11 Mathematical Induction [12]

The Principle of Mathematical Induction (PMI), which was introduced briefly in section 7 is a very powerful proof technique. There are many variants of this principle, and most students have seen some version of it. The version we discuss here is more complicated than the version typically taught in introductory courses, but has important advantages:

1. It fits well with the general method of proving universal assertions. (The more common methods do not.)

2. It is harder to misuse than the more common methods. (This is crucial; the more commonly taught versions of induction are often misapplied by students.)

Important. Even if you think you already know induction, you should learn to apply it according to the method presented here.

Before presenting the details of the principle of mathematical induction let's understand the situations to which it applies.

We've seen that to prove a universal assertion, we start by setting up the scenario that represents the hypothesis of the assertion. This scenario involves certain hypothetical objects, and certain assumptions. We then use the information of the scenario to work towards the desired conclusion.

The principle of mathematical induction says that in certain common situations there is an additional assumption, called the *induction assumption* or *induction hypothesis*, that you are permitted to add to your list of assumptions. We'll state this assumption below. As with any assumption you are not required to use it, but may use it if it is helpful.

The principle of mathematical induction is often useful when proving universal assertions when the universe of the assertion is:

- The set of nonnegative integers, or the set of positive integers, or the set of integers greater than or equal to some fixed number.

- The set of finite subsets of some set.

- The set of finite lists with entries in some set.

It is typically not useful if the universe of the assertion is the set of all real numbers, or involves infinite sets. As we'll see later, the principle applies more generally whenever the universe is partially ordered and the partial order satisfies a condition called the *descending chain condition*. But that's later; for now we'll start with the simplest situation for induction: when the universe is the set of nonnegative integers.

[12] Version 4/10/2015.

The principle of mathematical induction for nonnegative integers Suppose we want to prove a universal principle about the set of nonnegative integers, of the form:

> For all $n \in \mathbb{Z}_{\geq 0}$, we have $C(n)$,

As always, our proof of such an assertion starts something like:

> Suppose n is an arbitrary member of $\mathbb{Z}_{\geq 0}$. We must prove $C(n)$.

The principle of mathematical induction says that in such a proof you are permitted to use the following assumption, called the *induction assumption* or the *induction hypothesis*.

> For all $k \in \mathbb{Z}_{\geq 0}$ such that $k < n$, we have $C(k)$.

Some key questions Some questions you should be asking are:

1. What does the inductive assumption mean?
2. How is this assumption helpful in doing proofs?
3. Why are we alowed to make this assumption?

The simple (but not entirely satisfactory) answer to the third question is:

> The principle of mathematical induction is *safe to use*'; if used properly it will never lead you to think that you've proved an assertion that is false. In other words, any universal assertion that can be proved using the induction assumption is indeed true.

The reason why this answer may be unsatisfying is that it doesn't explain *why* the principle of mathematical induction is "safe to use". We'll discuss this later. For now, the student should simply accept that the principle is safe to use and concentrate on the first two questions above.

11.1 A first example of mathematical induction: recurrence equations

A sequence of real numbers is an infinite list indexed by either the set of positive integers, or the set of nonnegative integers. Sequences are most easily described as a function that expresses the nth term in the sequence in terms of n. For example the sequence with $a_n = 2n - 1$ for $i \geq 1$ is the sequence $1, 3, 5, \ldots$ of positive odd integers and the sequence $a_n = 1/n$ for $n \geq 1$ is the sequence $1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}$ of recipricols of integers.

Another common way to describe a sequence is by a *recurrence equation*. A recurrence equation for a sequence expresses the nth term (for each n) *as a function of the previous terms*.

Example 11.1. Consider the sequence $(b_n : n \geq 1)$ described by:

$$b_n = \begin{cases} b_{n-1} + 3 & \text{if } n \geq 2 \\ 1 & \text{if } n = 1. \end{cases}$$

We can figure out the terms of this sequence starting from $b_1 = 1$ by applying the recurrence equation, to get $b_2 - 4$, $b_3 = 7$, $b_4 = 10$, etc.

In the above definition of the sequence, we give a recurrence equation for b_n in terms of b_{n-1}. This definition is valid only for $n \geq 2$. For $n = 1$, we can't express b_1 in terms of b_0 since b_0 does not exist. Instead, the definition specifies a value for b_1, which is the *initial condition* for the sequence.

Example 11.2. Consider the sequence $(d_n : n \geq 1)$ given by:

$$d_n = \begin{cases} \frac{d_{n-1}^2}{d_{n-2}} & \text{if } n \geq 3 \\ 2 & \text{if } n = 1 \\ 3 & \text{if } n = 2 \end{cases}$$

We can compute $d_1 = 2$, $d_2 = 3$, $d_3 = \frac{9}{2}$, $d_4 = \frac{27}{4}$. In this recurrence, d_n is expressed as a function of the two previous terms. This recurrence is valid only for $n = 3$ since d_{n-2} is not defined for $n \leq 2$. So our initial condition specifies both d_1 and d_2.

Example 11.3. Consider the sequence $(c_n : n \geq 1)$ given by that for all $n \geq 1$,

$$c_n = 1 + \sum_{j=1}^{n-1} c_j$$

Here the recurrence expresses c_n as a function of *all* previous terms. Note that there is no separate initial condition. This is okay here because the recurrence equation is well-defined even for $n = 1$; in that case we get $c_1 = 1$ because the summation is the empty summation, which is defined to be 0. Again we can compute c_1, c_2, c_3 one term at a time by: $c_1 = 1$, $c_2 = 2$, $c_3 = 1 + 1 + 2 = 4$, $c_4 = 1 + 1 + 2 + 4 = 8$.

Example 11.4. Consider the sequence $(r_n : n \geq 1)$ given by:

$$d_n = \begin{cases} r_{n-1} + 1/r_{n-1} & \text{if } n \geq 2 \\ 1 & \text{if } n = 1. \end{cases}$$

Computing the first few terms we see that $r_1 = 1$, $r_2 = 2$, $r_3 = 2\frac{1}{2}$, $r_4 = 2\frac{9}{10}$.

A recurrence equation gives us an easy way to compute the terms one at a time, but does not immediately give us a good way to compute, or even estimate, specific terms in the sequence without computing all all the terms that come before. What we'd like is to *solve the recurrence*

which means to give a formula that expresses the nth term as an easily computable function of n.

The study of recurrence equations is a rich and interesting subject, with many parallels with the theory of differential equations. There is no general way known that can be recurrence equation, but methods have been developed for solving certain types of recurrences. These methods are quite elegant and interesting and very worthy of study, but our reason for studying recurrences here is different: they provide a simple illustration of the use of induction in proofs.

It is sometimes possible to guess a solution to a recurrence by discovering a pattern in the few terms. If we have a correct guess for a solution, we can usually prove our guess to be correct using mathematical induction.

Let's go back to the example of $(b_n : n \geq 1)$ above. Looking at the first few terms it's not hard to make a guess that $b_n = 3n - 2$ for all $n \geq 1$. Let's use induction to prove that this guess is correct.

Proposition 11.1. *Let $(b_n : n \geq 1)$ be the sequence defined by $b_1 = 1$ and for $n \geq 2$, $b_n = b_{n-1} + 3$. For all positive integers n, $b_n = 3n - 2$.*

Proof. Suppose n is an arbitrary positive integer; we must show that $b_n = 3n-2$. By induction we may assume that for all positive integers k that satisfy $k < n$, $b_k = 3k-2$. two cases: $n = 1$ and $n \geq 2$.
Case 1. Assume $n = 1$. Then $b_n = 1$ which equals $3(1) - 2$.
Case 2. Assume $n \geq 2$. Then $b_n = b_{n-1} + 3$. Since $n - 1 \geq 1$ we have that $n - 1$ is a positive integer less than n and so may use the induction hypothesis to say that $b_{n-1} = 3(n - 1) - 2 = 3n - 5$. Then $b_n = b_{n-1} + 3 = (3n - 5) + 3 = 3n - 2$ as required. □

Remark 11.1.

1. Notice that the proof breaks into two cases. In one case, we use the induction hypothesis and in the other we don't. This is typical. The case that uses the induction hypothesis is sometimes called the *inductive case* and the case that does not is called the *base case*. In this example, the base case consists only of the case $n = 1$. This is very common, but we'll see later that the base case may sometimes involve more than a single value of n.

2. Notice that in the *inductive case*, we apply the induction assumption to $n - 1$. This may look as though we are assuming what we are trying to prove, but we aren't! Here n represents an arbitrary positive integer, and we must draw a conclusion about n. We use the inductive assumption to say that the conclusion of the theorem holds for $n - 1$, not n.

3. Before applying the induction assumption to $n - 1$ (or to any number) we must check that it satisfies the hypotheses of the induction assumption, specifically, that it is less than n and is at least 1.

4. In the case $n = 1$, the induction assumption gives us no information since there are no positive integers k that are less than n.

Exercise 11.1. Use mathematical induction to prove that for all positive integers n, the nth odd number is $2n-1$.

Exercise 11.2. For the sequence $(c_n : n \geq 1)$ given above, it is not hard to guess that $c_n = 2^{n-1}$ for all n. Use mathematical induction to prove this.

Next we consider the sequence $(d_n : n \geq 1)$ defined by the above recurrence. It is not hard to guess that $d_n = 3^{n-1}/2^{n-2}$ for all $n \geq 1$.

Proposition 11.2. *The sequence $(d_n : n \geq 1)$ given by the recurrence $d_n = \frac{d_{n-1}^2}{d_{n-2}}$ for $n \geq 3$, and the initial conditions $d_1 = 2$, $d_2 = 3$, satisfies $d_n = 3^{n-1}/2^{n-2}$ for all $n \geq 1$.*

Proof. Suppose n is an arbitrary integer; we must show $d_n = 3^{n-1}/2^{n-2}$. We will use induction. Since the recurrence is only valid for $n \geq 3$ we break into cases according to whether $n \geq 3$ or $n \leq 2$.
Case 1. Assume $n \leq 2$. For $n = 1$ we have $3^{n-1}/2^{n-2} = 2$ as required, and for $n = 2$ we have $3^{n-1}/2^{n-2} = 3$ as required.
Case 2. Assume $n \geq 3$. Then $d_n = \frac{d_{n-1}^2}{d_{n-2}}$. Since $n-1$ and $n-2$ are at least 1 and less than n we can apply the induction hypothesis to conclude that $d_{n-1} = 3^{n-2}/2^{n-3}$ and $d_{n-2} = 3^{n-3}/2^{n-4}$. Substituting into the recurrence we get:

$$d_n = \left(\frac{3^{n-2}}{2^{n-3}}\right)^2 / \frac{3^{n-3}}{2^{n-4}} = \frac{3^{2n-4-(n-3)}}{2^{2n-6-(n-4)}} = \frac{3^{n-1}}{2^{n-2}}.$$

□

Sum sequences and simple recurrences Here's a common situation that leads to a recurrence equation. Given any sequence $a = a_1, a_2, \ldots$ is a sequence of numbers, we can form from a a new sequence $s = s_0, s_1, \ldots$, where s_j is the sum of the first j terms of a (and so $s_0 = 0$). We say that s is the *partial sum sequence of the sequence a*. The sequence $(s_n : n \geq 0)$ satisfies the recurrence equation $s_n = s_{n-1} + a_n$, with the initial condition $s_0 = 0$.

Consider the following example: Suppose $(a_j : j \geq 1)$ is the sequence of positive odd numbers and for each positive $n \geq 0$, s_n be the sum of the first n positive odd numbers. We have $s_0 = 0$, $s_1 = 1$, $s_2 = 1+3 = 4$, $s_3 = 1+3+5 = 9$ and $s_4 = 1+3+5+7 = 16$. The pattern suggests that $s_n = n^2$ for every nonnegative integer n and the obvious question is whether this pattern holds for all terms of the sum sequence. The answer is yes:

Theorem 11.3. *For all nonnegative integers n, the sum of the first n positive odd integers is n^2.*

Proof. For $j \geq 1$, let a_j denote the jth positive odd number and for $j \geq 0$, let s_j denote the sum of the first j positive odd integers. An earlier exercise shows that $a_j = 2j - 1$ for all positive integers j. Suppose n is an arbitrary nonnegative integer. We must show $s_n = n^2$. By induction, we may assume that for all nonnegative integers k that are less than n, $s_k = k^2$. We consider two cases:

Case 1. Assume $n = 0$. Then $s_0 = 0$ which is equal to 0^2 as required.
Case 2. Assume $n \geq 1$. We have $s_n = s_{n-1} + a_n = s_{n-1} + (2n-1)$. Since $n-1$ a nonnegative integer that is less than n we may use the induction hypothesis to say that $s_{n-1} = (n-1)^2$. Therefore $s_n = (n-1)^2 + 2n - 1 = n^2 - 2n + 1 + (2n-1) = n^2$, as required. □

Exercise 11.3. Use mathematical induction to prove that for any real number r and any nonnegative integer n we have $\sum_{i=1}^{n} r^i = \frac{1-r^{n+1}}{1-r}$.

Bounding the solution to a recurrence Earlier, we gave the following recurrence equation as an example: The sequence $(r_n : n \geq 1)$ is given by $r_1 = 1$, and $r_n = r_{n-1} + 1/r_{n-1}$ for $n \geq 3$. If you compute the first several values of r_n there is no obvious pattern, and in fact, there is no simple formula for d_n. When we don't have an exact formula, we can try to find upper bounds or lower bounds. By examining more terms of the sequence d_n, it is possible to make a guess of an upper bound, and verify it by induction:

Proposition 11.4. *For the sequence $(r_n : n \geq 1)$ defined above, we have that for all positive integers n, $r_n \geq \sqrt{2n-1}$ and $r_n \leq \sqrt{3n-2}$.*

We'll prove the upper bound and leave the lower bound as an exercise.

Proof. Suppose n is an arbitrary positive integer. We must show $r_n \leq \sqrt{3n-2}$. By induction we may assume that for all positive integers k satisfying $k < n$ we have $r_k \leq \sqrt{3k-2}$. We consider two cases.
Case 1. Assume $n = 1$. Then $d_1 = 1 \leq \sqrt{3(1)-2}$.
Case 2. Assume $n \geq 2$. We have $r_n = r_{n-1} + \frac{1}{r_{n-1}}$. By the induction hypothesis, we have $r_{n-1} \leq \sqrt{3n-5}$.

We'd like to say that since $r_n = r_{n-1} + \frac{1}{r_{n-1}}$ and $r_{n-1} \leq \sqrt{3n-5}$, that $r_n \leq \sqrt{3n-5} + \frac{1}{\sqrt{3n-5}}$. But it is not clear that this is valid. Why not? Well it's true that $r_{n-1} \leq \sqrt{3n-5}$ but when we use this to bound $\frac{1}{r_{n-1}}$ we don't get $\frac{1}{r_{n-1}} \leq \frac{1}{\sqrt{3n-5}}$ but rather we get $\frac{1}{r_{n-1}} \geq \frac{1}{\sqrt{3n-5}}$, with the inequality in the opposite direction to what we want!

So, instead of separately bounding r_{n-1} and $\frac{1}{r_{n-1}}$ we directly derive an upper bound on the sum. For this we need:

Proposition 11.5. *The function $f : (0, \infty) \longrightarrow \mathbb{R}$ given by $f(x) = x + 1/x$ is increasing on $[1, \infty)$.*

Exercise 11.4. Prove Lemma 11.5.

Using this Proposition, we have that since $\sqrt{3n-5} \geq r_{n-1} \geq 1$, $r_{n-1} + \frac{1}{r_{n-1}} \leq \sqrt{3n-5} + \frac{1}{\sqrt{3n-5}}$. Call the last quantity t. We want to show that $t \leq \sqrt{3n-2}$, We will do this by first showing that $t^2 \leq 3n-2$ and then deducing that $t \leq \sqrt{3n-2}$.

We have:

$$t^2 = (\sqrt{3n-5} + \frac{1}{\sqrt{3n-5}})^2 = 3n - 5 + 2 + \frac{1}{3n-2} \leq 3n - 2,$$

since for $n \geq 2$, $\frac{1}{3n-2} \leq 1$. So we've shown $t^2 \leq 3n-2$. We want to show that if you take square root of both sides the inequality still holds. For this we need:

Proposition 11.6. *The function $g : (0, \infty) \longrightarrow \mathbb{R}$ given by $g(x) = \sqrt{x}$ is increasing.*

Exercise 11.5. Prove Proposition 11.6.

From this and $t^2 \leq 3n-2$ we conclude that $t \leq \sqrt{3n-2}$ as required. □

Exercise 11.6. Prove the lower bound $r_n \geq \sqrt{2n-1}$ for all positive integers n.

Proving inequalities using PMI We now consider the problem of proving inequalities of the form "for all $n \in S$, $f(n) \geq g(n)$ where f and g are functions of the set of the positive integers, and S is a subset of the positive integers.

Example 11.5. Prove that for all nonnegative integers n, $2^n > n$.

We'll use induction. Let's think it through before writing the proof. When we prove $2^n > n$ we'll want to use the induction assumption to say $2^{n-1} > n-1$. We can do this provided that $n-1 \geq 0$. So we'll divide into two cases $n = 0$ and $n \geq 1$.

Proof. Suppose n is an arbitrary nonnegative integer. We must show that $2^n > n$. By induction, we may assume that for all nonnegative integers k, if $k < n$ then $2^k > k$.

We divide into two cases, $n = 0$ and $n \geq 1$.

Case 1. Assume $n = 0$. Then $2^n = 1 > 0 = n$.

Case 2. Assume $n \geq 1$. Then $n - 1 \geq 0$ so by the induction hypothesis, $2^{n-1} > n-1$. Note also that $2^{n-1} \geq 1$. Adding these two equations we get $2^{n-1} + 2^{n-1} > n$, so $2^n > n$, as required. so by the induction hypothesis, $2^{n-1} > n-1$. □

Example 11.6. Suppose we try to prove that for all nonnegative numbers n, $2^n \geq n^2$. We might try this by induction. Once again, we introduce n and assume that the result is true for $k = n-1$. We then get $2^{n-1} \geq (n-1)^2 \geq n^2 - 2n + 1$. If we add $2n-1$ to both sides we get: $2^{n-1} + 2n - 1 \geq n^2$. To finish the proof we'd like to show that $2^n \geq 2^{n-1} + 2n - 1$, and for this it's enough to show $2^{n-1} \geq 2n - 1$. But this inequality is not true for $n = 2$ or $n = 3$, though it is true for $n \geq 4$.

This suggests breaking into cases $n \leq 3$ and $n \geq 4$. But when we check $n = 3$, we find that the result is false since $2^3 < 3^2$. So instead of proving the proposition, we found a counterexample!

Next we ask: can we restrict the hypothesis to make a true proposition? Notice that the inequality is true for $\tilde{n} = 4$ and perhaps the following is true.

For all natural numbers n, if $n \geq 4$, then $2^n \geq n^2$.

When we try to prove this, we will use the induction hypothesis for $k = n-1$. We will then need that $n - 1 \geq 4$, so we'll need $n \geq 5$. This suggests we break into the cases $n = 4$ and $n \geq 5$.

Proof. Suppose n is an arbitrary nonnegative integer. Assume $n \geq 4$. We must show that $2^n \geq n^2$. By induction, we may assume that for all natural numbers k if $k < n$ then if $k \geq 4$, $2^k \geq k^2$. We split into two cases: $n = 4$ and $n \geq 4$.
Case 1. Assume $n = 4$. Then $2^4 = 4^2$.
Case 2. Assume $n \geq 5$. Then $n - 1$ is a natural number satisfying $n - 1 \geq 4$ and so by the induction hypothesis, $2^{n-1} > (n-1)^2$. Multiplying by 2 we get $2^n > 2(n-1)^2$. If we can show $2(n-1)^2 \geq n^2$ we'll be done, which is the same as $2(n-1)^2 - n^2 \geq 0$, which is the same as $n^2 - 4n + 2 \geq 0$. Since $n \geq 5$, we have $n^2 \geq 5n$ so $n^2 - 4n + 2 \geq n + 2 \geq 0$. Therefore $2(n-1)^2 \geq n^2$ and therefore $2^n \geq 2(n-1)^2 \geq n^2$ as required. □

Binomial coefficients So far, we've considered infinite sequences whose index set is the set of integers greater than some fixed integer.

In the same way that lists can have more complicated (finite) index sets, we can have infinite indexed families of numbers: For example we might consider the following: $(a_{n,k} : k, n \in \mathbb{Z}_{\geq 0})$ with $a_{n,k} = n^2 - k^2$. This is called a *doubly-indexed sequence* since it has two indices.

We now consider a pariticular doubly-indexed sequence of numbers $(c_{n,k} : k, n \in \mathbb{Z}, 0 \leq k \leq n\}$ given by the following:

$$c_{n,k} = \begin{cases} c_{n-1,k} + c_{n-1,k-1} & \text{if } 0 < k < n \\ c_{n,k} = 1 & \text{if } k = 0 \text{ or } k = n \end{cases}.$$

When we are given a recurrence like this, there are two important questions:

- Is there any doubly-indexed sequence that satisfies these conditions?
- Are there more than one doubly-indexed sequences these conditions?

Intuitively, we can argue that there is one, and only, one solution to this recurrence equation. For every nonnegative integer n we have $c_{n,0} = 1$ and $c_{n,n} = 1$. Using these we can compute $c_{n,k}$ for each n and k with $0 \leq k \leq n$. To do this we start with $n = 1$ and work our way up. For each n we compute $c_{n,k}$ for each k between 1 and $n - 1$ using the values of $c_{n-1,k}$ and $c_{n-1,k-1}$ already computed. This intuitive argument can be turned into a formal proof, but we won't do this here. Instead, let's assume that there is a unique doubly-indexed sequence $(c_{n,k} : 0 \leq k \leq n)$ satisfying the recurrence, and turn to the question of figuring out a formula for $c_{n,k}$.

Recall that the factorial function maps a nonnegative integer n to $n! = \prod_{i=1}^{n} i$. In the case $n = 0$, the product is empty, and we define $0! = 1$. Recall also that for integers k, n with $0 \leq k \leq n$, $\binom{n}{k} = \frac{n!}{k!(n-k)!}$. This gives us a doubly indexed sequence $(\binom{n}{k} : n, k \in \mathbb{Z}, 0 \leq k \leq n)$. The numbers $\binom{n}{k}$ are called the *binomial coefficients*.

Theorem 11.7. *Let $(c_{n,k} : 0 \leq k \leq n)$ be the doubly indexed sequence given by the above recurrence. Then for all nonnegative integers k, n with $k \leq n$ we have $c_{n,k} = \binom{n}{k}$.*

Proof. Suppose n and k are arbitrary nonnegative integers satisfying $k \leq n$. We must show $c_{n,k} = \binom{n}{k}$. We will use induction on n, which means that we may assume that for all nonnegative integers $j < n$, we have that for all nonnegative integers $i \leq j$, $c_{j,i} = \binom{j}{i}$.
Case 1. Assume $k = 0$ or $k = n$. Then $c_{n,k} = 1$ by definition and $\binom{n}{n} = \binom{n}{0} = \frac{n!}{n!0!} = 1$.

Case 2. Assume $0 < k < n$. Then $c_{n,k} = c_{n-1,k} + c_{n-1,k-1}$. By the induction hypothesis, since $0 \leq n-1 < n$ we have that $c_{n-1,k} = \binom{n-1}{k}$ and $c_{n-1,k-1} = \binom{n-1}{k-1}$. So we have:

$$\begin{aligned} c_{n,k} &= \frac{(n-1)!}{(n-1-k)!k!} + \frac{(n-1)!}{(n-k)!(k-1)!} \\ &= \frac{(n-1)!}{(n-1-k)!(k-1)!}(\frac{1}{k} + \frac{1}{n-k}) \\ &= \frac{(n-1)!}{(n-1-k)!(k-1)!}\frac{n}{(k)(n-k)} \\ &= \frac{n!}{(n-k)!k!} = \binom{n}{k}, \end{aligned}$$

as required. □

The Binomial Theorem Suppose a and b are real numbers. By algebraic manipulation, we have $(a+b)^2 = a^2 + 2ab + b^2$ and $(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$. Here we have expressed $(a+b)^2$ and $(a+b)^3$ as a sum of terms, where each term is a *monomial* in a and b, which means that it is a product of some number of a's and some number of b's times an integer coefficient.

Supose now that n is an arbitrary positive integer and we want to express $(a+b)^n$ as a sum of monomials. This is done by the binomial theorem.

Theorem 11.8. *(Binomial Theorem) For any nonnegative integer n and for any real numbers a and b,*

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

Exercise 11.7. Prove the Binomial Theorem.

11.2 Some proofs in elementary number theory

In all of the examples considered so far, when we used the induction hypothesis to prove some fact about n, we used it for $k = n-1$ or both $k = n-1$ and $k = n-2$. This is the most common use of induction, but sometimes looking at $n-1$ does not help, and we need different choices of k. Here are some examples that come up in elementary number theory. (Number theory is the study of the nonnegative integers.)

In this section we'll prove some basic facts that you already know, but probably don't know how to prove.

The decimal representation of an integer Our culture represents integers using the base 10 representation. In this representation we have 10 symbols called digits, which are 0,1,2,3,4,5,6,7,8,9 and which stand for the first 10 nonnegative integers. If $d_0, d_1, \ldots, d_k$ is a sequence of digits then when we write them in reverse order $d_k d_{k-1} \ldots, d_0$ (without commas) this means the number $\sum_{i=0}^{k} d_i 10^i$. This is called the *base 10* or *decimal representation* of an integer. When representing a positive integer, we insist the highest order digit be nonzero, so we don't allow 00353, and instead write 353. There are two key questions:

- Can every positive integer be represented in this way.
- Is the decimal representation of every positive integer unique?

Of course, our experience tells us that these things seem to be true. Now we'll prove them.

Theorem 11.9. *For every positive integer n, there is a unique sequence of digits $d_0, \ldots, d_k$ that gives the decimal representation of n.*

We'll prove this in two parts. First we prove that every positive integer n has a decimal representation. Then we'll prove that n has at most one decimal representation. In the proof of the first part, we'll use induction, but it will not be enough just to apply the induction hypothesis to $n-1$.

Proof. Suppose n is an arbitrary positive integer. We'll show that n has a unique decimal representation. First we prove that n has a decimal representation. Then we'll prove that any two such representations must be the same.

We start by showing that n has a decimal representation.

Case 1. If $n \leq 9$ then n has a single digit decimal representation.

Case 2. Assume $n \geq 10$. We divide into case depending on whether $10|n$ or not.

Subcase 2a. Assume n is divisible by 10. Let $m = n/10$. By the induction assumption, there are numbers $a_0, \ldots, a_t$ such that $m = \sum_{i=0}^{t} a_i 10^i$. Then $n = 10 * m$. Define $c_0, \ldots, c_{t+1}$ by $c_0 = 0$ and for $1 \leq j \leq t+1$, $c_j = a_{j-1}$. Then $n = \sum_{i=0}^{t} a_i 10^{i+1} = \sum_{j=1}^{t+1} a_{j-1} 10^j = \sum_{j=0}^{t+1} c_j 10^j$.

Subcase 2a. Assume 10 is not a divisor of n. Apply the induction hypothesis to $n-1$ to get a decimal representation $b_j b_{j-1} \ldots b_0$ for $n-1$. We claim that $b_0 < 9$. If not then $n-1-9$ is divisible by 10, and so $n-10$ is divisible by 10, contradicting that n is not divisible by 10. Since $b_0 < 9$ we can simply define $c_0 = b_0 + 1$ and $c_j = b_j$ for $j \geq 1$, and then $\sum_{i=0}^{j} c_i 10^i = n$.

This completes the proof that n has a decimal representation. Next we want to prove that the representation is unique.

Lemma 11.10. *For any positive integer j and for any sequence $a_0, \ldots, a_{j-1}$ of digits we have $10^j \geq \sum_{i=0}^{j-1} a_i 10^i$.*

Proof. Suppose j is a positive integer and that $a_0, \ldots, a_{j-1}$ is a sequence of digits. We have $\sum_{i=0}^{j-1} a_i 10^i \leq \sum_{i=0}^{j-1} 9 \times 10^i$, since $a_i \leq 9$ for each i. Now using the formula for geometric series, $\sum_{i=0}^{j-1} 10^i = (10^j - 1)/9$, so multiplying by 9 gives an upper bound of $10^j - 1$ on the sum. □

Now given the lemma, suppose that $d_j d_{j-1} \dots d_0$ and $c_k c_{k-1} \dots c_0$ are both decimal representations of n. Note that by the requirements on decimal representations $d_j \neq 0$ and $c_k \neq 0$. We need to show that these representations are the same. So we have to show $j = k$ and that two sequences have the same digits. We claim that $j = k$. By the lemma, $n = \sum_{i=0}^{j} d_i 10^i < 10^{j+1}$ and also $n \geq d_j 10^j \geq 10^j$. Similarly $n < 10^{k+1}$ and $n \geq 10^k$. So $10^{k+1} > n \geq 10^j$ which implies $k \geq j$ and $10^{j+1} > n \geq 10^k$ which implies $j \geq k$. Thus $j = k$.

Suppose for contradiction that $d_j \dots d_0$ and $c_j \dots c_0$ are different. Let h be the largest index such that $c_h \neq d_h$. We may assume that $d_h > c_h$ (the other case is similar.) Then:

$$\begin{aligned} \sum_{i=0}^{j} d_i 10^i - \sum_{i=0}^{j} c_i 10^i &= \sum_{i=0}^{j} (d_i - c_i) 10^i \\ &\geq \sum_{i=0}^{h} (d_i - c_i) 10^i \\ &\geq 10^h - \sum_{i=0}^{h-1} c_i 10^i. \end{aligned}$$

By the lemma, this difference is positive, which contradicts that both of these sequences represent the same number n. □

The prime factorization of integers. Recall that a factorization of a positive integer n is a list of positive integers, all greater than 1, whose product is n; the list may just be the single entry list (n). Recall that a prime number is an integer greater than 1 that has no divisors other than itself and 1. A prime factorization of n is a factorization of n consisting entirely of primes. It is intuitively clear that every number has a prime factorization, but proving it requires induction (or something similar).

Theorem 11.11. *Every integer greater than 2, has a factorization consisting entirely of primes.*

Proof. Suppose n is an arbitrary integer greater than 2.
Case 1. Assume n is prime. Then (n) is a prime factorization of n.
Case 2. Assume n is not prime. Then, by definition, there is a number we'll call k such that $1 < k < n$ and n/k is an integer. Since $1 < k < n$, we can apply the induction hypothesis to say that there is a list we'll call $(p_1, \dots, p_r)$ that is a prime factorization of k. Also, since n/k is an integer and $n/k < n$ (since $k > 1$) and $n/k > 1$ (since $k < n$), we can apply the induction hypothesis to n/k to say that there is a list we'll call $(q_1, \dots, q_s)$ that is a prime factorization of n/k. Then $(p_1, \dots, p_r, q_1, \dots, q_s)$ is a list of primes whose product is $k \times n/k = n$, so is a prime factorization of n. □

If we have one prime factorization of n, we can get another one by reordering the list. Is it possible to have two prime factorizations of n where one is not a rearrangement of the other? The answer is no. To formulate the theorem, let us say that a factorization $(p_1, \dots, p_k)$ of a number n is *nondecreasing* if $p_1 \leq \dots \leq p_k$.

Theorem 11.12. *(Fundamental theorem of arithmetic) For any integer $n \geq 2$, n has a unique nondecreasing prime factorization.*

Proof. Suppose n is an arbitrary integer. We already proved that n has at least one nondecreasing prime factorization, so now we show that there is at most one. If n is prime then (n) is the only factorization of n, so the result is true. So assume that n is not prime. Suppose that $(p_1, \ldots, p_k)$. $(q_1, \ldots, q_m)$ are nondecreasing factorization of n. We'll show that these two factorizations must be the same. We divide into two cases.
Case 1. Assume $p_1 = q_1$. Then $(p_2, \ldots, p_k)$ and $(q_2, \ldots, q_m)$ are both nondecreasing factorizations of the number $n/p_1 = n/q_1$. Since $p_1 \geq 2$ we have $n/p_1 < n$ and since n is not prime $n/p_1 > 1$. So we may apply induction to n/p_1 to conclude that the lists $(p_2, \ldots, p_k)$ and $(q_2, \ldots, q_m)$ are the same. So $(p_1, \ldots, p_k)$ is the same as $(q_1, \ldots, q_k)$.

Case 2. Assume $p_1 < q_1$. In this case we'll obtain a contradiction. By a theorem proved in class, there is a number $r \in \{0, \ldots, p_1 - 1\}$ such that $q_1 - r$ is divisible by p. Let $w = (q_2 \cdots q_m)$ and let $v = wr$ and $u = w(q_1 - r)$. First we'll construct a nondecreasing prime factorization of v. Note that $(r, q_2, \ldots, q_m)$ is a factorization and is nondecreasing (since $r \leq q_1 \leq q_2$) but may not be a prime factorization since r might not be prime. So let $(r_1, \ldots, r_t)$ be a nondecreasing prime factorization of r. Then $(r_1, \ldots, r_t, q_2, \ldots, q_m)$ is a nondecreasing prime factorization of v and since $v < n$, it is the unique such facgtorization. Notice that p_1 does not appear in this factorization since $r_1, \ldots, r_t$ are all at most r and $r < p_1$ and $p_1 < q_1 \leq q_2 \leq \cdots \leq q_m$.

Now we construct another prime factorization of v that includes p_1. This contradicts that v has a unique nondecreasing prime factorization.

Since $p_1|(q_1 - r)$ and $(q_1 - r)|u$ we have $p_1|u$. Since also $p_1|n$ we have p_1 divides $n - u$ which equals v. We can't have $v = p_1$ (since v has a prime factorization that does not include p_1) so $d = v/p_1$ is an integer that is larger than 2 and smaller than v. So d has a prime factorization that we'll call $(d_1, \ldots, d_s)$ and then $(p_1, d_1, \ldots, d_s)$ is a prime factorization of v that includes p_1. As mentioned above this is a contradiction to the fact that v has a unique nondecreasing prime factorization. □

11.3 Extended principle of mathematical induction

The principle of mathematical induction that we've been using is useful for universal principles whose domain is a subset of the natural numbers. We now extend this principle to other domains. Suppose T is any type of mathematical object and $s : T \longrightarrow \mathbb{Z}_{\geq 0}$ is a function. We think of s as a function that measures the "size" of objects in T. For example, if T is a set of lists, then for a list $L \in T$, we could define $s(L)$ to be the length of L. If T is a set of finite sets, we could define $s(X) = |X|$.
Extended Principle of Mathematical Induction (EPMI). Suppose the universe T has a size function s. Suppose we are proving a universal principle about objects in T of the form

For all $x \in T$, we have $C(x)$,

We start our proof:

Suppose x is an arbitrary member of T. We must prove $C(n)$.

The extended principle of mathematical induction says that in such a proof you are permitted to use the following assumption:

For all $y \in T$ if $s(y) < s(x)$, then $C(y)$.

The most common situation to use EPCI is when you are proving a universal principle about finite sets, and the function s used is $s(X) = |X|$.

When we use EPCI with the function s, we say that we are "using induction on $s(x)$".

Example. A *graph* G on the set V is a symmetric anti-reflexive relation on V. The elements of V are called *vertices*. If xGy we say that there is an *edge* between x and y. For a graph G on V we have the following definitions:

- The *G-degree* of $x \in V$ is the number of $y \in V$ such that xGy.
- If $W \subseteq V$, the *graph induced on* W is the graph H on W such that for all $x, y \in W$, xHy if and only if xGy. (So H is the graph obtained by restricting attention to W.)
- A subset I of V is *G-independent* provided that the graph H induced on I has no edges.

Theorem 11.13. *For any graph G on a finite set V, if every vertex has G-degree at most d, then V can be partitioned into $d+1$ or fewer sets that are each G-independent.*

Proof. Suppose G is a graph on V. Let d be the maximum G-degree of a vertex. We must show that there is a partition of G into at most $d+1$ G-independent sets.

We use induction on $|V|$.

Case 1. Assume $|V| = 1$. Then $\{V\}$ is the desired partition.

Case 2. Assume $|V| > 1$. Let $v \in V$ be arbitrary and let $W = V - v$. Let H be the graph induced on W. Clearly the maximum H-degree of any vertex in W is at most d. Since $|W| < |V|$, by the induction hypothesis there is a partition $\{I_1, \ldots, I_k\}$ of W into H-independent sets such that $k \leq d+1$.

Each of the sets in the partition is H-independent, and so is also G-independent. We now consider the number of sets in the partition.

Subcase a. $k \leq d$. Then add $\{v\}$ to the partition to get a partition of V into at most $d+1$ G-independent sets.

Subcase b. $k = d+1$. In this case we claim that for some j, the set $I_j \cup \{v\}$ is G-independent. For contradiction, suppose that every one of these sets is not G-independent. Then for each j between 1 and $d+1$, v has an edge to at least one vertex in i_j. This means that v has edges to at least $d+1$ other vertices, which is a contradiction to the hypothesis that the G-degree of v is at most d. So there is an index we'll call j such that $I_j \cup \{v\}$ is G-independent. So replace I_j by $I_j \cup \{v\}$ in the partition to get the desired partition of V. □

Example 11.7. Consider the following: **Theorem.** Let S be a finite set and let $\alpha : S \longrightarrow \mathbb{R}$.

Then:

$$\sum_{X:X\subseteq S}\prod_{x\in X}\alpha(x) = \prod_{x\in X}(1+\alpha(x)).$$

Exercise 11.8. Construct an example with S having 3 elements and check that this formula works on your example.

Proof. Suppose S is an arbitrary nonempty finite set and let $\alpha : S \longrightarrow \mathbb{R}$. We must show:

$$\sum_{X:X\subseteq S}\prod_{x\in X}\alpha(x) = \prod_{x\in S}(1+\alpha(x)).$$

We proceed by induction on $|S|$. We consider two cases, depending on whether $|S| = 1$ or not.

Case 1. Assume $|S| = 1$. Let s be the unique element of S. Then S has two subsets, itself and $\emptyset$, and the expressions on the left and right of the desired equality are both is $1 + \alpha(s)$

Case 2. Assume $|S| \geq 2$. Let z be an arbitrary member os S and let $T = S - \{z\}$.

Now, let's consider the expression on the right of what we are trying to prove:

$$\prod_{x\in S}(1+\alpha(x)) = (1+\alpha(z)) \times (\prod_{x\in T}(1+\alpha(x))).$$

Note that $T \neq \emptyset$ since $|S| \geq 2$ and $|T| < |S|$ so by the induction hypothesis, this equals:

$$(1+\alpha(z)) \times \sum_{X:X\subseteq T}\prod_{x\in X}\alpha(x).$$

Now we finish the proof by carefully manipulating the sums and products:

$$\begin{aligned}
(1+\alpha(z)) \times \sum_{X:X\subseteq T}\prod_{x\in X}\alpha(x) &= \sum_{X:X\subseteq T}\prod_{x\in X}\alpha(x) + \sum_{X:X\subseteq T}\alpha(z)\times\prod_{x\in X}\alpha(x) \\
&= \sum_{X:X\subseteq T}\prod_{x\in X}\alpha(x) + \sum_{X:X\subseteq T}\prod_{x\in X\cup\{z\}}\alpha(x) \\
&= \sum_{X:X\subseteq S\wedge z\notin X}\prod_{x\in X}\alpha(x) + \sum_{X:X\subseteq S\wedge z\in X}\prod_{x\in X}\alpha(x) \\
&= \sum_{X:X\subseteq S}\prod_{x\in X}\alpha(x).
\end{aligned}$$

This completes the proof. □