Math 79SI Notes

Mason Rogers

6 Mathematical Induction II

6.1 Background

Last week, we introduced induction as a technique to prove a family of statements $\{P_n\}_{n\in\mathbb{N}}$ by proving the implications $P_n \implies P_{n+1}$ and then proving P_1. We also saw a few examples which required checking multiple base cases (as in the proof of the explicit formula for Fibonacci numbers) or more complicated networks of implications (as in the proof of the AM-GM inequality). Two main ideas united all of the examples: all of the examples were algebraic in nature, and they all featured an exhaustive implication structure.

This week, we will broaden our understanding of induction by studying more diverse applications of inductive reasoning. We will look at inducting on geometric objects, mixing inductive reasoning with proof by contradiction, and most importantly, using induction to prove results other than formulas and inequalities. The role of exhaustive implications will still hold, but it will take less central of a role. Rather than specifically diagramming an implication network, we will develop a more abstract appreciation for induction as a tool for moving from a handful of established cases to all cases.

6.2 Examples

We open this section with a famous example of inducting on a geometric structure. Colloquially, the problem is usually framed as, 'How many pieces of cake can be cut with n straight-line cuts?' More formally, we are interested in computing the maximal number of regions into which a circular disk can be divided with n chords. As in many of the examples of the previous discussion of induction, we essentially want a formula for the maximum number C_n of regions formed by n chords. Here, however, our induction variable n has a genuine geometric meaning: the number of chords.

Whenever trying to prove that a result holds for all n, *we first need to figure out what to prove.* Drawing a few diagrams and playing with the arrangement of the chords suggests that $C_n = 2, 4, 7, 11, 16$ for $n = 1, 2, 3, 4, 5$, respectively. The drawings become more difficult to construct and decipher for higher n, but using the method in the lead-up to Proposition 5.1 suggests the formula $C_n = n(n+1)/2 + 1$. Recalling that the sum of the first n natural numbers $S_n = n(n+1)/2$, we conjecture $C_n = S_n + 1$.

Proposition 6.1. Let C_n denote the maximal number of regions into which a circle can be divided with n chords. For all $n \in \mathbb{N}$, $C_n = S_n + 1$.

Proof. In the proof that $S_n = n(n+1)/2$, we had to prove that two algebraic expressions for S_n were equal, namely $\sum_{i=1}^{n} i$ and $n(n+1)/2$. In this case, we do not have an expression for C_n in terms of an explicit summation, so we will need to adjust our approach. We aim to use a geometric argument to prove that $C_n = n + C_{n-1}$ for all $n > 1$. We already know that the S_n satisfy this recursion. If we can show that the C_n do as well, we can borrow the inductive step the argument in Proposition 5.1. Then, since any chord cuts a circle into two regions, we have our base case $C_1 = 2 = S_1 + 1$ and will be done.

This is where the proof requires an *understanding of the geometry*. Suppose we have $n-1$ chords cutting a circle into C regions. We first claim that the n-th chord can create at most n new regions. Each chord creates a new region by dividing a region that it passes through in two, so equivalently we claim that the n-th chord passes through the interiors of at most n preexisting regions. This follows from the *geometric* observation that if the n-th chord enters the interior of a new region then it crosses one of the first $n-1$ chords (which can happen at most $n-1$ times). Thus, accounting for the initial region in which the chord began, we get *at most* $C + n$ regions after placing the n-th chord. Since $C \leq C_{n-1}$, we conclude that $C_n \leq n + C_{n-1}$.

We have now placed an upper bound on how many new regions can be created by the n-th chord and aim to show that this bound *can* be achieved. Observe that it is possible to choose n lines in the coordinate plane such that they all intersect each other somewhere and no 3 intersect at the same point. We can do this inductively, for if we can place $n-1$ lines in such a fashion, we can place the n-th far enough from the origin to avoid all of the other intersection points and choose its slope to be unequal to any of the previously selected slopes. By the reasoning above, the n lines divide the plane into R_n regions where $R_1 = 2$ and $R_n = n + R_{n-1}$, with exact equality due to the facts that each line *does* intersect all the others and each intersection point is shared by only 2 lines. By scaling the plane, we can ensure that all of the lines' intersection points, and thus parts of all R_n regions, fit into the interior of a circle with any given radius. Thus, we have $R_n \leq C_n$ *and* $R_n = S_n + 1$, which along with the fact that $C_n \leq S_n + 1$ give $C_n = S_n + 1$ for all $n \in \mathbb{N}$. □

We can view the circle with n chords sliced (for $n = 1, 2, 3 \ldots$) as a collection of circles: one with just the first chord sliced, another with the first and second chords sliced, and so forth. Understanding the proof of the formula for C_n required us to understand how all of the dissected circles in this family depend on each other. Justifying a recursion took the majority of the work; finding the candidate formula just required an analogy to a familiar algebraic induction argument.

In addition to inducting on geometric objects, we can induct on combinatorial structures. For instance, suppose we want to count the number of size-k subcollections of a collection of n items. You may know that the answer is given by the binomial coefficient $\binom{n}{k}$, but it requires some care to *prove* that this is the correct quantity:

Proposition 6.2. The number of subsets with k elements of a set with n distinct elements is given by $\binom{n}{k}$ for $0 \leq k \leq n$.

Proof. We will prove this by inducting on k upon first choosing $n \geq 0$. Let S be a set with n distinct elements, and suppose that $\binom{n}{k}$ is the number of subsets of S with k elements for some k satisfying $0 \leq k < n$. We wish to count the number of subsets of S with $k+1$

elements. Let $i \in I$ index the collection of subsets $T_i \subset S$ with k elements and $j \in J$ index the collection of subsets $U_j \subset S$ with $k+1$ elements. For each T_i, we can form $n-k$ of the U_j by choosing each of the $n-k$ elements of the complement $S \setminus T_i$ and adding it to T_i. But there is repetition in this process: each set U_j is formed this way from exactly $k+1$ of the T_i, since eliminating each of the $k+1$ elements of any U_j results in distinct sets T_i. Thus, we have

$$|J| = \frac{n-k}{k+1}|I| = \frac{(n-k)n!}{(k+1)k!(n-k)!} = \frac{n!}{(k+1)!(n-(k+1))!} = \binom{n}{k+1}.$$

Our inductive step is complete, and it just remains to check the case $k = 0$ (which we also could have done at the outset). Observe that for all n, $\binom{n}{0} = 1$, which matches the number of empty subsets of a set of any size. We thus conclude that $\binom{n}{k}$ has the expected combinatorial interpretation for all k satisfying $0 \leq k \leq n$. □

Note that the preceding argument worked with a fixed n throughout, and for each fixed n, we performed a "finite induction", systematically working from $k = 0$ to $k = n$. Even though this is not an "official" induction on $k \in \mathbb{N}$ for fixed n, the style of the proof can still be regarded as inductive.

One of the exercises addresses why this binomial coefficient is also the coefficient of $x^k y^{n-k}$ in the expansion $(x+y)^n$, which has a similar combinatorial interpretation.

In addition to inducting on structures, we can induct on *processes*, which we will first do to prove the existence of prime factorizations for all natural numbers greater than 1. Our intuition is that any $n > 1$ is either prime or has a prime factor p_1, and if so, n/p_1 is either prime or has a prime factor p_2, and so on until we have a list of primes that multiply to n. Induction allows us to formalize this argument. In particular, we will need to use *strong induction*, whereby to prove the $n = k$ case, we assume not just the $n = k-1$ case, but *all* cases $n = k' < k$. This is helpful because the divisibility aspect of a given k has little to do with that of $k-1$, but much to do with that of the proper factors of k.

Proposition 6.3. Let $n > 1$ be a natural number. Then n has a prime factorization.

Proof. We argue by induction on $n \geq 2$ for the existence of a prime factorization. The case $n = 2$ holds because 2 is prime, so now suppose $n > 2$ and that all integers m such that $1 < m < n$ are known to have a prime factorization. If n is prime then it is its own prime factorization, and otherwise $n = ab$ for positive integer factors $a, b < n$. We cannot have $a = 1$ or $b = 1$ (since $ab = n$ with $a, b \neq n$), so $1 < a, b < n$. By our (strong) inductive hypothesis each of a and b is therefore a product of finitely many primes, so the same holds for $ab = n$. □

A slight variant on this technique, inducting on the degree of a polynomial, can be used to prove that a degree-n polynomial can have at most n roots. Instead of dividing out prime factors from n, we will divide out linear factors $(z - r)$ from a polynomial $p(z)$:

Proposition 6.4. Let $p(z) = c_n z^n + \ldots + c_1 z + c_0$ be a polynomial of degree $n \geq 1$ (i.e. $c_n \neq 0$) with coefficients $c_j \in \mathbb{C}$. Then p has at most n roots in $\mathbb{C}$.

Before beginning, we note that the proposition does not assert that p actually has n roots. For polynomials of positive degree with complex coefficients, the fundamental theorem of algebra guarantees that there are exactly n complex roots counted with multiplicity. But this is not necessarily true for other number systems such as $\mathbb{Q}$ or $\mathbb{R}$, and even in the complex numbers, it is generally not possible to give a formula for the roots as can be done for $n = 2$ and also $n = 3, 4$ with much effort.

Proof. We first establish the broader induction picture. Suppose $z = r$ is a root of $p(z)$. We claim that $p(z) = (z - r)q(z)$ for a polynomial $q(z)$. If so, $q(z)$ will have degree $n - 1$ (look at the top-degree parts of $z - r$, $q(z)$, and $p(z)$). Then by induction $q(z)$ has at most $n - 1$ roots. But any root a of $p(z)$ satisfies $0 = p(a) = (a - r)q(a)$, so there are at most n possibilities for a as desired. (Note that it might happen that r is also a root of q, so this argument only provides an upper bound on the number of roots.)

It remains to prove that if $p(r) = 0$, then $p(z) = (z - r)q(z)$ for a polynomial $q(z)$. Observe that $p(z) = p((z - r) + r)$, so we can express $p(z)$ as a polynomial in $z - r$, i.e. by expanding each $((z - r) + r)^j$ via the binomial formula we can find $d_0, d_1, \ldots, d_n \in \mathbb{C}$ such that

$$p(z) = d_n(z - r)^n + \ldots + d_1(z - r) + d_0.$$

Now it suffices to show that $d_0 = 0$. Evaluating at $z = r$ gives $p(r) = d_0$, but since $p(r) = 0$, we conclude that $d_0 = 0$. □

In some sense, we have proven that the process of dividing out linear factors corresponding to roots of a degree-n polynomial must terminate after at most n steps. In general, this style of induction is quite useful, and we will rely on it for several of the key statements we prove in our development of vector spaces at the end of the course.

We will now introduce techniques for combining inductive reasoning with proof by contradiction. The first technique is known as 'proof by infinite descent', which we will illustrate by proving a special case of Fermat's Last Theorem. The goal of the technique is to show that given an object satisfying a certain condition (e.g. a nontrivial solution to a Diophantine equation), we can construct a strictly 'smaller' one; we then use "inductive" ideas to create a contradiction!

We need a result about primitive Pythagorean triples, which we state without proof:

Lemma 6.5. Let (a, b, c) be a primitive Pythagorean triple (i.e. $a^2 + b^2 = c^2$ and a, b, and c are pairwise coprime positive integers). Then there exist coprime positive integers p and q such that (possibly after relabeling a and b) $c = p^2 + q^2$, $b = 2pq$, and $a = p^2 - q^2$.

The slickest proof of the lemma uses geometry; see the Further Reading section 6.4 for more information.

We will also use facts involving coprimality rather flexibly to avoid distracting from the rather complicated argument at hand. We now state the special case of Fermat's Last Theorem:

Proposition 6.6 (*Fermat*)**.** The equation $x^4 + y^4 = z^2$ has no integer solutions (x, y, z) satisfying $xyz \neq 0$.

Note that although Fermat's Last Theorem for exponent 4 concerns solutions of $x^4+y^4 = z^4$, here we prove something *stronger*: not even $x^4 + y^4 = z^2$ has a solution in $\mathbb{Z} \setminus \{0\}$. You will see in the proof below that if we only worked with the more limited version using z^4, the algebra would break down. Success requires a *suitably general* inductive hypothesis!

Proof. Suppose for the purpose of contradiction that (x, y, z) is an integer solution to $x^4 + y^4 = z^2$ with $xyz \neq 0$. We may and do change signs if necessary so $x, y, z \geq 1$. Notice that if two of x, y, z share a prime factor p, so does the third, which can be seen by rearranging the equation to isolate the third. We therefore may assume without loss of generality that x, y, and z are pairwise coprime, perhaps after dividing by the greatest common divisor of (x, y, z). This gives a primitive Pythagorean triple $(x^2)^2 + (y^2)^2 = z^2$, so by Proposition 6.5, we can choose coprime positive integers p and q such that $z^2 = p^2 + q^2, x^2 = 2pq$, and $y^2 = p^2 - q^2$.

Rearranging the equation for y^2 gives us another Pythagorean triple $q^2 + y^2 = p^2$. This triple is *primitive* because $\gcd(p, q) = 1$, and if any two of q, y, p shared a prime factor, then all three would by the argument above, which is impossible. Thus, there exist coprime positive integers a and b such that $p = a^2 + b^2$, $q = 2ab$, and $y = a^2 - b^2$. Notice that $a > 1$, for $a^2 - b^2 > 0$ implies that $a > b$, and $b \geq 1$.

Returning to our equation for x^2, we have that

$$x^2 = 2pq = 4ab(a^2 + b^2).$$

Since a and b are coprime, it follows that ab and $a^2 + b^2$ are coprime as well. Since $x^2 = 4ab(a^2 + b^2)$, any prime factor in the unique prime factorization of $ab(a^2 + b^2)$ must be present an even number of times. Since ab and $a^2 + b^2$ have no prime factors in common, this ensures that the positive integers ab and $a^2 + b^2$ are both perfect squares. But with ab a perfect square and a and b coprime and positive, a and b are themselves perfect squares.

Let P be the (positive integer) square root of $a^2 + b^2$, A be the (positive integer) square root of a, and B be the (positive integer) square root of b. We necessarily have $P^2 = A^4+B^4$, so (A, B, P) forms another nontrivial solution to our original equation! Moreover, since $a > 1$, $P^2 = a^2 + b^2 < a^4 + b^4 = z^2$, so $P < Z$ and our new solution is strictly 'smaller' than our old one.

Inductively via this process, we can generate as many new solutions as we want, each smaller than the previous. However, there cannot be more such steps than the initial value of z, for each new solution's third entry is at least 1 smaller than the previous solution's third entry. We have thus achieved a contradiction and conclude that there are no integer solutions (x, y, z) to $x^4 + y^4 = z^2$ satisfying $xyz \neq 0$. □

We now see why the method is called the method of infinite descent. We showed that we can choose smaller and smaller positive integer solutions ad infinitum if some solution existed, which is certainly absurd, so there is no such solution. This idea is one of Fermat's most fruitful discoveries, and it has developed into a powerful technique in modern number theory.

We will now conclude this section by finally proving the fundamental theorem of arithmetic. The strategy is known as 'contradicting a minimal counterexample', or occasionally the 'minimal criminal method' for short. We will proceed as follows: Suppose a property P

(e.g. uniqueness of prime factorizations) does *not* hold for all natural numbers. Then the set $S \subseteq \mathbb{N}$ on which P does not hold is a nonempty subset of $\mathbb{N}$, so it contains a least element n (our 'minimal criminal').[1] We will then use the *minimality* of n to achieve a contradiction to the failure of P and conclude that P holds for all $n \in \mathbb{N}$.

We begin with the following lemma:

Lemma 6.7. If p is a prime factor of $n \in \mathbb{N}$, then n has a prime factorization $p_1 \cdots p_k$ where p equals one of the p_i.

Proof. Suppose p is a prime factor of some $n \in \mathbb{N}$. If n is prime then $p = n$, so p is a prime factorization of n containing p. Otherwise, $n = pd$ for some natural number d satisfying $1 < d < n$. By Proposition 6.3, d has a prime factorization $p_1 \cdots p_k$, so $p \cdot p_1 \cdots p_k$ is a prime factorization of n containing p. □

Theorem 6.8 (*Fundamental Theorem of Arithmetic*)**.** If $n > 1$ is a natural number, n has a *unique* prime factorization up to rearrangement of the factors.

Proof. Having already proven existence of prime factorizations in Proposition 6.3, it remains to prove uniqueness. Suppose for the purpose of contradiction that the claim is not true, and let m be the smallest natural number greater than 1 having more than one prime factorization. Let $p_1 \cdots p_k$ and $q_1 \cdots q_\ell$ be prime factorizations of m that are *not* merely rearrangements of each other. Note that $k > 1$ and $\ell > 1$ since prime numbers necessarily have unique prime factorizations (of length 1) by the definition of primality.

We first claim that none of the p_i can equal any of the q_j, which we prove by contradiction. Suppose not, and without loss of generality (since we can *rearrange* the p_i and q_j), we may suppose $p_1 = q_1$. Then $p_2 \cdots p_k$ and $q_2 \cdots q_\ell$ are distinct (i.e. not differing by rearrangements alone) prime factorizations of $m/p_1 < m$, contradicting the minimality of m. Thus, the p_i and the q_j do not have any elements in common, as claimed.

Now rearrange factors so that $p_1 \le p_i$ for all i and $q_1 \le q_j$ for all j. Then $p_1^2 \le m$ and $q_1^2 \le m$ since $k, \ell \ge 2$ and $p_1 \le p_2, q_1 \le q_2$. Because $p_1 \ne q_1$, it follows that $p_1 q_1 < \max\{p_1, q_1\}^2 \le m$.

Let $n = m - p_1 q_1$, so $0 < n < m$. We can do a bit better than that lower bound:[2]

$$n = m - p_1 q_1 \ge \max\{p_1, q_1\}^2 - p_1 q_1 = |p_1 - q_1| \max\{p_1, q_1\} \ge 1 \cdot 2 = 2.$$

This gives $1 < n < m$, so by the inductive assumption n has a *unique* prime factorization.

Next, note that since p_1 divides both m and $p_1 q_1$, we have that p_1 divides $m - p_1 q_1 = n$; likewise, $q_1 \mid n$. Thus, by Lemma 6.7, n must have a prime factorization containing p_1 and a prime factorization containing q_1. But n has a *unique* prime factorization by the inductive hypothesis, so p_1 and q_1 must appear in the *same* prime factorization of n. We therefore have $p_1 q_1 \mid n$. (This is the key step of the entire argument.) Consequently, $p_1 q_1$ divides $n + p_1 q_1 = m$. Dividing through by p_1, we see that $q_1 \mid (m/p_1)$. Since $1 < m/p_1 < m$ (recall

[1] The existence of such an n is known as the well-ordering principle; this is logically equivalent to mathematical induction in a suitable sense we will not discuss here. More information is available in the Further Reading section 6.4.

[2] Here we use the equality $\max\{x, y\}^2 - xy = |x - y| \max\{x, y\}$ for all $x, y \in \mathbb{R}$, which can be checked by noting that the assertion is insensitive to swapping x and y, so we can assume $x \ge y$ and evaluate.

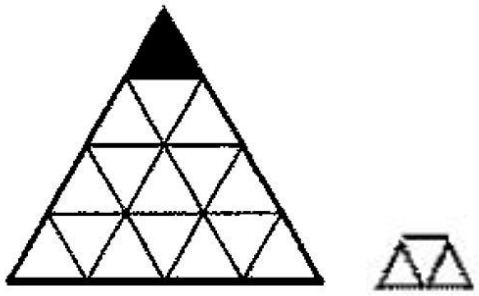

Figure 1: Image of T_2 and a small trapezoid.

$k \geq 2$), by the minimality of m the prime factorization $p_2 \cdots p_k$ of m/p_1 is unique, but q_1 does not appear here. This is a contradiction, so m cannot exist. We conclude that if $n > 1$ is a natural number, n has a unique prime factorization. □

We can also view this proof as a network of implications. Let P_n be the statement 'the prime factorization of n is unique' for each $n \geq 2$. We then prove

$$P_2 \text{ and } P_3 \text{ and } \ldots \text{ and } P_{m-1} \implies P_m$$

by contradiction.

These examples hint at the flexibility of mathematical induction, but they still leave many applications of induction unexplored. Many proofs of key theorems in all fields of mathematics use induction in some way, so it is in general a good tool to keep in mind regardless of the subject matter at hand.

6.3 Exercises

1. Consider the setting of Proposition 6.1, in which we cut a circular cake (perhaps oddly and unequally) into pieces with n straight-line cuts. Suppose you have two flavors of frosting. Prove that you can frost each piece of cake with one of the two flavors such that no two adjacent pieces have the same flavor of frosting. (We define pieces to be adjacent if they share an edge, but not if they just share a vertex.)

2. An equilateral triangle can be cut into 4^n smaller equilateral triangles by repeatedly cutting each triangle into 4 congruent pieces as in a Triforce (see Figure 1). Let T_n be the trapezoid constructed performing this operation and removing one of the small triangles in the corner of the original. We define a 'small trapezoid' to be the trapezoid formed by placing 3 small triangles side by side pointing in alternating directions. Prove that T_n can be constructed as a tessellation[3] of small trapezoids.

3. In Proposition 6.2, we proved that the number of subcollections with k items of a collection with n items is given by $\binom{n}{k}$. Give an interpretation of this result without

[3] A *tessellation* is a tiling of the plane with shapes that do not overlap or leave gaps.

another induction that explains why the coefficient of $x^k y^{n-k}$ in $(x+y)^n$ is also given by $\binom{n}{k}$. This proves the Binomial Theorem:

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

4. In this problem, you will generalize the binomial theorem to the multinomial theorem.

   (a) Identify and prove via mathematical induction an analogue to the binomial theorem for expanding powers of trinomials $(x+y+z)^n$. (*Hint: It may help to think of the binomial theorem as* $(x+y)^n = \sum_{i+j=n} \binom{n}{i,j} x^i y^j$, *where* $\binom{n}{i,j}$ *means* $n!/(i!j!)$.)

   (b) Identify and prove via mathematical induction a formula for expanding powers of multinomials $(x_1 + \ldots + x_m)^n$ for any $m \geq 2$.

5. Let $f_1, \ldots, f_n$ be differentiable functions on $\mathbb{R}$. Recall the product rule, which states for differentiable functions g_1 and g_2 that $(g_1 g_2)' = g_1' g_2 + g_1 g_2'$. Conjecture a formula for

$$\frac{d^k}{dx^k}\left[\prod_{i=1}^{n} f_i\right]$$

   by considering small n, and prove it via induction.

6. Let S be a finite set. Prove in two ways that the number of subsets of S with even cardinality equals the number of subsets of S with odd cardinality, first by constructing a bijection between the collections of even and odd subsets of S, then by using the binomial theorem.

7. Use the binomial theorem to give a more efficient proof of Corollary 5.6.

8. Prove that for all $n \geq 6$, any square can be cut into n (not necessarily congruent) smaller squares. (*Hint: Construct as your base case a division of a large square into* $2n$ *smaller squares for any* $n \geq 2$.)

9. Prove that for all $m, n \in \mathbb{N}$ that $\mathbb{R}^m$ and $\mathbb{R}^n$ have the same cardinality by describing a bijection between them. (*Hint: Use the Peano curve from the previous section's exercise 8 to start with a bijection between* $\mathbb{R}$ *and* $\mathbb{R}^2$.)

6.4 Further Reading

"Mathematical Induction: variants and subtleties", Amites Sarkar	A guide to many of the variants of induction introduced in this section and more, along with a few challenging exercises
"Pythagorean Triples", Keith Conrad	A geometric proof of the formula for primitive Pythagorean triples and more relevant background information on the subject. math.uconn.edu/~kconrad/blurbs/ugradnumthy/pythagtriple.pdf
Wikipedia entry for the well-ordering principle	More information about the well-ordering principle and how it applies in disproving minimal counterexamples. en.wikipedia.org/wiki/Well-ordering_principle