the number of r-element subsets of S.*

Proof. We do this by induction on n, the case $n = 1$ being obvious.

Let S be a set with n elements. The statement is true when $r = 0$ or n, since there is only one subset of S with n elements, namely S, and only one with no elements.

Assume, then, that $n > 1$ and $1 \le r \le n-1$. Let y be an fixed element of S. Let S_0 be the set of all the elements of S except y. S_0 is then a set with $n-1$ elements. Divide the collection of all r-element subsets of S into two piles, one consisting of those subsets containing y, the other consisting of those subsets not containing y. The first pile consists of exactly those subsets of S obtained by taking an $(r-1)$-element subset of S_0 and adjoining y. By induction applied to S_0, there are $c(n-1,r-1)$ of these. The second pile consists exactly of the r-element subsets of S_0, of which there are $c(n-1,r)$, again by induction. Thus the number of r-element subsets of S is $c(n-1,r-1)+c(n-1,r) = c(n,r)$, which is what we wished to show. □

The entries of Pascal's triangle can be computed by the following:

Lemma 12.

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

Proof. Induction on n. The case $n = 0$ is obvious:

$$\frac{0!}{0!0!} = 1 = c(0,0),$$

Given $n > 0$, assume that for all r with $0 \le r \le n-1$,

$$c(n-1,r) = \frac{(n-1)!}{r!(n-1-r)!}.$$

Now

$$c(n,0) = 1 = \frac{n!}{0!(n-0)!}, \quad c(n,n) = 1 = \frac{n!}{n!(n-n)!}$$

so the lemma is true for $c(n,r)$ when $r = 0$ or n. For $1 \le r \le n-1$,

$$\begin{aligned} c(n,r) &= c(n-1,r-1) + c(n-1,r) \\ &= \frac{(n-1)!}{(r-1)!(n-r)!} + \frac{(n-1)!}{(r)!(n-1-r)!} \\ &= \frac{(n-1)!}{(r-1)!(n-1-r)!}\left[\frac{1}{n-r} + \frac{1}{r}\right] \\ &= \frac{(n-1)!}{(r-1)!(n-1-r)!} \cdot \frac{n}{(n-r)r} \\ &= \frac{n!}{r!(n-r)!} \end{aligned}$$

as was to be shown. The lemma is therefore proved by induction. □

Corollary 13. $\binom{n-1}{r-1} + \binom{n-1}{r} = \binom{n}{r}$.

We therefore know that for each n, $\binom{n}{0} = \binom{n}{n} = 1$, and $\binom{n}{r} = \binom{n-1}{r} + \binom{n-1}{r-1}$ for $1 \leq r \leq n-1$. Using these facts we can prove the Binomial Theorem by induction on n.

Proof of the Binomial Theorem. For $n = 1$, $(x+y) = \binom{1}{0}x + \binom{1}{1}y$ so the binomial theorem is true when $n = 1$. Assume $n > 1$ and the theorem is true for $n-1$, that is,

$$(x+y)^{n-1} = \binom{n-1}{0}x^{n-1} + \binom{n-1}{1}x^{n-2}y^2 + \ldots + \binom{n-1}{r}x^{n-1-r}y^r + \ldots + \binom{n-1}{n-1}y^{n-1}.$$

We compute $(x+y)^n$ as follows:

$$(x+y)^n = (x+y)\cdot(x+y)^{n-1} = x(x+y)^{n-1} + y(x+y)^{n-1}.$$

Multiplying the expansion of $(x+y)^{n-1}$, above, by x and by y, and adding, we get

$$(x+y)^n = \binom{n-1}{0}x^n + \binom{n-1}{1}x^{n-1}y + \ldots + \binom{n-1}{n-1}xy^{n-1} + \binom{n-1}{0}x^{n-1}y + \ldots + \binom{n-1}{n-2}xy^{n-1} + \binom{n-1}{n-1}y^n.$$

Thus the coefficient of $x^{n-r}y^r$ for $r = 1, \ldots, n-1$ is

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

by Lemma 3. Since

$$\binom{n-1}{0} = 1 = \binom{n}{0}, \binom{n-1}{n-1} = 1 = \binom{n}{n},$$

we see that

$$(x+y)^n = \binom{n}{0}x^n + \ldots + \binom{n}{r}x^{n-r}y^r + \ldots + \binom{n}{n}y^n,$$

which proves the Binomial Theorem by induction. □

Exercises.

36. Prove that the sum of the elements of the nth row of Pascal's triangle is 2^n for each n. (How many subsets of a set with n elements are there?)

37. Prove that

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

for all s and all $n \geq s$.

38. Prove that for all $n \geq 1$,

$$\binom{n}{0}^2 + \binom{n}{1}^2 + \ldots + \binom{n}{n}^2 = \binom{2n}{n}.$$