

Math 109 - Examples of Proof by Induction

In this handout we illustrate proofs by induction from several areas of mathematics: linear algebra, algebra, and calculus. Becoming comfortable with induction proofs is almost entirely a matter of having lots of experience.

Induction proofs of summation identities like $\sum_{k=1}^n k = n(n+1)/2$ are not good models for general induction proofs, because most proofs which use induction involve the proof of *properties* (of numbers or functions or other objects) rather than algebraic identities.

Moreover, while the inductive step in the proof of a summation identity involves a direct *derivation* of the new case from a previously proved case (often by adding a common term to both sides of an equation), many induction proofs have an inductive step which involves a *reduction* of the new case to some previously proved case.

For example, theorems about polynomials that are proved by induction on the degree often reduce a theorem about polynomials of degree $d+1$ to a theorem about polynomials of degree d (or of degree at most d) instead of starting with polynomials of degree d and building up to polynomials of degree $d+1$.

Linear Algebra

Theorem 1 *Suppose $B = MAM^{-1}$, where A and B are $n \times n$ matrices and M is an invertible $n \times n$ matrix. Then $B^k = MA^kM^{-1}$ for all integers $k \geq 0$. If A and B are invertible, this equation is true for all integers k .*

Proof. We argue by induction on k , the exponent. (Not on n , the dimension of the matrix!)

The result is obvious for $k=0$, when both sides equal the $n \times n$ identity matrix I . When $k=1$, the equation $MA^1M^{-1} = B^1$ is just the original condition $MAM^{-1} = B$.

Let's see what happens in the case when $k=2$:

$$\begin{aligned} B^2 &= B \cdot B \\ &= (MAM^{-1}) \cdot (MAM^{-1}) \\ &= MA(M^{-1}M)AM^{-1} \\ &= MAIAM^{-1} \\ &= MAAM^{-1} \\ &= MA^2M^{-1} \end{aligned}$$

Now assume the result is established for exponent k . Then

$$\begin{aligned} B^{k+1} &= B^k \cdot B \\ &= (MA^kM^{-1}) \cdot (MAM^{-1}) \\ &= MA^k(M^{-1}M)AM^{-1} \\ &= MA^kIAM^{-1} \\ &= MA^k \cdot AM^{-1} \\ &= MA^{k+1}M^{-1} \end{aligned}$$

Thus, the result is true for exponent $k+1$ if it is true for exponent k .

Since the base case $k = 1$ is true, and assuming the k^{th} case is true implies the $(k + 1)^{\text{th}}$ case is true, we conclude that the theorem is true for all integers $k \geq 0$.

If A and B are invertible, the result holds for negative exponents as well, since for $k > 0$

$$\begin{aligned}
 (MA^k M^{-1}) \cdot (MA^{-k} M^{-1}) &= MA^k (M^{-1} M) A^{-k} M^{-1} \\
 &= MA^k I A^{-k} M^{-1} \\
 &= MA^k A^{-k} M^{-1} \\
 &= M I M^{-1} \\
 &= M M^{-1} \\
 &= I,
 \end{aligned}$$

and thus

$$\begin{aligned}
 MA^{-k} M^{-1} &= \text{inverse of } MA^k M^{-1} \\
 &= \text{inverse of } B^k \quad (\text{by the result for } k > 0) \\
 &= B^{-k}. \quad \square
 \end{aligned}$$

Algebra

Theorem 2 For any integer $n \geq 1$ and any $a \in \mathbf{R}$, $x^n - a^n = (x - a)Q(x)$ for some polynomial $Q(x)$ of degree $n - 1$.

Proof. We induct on the exponent n .

When $n = 1$, $x^1 - a^1 = (x - a) \cdot 1$, so we let $Q(x) = 1$.

Now assume that the theorem is true for n . We must show that it also holds true for $n + 1$. Observe that

$$\begin{aligned}
 x^{n+1} - a^{n+1} &= x^n \cdot x - a^n \cdot a \\
 &= (x^n - a^n + a^n) \cdot x - a^n \cdot a \quad (\text{a propitious zero}) \\
 &= (x^n - a^n) \cdot x + a^n \cdot x - a^n \cdot a \\
 &= (x^n - a^n) \cdot x + a^n \cdot (x - a)
 \end{aligned}$$

By the inductive hypothesis, $x^n - a^n = (x - a)Q(x)$ where $Q(x)$ has degree $n - 1$. Thus,

$$\begin{aligned}
 x^{n+1} - a^{n+1} &= (x - a)Q(x) \cdot x + a^n \cdot (x - a) \\
 &= (x - a)(x \cdot Q(x) + a^n)
 \end{aligned}$$

Since $Q(x)$ has degree $n - 1$, $x \cdot Q(x)$ has degree $(n - 1) + 1 = n > 0$, and so $x \cdot Q(x) + a^n$ also has degree n . Let $x \cdot Q(x) + a^n$ be the “new” choice of polynomial, thus establishing the theorem for the $n + 1$ case.

The base case $n = 1$ is true, and the n^{th} case being true implies the $(n + 1)^{\text{th}}$ case is true, so by induction the theorem holds true for all positive integers n . \square

Remark 1: Writing the polynomial $Q(x)$ as $Q_{n,a}(x)$ to indicate its dependence on n and a , we gave in the proof the recursion $Q_{n+1,a}(x) = xQ_{n,a}(x) + a^n$, which lets us compute $Q(x)$ for small n starting with $Q_{1,a}(x) = 1$:

$$Q_{1,a}(x) = 1, \quad Q_{2,a}(x) = x + a, \quad Q_{3,a}(x) = x^2 + ax + a^2.$$

You can show (by induction on n !) that

$$Q_{n,a}(x) = x^{n-1} + ax^{n-2} + \cdots + a^{n-2}x + a^{n-1} = \sum_{i=0}^{n-1} a^i x^{n-1-i}.$$

Remark 2: By the first remark, when a is real $Q(x)$ has real coefficients.

Theorem 3 *Let $f(x)$ be a nonconstant polynomial with real coefficients, with degree d . Then $f(x)$ has at most d real roots.*

Remark: We can't replace "at most d real roots" with "exactly d real roots" since there are nonconstant polynomials like $x^2 + 1$ which have real coefficients and no real roots.

Proof. We induct on the degree d of $f(x)$. Note $d \geq 1$.

A polynomial of degree 1 with real coefficients is of the form $f(x) = ax + b$, where a and b are real and $a \neq 0$. This has exactly one root, namely $-b/a$, and thus *at most* one real root. That settles the theorem for $d = 1$.

Now assume the theorem is true for all polynomials of degree d with real coefficients. We verify the theorem for all polynomials of degree $d + 1$ with real coefficients.

A typical polynomial of degree $d + 1$ with real coefficients is

$$f(x) = c_{d+1}x^{d+1} + c_d x^d + \cdots + c_1 x + c_0, \tag{1}$$

where $c_j \in \mathbf{R}$ and $c_{d+1} \neq 0$. If $f(x)$ has no real roots, then we're done, since $0 \leq d + 1$. If $f(x)$ has a real root, say r , then

$$0 = c_{d+1}r^{d+1} + c_d r^d + \cdots + c_1 r + c_0. \tag{2}$$

Subtracting (2) from (1), the terms c_0 cancel and we get

$$f(x) = c_{d+1}(x^{d+1} - r^{d+1}) + c_d(x^d - r^d) + \cdots + c_1(x - r) = \sum_{j=1}^{d+1} c_j(x^j - r^j). \tag{3}$$

By Theorem 2 on this handout (!),

$$x^j - r^j = (x - r)Q_j(x) \tag{4}$$

for some polynomial $Q_j(x)$ of degree $j - 1$. By the remarks after the proof of Theorem 2, $Q_j(x)$ has real coefficients since r is real. Substituting (4) into (3), we have

$$\begin{aligned}
f(x) &= \sum_{j=1}^{d+1} c_j(x-r)Q_j(x) \\
&= (x-r) \sum_{j=1}^{d+1} c_j Q_j(x) \\
&= (x-r) \underbrace{(c_{d+1} Q_{d+1}(x))}_{\neq 0} + \underbrace{\cdots + c_1 Q_1(x)}_{\text{lower degree}}.
\end{aligned}$$

Since $c_{d+1}Q_{d+1}(x)$ is a polynomial of degree d , and each lower degree polynomial does not decrease the degree of the second factor, the second factor has degree d . Since each $Q_j(x)$ has real coefficients and all c_j are real, the second factor has real coefficients. We can therefore apply the inductive hypothesis to the second factor and conclude that the second factor has at most d real roots. Since any root of $f(x)$ is either r or a root of the second factor, we conclude $f(x)$ has at most $d + 1$ real roots. As $f(x)$ was an arbitrary polynomial of degree $d + 1$ with real coefficients, we have shown that the d^{th} case being true implies the $(d + 1)^{\text{th}}$ case is true. By induction, the theorem holds true for all nonconstant polynomials. \square

Remark: The theorem also holds for polynomials of degree $d = 0$ (i.e., constant polynomials) except for the polynomial 0. That is, a nonzero constant polynomial has 0 real roots, and 0 is the degree of a nonzero constant polynomial. Note that the polynomial 0 has all numbers as roots, so the theorem can't be extended to include the polynomial 0. In fact, usually the polynomial 0 isn't considered to have a degree, since the definition of the degree of a polynomial (namely, the exponent of the largest power of x with a nonzero coefficient) doesn't make any sense for the polynomial 0.

Our next theorem uses the "strong" form of induction, where we argue from all earlier cases to the next case rather than from one case to the next case.

Theorem 4 *i) Every integer $n > 1$ has a prime factor.*
ii) Every nonconstant polynomial has an irreducible factor.

Remember that a positive integer is called prime when its only positive integer factors are 1 and itself. A nonconstant polynomial is called irreducible when its only polynomial factors are constants and constant multiples of itself. (For example, $x = 2(x/2) = 5(x/5)$ are factorizations of x which only involve modifications by constant multiples. The polynomial x is irreducible.)

Proof. For part (i), we induct on n .

The integer 2 is prime, and 2 is a factor of 2, so the case $n = 2$ is settled.

Assuming every integer $\leq n$ has a prime factor, consider now the integer $n + 1$. If $n + 1$ is prime, then $n + 1$ has a prime factor (namely itself). If $n + 1$ is not prime, then we can factor $n + 1$, say $n + 1 = ab$ where $2 \leq a, b < n + 1$. By our (strong) inductive assumption,

the condition $2 \leq a \leq n$ implies a has a prime factor, and this prime will also be a factor of $n + 1$ since a is a factor of $n + 1$. Thus $n + 1$ has a prime factor and we are done.

For part (ii), we induct on the degree d of a nonconstant polynomial. This proof will be very similar to part (i), with “integer” replaced by “polynomial” and “prime” replaced by “irreducible.”

When $d = 1$, the polynomial is linear. Linear polynomials are irreducible, so the case $d = 1$ is settled.

Assuming every nonconstant polynomial with degree $\leq d$ has an irreducible factor, consider a polynomial $f(x)$ with degree $d + 1$. If $f(x)$ is irreducible, then $f(x)$ has an irreducible factor (namely itself). If $f(x)$ is not irreducible, then we can factor $f(x)$, say $f(x) = g(x)h(x)$ where $g(x)$ and $h(x)$ are nonconstant, so $1 \leq \deg g(x)$, $\deg h(x) < d + 1$. By our (strong) inductive assumption, $g(x)$ has an irreducible factor, and this irreducible polynomial will also be a factor of $f(x)$ since $g(x)$ is a factor of $f(x)$. Thus $f(x)$ has an irreducible factor and we are done. \square

Calculus

Theorem 5 For differentiable functions $f_1(x), \dots, f_n(x)$,

$$\frac{(f_1(x) \cdots f_n(x))'}{f_1(x) \cdots f_n(x)} = \frac{f_1'(x)}{f_1(x)} + \cdots + \frac{f_n'(x)}{f_n(x)}.$$

Proof. We induct on n , the number of functions.

When $n = 1$, it is clear since both sides equal $f_1'(x)/f_1(x)$.

When $n = 2$, the result follows from the product rule

$$(f_1(x) \cdot f_2(x))' = f_1'(x) \cdot f_2(x) + f_1(x) \cdot f_2'(x)$$

by dividing both sides by $f_1(x)f_2(x)$. (Check this!)

Now assume the result for n functions. When $f_1(x), \dots, f_{n+1}(x)$ are differentiable functions, we write their product as

$$f_1(x)f_2(x) \cdots f_{n+1}(x) = (f_1(x) \cdots f_n(x)) \cdot f_{n+1}(x).$$

Considering $f_1(x) \cdots f_n(x)$ as a single function, we can use the case $n = 2$:

$$\begin{aligned} \frac{(f_1(x) \cdots f_{n+1}(x))'}{f_1(x) \cdots f_{n+1}(x)} &= \frac{((f_1(x) \cdots f_n(x)) \cdot f_{n+1}(x))'}{(f_1(x) \cdots f_n(x)) \cdot f_{n+1}(x)} \\ &= \frac{(f_1(x) \cdots f_n(x))'}{f_1(x) \cdots f_n(x)} + \frac{f_{n+1}'(x)}{f_{n+1}(x)} && \text{(Case } n = 2) \\ &= \frac{f_1'(x)}{f_1(x)} + \cdots + \frac{f_n'(x)}{f_n(x)} + \frac{f_{n+1}'(x)}{f_{n+1}(x)} && \text{(Inductive Hypothesis)} \end{aligned}$$

and this is what we needed to show for $n + 1$ functions. \square

Remark From a logical point of view, our proof has a gap in the case $n = 2$: we appealed to everyone's familiarity with the product rule rather than include a proof of it. If we were to give a complete proof of the theorem, we should give a proof of the product rule, which would involve going back to the rigorous definition of derivatives involving limits and ε 's and δ 's. The inductive step in the proof of Theorem 5 is much simpler than the proof of the product rule, which illustrates a subtle point: some induction proofs have their primary technical difficulty not in the inductive step, but in one of the initial cases.