Proving Theorems (and other statements) February 4, 2024

By Susan Ruff, Peter Shor, and Michel Goemans

1 What is the role of proofs in the doing of mathematics?

As mathematicians tackle research problems, they sometimes come to believe they've figured out something true. A proof is a mathematician's way of checking whether their belief is correct. If it is, the proof is also their way of certifying to other mathematicians that the belief is true and, ideally, of helping other mathematicians to understand *why* it's true. Proof is necessary, because often when a mathematician checks their belief by trying to write a proof, they discover instead that their belief isn't quite right and needs to be modified, or that it's true but they didn't correctly understand *why* it's true. Hence, part of the value of writing a proof is that doing so can help the mathematician to better understand what's going on. The role of proofs in mathematics research is illustrated in Figure 1.

One of the purposes of this class is to teach you how to write proofs. In this class you will be asked to prove statements like, "For any positive integer n, the number of ways to triangulate an $(n+2)$-gon with non-crossing diagonals is equal to $\frac{1}{n+1}\binom{2n}{n}$." This handout provides a list of tips for understanding a statement, identifying why it's true, choosing a proof strategy, writing the proof, and checking it. The rest of the handout briefly presents some proof strategies you'll need in this class. More guidance can be found in proof-writing textbooks such as Antonella Cupillari's *The Nuts and Bolts of Proofs* [2].

2 Strategies for Generating Proofs

1. **Take time to thoroughly understand the theorem statement.**

   - Check that you know the meaning of every term. If you look up the meaning of a term, be aware that, in a carefully-written definition, every word is important. For example, in the opening statement, a k-gon is a convex polygon with k sides. Also the term "positive integer" is not to be confused with "nonnegative integer"; a *positive* integer n satisfies $n > 0$ (i.e. $n \geq 1$) while a *nonnegative* integer n is greater or equal to 0, i.e. $n \geq 0$. In the opening statement, the smallest polygon to consider is thus the triangle corresponding to $n = 1$.
   - For your own sake, translate the theorem statement into more familiar notation to ease understanding.
     - For example, $\sum_{j=1}^{n} \frac{1}{j^2} < \frac{\pi^2}{6}$ states that $1 + \frac{1}{4} + \frac{1}{9} + \cdots + \frac{1}{n^2} < \frac{\pi^2}{6}$.
   - To check that you understand the statement, try a few examples. For the opening statement about triangulations of a polygon, check that the number of triangulations of a triangle is indeed $\frac{1}{2}\binom{2}{1} = 1$, of a square is indeed $\frac{1}{3}\binom{4}{2} = 2$, and continue with a few more values of n (until you are either convinced that the statement is potentially true, or the checking is too complicated). In the other example above, check the statement for several values of n; for example, $1 + \frac{1}{4} + \frac{1}{9} + \frac{1}{16} + \frac{1}{25} = 1.46361\cdots$ is indeed less than $\frac{\pi^2}{6} = 1.64493\cdots$

- Identify the hypotheses and conclusions by rewriting the theorem statement in if-then form: *If [hypotheses] then [conclusions].*
  - The hypotheses and conclusions are important because you will use the hypotheses to prove the conclusions.
  - e.g., “No three positive integers x, y and z satisfy $x^n + y^n = z^n$ for any integer n greater than 2” (Fermat’s last theorem) can be rewritten as “*If* n is an integer greater than 2 *then* there do not exist positive integers x, y and z with $x^n + y^n = z^n$.
  - E.g., “There are infinitely many primes” could be recast as “If p is a prime, then there is some $q > p$ such that q is a prime.” One would need to argue that these two statements are equivalent.
  - If you try to write a statement in if-then form you may find that the hypotheses aren’t mentioned explicitly. For example, the statement $\sum_{j=1}^{n} j = \frac{n(n+1)}{2}$ has the hypothesis “n is a natural number”—this hypothesis is implied by the summation.
- Sometimes words are difficult to work with in a proof: rewrite the statement using notation that will be easier to work with. For example, if a statement is about the digits of a number, it will be easier to do arithmetic in the proof if you can refer to each digit, so the following notation is likely to be helpful.

  Definition: Given an integer n with k digits, let a_i be the ith least-significant digit where i goes from 0 to $k - 1$, and by convention the 0th least-significant digit is the unit digit. This means that $n = \sum_{i=0}^{k-1} a_i 10^i$ and $0 \le a_i \le 9$. For example, if $n = 1472$, then $a_0 = 2$ and $a_2 = 4$.

2. **Try to determine why the statement is true.**
   - The steps above to understand the statement may make clear why the statement is true. If not:
   - *Try to prove a simpler case.* For example, if the theorem makes a claim about all natural numbers n, try a small value of n to gain insight about why the statement is true. *Caution!* Explaining why the statement is true for some small n is not a proof. Your proof must generalize to make clear why the statement is true for all values of n.
   - *Try to find a counter-example.* You’re unlikely to find one, but trying to do so can give insights about why the statement is true. And you may realize why each hypothesis is necessary.
3. **Choose a proof strategy.** Each strategy is explained further in Section 4.
   - If the steps above for “understanding the theorem statement” make clear why the conclusions follow from the hypotheses, then write a *direct proof.*
   - If looking for a counterexample provides insight, try a *proof by contradiction.*
   - If the statement involves irrational numbers, try a *proof by contradiction.*
     - E.g., the following statement can be (most easily) proved by contradiction: “$\sqrt{2}$ is irrational.”
   - To prove a statement involving a natural number, a *proof by induction* may work.

    - E.g., the statement $\sum_{j=1}^{n} j = \frac{n(n+1)}{2}$ can be proved by induction (the summation implies that n is a natural number).

  To choose the right inductive hypothesis might be tricky, as sometimes one needs to prove a stronger statement (and thus a stronger inductive hypothesis) to use induction.

- To prove that two finite sets A and B are the same size, a *bijective proof* may work.
    - The crux of a bijective proof is to identify a bijection between the two sets. Or if the statement to prove consists of counting the number of elements in A then the creative step is to find the right B (whose cardinality is easy/easier to establish) and a bijection between A and B.
- A theorem statement that says "if and only if" (or its abbreviation "iff") is likely to require a two-part proof. To prove the statement "P if and only if Q," separately prove the two statements "If P then Q" and "If Q then P."

4. **Write the proof** Particular kinds of proof have particular structures. For more information about each kind of proof, see Section 4.

    - *Level of detail & rigor* The appropriate level of detail and rigor depends on the context. Your goal is to make the proof *clear* and *convincing* for your *target audience.* Unless the assignment says otherwise, consider your target audience to be a classmate who doesn't know how to do the proof. Writing at the appropriate level of detail is difficult, as the audience may be varied. This handout is written for students who haven't had an exposure to proofs, and is too verbose and detailed for those who have.

5. **Check the proof**

    - Reread the assignment. Did you prove precisely what you were supposed to?
    - If the proof uses contradiction, could the proof be recast as a direct proof? Would this improve the readability or the flow of the proof?
    - Examine the logic of the proof, ensuring that every claim is sufficiently supported. It can help to draw the logic, as illustrated in the appendix.
    - Identify how each of the hypotheses is used in the proof. Does the statement still hold if we remove one of the hypotheses?
    - Reread the proof from the point of view of your target audience. Is the logic easy to follow?
    - Check the notation: Would the proof be easier to follow if some words were replaced with more precise notation? if some of the notation were replaced with more intuitive but equally precise words? Is all notation introduced?
    - You'll receive further instruction and feedback on writing mathematics. Use these to create your own proof-writing/editing checklist. Review the checklist before you submit your work.

3 Example Application of Proof-Generation Strategies

Suppose you are given the following statement to prove.

Theorem 1. *Every number whose digits sum to a multiple of 9 is itself divisible by 9.*

This section illustrates how you could apply a sequence of proof-generation strategies to write a proof of this statement.

Proof-generation strategy

Identify the hypothesis and conclusion by writing the theorem in if-then form.

The theorem can be rewritten as

Theorem 1. *If the sum of the digits of a number is a multiple of 9 then the number is divisible by 9.*

The hypotheses are (implicitly stated) "the number is a natural number" and "the sum of the digits is a multiple of 9" and the conclusion is "the number is divisible by 9." We must use the hypotheses to prove the conclusion.

Proof-generation strategy

Rewrite the statement using notation that will be easier to work with.

If a natural number n has k digits, we can represent each digit by a_i, where $n = \sum_{i=0}^{k-1} a_i 10^i$ and $0 \leq a_i \leq 9$. So we must prove the following statement:

Theorem 1. *If $\sum_{i=0}^{k-1} a_i$ is divisible by 9 then $\sum_{i=0}^{k-1} a_i 10^i$ is divisible by 9.*

Proof-generation strategy

Try to prove a simpler case.

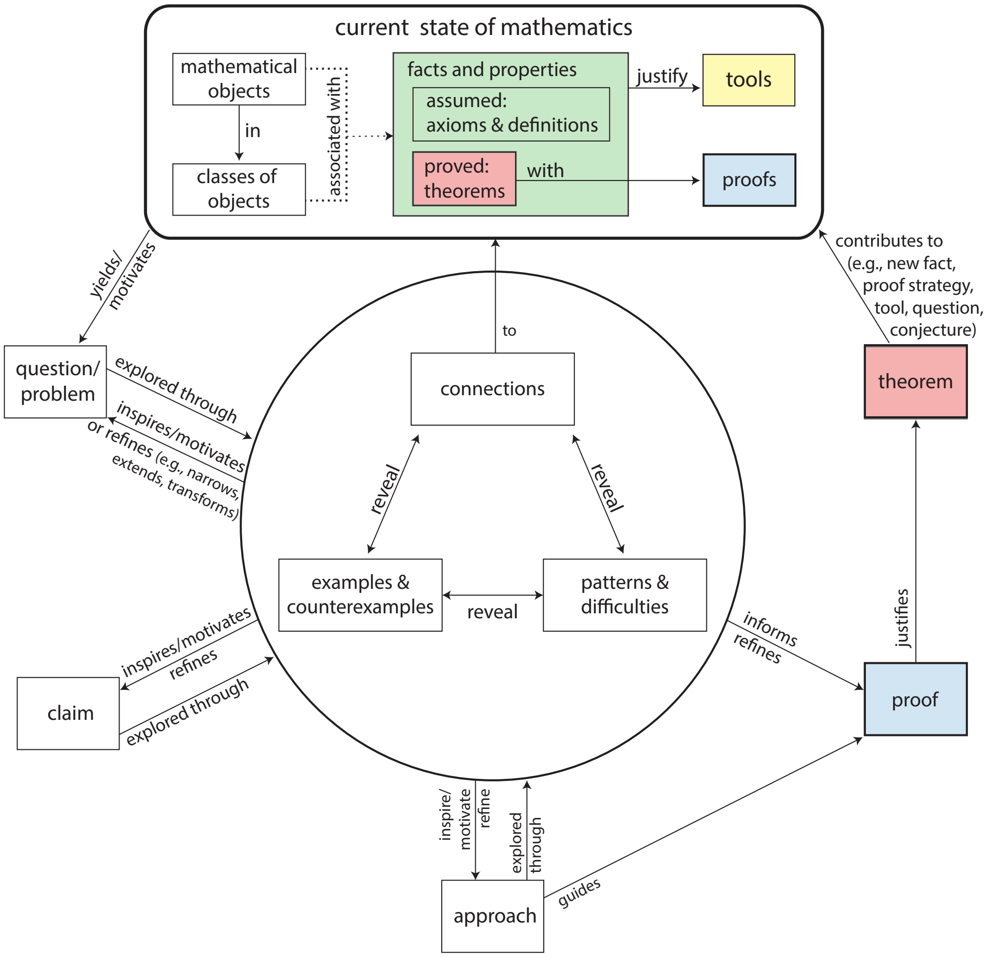
First try proving the theorem for $k = 2$.

Theorem 1′. *If $a_0 + a_1$ is divisible by 9, then $a_0 + 10a_1$ is divisible by 9.*

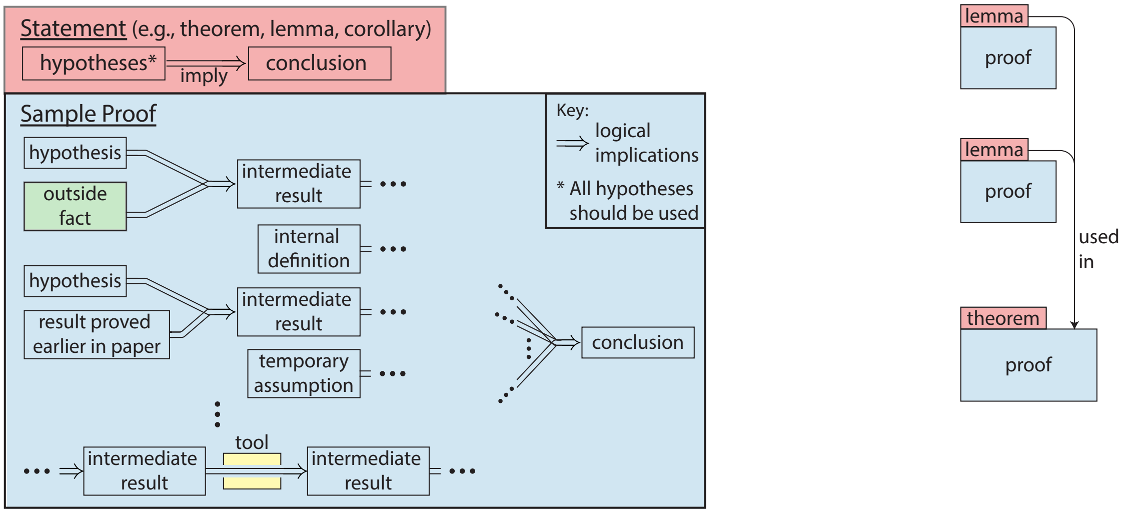
As you look for connections between these expressions, you may notice that $(a_0 + 10a_1) - (a_0 + a_1) = 9a_1$, which is divisible by 9. You can use this observation to write a proof.

Figure 1: Diagram of Proof-based Mathematics (next page)
The figure on the next page illustrates both the role of proof within mathematics research and what a proof is: specific proofs are illustrated in the appendix. This diagram was created by Malcah Effron, Susan Ruff, and Ari Nieh by interviewing MIT mathematicians and analyzing their research articles, as part of research in various disciplines at MIT, led by Andreas Karatsolis and Suzanne Lane and funded by the Davis Educational Foundation.

Mathematics Reasoning Diagram



What is a proof?



Proof of Theorem 1′. Note that $a_0 + 10a_1 = (a_0 + a_1) + 9a_1$. Both terms on the right-hand side are divisible by 9, so $a_0 + 10a_1$ is divisible by 9. □

You can then try to use the same strategy to prove the more general statement:

$$\sum_{i=0}^{k-1} a_i 10^i - \sum_{i=0}^{k-1} a_i = \sum_{i=0}^{k-1} a_i(10^i - 1),$$

which is divisible by 9 because $10^i - 1$ is divisible by 9.

Draft proof of Theorem 1. Note that

$$\sum_{i=0}^{k-1} a_i 10^i = \sum_{i=0}^{k-1} a_i + \sum_{i=0}^{k-1} a_i(10^i - 1).$$

The second sum on the right-hand side is divisible by 9 because $10^i - 1$ is divisible by 9. Since both sums of the right-hand side are divisible by 9, so too is $\sum_{i=0}^{k-1} a_i 10^i$. □

Proof-generation strategy

Reread the assignment.

The assigned statement to prove was "Every number whose digits sum to a multiple of 9 is itself divisible by 9." Because the statement does not include the notation, the notation must be introduced within the proof.

Proof-generation strategy

Examine the logic of the proof: ensure that every claim is sufficiently supported.

Why is $10^i - 1$ divisible by 9? Whether this claim needs justification and how best to justify it depends on the audience and context, but this final proof provides some justification:

Theorem 1. *Every number whose digits sum to a multiple of 9 is itself divisible by 9.*

Proof. Suppose the sum of the digits of a number n is divisible by 9. Let k be the number of digits of n. We can represent n as $n = \sum_{i=0}^{k-1} a_i 10^i$ where $0 \leq a_i \leq 9$ corresponds to the $(i+1)$th least significant digit of n. Our assumption says that $\sum_{i=0}^{k-1} a_i$ is divisible by 9.

Notice that

$$\sum_{i=0}^{k-1} a_i + \sum_{i=0}^{k-1} a_i(10^i - 1) = \sum_{i=0}^{k-1} a_i 10^i = n.$$

Thus, to show n is divisible by 9, it suffices to show that $\sum_{i=0}^{k-1} a_i(10^i - 1)$ is divisible by 9. But for $i \geq 1$, $10^i - 1 = 999 \cdots 9$ (with i nines in the decimal representation), and is thus divisible by 9. It follows that $\sum_{i=0}^{k-1} a_i(10^i - 1)$ is divisible by 9, so we are done. □

Proof-generation strategy

Reread the proof from the point of view of your target audience.

Your goal is to make the proof clear and convincing for your target audience, who may not be satisfied by the justification above for $10^i - 1$ being a multiple of 9. There are several more rigorous ways to show this fact, and the best may depend on what the reader may be familiar with. One could have said "modular arithmetic implies that $10^i - 1$ is a multiple of 9" if the target audience can be assumed to be familiar with modular arithmetic. Or one can be more explicit in the use of modular arithmetic by saying: $10 \equiv 1 \pmod 9$ implies that $10^i \equiv 1^i \equiv 1 \pmod 9$, and thus $10^i - 1$ is a multiple of 9. Or one could use the binomial formula to argue this (if the target audience may not be familiar with the binomial formula, one may first state it and give a reference), or even directly from first principles, by using induction on i.

4 Types of Proof

The following pages explain various types of proof, in terms of the general logic and structure of the proof. Throughout, H stands for the hypotheses and C stands for the conclusions, so the goal is to prove "If H then C" or, in logic notation, H $\Rightarrow$ C.

4.1 Direct Proof

To write a direct proof, show that C is true by using H, definitions of terms used in H, and any other facts that are already accepted as true by your target audience. For example, the proof of Theorem 1 in Section 3 is a direct proof: its logic is diagrammed in Figure 4 in the appendix.

4.1.1 Pigeonhole Principle

Many concepts in mathematics are useful for crafting direct proofs. One rather basic one goes by the odd-name of the *Pigeonhole Principle.* The basic version of the principle is as follows.

Pigeonhole Principle. *Suppose you have n pigeons and m pigeonholes, with $n > m$. Then, if every pigeon is in a hole, some hole must contain at least two pigeons.*

While the advanced version of the principle says that

Theorem 2. *Let A be a set of 7-digit numbers. If A has 30 elements, then it has two disjoint subsets B and C such that the sum of the elements of B equals the sum of the elements of C.*

There are many ways of writing a statement, but precision is important. When writing "it has two disjoint subsets B and C," we could have instead written "there exist $B \subset A$ and $C \subset A$ with $A \cap B = \emptyset$." Both ways of writing this statement are equally precise.

Proof. We will use the pigeonhole principle: the possible distinct nonempty subsets of A will be the pigeons and the possible sums of elements will be the pigeonholes.

Because A has 30 elements and each may or may not appear in a subset of A, there are $2^{30} - 1$ possible nonempty subsets. Because A's 30 elements are each between 0 and 10^7, the sum of the elements of any subset is less than $30 \cdot 10^7$, which is less than $2^{30} - 1 > 10^9$.

Thus, since there are more subsets (pigeons) than sums (holes), there must be two subsets that have the same sum. These two subsets might not be disjoint, but we can eliminate any element that appears in both of them while keeping their sums equal. If we do this, the resulting sets are nonempty because the original two subsets were different. □

The logic of this pigeonhole principle proof is diagrammed in Figure 5 in the appendix.

4.2 Contrapositive/Contradiction

A statement and its *contrapositive* are logically equivalent, so proving one proves the other. The contrapositive of "If H then C" is "if *not C* then *not H*." Here, "not C" means the logical negation of C, also denoted by $\neg C$. For example, when talking about natural numbers, the logical negation of "x is odd" is "x is even." In logical notation, the contrapositive of $H \Rightarrow C$ is $\neg C \Rightarrow \neg H$.

Proof by taking the Contrapositive statement. Instead of proving $H \Rightarrow C$, we can prove equivalently the contrapositive statement $\neg C \Rightarrow \neg H$. For example, consider the following statement:

> "If x is a prime number and $x > 2$ then x is odd."

- The negation of the conclusion "x is odd" is "x is even."
- The negation of the hypothesis "x is prime and $x > 2$" is "x is not prime or $x \leq 2$."
- So the contrapositive of the statement "If x is prime and $x > 2$, then x is odd" is the statement "If x is even then either x is not prime or $x \leq 2$."

This contrapositive proof is diagrammed in Figure 6 in the appendix.

It is important to emphasize that "not (A *and* B)" is "not(A) *or* not(B)". In logical notational, one writes that $\neg(A \wedge B) = \neg(A) \vee \neg(B)$ where $\wedge$ denotes *and* and $\vee$ denotes *or*. Also the negation of the statement "for all x, we have $A(x)$" (where $A(x)$ is some statement that depends on x) is "there exists x such that not $A(x)$". Written formally, this is saying that $\neg(\forall x : A(x))$ is equivalent to $\exists x : \neg(A(x))$, where $\forall$ means "for all" and $\exists$ means "there exists".

4.2.1 Proof by Contradiction

A proof by contradiction is a variant of proving the contrapositive. Instead of showing that *not C* implies *not H*, one assumes that *not C* and *H* are both true and derive a contradiction. In the example above one would use "x is even" and "x is a prime and $x > 2$" to reach a contradiction.

Skeleton Proof by Contradiction Proofs by contradiction have a common structure:

Theorem. *If [hypothesis] then [conclusion].*

Proof. Assume for the sake of contradiction that... [negation of conclusion]. Then... [logic that uses hypothesis and negation of conclusion and reaches a contradiction]. But this is a contradiction, so... [conclusion]. □

Although this structure is commonly used, the wording that signals the structure may vary. The important aspects are to somehow clearly indicate the following:

- What is assumed for the sake of contradiction (e.g., "Suppose to the contrary that…")
- When contradiction is reached (e.g., "…however, we know…so our assumption must be false.")

4.2.2 Examples of proofs by contradiction

The examples below are based on Example 11 in *The Nuts and Bolts of Proof* [2, pp. 28-29]. The logic of the first is diagrammed in Figure 7 in the appendix.

Theorem 3. *If* $0 < x < 1$*, then* $x^2 < x$*.*

Proof. Assume for the sake of contradiction that $x^2 \geq x$. Then $x^2 - x \geq 0$, so $x(x-1) \geq 0$. But for this product to be non-negative, because x is positive, it must be that $x - 1 \geq 0$. So $x \geq 1$. But this contradicts the hypothesis that $x < 1$. So our assumption must be false, and hence $x^2 < x$. □

Trying contradiction is a good way to draft a proof, but often such proofs can be recast as direct proofs, which are often shorter and easier to read and which may give readers greater insight into why the statement is true.

Theorem 4. *If* $0 < x < 1$*, then* $x^2 < x$*.*

Proof. Because x is positive, if we multiply both sides of $x < 1$ by x, we obtain the desired result: $x^2 < x$. □

The following example illustrates a brief contradiction argument (in boldface) within a longer proof (by contradiction itself). It is from Aigner & Ziegler's *Proofs from THE BOOK, 3rd ed.*, [1, p. 3], and usually attributed to Euclid (Elements IX,20). It shows that the sequence of primes does not end.

Proof. Assume that the set of primes is finite, and let $\{p_1, \cdots, p_r\}$ be the set of all primes. Now consider the number $n = p_1 p_2 \cdots p_r + 1$. As n is not in the set of primes, it has a prime divisor $p < n$. But p is not one of the p_i; **otherwise p would be a divisor of n and of the product $p_1 p_2 \cdots p_r$ and thus also of the difference $n - p_1 p_2 \cdots p_r = 1$, which is impossible.** So a finite set $\{p_1, \cdots, p_r\}$ cannot be the collection of *all* primes. □

4.3 Proof by Induction

To prove a statement that is valid for all integers n starting at the certain value (i.e. all nonnegative integers, i.e. $n \geq 0$, or all positive integers, i.e. $n \geq 1$) or all values of n satisfying certain properties, a proof by induction can be useful and one would need to complete the following steps:

- Prove the statement for the "base case": the smallest value(s) of n for which the statement needs to be verified.
- Assume that the statement is true for $n = k$. Use this assumption to prove that the statement is true for $n = k + 1$. Doing so is known as the "inductive step."

Proof by induction works like knocking over a line of dominoes. For example, if the base case says the statement is true for $n = 0$ and the inductive step says it's true for the next n, then the statement must be true for $n = 1$. But the inductive step again says it's true for the next n, so the statement must also be true for $n = 2$. And so on forever.

Carefully choosing the inductive hypothesis itself and the parameter n in order to be able to prove the statement being considered (or even a stronger statement) is an art. For example, some statement about any positive integer m could be proved by induction on the number n of prime factors in m (rather than induction on m itself). The base case would then correspond to all prime numbers, and the inductive step would then argue that if the statement is true for any number with k prime factors, it is true for any number with $k + 1$ prime factors. Or a statement about properties of a graph could be attacked by induction by considering the number of nodes of the graph, or the number of edges, or the number of connected components, and the list goes on.

Proof by strong induction. A variant of induction is known as *strong induction.* This is similar to induction, except that the inductive step uses a stronger assumption:

- Inductive step: Assume that the statement is true **for all** n **with** $n \leq k$. Use this assumption to prove that the statement is true for $n = k + 1$.

4.3.1 Skeleton Proof by Induction

Inductive proofs have a common structure.

Theorem. *If... [hypotheses, including the (perhaps implied) hypothesis that n is a natural number], then... [conclusion involving n].*

Proof. We proceed by induction.
Base case: For $n = \ldots$ [smallest value(s) of n, e.g., $n = 1$], we know that... [logic showing that the conclusion is true for these values].
Inductive step: Assume that... [conclusion, with n replaced by k. This assumption is called the "inductive hypothesis."] We need to show that... [conclusion, with n replaced by $k + 1$]. But we can see that... [Logic that uses the former to reach the latter.] □

Although this structure is commonly used, the wording and notation may vary. The important aspects are to somehow clearly indicate the following:

- The base case.
- The inductive hypothesis.
- The statement that is proved in the inductive step.

4.3.2 Examples

The following example is written for an audience familiar with the conventional structure of proofs by induction, with comments between brackets. Its logic is diagrammed in Figure 8 in the appendix.

Theorem 5. *For $n \geq 1$,*

$$\sum_{j=1}^{n} j = \frac{n(n+1)}{2}.$$

Proof. We proceed by induction on n. [Here, it is clear that the induction would be "on n," so this could be omitted, although stating this never hurts.] The statement holds for $n = 1$. ["For $n = 1$, it is true that $1 = \frac{1(2)}{2}$," would be too detailed for the target audience.]

Assume now the statement is true for $n - 1$, i.e. $\sum_{j=1}^{n-1} j = \frac{(n-1)n}{2}$. Then

$$\sum_{j=1}^{n} j = \left(\sum_{j=1}^{n-1} j\right) + n = \frac{(n-1)n}{2} + n = \frac{n(n+1)}{2}.$$

[If one feels more details need to be given, one could add "the second equality following from the inductive hypothesis."] So we are done. [Or "This proves the desired statement."] □

Caution! *Take care when choosing the base case(s), as it has to include all the cases when the inductive step fails to hold. Otherwise the statement's truth cannot propagate from the base case(s) to all the values of n.*

The following classic proof illustrates how a poor choice of base case can yield an incorrect result.

Bad Theorem. *In any herd, all cows are the same color.*

Proof. We proceed by induction on the size of the herd of cows.

For the base case, consider a herd of only one cow. Clearly, all cows in the herd are the same color–let's call this color "orange".

For the inductive step, assume that all herds with n cows are entirely orange and consider a herd with $n + 1$ cows. Temporarily remove one cow, so the herd contains only n cows. By the inductive hypothesis, this herd is entirely orange. Now bring back the removed cow and temporarily remove a different one. This new herd also contains only n cows and so is entirely orange. Thus the cow that was originally removed is orange, and the herd of $n + 1$ cows is entirely orange. □

The above proof by induction fails because the logic of the inductive step doesn't work when the size of the herd is 2. So the base case should have included the case $n = 2$ (where the statement fails to hold).

The following example uses strong induction and requires two base cases.

Theorem 6. *If F_i is the i^{th} Fibonacci number, defined by $F_i = F_{i-1} + F_{i-2}$ for $i \geq 2$ and $F_0 = F_1 = 1$, then, for any $k \geq 2$:*

$$2F_k = F_{k+1} + F_{k-2}. \tag{1}$$

[The assumption that $k \geq 2$ is needed; otherwise (1) would not make sense.]

Proof. We use strong induction.

We start with the inductive step. Assume that (1) holds for all k less than n. We must show that (1) holds also for $k = n$. In particular, assume that (1) is true for $k = n - 1$ and $k = n - 2$ where $n \geq 4$. We thus have the following two equations:

$$\begin{aligned} 2F_{n-1} &= F_n + F_{n-3} \\ 2F_{n-2} &= F_{n-1} + F_{n-4}. \end{aligned}$$

Adding the respective sides of these equations yields

$$(2F_{n-1} + 2F_{n-2}) = (F_n + F_{n-1}) + (F_{n-3} + F_{n-4}).$$

Since the Fibonacci numbers are defined by $F_i = F_{i-1} + F_{i-2}$, we can simplify:

$$2F_n = F_{n+1} + F_{n-2}.$$

This completes the inductive step of the proof.

The base case is when $k = 2$ or $k = 3$. We verify that

$$2F_2 = 2 * 2 = 3 + 1 = F_3 + F_0$$

and

$$2F_3 = 6 = 5 + 1 = F_4 + F_1.$$

This completes this proof by induction. □

Notice that in the inductive step, we had to assume that $n \geq 4$ since we assumed the result to be true for $k = n - 1$ and $k = n - 2$, and the statement is only defined when $k \geq 2$ ($n - 1 \geq 2$ and $n - 2 \geq 2$ mean that $n \geq 4$). In our base case, we therefore had to consider all the cases not covered by the inductive step, namely $k = 2$ and $k = 3$. Only considering the base case $k = 2$ would not have been sufficient, since the proof of the inductive step relied on the truth of (1) for both $k = n - 1$ and $k = n - 2$. Instead, we must treat $k = 3$ as another base case. One could wonder though whether we could simply modify the statement in the theorem and assume there that $k \geq 4$. But if we do so, the inductive hypothesis would then require that $n-1 \geq 4$ and $n-2 \geq 4$, i.e. that $n \geq 6$, and we would still be missing the cases $k = 4$ and $k = 5$.

4.4 Bijective Proof

A bijective proof may be useful for counting problems, when one needs to derive the number of objects with a certain property. The principle is to reduce the question to another simpler one, for which the solution can be derived more easily.

Informally, a *bijection* between sets A and B matches each element in A to exactly one element in B and vice versa. Formally, a *bijection* is defined as a *function* that is both *injective* and *surjective*. The function $f : A \to B$ is *injective* if each element of B is the image of *at most* one element of A, and it is *surjective* if each element of B is the image of *at least* one element of A. Thus if a function f is both injective and surjective, each element of B is the image of exactly one element of A. A synonym for injective is "one-to-one" and a synonym for surjective is "onto."

A bijection between sets A and B implies that A and B have the same number elements (or are both infinite). Counting the number of elements of one of the sets, say B, may (appear to) be simpler than counting the number of elements of the other. If one needs to count the number of elements of a set A, the creative part is to choose the right set B (more easily counted) and the right function f from A and B. Then one has to carefully argue that f is indeed a bijection.

Proof of Bijection 1. To prove that a function $f : A \to B$ is a bijection, prove that f is both an injection and a surjection:

1. To prove f is an injection, prove the following statement:

   If $a_1 \neq a_2$ for $a_1, a_2 \in A$, then $f(a_1) \neq f(a_2)$.

2. To prove f is a surjection, prove the following statement:

   If $b \in B$, then there exists some $a \in A$ for which $f(a) = b$.

Proof of Bijection 2 Another way to prove that a function $f : A \to B$ is a bijection is to show that it has an inverse:

- To prove that the function $g : B \to A$ is the inverse of f, show that $g(f(a)) = a$ for all $a \in A$ and that $f(g(b)) = b$ for all $b \in B$.

4.4.1 Example of a bijective proof

The following example comes from combinatorics. A *partition* is a decomposition of a positive integer into positive integers. For example, the number 5 has seven partitions:

5

$4+1$

$3+2$

$3+1+1$

$2+2+1$

$2+1+1+1$

$1+1+1+1+1$

The partition $4+1$ is considered to be the same as the partition $1+4$ so, by convention, partitions are presented as a non-increasing sequence.

Theorem 7. *The number of partitions of n into k parts is the same as the number of partitions with largest part k.*

Proof-generation strategy: first check your understanding by trying an example. There are two partitions of 5 into 3 parts: $3+1+1$ and $2+2+1$. There are also two partitions with largest part 3. They are $3+2$ and $3+1+1$. Do a few more examples to get reasonably convinced.

Proof-generation strategy: formulate the problem in a different way, e.g., visually. Look at each partition of n as a collection of n dots on the coordinate plane, as in Figure 2. A partition with the ith part being a_i is represented by a_i dots at $x = i$ from $y = 1$ to $y = a_i$, and this is done for every i.

Then flipping the dots across the line $y = x$ changes a partition with k parts into a partition with largest part k, as illustrated in Figure 3[1].

[1] To simplify the explanation, Figures 2 and 3 use Cartesian coordinates. But partitions are conventionally illustrated with Young diagrams or Ferrer diagrams, which place the origin in the upper left as for labeling matrix entries.

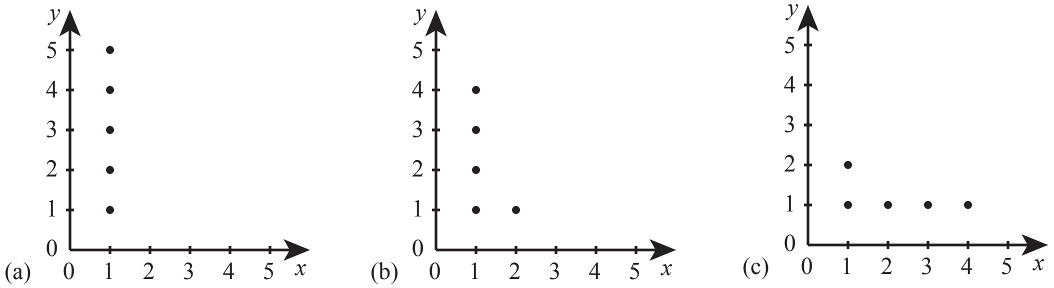


Figure 2: Dot diagrams for a few partitions of 5: (a) 5, (b) $4+1$, (c) $2+1+1+1$

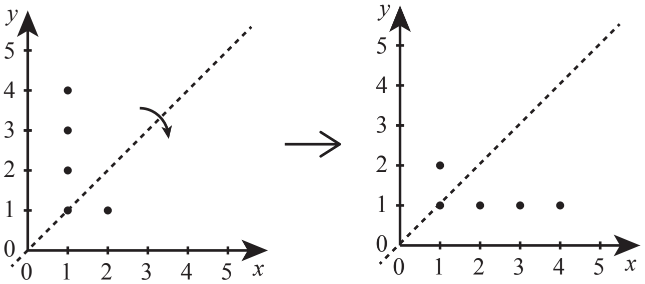


Figure 3: Reflecting a dot diagram across the line $y = x$ changes a partition with k parts into a partition with largest part k. In this example, a partition with 2 parts $(4+1)$ becomes a partition with largest part 2 (that is, $2+1+1+1$).

Proof of Theorem 7. Let A be the set of partitions of n into k parts, and let B be the set of partitions of n with largest part k. To prove the theorem, we identify a bijection between A and B.

To each partition $a_1 + a_2 + \cdots + a_k$ associate the following collection of points:

$$(1,1), \ldots, (1, a_1), \;\; (2,1), \ldots, (2, a_2), \;\; \ldots, \;\; (k,1), \ldots, (k, a_k).$$

Consider the function $f : A \to B$ that takes each point (x, y) and replaces it with the point (y, x), as illustrated in Figure 3. The function f is its own inverse, so it is a bijection. Because a bijection exists between A and B, the two sets are the same size, so the number of partitions of n into k parts is the same is the number of partitions of n with largest part k. □

We could made the proof without reference to the point diagram by defining the resulting partition with $\ell = a_1$ parts as $b_1 + b_2 + \cdots + b_\ell$ where $b_j = |\{i : a_i \geq j\}|$ for $j = 1, \cdots \ell$.

References

[1] Aigner, M., Ziegler, G.M., *Proofs from THE BOOK*, 3rd Ed., Springer-Verlag, 2004.

[2] Cupillari, A., *The Nuts and Bolts of Proofs*, 3rd Ed., Elsevier Academic Press, 2005.

A Diagramming Proofs

Drawing the logic of a proof you're writing can be a useful strategy for checking that you've sufficiently justified all claims. Similarly, as you read a proof, drawing it can help you ensure you understand its logic. In this appendix, we give sample proof diagrams for two direct proofs, one of which is a pigeonhole proof (Figures 4–5), a proof by contrapositive (Figure 6), a proof by contradiction (Figure 7), and a proof by induction (Figure 8). All proofs are from earlier in this document. Notice that although the different proof strategies have different structures, each proof derives the conclusion by using only the hypotheses and accepted outside facts such as definitions, the pigeonhole principle, and rules of arithmetic.

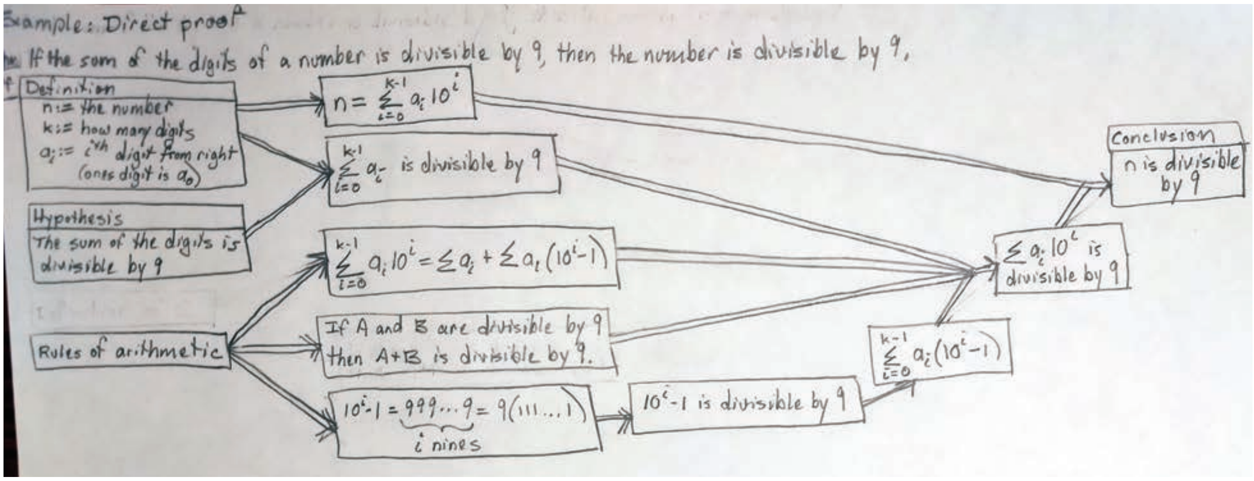

Example: Direct proof
If the sum of the digits of a number is divisible by 9, then the number is divisible by 9.
Definition
n:= the number
k:= how many digits
a_i:= i^{th} digit from right
(ones digit is a_0)
Hypothesis
The sum of the digits is divisible by 9
Rules of arithmetic
$n = \sum_{i=0}^{k-1} a_i 10^i$
$\sum_{i=0}^{k-1} a_i$ is divisible by 9
$\sum_{i=0}^{k-1} a_i 10^i = \sum a_i + \sum a_i (10^i - 1)$
If A and B are divisible by 9 then A+B is divisible by 9.
$10^i - 1 = \underbrace{999\ldots9}_{i \text{ nines}} = 9(111\ldots1)$
$10^i - 1$ is divisible by 9
$\sum_{i=0}^{k-1} a_i (10^i - 1)$
$\sum a_i 10^i$ is divisible by 9
Conclusion
n is divisible by 9

Figure 4: The direct proof of Theorem 1 from Section 3

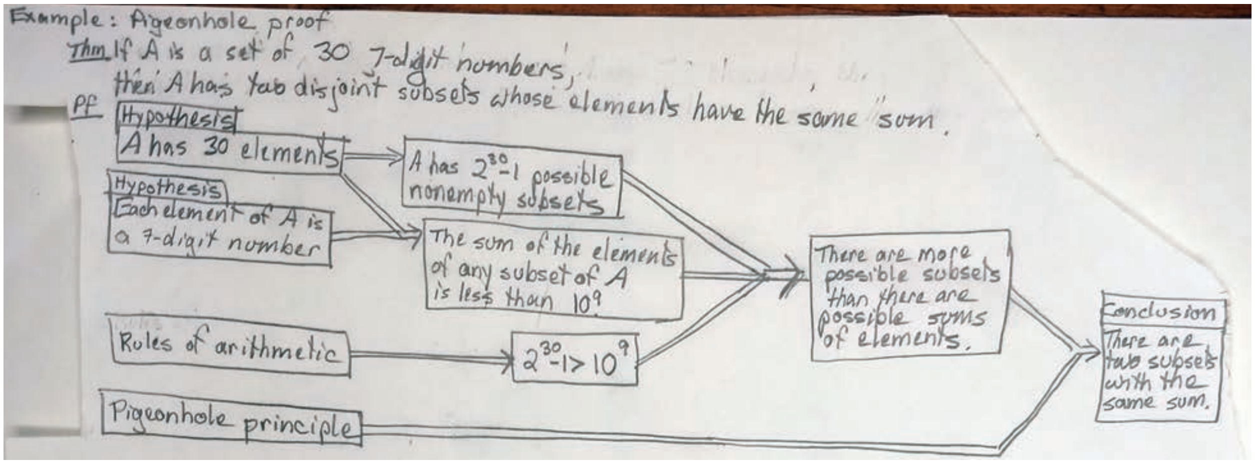

Example: Pigeonhole proof
Thm If A is a set of 30 7-digit numbers,
then A has two disjoint subsets whose elements have the same sum.
Pf
Hypothesis
A has 30 elements
Hypothesis
Each element of A is a 7-digit number
A has $2^{30}-1$ possible nonempty subsets
The sum of the elements of any subset of A is less than 10^9
Rules of arithmetic
$2^{30}-1 > 10^9$
There are more possible subsets than there are possible sums of elements.
Pigeonhole principle
Conclusion
There are two subsets with the same sum.

Figure 5: The pigeonhole proof of Theorem 2 from Section 4.1.1

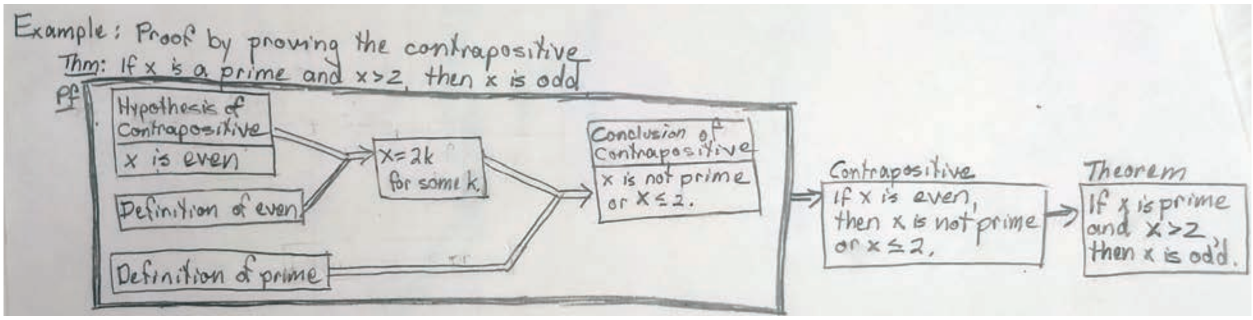

Example: Proof by proving the contrapositive
Thm: If x is a prime and x>2, then x is odd
Pf
Hypothesis of Contrapositive
x is even
Definition of even
x=2k for some k
Definition of prime
Conclusion of Contrapositive
x is not prime or x≤2.
Contrapositive
If x is even, then x is not prime or x≤2.
Theorem
If x is prime and x>2 then x is odd.

Figure 6: The proof by contrapositive of the statement from Section 4.2

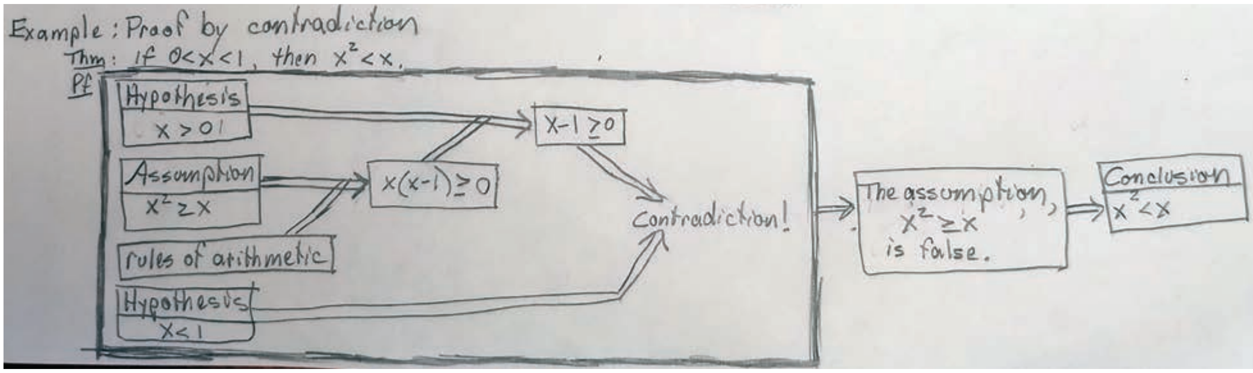


Figure 7: The proof by contradiction of Theorem 3 from Section 4.2.2

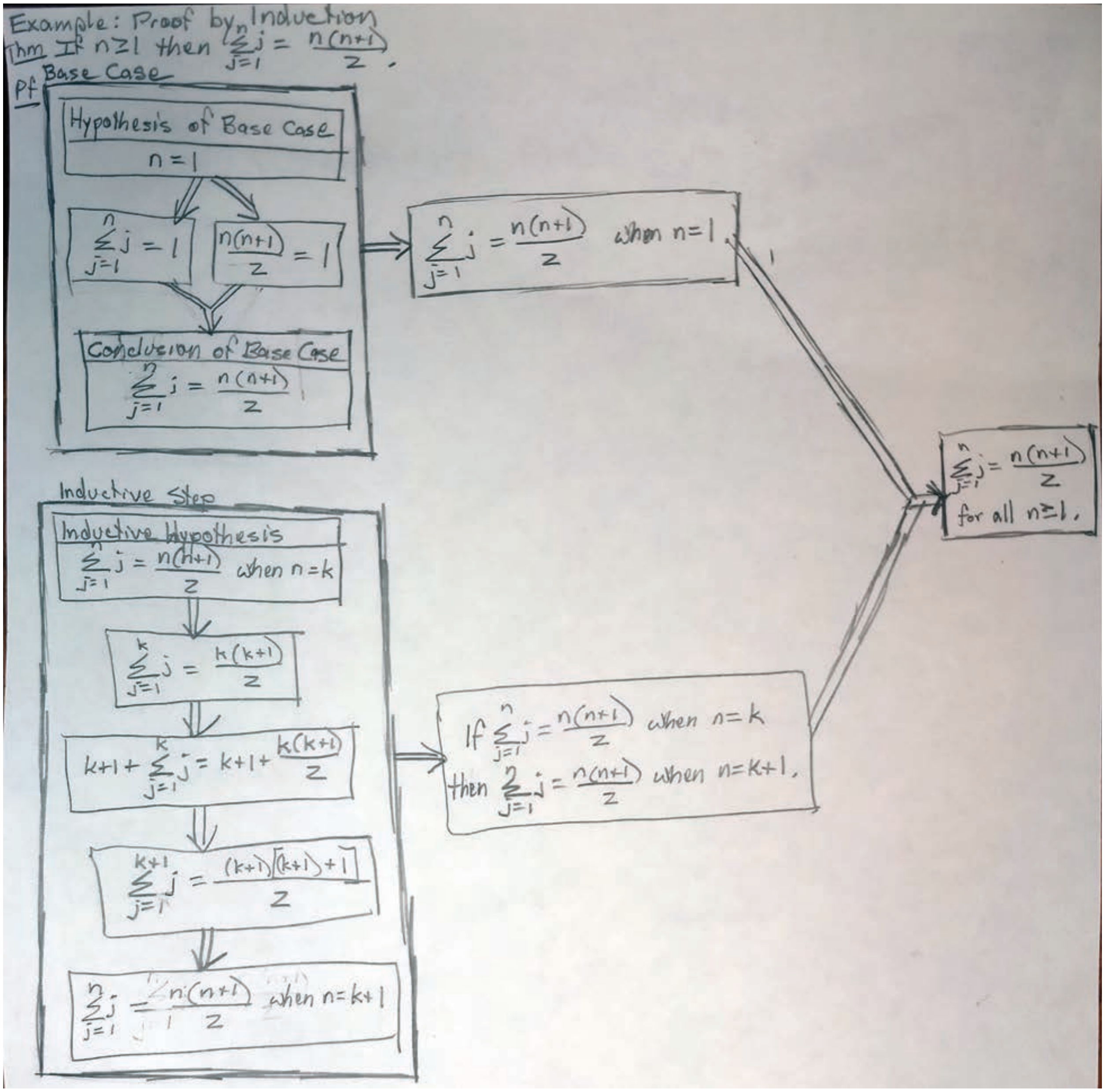

Example: Proof by Induction
Thm If $n \geq 1$ then $\sum_{j=1}^{n} j = \frac{n(n+1)}{2}$.
Pf
Base Case
Hypothesis of Base Case
$n=1$
$\sum_{j=1}^{n} j = 1$
$\frac{n(n+1)}{2} = 1$
Conclusion of Base Case
$\sum_{j=1}^{n} j = \frac{n(n+1)}{2}$
$\sum_{j=1}^{n} j = \frac{n(n+1)}{2}$ when $n=1$.
1
$\sum_{j=1}^{n} j = \frac{n(n+1)}{2}$ for all $n \geq 1$.
Inductive Step
Inductive Hypothesis
$\sum_{j=1}^{n} j = \frac{n(n+1)}{2}$ when $n=k$
$\sum_{j=1}^{k} j = \frac{k(k+1)}{2}$
$k+1+\sum_{j=1}^{k} j = k+1+\frac{k(k+1)}{2}$
$\sum_{j=1}^{k+1} j = \frac{(k+1)[(k+1)+1]}{2}$
$\sum_{j=1}^{n} j = \frac{n(n+1)}{2}$ when $n=k+1$
If $\sum_{j=1}^{n} j = \frac{n(n+1)}{2}$ when $n=k$
then $\sum_{j=1}^{n} j = \frac{n(n+1)}{2}$ when $n=k+1$.

Figure 8: The proof by induction of Theorem 5 from Section 4.3.2