1-2016

Discrete Mathematics: Chapter 3, Mathematical Induction and Peano Arithmetic

Calvin Jongsma
Dordt College, calvin.jongsma@dordt.edu

Discrete Mathematics: Chapter 3, Mathematical Induction and Peano Arithmetic

Abstract

In this chapter we will study one more very important proof technique along with some variants, and we will consider their counterparts for making mathematical definitions. This connects up with ideas that are central in computer science, too. As we proceed, we will briefly pause to look at how arithmetic can be treated as a deductive theory. This material will give us a good basis for working with natural numbers later in the text.

Keywords

induction, arithmetic, Giuseppe Peano, proof, logic, numbers

Disciplines

Christianity | Computer Sciences | Mathematics

Comments

- From Discrete Mathematics: An Integrated Approach, a self-published textbook for use in Math 212
-

✠ Chapter 3 ✠

MATHEMATICAL INDUCTION & PEANO ARITHMETIC

3.1 Mathematical Induction and Recursion

In this chapter we will study one more very important proof technique along with some variants, and we will consider their counterparts for making mathematical definitions. This connects up with ideas that are central in computer science, too. As we proceed, we will briefly pause to look at how arithmetic can be treated as a deductive theory. This material will give us a good basis for working with natural numbers later in the text.

Since the Natural Deduction System we adopted for *Predicate Logic* (Chapter 2) is complete and includes all the inference rules for *Sentential Logic* (Chapter 1), you may wonder what is missing now. The answer this time is different than before (Section 2.1), when we noted that SL's completeness was only system-dependent; we are not about to argue for extending our logic any further. What we have in PL is adequate for formalizing mathematical argumentation. The proof strategy we will introduce in this section is instead a technique that arises from arithmetic, and as such it is not part of logic. Different branches of mathematics have different sorts of proof strategies; the one we consider here is central because of the role played by natural numbers throughout mathematics.

PL supplies two main methods for proving universal sentences: the direct method of *Universal Generalization* and the indirect method of *Proof by Contradiction*. When the universal quantifier ranges over the set of natural numbers $\mathbb{N} = \{0, 1, 2, \ldots\}$, however, it turns out we have as well the more specialized proof strategy known as *Proof by Mathematical Induction* (*PMI*). This will be our focus here.

In this section we will consider the most basic form of *PMI*. We will explain the overall proof strategy, give an intuitive argument for its soundness, illustrate it with examples taken from various fields of mathematics, and show how *Recursive Definition* is related to *PMI*. In Section 3.2 we will look at some important variations of this proof strategy. Then in Section 3.3 we will explore the theoretical basis of *Proof by Mathematical Induction* and see how that fits into the axiomatic development of arithmetic.

Introduction to Mathematical Induction: Tower of Hanoi

Tower of Hanoi

We'll introduce *Proof by Mathematical Induction* by analyzing the *Tower of Hanoi*. This game is a favorite of mathematicians, computer scientists, and neuro-psychologists because of the thought process it stimulates. It is a single-person game/puzzle* played by moving a column of discs one at a time from a starting peg onto a terminal peg, using a third peg for temporary storage, never placing a larger disc on top of a smaller one. Using a very small number of discs, say 1, 2, or 3, this is not too hard to do. For a larger number of discs, even for 5 or 6, however, it may not even be immediately obvious to you that the game can be successfully played. And, assuming it can be done, determining the least number of moves required to complete the game for any given number of discs may seem like an impossible task. How will you know that your moves can't be improved upon by someone with a more ingenious approach?

Using an inductive approach, we'll see that the game can be successfully played, and we'll determine the optimal number of moves, regardless of the number of discs involved. Before you proceed to read the following analysis, you might want to try the game yourself with three or

* Invented by the mathematician and Fibonacci afficionado E. Lucas in 1883, this game and its history can be found on numerous web sites, some of which allow you to play a timed game for different numbers of discs.

four discs. If you don't have the game at hand to play, try it with a quarter, a nickel, a penny, and a dime, putting three spots on a piece of paper to represent the three pegs.

For a single disc, the game obviously takes 1 move. Clearly this number is minimal; the game can't be completed in fewer moves.

– Two discs can be transferred in a minimum of 3 moves:
  1) move the small disc to the temporary peg;
  2) place the large disc on the terminal peg; and
  3) put the small disc back on top of the large one.
– Three discs require a minimum of 7 moves.
– How many moves are required if you start with four discs? with five discs? in general?

To show that the game is possible and to determine the minimum number of moves needed for a large number of discs without actually continuing to play the game, which is getting increasingly complex, you might take the following tack: tabulate your initial results, and look for a formula that expresses the pattern.

Number of Discs	Minimal Number of Moves
1	1
2	3
3	7
4	?
5	?
n	??

This approach is often helpful if you have a good-sized sample of values. In this case, however, working the problem further by playing a few more games to produce enough data from which to conjecture the general relationship holding between the number of discs n and the number of moves m_n would be time-consuming, frustrating, and probably error-ridden, since it is easy to lose track of what you're doing or make moves that turn out to be dead-ends or repetitious.

What we really need in addition to the concrete data already obtained is an insight into a uniform procedure by which the number of moves can be determined. How can we argue (a thought experiment, now) that the above data is correct and then extrapolate to get further correct values?

It would be advantageous if we could always build on past successes to obtain the next result. Let's see how this can be done, starting with $n = 2$. To move two discs, move the top one to the temporary peg; then move the other disc to the terminal peg; finally, move the small disc back on top of the other one, for a total of 3 moves minimum. For three discs, first move the top two discs (in the way just prescribed, of course; but since we know this can be done, don't bother doing it one disc at a time) to the temporary holding peg with the minimum number of moves (3); then move the bottom disc to the terminal peg (1 move); and finally, move the two smaller discs onto that disc in as few moves as possible (3 again). The total number of moves required for the whole process is thus 7.

Generalizing, at each stage we can move the n top discs to the temporary peg in, say, m_n moves, move the bottom disc to the terminal peg in 1 move, and then move the n discs back on top of the large disc in another m_n moves. The total moves for $n + 1$ discs is thus $2m_n + 1$ moves. Beginning with $n = 0$ (or starting with $n = 1$, if you don't like the idea of "playing" the game without a disc), you can generate the following sequence of values for m_n:

Number of Discs	Minimal Number of Moves
0	0
1	$2 \cdot 0 + 1\ = 1$
2	$2 \cdot 1 + 1\ = 3$
3	$2 \cdot 3 + 1\ = 7$
4	$2 \cdot 7 + 1\ = 15$
5	$2 \cdot 15 + 1\ = 31$
6	$2 \cdot 31 + 1\ = 63$
7	$2 \cdot 63 + 1\ = 127$
n	$\mathbf{m_n}$
$n+1$	$2 \cdot \mathbf{m_n} + 1$

Tower of Hanoi Moves

This recursive procedure generates a sequence of values for the optimal number of moves m_n required for moving n discs:

$$m_0 = 0$$

$$m_{n+1} = 2m_n + 1$$

This does not yet explicitly define m_n in terms of n, which is really what we want, but at least it convinces us that the game can in principle be played efficiently with any number of discs, and it generates plenty of accurate values to help us determine the pattern.

Since doubling occurs in moving from each step to the next, the number 2 will play a role in the formula. Putting the above values in terms of 2, we see that

$$\begin{aligned} m_0 + 1 &= 1 \\ m_{n+1} + 1 &= 2m_n + 2 \\ &= 2(m_n + 1). \end{aligned}$$

This sequence of numbers proceeds by simple doubling, so now we have a sequence of powers of 2: 1, 2, 4, 8, 16, and so on. In general, therefore, it is clear that $m_n + 1 = 2^n$. Relating this back to the original sequence of values m_n, we get $m_n = 2^n - 1$. You may have seen this pattern earlier; our argument helps convince us that it is correct.

Having found the result, the proof that it is correct only requires marshaling the above ideas into a coherent three-step argument.

1) $2^n - 1$ is certainly the minimal number of moves when $n = 0$ or when $n = 1$.
2) Given any number of discs k for which the minimum number of moves is known to be $2^k - 1$, it follows from how we must move the discs that the minimum number of moves for $n = k + 1$ discs is $2(2^k - 1) + 1 = 2^{k+1} - 1 = 2^n - 1$.
3) Thus, combining steps 1) and 2), we can conclude that the minimum number of moves for n discs is exactly $m_n = 2^n - 1$ for every n.
   For since the formula works for $n = 0$ (step 1), it must work for $n = 0 + 1 = 1$ by step 2. And since it works for $n = 1$, it must work for $n = 1 + 1 = 2$, again by step 2. Repeating the argument-loop of step 2 as needed, we can show that the formula holds for any natural number whatsoever.

Proof by Mathematical Induction

Proof by Mathematical Induction (*PMI*) is the specialized method of proving a result $P(n)$ for all natural numbers n by means of the three-step process we just described. We will schematize it more generally here and name each step for future reference:

Proof by Mathematical Induction

1) *Anchor Step/Base Case*
   Prove $P(0)$.
2) *Induction Step*
   Assume $P(k)$ for an arbitrary natural number k; (the *Induction Hypothesis*)
   prove $P(k+1)$.
3) *Conclusion*
   Conclude $(\forall n \in \mathbb{N})P(n)$.

To employ an analogy to explain why this proof technique works, visualize an infinite sequence of dominoes P_n waiting to be knocked over (every kid's dream). In order to get all the dominoes to fall, you need to push over the lead domino P_0 (the analog of proving the anchor step), and you must make sure all the dominoes are lined up so that each domino P_k knocks over the next one P_{k+1} (the analog of proving the induction step). If this is done, all the dominoes will eventually fall (the analog of drawing a universal conclusion). Alternatively, think of proving a proposition for all natural numbers via mathematical induction as analogous to climbing up an infinitely long ladder. To get on every rung you first have to get on at the bottom (the anchor step) and you need to have a mechanism or procedure that will move you from each step to the next one (the induction hypothesis).

If you look closely at the above schema for *Proof by Mathematical Induction*, you may find the induction step rather perplexing. It looks for all the world like you start by assuming the very thing that needs proving.

Question: "Isn't the assumption that $P(k)$ holds for any natural number $k \geq 0$ exactly the conclusion we need to prove, only using a different variable name?"
Answer: "Yes."
Question: "Well, ... isn't this circular reasoning, then, something we're supposed to avoid like the plague?!"
Answer: "Now the answer is 'No'."

Familiarity with suppositional proofs from *Sentential* and *Predicate Logic* should help you overcome the feeling that something illegitimate is going on here. What you are *actually* doing in the induction step of *PMI* is *temporarily supposing* $P(k)$ as a *working hypothesis* in order to *show* $P(k+1)$ via *CP*; that is, $P(k)$ is assumed in a *subproof* of the main proof in order to conclude the *conditional* sentence $P(k) \rightarrow P(k+1)$. By *UG*, then, all that you can conclude from this step alone in the main part of the proof is that a universal *conditional* holds. In order to conclude the desired unconditional universal sentence, $(\forall n)P(n)$, you must have the anchor step as well. $P(1)$, $P(2)$, $P(3)$, and so on all follow from linking together steps one and two and successively applying step two to each one of your new results to generate the next one (via *UI* and *MP*). Thus, since $P(n)$ can be proved for any value of n, you are entitled by *PMI* to *conclude* the desired universal statement in step 3: $(\forall n)P(n)$. Both steps one and two are needed to guarantee the validity of the conclusion in step three. If either of these steps is missing, you can prove false statements (see Exercises 8 and 3.2-14).

To summarize: to prove a universal sentence of the form $(\forall n \in \mathbb{N})P(n)$, you have several proof strategies you can try. You can use the methods discussed in Chapter 2, proving it directly by means of *UG* or indirectly by *NE*, using *UN*; or you can make use of the new method of *PMI*. This latter method is often your best choice, though it can sometimes be avoided.

We'll illustrate *Proof by Mathematical Induction* with a couple of examples. The first result was known already to Archimedes, but it was independently rediscovered by a precocious young Gauss, who used it to add up the first 100 numbers, instantaneously solving a problem given to his class by a grade-school teacher looking for some free time.

✠ **EXAMPLE 3.1 - 1**

Prove Gauss's formula for the sum of a finite arithmetic sequence:

$$0+1+2+\cdots+n=\frac{n(n+1)}{2}.$$

Solution

We will use the three-step method to prove this by *Mathematical Induction*.

Proof:

1) *Anchor Step*
   $0=(0\cdot 1)/2\,.$
2) *Induction Step*

$$\begin{aligned}
&\text{Suppose } 0\ +\ 1\ +\ 2\ +\ \cdots\ +\ k=\frac{k(k+1)}{2}\,. && \text{Indn Hyp}\\
&\text{Then } 0+1+2+\cdots+k+(k+1)=\frac{k(k+1)}{2}+(k+1) && \text{Sub}\\
&\qquad =\frac{k(k+1)+2(k+1)}{2} && \text{Algebra}\\
&\qquad =\frac{(k+1)(k+2)}{2}\,. && \text{Factoring}
\end{aligned}$$

3) *Conclusion*

$$\text{Therefore, } 0\ +\ 1\ +\ 2\ +\ \cdots\ +\ n=\frac{n(n+1)}{2}\,.\ \blacksquare \qquad\qquad \text{PMI}$$

As this example shows, if the statement to be proved is an equation, your induction step argument should begin with one side of the equation to be proved (when $n=k+1$) and move toward the other side, using the induction hypothesis (when $n=k$) via substitution to obtain new expressions equal to the original one. A similar approach works with inequalities, as the next example illustrates.

✠ **EXAMPLE 3.1 - 2**

Show for any real numbers a and b that if $a\le b$, then $na\le nb$ for all natural numbers n. You may assume the following Additivity Property for $\le$: $x\le y\rightarrow x+z\le y+z$.

Solution

We will use a combination of both *Universal Generalization* and *PMI* here.
We first suppose that a and b are any two real numbers (for *UG*) and that $a\le b$ (for *CP*).
To show $(\forall n)(na\le nb)$, we will use induction on n.

Proof:

1) *Anchor Step*
   Since $0\cdot a=0=0\cdot b$ for any a and b, we certainly have $0\cdot a\le 0\cdot b$ for $a\le b$.
2) *Induction Step*

$$\begin{aligned}
&\text{Suppose}\quad ka\le kb. && \text{Indn Hyp}\\
&\text{Then } (k+1)a=ka+a && \text{Algebra}\\
&\qquad\qquad \le ka+b && \text{Add Prop } (a\le b)\\
&\qquad\qquad \le kb+b && \text{Add Prop } (ka\le kb \text{ by spsn})\\
&\qquad\qquad \le (k+1)b. && \text{Factoring}
\end{aligned}$$

3) *Conclusion*
   Therefore, $na\le nb$ for all n. $\blacksquare$ PMI

Mathematical Induction and Recursive Definitions

Proof by Mathematical Induction often goes hand-in-hand with inductive definition. To symbolize some derived operation, relation, or property for the natural numbers, you may be able to define it all at once via some logical equivalence, as we did earlier with the notions of being even and prime, and as we did in defining divisibility. However, there will be times when you have to define a notion piece-meal, successively: define it first for 0, then for 1, for 2, and so on. Such a process will never terminate, of course, so what is needed is an inductive process with a kick-forward mechanism to help you define a notion successively-all-at-once for infinitely many cases. This sort of definition is known as *Recursive Definition*. The meaning of the defined notion for each given number thus depends upon its meaning for earlier numbers.

Simple recursive definitions consist of two parts, corresponding to the first two parts of *PMI*: an initialization step defines the concept for 0, and the second one tells how it is defined for any number once it is defined for its predecessor. Such a process uniquely defines the concept involved. We state an informal version of this claim in the following theorem. Its truth should be intuitively clear; proving it rigorously requires a careful set-theoretic argument that we are not set up to do.

THEOREM*: *Recursive Definitions Are Well-Defined

If a concept is defined recursively by defining it first for $n = 0$, and if it is defined for $n = k + 1$ in terms of its meaning for $n = k$, then the concept is uniquely defined for all natural numbers.

To show how recursive definitions are made and how they are used in inductive proofs, we will present a recursive definition for exponentiation and then prove a basic law for exponents. Other laws will be left as exercises (see Exercises 32-34 and 3.2.22 - 26).

✠ EXAMPLE 3.1 - 3

Define exponentiation for natural number exponents.

Solution

Let a be an arbitrary non-zero real number. Then

1) $a^0 = 1$, and
2) $a^{k+1} = a^k \cdot a$.

This defines the binary operation of exponentiation for any natural number exponent n. It stipulates that the zeroth power of a non-zero number is 1, and it defines any other power of such a base as the product of the preceding power and the number itself. Thus, using steps 2 and 1 repeatedly, you can in principle generate any natural power of a. The first few of these are given below:

$$a^1 = a^0 \cdot a = a$$
$$a^2 = a^1 \cdot a = a \cdot a$$
$$a^3 = a^2 \cdot a = a \cdot a \cdot a$$

✠ EXAMPLE 3.1 - 4

Using the above definition for exponentiation (and various algebraic properties of addition and multiplication), establish the following law of exponents, where $a \neq 0$ is a real number and both m and n are natural numbers: $a^m \cdot a^n = a^{m+n}$.

Solution

Proof:

Suppose a is any non-zero real number and m is a natural number. For such an a and m, we will prove the law for any natural number n by *PMI*.

1) *Anchor Step*
$a^m \cdot a^0 = a^m \cdot 1 = a^m$ for any m by the first part of the recursive definition, substitution, and the multiplicative property of 1. So the law holds when $n = 0$.

2) *Induction Step*

$$\begin{array}{lll}
\text{Suppose } a^m \cdot a^k & = a^{m+k}\,. & \text{Indn Hyp} \\
\text{Then } \; a^m \cdot a^{k+1} & = a^m \cdot (a^k \cdot a) & \text{Defn, Sub} \\
 & = (a^m \cdot a^k) \cdot a & \text{Algebra} \\
 & = a^{m+k} \cdot a & \text{Sub} \\
 & = a^{(m+k)+1} & \text{Defn, Sub} \\
 & = a^{m+(k+1)} & \text{Assoc for } +
\end{array}$$

3) *Conclusion*
Therefore, $a^m \cdot a^n = a^{m+n}$ for all natural numbers n by *PMI*.

Since a is an arbitrary non-zero real number and m is an arbitrary natural number, the conclusion holds for any real $a \neq 0$ and any natural numbers m and n by *UG*. ■

The sort of argument given in this last example is typical. Many times *Proof by Mathematical Induction* will draw upon a recursive definition, if not explicitly, at least implicitly in making use of an idea that at bottom is defined recursively.

Aside on Proof Style

This is as good a time as any to make a few comments about differing proof styles. While our proof analyses may continue on occasion to identify key logical rules of inference employed in a proof, we will no longer be putting our arguments into the standard proof diagram format we developed for logic. We will now begin writing proofs in a more conventional mathematical style, using what we know about logic to help us *choose a proof strategy* for constructing the argument. It is particularly appropriate to make a shift in proof style at this point because we do not want to encumber proofs involving algebraic or arithmetic computations with the logical detail that would ensue from spelling out all the laws involved (recall Example 2.4-12). In presenting our arguments, we may at times still use a two column format for clarity, but we will now cite as our reasons certain mathematical results, or "algebra", or the name of some technique, such as "factoring". You may do likewise in working your homework problems.

If you write your proofs in an informal paragraph style, you may want to merge your *Backward-Forward Proof Analysis* with your proof so that the reader can better follow your train of thought. You might argue somewhat as follows to show that premises P_1, P_2, . . . , P_n prove a conclusion Q: "Q follows from R, and that in turn will hold if S is the case, and S will be true if . . . if T is true; but T can be deduced from the premises P_1, P_2, . . . , P_n". You would then merely derive T as a consequence of the premises and consider your proof finished without any further argument. However, if you incorporate a *Backward-Forward Proof Analysis* in your informal argument in this way, you should at the very least use key words like "know" or "holds" to indicate results that are known to hold and words like "want to show" or "need to prove" to indicate results you would like to deduce but still do not have. Unless you use indicators like this, your proofs are bound to confuse both you and your reader; upon returning to an earlier part of your argument, you may no longer be sure which results are already established and which ones still need to be proved. For this reason, many mathematics textbooks and instructors insist that your argument be given completely in the forward direction.

EXERCISE SET 3.1

Problems 1 - 7: Divisibility and Induction

*Prove the following divisibility results using PMI. Recall that the notation $a \mid b$, read **a divides b**, means that $b = ma$ for some integer m; that is, a divides b exactly, leaving no remainder.*

1. Show that $2 \mid 3^n - 1$

*2. Show that $3 \mid 4^n - 1$ for all natural numbers n.

3. By analogy with Exercises 1 and 2, conjecture a corresponding divisibility result for 4 and then prove it, using *PMI*: $4 \mid$ ____________.

4. Based on the pattern exhibited in Exercises 1 - 3, conjecture a divisibility result for m and then prove it, using *PMI*: $m \mid$ ____________.

5. Show that $3 \mid n^3 + 2n$ for all natural numbers n.

EC 6. Show that $5 \mid n^5 - n$ for all natural numbers n.

7. Show that $x^5/5 + x^3/3 + 7x/15$ is a natural number for all natural numbers.

Problems 8 - 10: Exploring PMI and Recursion

Work the following problems, which explore aspects of PMI.

*8. Is the proposition "$n^2 + n + 17$ is prime for all natural numbers" true or false? If it is true, prove it by means of *PMI*. If it is false, indicate where such a proof by induction breaks down.

9. Explain in your own words why *PMI* is a valid form of argumentation for mathematics. Is this a form of argumentation that you have used before?

10. Explain in your own words how recursive definition defines a concept for all natural numbers.

Problems 11 - 14: Adding Up Exponentials

Prove the following summation formulas using PMI. Recall that $\displaystyle\sum_{i=0}^{n} a_i = a_0 + a_1 + \cdots + a_n$

11. $\displaystyle\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$

*12. $\displaystyle\sum_{i=0}^{n} 3^i = \frac{3^{n+1} - 1}{2}$

13. Based on the pattern in Exercises 11 and 12, conjecture a formula for $\displaystyle\sum_{i=0}^{n} 4^i$ and then prove your result.

14. Generalize the results of Exercises 11 – 13: conjecture a formula for $\displaystyle\sum_{i=0}^{n} r^i$ and then prove your result.

Problems 15 - 18: Finite Geometric Sequences

*Work the following problems involving geometric sequences. A **geometric sequence** is a sequence of numbers $a_0, a_1, \ldots, a_n$ such that each new term is a constant multiple of the last one.*

*15. List the first few terms of the geometric sequence that starts with $a_0 = 32$ and proceeds by repeated halving. What is a_{100} for this sequence?

*16. Give a formal recursive definition for a geometric sequence whose first term is a and whose constant multiple is r.

17. Conjecture a formula for the general term a_n of a geometric sequence in terms of the first term a and the constant multiple r. Then prove your result from the definition of a_n, using *PMI*.

18. Show, using *PMI*, that if a principal of A_0 dollars is deposited and left for a time in an account that yields $100r$ percent interest per period, compounded once per period, then the amount A that has accumulated after t full periods is given by the formula $A(t) = A_0(1 + r)^t$. Tell why these amounts form a geometric sequence; what is the first term and the constant multiple for this sequence?

Problems 19 - 20: Finite Geometric Series

Work the following problems involving geometric series. A ***finite geometric series*** *is a sum* $S_n = \sum_{i=0}^{n} a_i$ *in which the terms* a_i *form a geometric sequence.*

19. Determine and prove a closed formula giving the value of S_n in terms of the first term a_0 and the common ratio r. Hint: Write out the terms of the series using only a_0 and r; then factor out a_0 and multiply the rest by $\frac{1-r}{1-r}$; simplify to obtain a simple formula for the sum; prove your formula using *PMI*. Alternatively, after factoring, apply Exercise 14 if you have worked it.

20. Use the formula you developed in Exercise 19 to determine the sum of the first 12 terms of a geometric series whose first term is 32 and whose common multiple is 1/2. (Caution: a_0 is the *first* term.)

Problems 21 - 24: Finite Arithmetic Sequences

Work the following problems involving geometric sequences. A ***arithmetic sequence*** *is a sequence of numbers* $a_0, a_1, \ldots, a_n$ *such that each new term is a constant difference* d *more than the last one.*

21. Explain why successive odd numbers form an arithmetic sequence. What is a_0? What is d? What is a_{25}? Which a_n is 99?

22. A job initially pays $6.50 per hour. If an employee working this job receives a 25 cent raise each half year, how much will she be earning per hour after 15 years?

23. Give a formal recursive definition for an arithmetic sequence whose first term is a and whose constant difference is d.

24. Conjecture a formula for the general term a_n of an arithmetic sequence in terms of the first term a and the constant difference d. Then prove your result from the definition of a_n, using *PMI*.

Problems 25 - 28: Finite Arithmetic Series

Work the following problems involving arithmetic series. A ***finite arithmetic series*** *is a sum* $S_n = \sum_{i=0}^{n} a_i$ *in which the terms* a_i *form an arithmetic sequence.*

25. Add up all even numbers less than or equal to 100. Note that you can factor a 2 out of each term and apply Example 1.

26. Determine the sum of all odd numbers less than 100.

27. Determine and prove a general formula giving the sum of a finite arithmetic series in terms of the first term a_0 and the common difference d.

*28. *Galileo's Law*
Formulate and prove via *PMI* the result related to *Galileo's Time-Squared Law*: the sum of all successive odd positive integers up to a given one is a perfect square. Hint: take $a_i = 2i + 1$ and determine what square the series adds up to by looking at some examples/values for n.

Problems 29 - 31: Finite Power Series

Prove the following formulas for series of powers using PMI.

*29. $\sum_{i=0}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$

30. $\sum_{i=0}^{n} i^3 = \left[\frac{n(n+1)}{2}\right]^2 = \left(\sum_{i=0}^{n} i\right)^2$

31. $\sum_{i=0}^{n} i^4 = \frac{n(n+1)(2n+1)(3n^2+3n-1)}{30}$

Problems 32 - 34: Laws of Exponents for Natural Numbers

Prove the following results for exponentiation with natural number exponents. You may use the recursive definition of Example 3, the law of Example 4, and any general laws that hold for addition or multiplication.

*32. $(a^m)^n = a^{m\cdot n}$

33. $a^n \cdot b^n = (a \cdot b)^n$

34. $a^n/a^m = a^{n-m}$, $m \leq n$. Hint: do induction on n; generalize on m.

Problems 35 - 37: Factorials

Work the following problems on factorials. Recall that $n!$ is the product of all positive integers from 1 to n inclusive, with $0! = 1$ by convention.

*35. Give a recursive definition of $n!$ for all natural numbers n. Pattern your definition on that given in Example 3 for exponentiation: i.e., tell what 0! is and what $(n+1)!$ is in terms of $n!$.

36. Using your definition Exercise 35, explicitly show that $1! = 1$, $2! = 2 = 1 \cdot 2$, and $3! = 6 = 1 \cdot 2 \cdot 3$. For $n \geq 1$, what familiar formula does your recursive definition in part a lead to?

*37. Using the definition of factorial from Exercise 35 and *PMI*, prove that $\displaystyle\sum_{i=0}^{n} i \cdot i! = (n+1)! - 1$.

Problems 38 - 39: Formulas for Recursive Sequences

Find formulas for the following sequences, giving a_n in terms of n. Then prove the formulas using PMI.

38. $a_0 = 0$, $a_{n+1} = \dfrac{2 + a_n}{3}$

EC 39. $a_0 = 0$, $a_{n+1} = 3a_n + 1$

Problems 40 - 41: Mathematical Results

Prove the following mathematical results, using PMI where appropriate.

40. Prove Bernoulli's Inequality: $(1+b)^n \geq 1+bn$ for $b > -1$, $b \in \mathbb{R}$, $n \in \mathbb{N}$. You may use any basic results about exponentiation and the order relation $\leq$. Point out where $b > -1$ enters into your proof.

41. *De Moivre's Formula*

a. Using the summation rules for sine and cosine $[\sin(\alpha+\beta) = \sin\alpha\cos\beta + \sin\beta\cos\alpha$; $\cos(\alpha+\beta) = \cos\alpha\cos\beta - \sin\alpha\sin\beta]$ and the fact that $i^2 = -1$, show that $(\cos\theta_1 + i\sin\theta_1)\cdot(\cos\theta_2 + i\sin\theta_2) = \cos(\theta_1+\theta_2) + i\sin(\theta_1+\theta_2)$.

b. Using the result of part a, prove that $(\cos\theta + i\sin\theta)^n = \cos(n\theta) + i\sin(n\theta)$ for all natural numbers n.

HINTS TO STARRED EXERCISES 3.1

2. In the induction step it will help to rewrite -1 in the form $-4+3$.
8. Consider a few different values for n before deciding.
12. Recall that $\displaystyle\sum_{i=0}^{k+1} 3^i = \sum_{i=0}^{k} 3^i + 3^{k+1}$.
15. Find a formula for a_n that involves a power of $\frac{1}{2}$.
16. [No hint.]
28. [No hint.]
29. You'll need to combine fractions and factor in the induction step. You can also expand expressions and then factor, but that will make the process longer.
32. Let m be an arbitrary natural number, then use induction on n.
35. [No hint.]
37. Factor the expression you get when you expand $\displaystyle\sum_{i=0}^{k+1} i \cdot i!$.

3.2 Variations on Induction and Recursion

In many mathematical settings *PMI* may seem like the natural proof strategy to try, and yet either it doesn't strictly apply in a form needed for the problem, or else the induction step doesn't go through as needed. In these cases, a different form of *Proof by Mathematical Induction* might still work. We will consider a couple of these variants in this section, and we will look at another version of recursive definition as well.

Modified Proof by Mathematical Induction (*Mod PMI*)

Suppose we want to prove some statement $P(n)$ not for all natural numbers n, but for some segment of the natural numbers or the integers. If this is the case, we may need to use a modified form of *Proof by Mathematical Induction*. For example, results that hold true for all n-sided polygons require $n \geq 3$; such a result makes no sense for $n < 3$. Here, then, we need a version of *PMI* that begins with 3 instead of 0 and then continues through all natural numbers greater than 3.

On the other hand, we might want to prove a statement for a sequence of numbers that is more inclusive than the set of natural numbers. We might want to prove a result, for instance, that holds for all integers greater than or equal to, say, -2. Whatever our starting point, we should be able to use a modified version of induction that applies to the segment of integers greater than or equal to that number.

Like *PMI*, *Modified Proof by Mathematical Induction* (*Mod PMI*) draws its final conclusion based upon an anchor step and an induction step. However, both of these steps as well as the conclusion are modified to fit the particular situation. *Mod PMI* is schematized as follows, where the universe of discourse is assumed to be $\mathbb{Z}$, the set of integers.

***Modified Proof by Mathematical Induction* (*Mod PMI*)**

1) *Modified Anchor Step*
   Prove $P(n_0)$.
2) *Modified Induction Step*
   Assume $P(k)$ for an arbitrary $k \geq n_0$;
   prove $P(k+1)$.
3) *Modified Conclusion*
   Conclude $(\forall n \geq n_0)P(n)$.

Even in cases where it is possible to use ordinary *PMI* in a rather natural way, it is sometimes necessary to prove the formula $P(1)$ in addition to the standard anchor step $P(0)$ because the induction step requires both cases in order to go through. Sometimes $P(1)$ follows immediately, but sometimes it may require a separate induction proof of its own. We will see cases of this when we begin to develop *Peano Arithmetic* in Section 3.3. In these sorts of proofs, two anchor steps seem to be needed; one, showing that $P(0)$ holds, to satisfy the technical requirement of *PMI*, and the other, showing $P(1)$, to help prove the induction step. This amounts to proving the case for $n = 0$ separately and then using *Mod PMI*, starting at $n = 1$.

We will illustrate modified induction in the next example. Our proof will contain a mixture of backward and forward argumentation in the induction step, something that is typical of informal mathematical arguments presented in a mathematics class or a textbook.

✠ **EXAMPLE 3.2 - 1**

Show that $n^3 < n!$ for all $n \geq 6$.

Solution

Our proof uses a modified inductive argument (*Mod PMI*). In order to establish the induction step for the original statement, it turns out to be helpful to prove another inequality first. This result forms a removable part of the overall argument, and can be taken out as a separate proposition if desired. This can likewise be proved by *Mathematical Induction* (see Exercise 4), but we will make use of some results that permit us to avoid it.

Proof:

1) *Anchor Step*

   $6^3 < 6!$; i.e., $216 < 720$.
   [Note that 6 is the best we can do for n_0: $125 > 120$.
   While the result holds for $n = 0$, it fails for $n = 1, \ldots, 5$.]

2) *Induction Step*

   Suppose that $k^3 < k!$ for any $k \geq 6$.
   We want to show that $(k+1)^3 < (k+1)!$.
   We will use a backward argument to show this; a forward argument would appear unmotivated. Since the first part of the argument is reversible, we will use *iff*.

$$\begin{array}{lll} & (k+1)^3 < (k+1)! & \text{Desired Conclusion} \\ \text{iff} & (k+1)^3 < k!\,(k+1) & \text{Factoring} \\ \text{iff} & (k+1)^2 < k! & \text{Canceling } (k \neq -1) \end{array}$$

   We know $k^3 < k!$ by our induction hypothesis. If we can also show that $(k+1)^2 < k^3$, these two inequalities can be combined to prove $(k+1)^2 < k!$, our desired inequality. Thus, we only need to show that $(k+1)^2 < k^3$ for $k \geq 6$ to conclude the proof.

   This result actually holds for $k \geq 3$, as we will prove. For some variety, we will give two proofs to illustrate different paths that could be taken.

   ***Proof* 1:**

$$\begin{array}{lrl} & k^3 > (k+1)^2 & \text{Desired Conclusion} \\ \text{iff} & k^3 - k^2 - 2k > 1 & \text{Algebra} \\ \text{iff} & k(k+1)(k-2) > 1 & \text{Factoring} \end{array}$$

   But since $k \geq 3$, each of these left-hand side factors is larger than 1, and so the product is also larger than 1 (see also Exercise 3). ■

   ***Proof* 2:**

   In this proof, we will argue the above result by first replacing one k in k^3 by the value 3, which is smaller than k, and then showing that $3k^2 > (k+1)^2$. If this holds, the original inequality will, too.

$$\begin{array}{lrl} & k^3 > (k+1)^2 & \text{Desired Conclusion} \\ \text{if} & 3k^2 > (k+1)^2 & \text{Since } k \geq 3,\ k^3 \geq 3k^2 \\ \text{iff} & 2k^2 - 2k > 1 & \text{Algebra} \\ \text{iff} & 2k(k-1) > 1 & \text{Factoring} \end{array}$$

   But for $k \geq 3$, $2k > 1$ and $k - 1 > 1$ (you can show these, too, by *PMI* if you *really* want to go overboard with mathematical induction), and so $2k(k-1) > 1$. ■

3) *Conclusion*

   By *Mod PMI*, $n^3 < n!$ for all $n \geq 6$. ■

As this example shows, if a non-trivial result that you haven't yet demonstrated is required in the middle of an induction step, you first need to prove *that* proposition. It may be possible to do this by means of a simple argument, or the proposition may itself need some form of induction argument. Whether or not a proof requires multiple inductions partly depends upon how much you already know before you start.

Mathematical Induction and the Integers

To prove a proposition $P(n)$ not merely for all integers greater than some initial integer n_0, but for all integers, positive, negative, and zero, we typically proceed as follows. We use ordinary *PMI* to prove that $P(n)$ holds for all natural numbers (or else we use *Mod PMI* to show $P(n)$ holds for all positive integers and do $P(0)$ separately), and then we use the *result* just proved (that $P(n)$ holds for $n \in \mathbb{N}$ or $n \in \mathbb{N}^+$) to show that $P(n)$ also holds for negative integers $n \in \mathbb{Z}^-$. We could develop a form of *PMI* for negative integers, but this is not normally done; the result already proved generally enables us to prove the more general result and so avoid a further induction proof.

For example, we can show that the additive law for exponents (see Example 3.1-4) holds for all integral exponents m and n. In order to do this, of course, we first need a definition for negative exponents. Here, too, induction (recursion) can be avoided by building upon the recursive definition for natural number exponents.

✠ **EXAMPLE 3.2 - 2**

Define negative exponents.

Solution

The following definition does the job.

Defn: *Let n be any positive integer and a be any non-zero real number. Then* $a^{-n} = 1/a^n$.

Since a^n is already defined for positive integers (see Example 3.1-3) and never yields 0 (since $a \neq 0$), our symbolism is well-defined.
In defining the notation a^{-n}, we are naturally free to choose any definition we wish, but in fact it has been chosen so that the various laws of exponents will continue to hold for negative exponents. Showing this in several instances will be left for the exercises (see Example 4 and Exercises 22 – 26).

In the next two examples we will first show that the definition just given extends to all integers n, and then we will get a start on demonstrating the addition law for integral exponents.

✠ **EXAMPLE 3.2 - 3**

Show that $a^{-n} = 1/a^n$ for all integers n.

Solution

Proof:

Assuming the definition just given, we will argue by cases and so avoid induction.

Case 1: $n = 0$

$a^{-0} = a^0$	Arithmetic
$= 1$	Defn of Exponents
$= 1/1$	Arithmetic
$= 1/a^0$	Defn of Exponents, Sub

Case 2: $n \in \mathbb{Z}^+$

$a^{-n} = 1/a^n$	Defn of Negative Exponents

Case 3: $n \in \mathbb{Z}^-$

Let p be the positive natural number associated with n: i.e., $p = -n$.

$a^{-n} = a^p$	Sub
$= 1/(1/a^p)$	Reciprocals, Algebra
$= 1/a^{-p}$	Defn of Negative Exponents, Sub
$= 1/a^n$	Sub

Since we have now shown the result for all possible cases, $a^{-n} = 1/a^n$ for all integers n. ■

✠ **EXAMPLE 3.2 - 4**

Prove the addition law, $a^m \cdot a^n = a^{m+n}$, for any natural number m and any integer n.

Solution

Proof:

Assuming the usual laws of exponents for pairs of natural number exponents, we will show the result by dividing it into two cases. The second case will appeal to a result in the exercises that only requires earlier results to be proved.

Case 1: When both m and n are natural numbers, we proved this in Example 3.1-4.

Case 2: Now suppose that m is a natural number and n is a negative integer; let p be the non-negative natural number associated with n: i.e., $p = -n$, $n = -p$.

$$\begin{aligned} a^m \cdot a^n &= a^m \cdot a^{-p} && \text{Sub} \\ &= a^m \cdot (1/a^p) && \text{Defn of Negative Exponents} \\ &= a^m/a^p && \text{Meaning of Division} \\ &= a^{m-p} && \text{See Exercise 25} \\ &= a^{m+-p} && \text{Meaning of Subtraction} \\ &= a^{m+n} && \text{Sub} \end{aligned}$$

Since we have shown the result for all possible cases, $a^m \cdot a^n = a^{m+n}$ for all natural numbers m and all integers n. ■

Strong Proof by Mathematical Induction

Some theorems look like they ought to yield to an attack by *PMI* or *Mod PMI*, but when this is tried, the induction step turns out to be unworkable. No matter how hard you try to prove $P(k+1)$ based upon the hypothesis $P(k)$, you find yourself unable to relate them deductively. The problem in such situations is usually that the induction hypothesis is unduly restrictive: strictly speaking, in order to show the inductive conclusion, you have only the hypothesis $P(k)$ to work with. If the two cases $P(k)$ and $P(k+1)$ aren't nicely related, the deduction may not go through. Yet $P(k+1)$ may seem to depend upon earlier cases of $P(n)$. Since these $P(n)$ can be considered already established by the time you're dealing with $P(k+1)$, you ought be able to use any one of them to help demonstrate $P(k+1)$, not just $P(k)$; i.e., you should be allowed to use $P(n)$ for *all earlier n*.

This is the intuition behind the proof schema called *Strong Proof by Mathematical Induction* (*Strong PMI*). The anchor step here is the same as that of *PMI*, but the induction step we choose is quite different. The induction argument could be formulated to suppose all $P(n)$ for $n < k+1$ in order to prove $P(k+1)$, but since this new inductive procedure does not relate a result to that for its immediate predecessor, there is no good reason for using successors $k+1$ as the focus of the induction step. We therefore formulate strong or generalized induction in terms of arbitrary numbers k instead. Schematically, we have the following:

Strong Proof by Mathematical Induction (Strong PMI)

1) *Anchor Step*
   Prove $P(0)$.
2) *Strong Induction Step*
   Assume $P(n)$ for all integers n, $0 \le n < k$;
   prove $P(k)$.
3) *Conclusion*
   Conclude $\forall n P(n)$.

This procedure can be modified in the obvious way to deal with all integers from some point n_0 on, just as ordinary induction was. We will illustrate this in the following classic example from number theory.

✠ **EXAMPLE 3.2 - 5**

Show that every natural number greater than or equal to 2 has a prime factor.

Solution

First recall that a natural number $n \geq 2$ is prime iff there is no pair of strictly smaller natural numbers a and b such that $a \cdot b = n$.

Proof:

We begin our induction at $n = 2$, using strong induction for the induction step, since the factors of a number can't be related to the number's immediate predecessor.

1) *Anchor Step*
   Certainly 2 has a prime factor, since it is already prime and a factor of itself.
2) *Induction Step*
   Suppose all numbers $n < k$ have prime factors.
   The number k is either prime or not prime (LEM); we'll consider each case in turn.
   Case 1: k is prime.
   Then k has a prime factor, namely, itself.
   Case 2: k is not prime.
   If k is not prime, then $k = a \cdot b$, for numbers a, b less than k and not equal to 1.
   The strong induction hypothesis applies to $n = a$, so a has a prime factor.
   But any factor of a is also a factor of k; so k has a prime factor as well.
   Thus in all cases, k has a prime factor.
3) *Conclusion*
   All integers greater than or equal to 2 have prime factors. ■

Modified Recursive Definitions

Associated with *Mod PMI* and *Strong PMI* are corresponding forms of *Recursive Definition*. Recursive definitions may begin with an integer other than 0, and they may define a concept for a number in terms of its meaning for one or more preceding numbers, whether or not they immediately precede the number under consideration. A good example of such a definition is the one for the *Fibonacci sequence*. Since each term of this sequence is defined in terms of the two preceding values, the initial step includes the first two values of the sequence.

✠ **EXAMPLE 3.2 - 6**

The Fibonacci sequence begins with the pair of numbers $F_1 = 1$, $F_2 = 1$, and each term F_n thereafter is generated as the sum of the two preceding ones. Give a recursive definition of this sequence.

Solution

Letting F_n stand for the n^{th} term in the Fibonacci sequence, we have the following definition:

1) $F_1 = 1, \quad F_2 = 1;$ [Alternatively: let $F_0 = 0, \quad F_1 = 1$.]
2) $F_{n+2} = F_n + F_{n+1}$.

Exploring the properties and applications of the prolific Fibonacci sequence and related sequences is a full-time enterprise; many things are known about such sequences. We will state one here and leave a number of others for the exercises (see Exercises 30 − 45).

✠ **EXAMPLE 3.2 - 7**

Show that every third Fibonacci number is even: i.e., show $F_3 \mid F_{3n}$.

Solution

Proof:

We will prove this using *Mod PMI*, starting the induction with $n = 1$.

1) *Anchor Step*
   $F_3 = 2$, which is even.
2) *Induction Step*

Suppose that F_{3k} is even.	Indn Hyp
Then $F_{3(k+1)} = F_{3k+3}$	Algebra
$= F_{3k+1} + F_{3k+2}$	Defn of Fibonacci Sequence
$= F_{3k+1} + (F_{3k} + F_{3k+1})$	Defn of Fibonacci Sequence
$= 2F_{3k+1} + F_{3k}$.	Algebra

   Thus, being the sum of two even numbers, $F_{3(k+1)}$ is even.
3) *Conclusion*
   Therefore F_{3n} is even for all positive integers. ∎

EXERCISE SET 3.2

Problems 1 - 2: Triangular Numbers

Square numbers *are familiar to everyone: they're numbers of the form* n^2*. Geometrically, these are numbers that can be represented by a square* $n \times n$ *array of dots. Other figurate numbers can be defined similarly.* ***Triangular numbers*** T_n*, for example, are the numbers* $1, 3, 6, 10, \ldots,$ *numbers that can be represented by a triangular array of dots of size* $1 + 2 + 3 + \cdots + n$*. These numbers were introduced in Example* 3.1-1*.*

*1. Prove that the sum of two successive triangular numbers, $T_{n-1} + T_n$, is a perfect square in the following two ways.
   a. First find which square T_{n-1} and T_n add up to. Then prove your equation by using algebra on the triangular number formulas resulting from Example 3.1-1.
   b. Show that $T_{n-1} + T_n$ equals the square you found in part *a* by using *Mod PMI*. This time use the relationship that captures how triangular numbers are constructed: $T_{m+1} = T_m + (m + 1)$.

2. Prove that $\displaystyle\sum_{k=1}^{n} T_k = \frac{n+2}{3} T_n$ using *Mod PMI.*

Problems 3 - 7: Inequalities and Induction

Using Mod PMI and any general results you know regarding addition, multiplication, exponentiation, factorials, or the order relations $<$ *and* $>$*, prove the following results.*

*3. $m \cdot n > 1$ for all natural numbers m and n greater than 1.

4. $n^3 > (n + 1)^2$ for all natural numbers $n \geq 3$.

*5. $2^n > n^2$ for all $n \geq 5$.

6. If $0 < a < 1$, then $a^n < 1$ for any positive integer n.

7. $n! > 2^n$ for $n \geq 4$.

Problems 8 - 10: Geometry and Induction

Prove the following geometric results using Mod PMI.

8. *Total Squares*
   How many different squares (any size) are there in a checkerboard of size 1×1? 2×2? 8×8? $n \times n$? Argue your claims; use *Mod PMI* for the general case.

9. Determine and prove a formula giving the maximum number of intersection points for a collection of two or more lines.

10. Formulate and prove a formula that gives the sum in degrees of all the interior angles of a convex (non-indented) polygon as a function of the number of sides. Does this result hold for polygons in general?

Problems 11 - 12: True or False

Are the following statements true or false? Explain your answer.

11. *Strong PMI* is used to prove a result for all the integers, not only the natural numbers.

12. *Mod PMI* differs from *PMI* in its anchor step.

Problems 13 - 14: Exploring forms of PMI

Answer the following questions about the method of Proof by Mathematical Induction.

13. Explain why *Mod PMI* and *Strong PMI* are useful for proving certain mathematical propositions.

*14. What is wrong with the following argument showing that all members of this class will receive exactly the same grade? (A's, of course — or perhaps not, if the error can't be detected! Better all work on this one together.)

Proof:

If there were only one member in the class, then obviously every member in the class would receive the same grade, so the result holds for $n = 1$.

Suppose, now, that the result holds for any class of size $n = k$. The following argument shows that it must hold for any class of size $n = k + 1$, too.

> Take a class of size $n = k + 1$ and temporarily excuse one member. Then, by the induction hypothesis, the remaining k students will all receive the same grade.
>
> Now bring that student back into the class and send one of the others out. Again, the k students that remain will all receive the same grade by the induction hypothesis.
>
> But we've already established that the student who is out will receive that grade.
>
> Thus all $k + 1$ students must receive the same grade.

Therefore, by *Mod PMI*, no matter what size the class, all students must receive the same grade. ■

Problems 15 - 18: Finite Series of Products

Prove the following, using some form of induction.

15. $\displaystyle\sum_{i=0}^{n} i(i+1) = \frac{n(n+1)(n+2)}{3}$

16. $\displaystyle\sum_{i=1}^{n} (2i-1)(2i+1) = \frac{n(4n^2+6n-1)}{3}$

17. $\displaystyle\sum_{i=1}^{n} \frac{1}{(2i-1)(2i+1)} = \frac{n}{2n+1}$

*18. Determine and prove a formula giving the total for $\displaystyle\sum_{i=1}^{n} \frac{1}{i(i+1)}$.

Hint: try $n = 1, 2, 3$ to conjecture the formula.

Problems 19 - 21: Finite Products

The finite product $a_1 \cdot a_2 \cdot (\cdots) \cdot a_n$ is denoted in compact form by $\displaystyle\prod_{i=1}^{n} a_i$.

*19. Give a recursive definition of $\displaystyle\prod_{i=1}^{n} a_i$.

*20. Using *Mod PMI*, prove that $\displaystyle\prod_{i=2}^{n}(1 - \frac{1}{i}) = \frac{1}{n}$ for all $n \geq 2$.

21. Using *Mod PMI*, prove that $\prod_{i=2}^{n}(1 - \frac{1}{i^2}) = \frac{n+1}{2n}$ for all $n \geq 2$.

Problems 22 - 26: Laws of Exponents for Integers

Prove the following results using Example 3.1 - 4*, Exercises* 32 – 34 *from Section* 3.1*, Examples* 2*,* 3*, or* 4 *above, or any basic results of arithmetic or algebra not related to exponents. You may also use any result that appears above the one you are working. Use induction where it seems appropriate.*

22. $a^m \cdot a^n = a^{m+n}$, where m and n are any integers.

23. $(a^m)^n = a^{m \cdot n}$, where m and n are any integers.

24. $(a \cdot b)^n = a^n \cdot b^n$, where n is any integer.

25. $a^n/a^m = a^{n-m}$, where m and n are any natural numbers.

26. $a^n/a^m = a^{n-m}$, where m and n are any integers.

Problems 27 - 29: Differentiation and Induction

Work the following, as instructed.

27. Use *Mathematical Induction* to prove the ordinary power rule for differentiation: $D(x^n) = nx^{n-1}$, $n \in \mathbb{N}^+$. In working your proof, you may assume the product rule for differentiation, $D(f(x) \cdot g(x)) = f'(x) \cdot g(x) + f(x) \cdot g'(x)$, and the fact that $D(x) = 1$.

28. Prove the differentiation power rule for functions raised to positive integer exponents: $D([u(x)]^n) = n[u(x)]^{n-1} \cdot u'(x)$, $n \in \mathbb{N}^+$. In working your proof, you may assume the product rule for differentiation, $D(f(x) \cdot g(x)) = f'(x) \cdot g(x) + f(x) \cdot g'(x)$, and the result of Exercise 27.

29. Prove the differentiation power rule for functions for all non-zero integer exponents n: $D([u(x)]^n) = n[u(x)]^{n-1} \cdot u'(x)$. You may use your work from Exercise 28 and the reciprocal rule for differentiating: $D(1/g(x)) = -g'(x)/[g(x)]^2$.

Problems 30 - 33: Fibonacci Sequence and Sums

Prove the following results about the Fibonacci sequence (*see Example* 6)*, using induction where needed.*

30. $\sum_{i=1}^{n} F_i = F_{n+2} - 1$

31. $\sum_{n+1}^{n+20} F_i = F_{n+22} - F_{n+2}$

32. F_{10} divides $\sum_{n+1}^{n+20} F_i$

EC 33. Every natural number can be expressed as the sum of distinct Fibonacci numbers.

Problems 34 - 41: Fibonacci Sequence and Divisibility Results

Prove the following results about the Fibonacci sequence (*see Example* 6)*, using induction where needed.*

*34. F_n and F_{n+1} are relatively prime; i.e., have no factors other than 1 in common.

35. F_{3n+1} and F_{3n+2} are both odd numbers.

*36. F_{4n} is divisible by 3.

37. F_{5n} is divisible by 5.

38. F_{6n} is divisible by 8.

EC 39. $F_{m+n} = F_{n-1} \cdot F_m + F_n \cdot F_{m+1}$ for $n \geq 2$, $m \in \mathbb{N}$.

EC 40. Note the results of Example 7 and Exercises 36 - 38. On the basis of the pattern being developed, what would you conjecture about $F_{m \cdot n}$? Test your conjecture on two more cases; if it is correct, prove your conjecture. You may find Exercise 39 helpful.

41. Which Fibonacci terms can be prime numbers/are Fibonacci primes? What subscripts must the Fibonacci primes have? Is the converse of your conclusion also true? Why or why not? (Note: it is not known whether there are infinitely many Fibonacci primes.)

Problems 42 - 45: Fibonacci Sequence, Squares, and Products

Prove (and find, where indicated) the following formulas for the Fibonacci sequence (see Example 6). Not all will need mathematical induction.

42. $1^2 + 1^2 = 2$, $1^2 + 2^2 = 5$, ... ; $F_n^2 + F_{n+1}^2 =$?? .

43. $1^2 + 1^2 = 2$, $1^2 + 1^2 + 2^2 = 6$, $1^2 + 1^2 + 2^2 + 3^2 = 15$, ... ; $\sum_{i=1}^{n} F_i^2 =$?? .

44. $F_{n+1}^2 = F_n \cdot F_{n+2} + (-1)^n$.

45. $F_n \cdot F_{n+3} = F_{n+2}^2 - F_{n+1}^2$.

*46. *Binary Representation of Natural Numbers*

*a. Prove by means of an induction argument that every positive integer m can be uniquely expressed as the sum of distinct binary powers (powers in the form 2^m).

b. Explain why all numbers m satisfying $0 \leq m < 2^n$ can be uniquely represented in base two notation by an n-place binary digit (bit) numeral $b_{n-1}b_{n-2}\cdots b_1 b_0$, where each b_i is either 0 or 1 and $m = b_{n-1} \cdot 2^{n-1} + b_{n-2} \cdot 2^{n-2} + \cdots + b_1 \cdot 2^1 + b_0 \cdot 2^0$.

c. Can the result in parts a and b be generalized to other bases? How?

47. An action $*$ on the set of rational numbers is defined recursively for all rational numbers a and all natural number operators n by the two equations

$0 * a = a$, and
$(k+1) * a = (k * a)/2$.

a. Prove that $n * a = a/2^n$ for all n. You may use the definition just given and any results you think you need from ordinary arithmetic.

b. Prove that $(m * a) \cdot (n * b) = (m + n) * (a \cdot b)$. You may use the definition given, the result of part a, and any results from ordinary arithmetic.

48. Show the following results concerning $\sqrt[n]{n!}$ for all positive integers n:

a. $\sqrt[n]{n!} > n/3$

b. $\sqrt[n]{n!} > n/e$

c. Can a better approximation n/c be found for $\sqrt[n]{n!}$? Why or why not?

HINTS TO STARRED EXERCISES 3.2

1. To find the formula, look at some examples with $n = 2, 3, 4$ and then generalize.

   a. Use the formulas for T_{n-1} and T_n that result from Example 3.1-1 and do the algebra.

   b. The induction step needs to relate $(T_k + T_{k+1})$ to $(T_{k-1} + T_k)$, using the relation $T_{m+1} = T_m + (m+1)$ for the appropriate m.

3. Use any m and do induction on n.

5. Proceed somewhat similarly to Example 1.

14. [No hint.]

18. See the hint given. This one is similar to Example 3.1-1.

19. Define $\prod_{i=1}^{n+1} a_i$ in terms of $\prod_{i=1}^{n} a_i$.

20. This uses (at least implicitly) the recursive definition you developed in Exercise 19 in the induction step.

34. For the induction step, use the fact that if d is a divisor of two numbers, it also divides their difference.

36. To make the induction step work, rewrite $F_{4(k+1)}$ as a sum of earlier terms via the Fibonacci sequence definition.

46. a. Use strong induction here, taking two cases: n is an exact multiple 2^m, or n is not.

3.3 Peano Postulates and Peano Arithmetic

Mathematical Induction is a proof technique used to prove universal statements about natural numbers. As such, its native home is the arithmetic of the natural numbers. It has applications to many other areas of mathematics, since these also use natural numbers, but it is first of all a method of proof associated with arithmetic. In this section we will explore the place and role of induction in the development of axiomatic arithmetic, and we will see more precisely how and why *PMI* is a valid method of argumentation.

Axiomatic arithmetic may sound like an oxymoron. Perhaps you're thinking, "Isn't arithmetic concerned with calculations? Doesn't it just deal with how to apply certain computational algorithms, like long division, to numbers expressed in our base-ten place-value system? How can this be part of an deductive axiomatic theory? We never saw any proofs in arithmetic; only in more advanced fields of mathematics like geometry and trigonometry."

If this is what you're thinking, you're in good company. Arithmetic is certainly taught in elementary school without any concern for proof. Children aren't able (and shouldn't be expected) to follow deductive arguments when they first learn the techniques of calculation. Moreover, most civilizations have treated arithmetic as little more than a collection of specialized techniques for computation. In fact, the general algebraic structure of arithmetic remained submerged beneath the rules of calculation for a long time. Algorithmic mathematics wasn't really considered a part of deductive mathematics until about one hundred fifty years ago. Then mathematicians began investigating the nature of different number systems in more depth, finally organizing them deductively. We'll say a few more words about this before getting into the technical details of axiomatic arithmetic.

Brief Historical Context

In the nineteenth century, for a variety of technical and educational reasons, mathematicians became more concerned with the axiomatic basis and deductive structure of their discipline. In the process of attempting to provide a rigorous foundation for calculus, they were led to reconsider the foundations of algebra and ordinary arithmetic as well. A program of *arithmetization* was mounted in the nineteenth century that in the end attempted to define real numbers in terms of set theoretical notions and rational numbers, rational numbers in terms of set theory and integers, and integers in terms of set theory and natural numbers. Some mathematicians went further and subjected natural numbers to a treatment involving nothing but set theory. Others, however, accepted the natural numbers as an appropriate starting point and axiomatized them instead.

Two mathematicians who analyzed the natural number system in order to give a deductive basis for arithmetic were Richard Dedekind (1888), who used notions from set theory to provide a foundation for the natural numbers, and, independently, Giuseppe Peano (1889), who took the natural numbers as primitive and gave a list of axioms for them. These axioms are now known as the *Peano Postulates*, though they might better be called the *Dedekind-Peano Postulates*, since Dedekind was first to isolate the key properties of the natural numbers. Peano went on to develop arithmetic deductively from his system of axioms, something Dedekind did not do, so the arithmetic of the natural numbers is (rightly) called *Peano Arithmetic*.

The Peano Postulates for the Natural Numbers

Your introduction to arithmetic as a very young child was undoubtedly learning to recite the list of counting numbers in their proper order, perhaps while touching various objects in front of you. You didn't know at first exactly how the numbers were related to one another or just how they referred to the collection of objects you were counting, but it was impressed upon you that you had to start with the first number and then continue in a definite succession.

In time you also learned that the sequence of counting numbers never stopped, but that if you went on counting long enough and were helped with some new unit names like 'thousand', you could get to any one of them. You also learned how to use counting (perhaps on your fingers) to do simple arithmetic: adding is done by counting forward, and subtracting by counting backwards. Thus, counting formed the basis for your entire knowledge of arithmetic. You also learned other things about addition and subtraction, multiplication and division, but these built upon what you already knew from counting.

Peano's approach to arithmetic closely parallels this way of learning about numbers and computation. He takes the notion of the natural numbers occurring in ordered succession as the basis for developing all of arithmetic into a deductive theory. Surprisingly, he found that four simple postulates, stating some obvious properties of the sequence of natural numbers, together with a fifth more complex closure postulate formed a sufficient axiomatic foundation for arithmetic. We will first state these postulates informally in ordinary mathematical English, and then we will write them formally using the language of PL. When we formalize the *Peano Postulates* as axioms of *Peano Arithmetic*, our list of postulates shrinks down to just three axioms, for two of them are covered by the way PL expresses sentences.* We will treat the first four postulates here; the fifth postulate will be formulated and analyzed in the next sub-section.

Peano Postulates

1) 0 is a natural number.
2) Every natural number has a unique successor.
3) 0 is not the successor of any natural number.
4) Distinct natural numbers have distinct successors.
5) *Axiom of Mathematical Induction*

We can sum these axioms up by saying that the natural numbers are precisely all those numbers gotten by starting with 0 and proceeding forward through all its successors, each number after 0 having both a unique successor and a unique predecessor.

Now, order to design a PL language to formulate the axioms (and theory) of arithmetic, we only need two symbols in addition to the usual logical symbols. We'll take 0 as a constant symbol (intended to represent the smallest or first** element of $\mathbb{N}$) and $\mathcal{S}$ as a function symbol (intended to represent the successor function: $\mathcal{S}(x)$ denotes the successor of x, the next number after x, in the usual ordering of $\mathbb{N}$).† No other symbols need to be taken as primitive; we can introduce them when wanted via definitions.

Using such a PL language, we will now see how to formalize the first four *Peano Postulates*. The first postulate, which claims that 0 is a natural number, gets omitted in a formal treatment, because it is already presupposed by our conventions regarding PL notation. If 0 is a constant symbol, then it must necessarily stand for some distinguished member of the universe of discourse, the set of natural numbers.

The second postulate, that successors of numbers are unique, suffers the same fate as the first. If $\mathcal{S}$ stands for the successor function, then $\mathcal{S}(x)$ must be defined for all x and this output has to be unique: that's what it means for $\mathcal{S}$ to be a function symbol. Thus this postulate is also omitted in a formal listing of the *Peano Postulates*.

* However, when arithmetic is developed as a sub-theory of set theory, all five of these postulates will play a genuine role.

** There is no complete unanimity among mathematicians about whether $\mathbb{N}$ should include 0 or begin with 1. Even Peano waffled on this. We are including 0 since it, like all the other counting numbers, can be thought of as the numerosity of the empty set $\emptyset$. Besides, we can use the symbol $\mathbb{N}^+$ to represent the positive natural numbers.

† We're avoiding the notation $x + 1$ here for the successor of x since we have yet to define addition, which will be done in terms of the successor function. An alternative notation might be x^+, but we don't want to use $+$ in two different senses or give the appearance that addition is being used in a circular way prior to its formal definition.

The third postulate, that 0 is not the successor of any natural number, does need to be expressly postulated. It can be formulated by either of the following two logical equivalents:

$$\neg\exists x(\mathcal{S}(x) = 0) \qquad \text{or} \qquad \forall x(\mathcal{S}(x) \neq 0)\,.$$

We will choose the latter formulation because it is a universal sentence, but the former immediately follows from it by *EN*. This gives us our first axiom for *Peano Arithmetic*. We will formulate it (and later propositions in *Peano Arithmetic*) by using variables from the middle of the alphabet to stand for natural numbers. Note that quantifiers here are assumed to range over natural numbers; $\mathbb{N}$ is our intended universe of discourse, so we do not say that the variables represent natural numbers within the sentences themselves.

AXIOM* 3.3 - 1: *Successors Are Non-Zero
$\forall n(\mathcal{S}(n) \neq 0)$

The fourth postulate, which says that distinct numbers have distinct successors, can be formulated by either of the following two equivalents:

$$\forall x\forall y(x \neq y \to \mathcal{S}(x) \neq \mathcal{S}(y)) \qquad \text{or} \qquad \forall x\forall y(\mathcal{S}(x) = \mathcal{S}(y) \to x = y)\,.$$

Here we will also choose the second formulation, which can be thought of as saying that predecessors of successors are unique. The first more negative formulation follows from this proposition via *Conpsn* when needed.

AXIOM* 3.3 - 2: *Predecessors of Successors Are Unique
$\forall n\forall m(\mathcal{S}(n) = \mathcal{S}(m) \to n = m)$

The Axiom of Mathematical Induction

The fifth Peano Postulate, which captures the essence of *Mathematical Induction*, is the most important one of the whole group. We will also state this postulate both in informal and formal versions. We will then show how it underlies *Proof by Mathematical Induction*.

Intuitively, the *Axiom of Mathematical Induction* says that the set of natural numbers $\mathbb{N}$ can be generated by starting with 0 and repeatedly applying the successor function to its previous output: all natural numbers are gotten by counting on from 0.

We can put this more precisely using set terminology. If a set of natural numbers contains 0 and also contains the successor of every number it contains, then it is the entire set of natural numbers. Put more symbolically, if P is a subset of $\mathbb{N}$ such that P contains the number 0 and P contains the successor $\mathcal{S}(k)$ of a number whenever it contains the number k, then $\mathsf{P} = \mathbb{N}$.

An alternative way to express the *Axiom of Mathematical Induction* that doesn't presuppose an underlying set theory is gotten by substituting a property P for the set P: let $P(n)$ stand for the property of n belonging to P. Our principle can thus be formulated by:

> *If $P(0)$ is the case, and if $P(\mathcal{S}(k))$ is the case whenever $P(k)$ is the case, then $P(n)$ is the case for all natural numbers n.*

Assuming $\mathbb{N}$ as the intended universe of discourse so the quantifier "for all" automatically means "for all natural numbers," and dropping out the semantic references about properties "being the case," we obtain the following formal statement of the *Induction Axiom*.

AXIOM* 3.3 - 3: *Axiom of Mathematical Induction
$P(0) \wedge \forall k(P(k) \to P(\mathcal{S}(k))) \to \forall n P(n)$

This is our official version of the *Induction Axiom*, but we will append a few qualifying remarks. Rather than thinking of $P(n)$ as standing for the sentence "n has property P," $P(n)$ can be taken (as we did in PL) to represent any *statement* of *Peano Arithmetic* containing n as a free variable. And $P(0)$ is actually $P(0|n)$, the statement gotten by uniformly substituting 0 for n in $P(n)$. Moreover, since the axiom is intended to hold for any such formula P whatsoever, there is an implicit typed quantifier "for all formulas P" heading up the *Axiom of Induction* (or, we can assume one axiom for each formula P, giving us a host of axioms, called an *axiom schema*, instead of a single axiom). Finally, since the successor of a number k is $k+1$ (as it will be officially, once we define addition), we will eventually be able to replace $\mathcal{S}(k)$ by $k+1$ in our formulation, yielding the following, easier to understand version of the axiom:

Induction Axiom, Additive Form: $P(0) \wedge \forall k(P(k) \to P(k+1)) \to \forall n P(n)$.

We will use this form of the axiom in the next section to demonstrate its relation to *PMI*; but when we begin our development of *Peano Arithmetic* proper, we will revert to using the basic form involving the successor function until after we have defined addition and 1 and have actually proved that $\mathcal{S}(k) = k+1$.

The truth of the *Axiom of Induction* should be fairly obvious to anyone who understands what it says and is familiar with the natural numbers. For consider this axiom in its set theoretical formulation. Let P be a set that contains 0 and is *closed* under the successor function. Then since P contains 0, it also contains $1 = \mathcal{S}(0)$ (because P contains $\mathcal{S}(k)$ whenever it contains k); and now since it contains 1, it must also contain $2 = \mathcal{S}(1)$ (same reasoning); and so on. P must therefore contain all the natural numbers.

While no one would argue with the truth of *Axiom* 3, one might challenge taking it as *axiomatic* instead of proving it. After all, doesn't the reasoning just outlined show that any natural number n is a member of P?

But this line of reasoning is faulty and may indicate a misunderstanding of the character of the formal deductive enterprise we are now engaged in. For, in axiomatizing *Peano Arithmetic*, we are in a real sense placing limits upon the nature of its models. Prior to *Axiom* 3, we have only established that a model $\mathbb{N}$ for *Peano Arithmetic* must contain a non-successor element 0 and that predecessors of successors must be unique. We still don't know, for example, whether all non-zero numbers are successors, nor, even if they are, whether they can be obtained as the eventual successors of 0. And, as a matter of fact, these results *don't follow* from the other two axioms. It is relatively easy to concoct interpretations in which *Axiom* 1 and *Axiom* 2 are true but these properties fail, and so *Axiom* 3 is false of these models (see Exercises 31 – 36). Thus, while we can show that any number of successors of 0 are in P, we are not in a position to claim that $\mathsf{P} = \mathbb{N}$, that all natural numbers lie in P.

In order to draw the conclusion that all natural numbers belong to P, we would have to use something like *Proof by Mathematical Induction*. But we have to be extra careful here. Keep in mind that we're developing *Peano Arithmetic* deductively from an axiomatic basis, so all we have available to use at this point are the rules of inference from PL and the axioms we're adopting for *PA*. As we noted in Section 3.1, *PMI* is not a rule of inference from logic. It needs justification itself and will shortly be legitimized by appealing to the *Axiom of Mathematical Induction*; it would be circular to use it here, then, to prove the axiom that supports it. Since *Axiom* 3 is nevertheless true of the natural numbers, we are forced to adopt it as an axiom, as an unproved truth about the natural numbers.

Proof by Mathematical Induction

In order to understand the connection between *Proof by Mathematical Induction* and the *Axiom of Mathematical Induction*, we will take a second look at how *PMI* proceeds. We begin with an anchor step, proving $P(0)$. The induction step of *PMI* is actually a subproof: we suppose $P(k)$ for an arbitrary natural number k, and we then deduce $P(k+1)$. We would now like to conclude $\forall n P(n)$ via *PMI*. However, this conclusion does not follow from the rules of inference for PL. Based upon the suppositional argument we have, we can only conclude the conditional $P(k) \to P(k+1)$ in the main part of our proof via *CP*. Since k was an arbitrary natural number (a generic representative), however, we may continue by concluding the universal conditional $\forall k(P(k) \to P(k+1))$.

At this point our proof options branch. We'll look at two possible ways we might proceed toward our goal.

In the first way, we can next instantiate our universal sentence to obtain $P(0) \to P(0+1)$. We can then combine this step with the anchor step $P(0)$ via *MP* to conclude $P(1)$, since $0+1=1$. Next, we can instantiate to obtain $P(1) \to P(1+1)$. Combining this with $P(1)$, we can conclude $P(2)$, again using *MP*. Repeating this process any finite number of times, we can show $P(k_0)$ for any definite natural number k_0. However, we will never be able to prove $P(n)$ for every natural number n in this way; it would take an infinitely long proof, which would never come to an end. Nor will we be able to generalize via *UG* to get $\forall n P(n)$, since all our unconditional sentences $P(k_0)$ are particular ones, and we can't generalize from specific examples. We are thus at an impasse as far as proving the universal unconditional statement we want, even though we can prove that any particular natural number k_0 satisfies $P(n)$.

The second way we might continue our proof from the universal conditional (see step n_5 in the proof diagram below) is the following. We can use *Conj* to combine our anchor step $P(0)$ with $\forall k(P(k) \to P(k+1))$ to get $P(0) \wedge \forall k(P(k) \to P(k+1))$ (step n_6). How does this help? Well, it still won't help to get $\forall n P(n)$ unless we have some way to combine this sentence with another one that will then yield the desired universal conclusion. But this is precisely what the *Axiom of Mathematical Induction* gives us: $[P(0) \wedge \forall k(P(k) \to P(k+1))] \to \forall n P(n)$. Asserting this axiom ($n_7$) and applying *MP* ($n_8$), we can conclude what's wanted.

n_1	$P(0)$	$\cdots$
n_2	$\quad P(k)$	Spsn for CP
	$\quad\quad .$	
	$\quad\quad .$	
	$\quad\quad .$	
n_3	$\quad P(k+1)$	$\cdots$
n_4	$P(k) \to P(k+1)$	CP n_2-n_3
n_5	$\forall k(P(k) \to P(k+1))$	UG n_4
n_6	$P(0) \wedge \forall k(P(k) \to P(k+1))$	Conj n_1, n_5
n_7	$[P(0) \wedge \forall k(P(k) \to P(k+1))] \to \forall n P(n)$	Ax Math Indn
n_8	$\forall n P(n)$	MP n_7, n_6

The three-step proof technique of *PMI* that we studied in Section 3.1 thus finds its justification in PL's ordinary *Inference Rules* and in the *Axiom of Mathematical Induction*. To reiterate what we said earlier, *PMI* is not a general rule of logical inference, but a specialized proof technique of arithmetic. In using induction to prove a mathematical statement, however, even for developing *Peano Arithmetic*, we do not have to restrict ourselves to using only PL's rules of inference and the *Peano Postulates*. Having shown in the above proof diagram that *PMI* proofs can be made completely rigorous, you may continue to use the less formal three-step proof technique. *PMI* is the proof-theoretic counterpart of the *Axiom of Induction* and is usually applied in place of the axiom itself. This approach keeps induction proofs more manageable than if *Axiom* 3 is used directly as we've just done.

The variations on *Mathematical Induction* that we considered in Section 3.2, *Mod PMI* and *Strong PMI*, can be justified by means of associated induction propositions, which can in turn be proved by the *Axiom of Mathematical Induction*, though it requires a bit of work. We will assume the validity of these results and leave a demonstration of it as an exercise (see Exercises 39 − 40). This being the case, you may use any form of *Proof by Mathematical Induction* as you prove propositions in *Peano Arithmetic*.

Peano Arithmetic: Addition

We will now begin a more systematic treatment of *Peano Arithmetic*. We will look closely at how the process of axiomatizing arithmetic proceeds, but not with the intent of developing all of *Peano Arithmetic* in a strict, deductive fashion. Our purpose here and in the later theories that we develop axiomatically is only to present samples of how mathematical theories can in principle be developed in scrupulously logical fashion from rigorous foundations. You will probably find proceeding this way to be both frustrating and exhilarating: you have very little to work with at the outset (only the *Peano Postulates* and *Predicate Logic*), and you will have to check continually that what you are using in your proofs is justified by what you've already proved (rather than by what you already know from earlier courses), but accomplishing each new task can give a real sense of deductive accomplishment. You'll be building a mammoth skyscraper using only bricks and mortar. Or, to use a computer science analogy, you'll be implementing highly complicated computations by doing simple manipulations of sequences of 0s and 1s on the machine level.

We will start out by once more listing the three *Peano Postulates* that form the deductive basis of our theory. We will also state a successor version of the proof strategy *PMI*, though we will not have much occasion to use it here in this primitive form (cf. Exercises 3 – 6).

THE PEANO POSTULATES

AXIOM* 3.3 - 1: *Zero is not a Successor

$\forall n(\mathcal{S}(n) \neq 0)$

AXIOM* 3.3 - 2: *Predecessors of Successors Are Unique

$\forall n \forall m(\mathcal{S}(n) = \mathcal{S}(m) \rightarrow n = m)$

AXIOM* 3.3 - 3: *Axiom of Mathematical Induction

$P(0) \wedge \forall k(P(k) \rightarrow P(\mathcal{S}(k)) \rightarrow \forall n P(n)$

PROOF TECHNIQUE: Proof by Mathematical Induction (Successor Version)

Given $P(0)$ and a deduction of $P(\mathcal{S}(k))$ from $P(k)$ for an arbitrary natural number k, conclude $\forall n P(n)$.

Amazingly enough, with just these three *Peano Postulates*, it is possible to *prove all the laws* that underlie the computational algorithms of ordinary arithmetic: the commutative laws, the associative laws, the distributive laws, the cancellation laws, and so on. These laws govern the binary operations of addition and multiplication, which we will define recursively in terms of the successor function. Other operations and relations of ordinary arithmetic, such as exponentiation, limited or partial subtraction and division, the order relation of less-than, and the relation of divisibility, can likewise be treated by appropriate definitions and proofs, based in the final analysis upon the *Peano Postulates*. Once an operation or relation is defined, it may of course be used to define other ones. The successor function will be the ultimate basis of everything we do, but not everything needs to be defined in terms of the successor function. For example, once addition is defined, we will be able to use it to define multiplication, and then multiplication can be used to define exponentiation (see Section 3.1).

A few things can be proved about simple successors (see Exercises 3 and 5), but before we get to anything very interesting we need to define the other familiar operations. Just using counting gets rather monotonous and complicated.

We will begin with a recursive definition for addition. Note here that induction is used on the second number n; m is taken to be any natural number.

DEFINITION* 3.3 - 1: *Addition of Natural Numbers (Successor Version)

Let m be an arbitrary natural number. Then $m + n$ is defined recursively by the following:

a) $m + 0 = m$

b) $m + \mathcal{S}(k) = \mathcal{S}(m + k)$ *for any natural number k*

In this definition, equation a defines adding 0 to a number, while equation b tells how to add the successor of a number on the basis of knowing how to add the preceding number. Since m was arbitrarily chosen at the outset, we have uniquely defined the binary operation of addition for any two natural numbers m and n. This fact is a result of the theorem cited in Section 3.1 regarding recursive definitions. That result continues to hold in *Peano Arithmetic*; it is proved using the *Axiom of Mathematical Induction*.

These two equations make up the official definition of addition. To put this second equation in a more recognizable form, though, we will first define the number 1 and prove an elementary proposition that does not require *PMI*.

DEFINITION* 3.3 - 2: *Definition of 1

$1 = \mathcal{S}(0)$

Using the definition of 1 along with the definition of addition, we can prove the following proposition, which allows us to revert to our familiar notation for the successor of a number.

PROPOSITION* 3.3 - 1: *Successors and Adding 1

$\forall m(m + 1 = \mathcal{S}(m))$

Proof:

$m + 1 = m + \mathcal{S}(0)$	Defn of 1; Sub
$= \mathcal{S}(m + 0)$	Defn of Addn, Eqn b
$= \mathcal{S}(m)$	Defn of Addn, Eqn a; Sub ■

Hardly a deep result, but worth noting nevertheless. Using this result and substitution, the recursive definition for addition can be given the following, more standard formulation, which we will label a definition, though it is really a proposition following from the last proposition and the definition of addition.

DEFINITION* 3.3 - 3: *Addition of Natural Numbers (Standard Version)

Let m be an arbitrary natural number. Then $m + n$ is recursively defined by

a) $m + 0 = m$
b) $m + (k + 1) = (m + k) + 1$

Note that in the second equation of this definition we do *not* write $m + k + 1$ without using parentheses. The operation of addition is a *binary operation*, so only two numbers can be combined at a time. Only after a sum is obtained, indicated by grouping it inside parentheses, can it be used as part of another addition result. As we go on to develop our results in *Peano Arithmetic*, we must continue to be *absolutely picky about the use of parentheses*, so that we do not tacitly assume a result that hasn't yet been proved. The only results we may use are those that have been proved, no matter how elementary they may seem. That's the way things need to be done when you're proceeding axiomatically: you must constantly be on your guard against circular reasoning and smuggling results into your arguments that are not warranted by the premises. This is what makes the deductive development of arithmetic difficult for college mathematics students: they know far too much!

Once we have the result of *Proposition* 1, the *Axiom of Induction* and its counterpart *PMI* can be reformulated in the familiar terms of adding 1 to a number instead of taking its successor (see above). *This is the form we will be using, therefore, from this point on.*

Taking the recursive definition of addition, the definition of 1, and the above proposition identifying successors with one-more-thans, we can begin to prove some more complex results about addition. We will give a couple of propositions here and leave others to be done in the exercises (see Exercises 11-12).

PROPOSITION* 3.3 - 2: *0 is an Additive Identity

$\forall m(m + 0 = m = 0 + m)$

***Proof*:**

We already know from the definition of addition, Equation 1a, that $m + 0 = m$ for all natural numbers m, so all that remains to be proved is that $0 + m = m$. This will be proved by induction on m.

1) *Anchor step*

$0 + 0 = 0$	Defn of Addn, Eqn a

2) *Induction step*

Suppose that $0 + k = k$.	Indn Hyp
Then $\quad 0 + (k + 1) = (0 + k) + 1$	Defn of Addn, Eqn b
$\qquad\qquad\qquad\quad = k + 1$	Sub

3) *Conclusion*

Thus, $\quad \forall m(0 + m = m)$.	PMI ■

We actually know more than that 0 is *an* identity for addition of natural numbers. In Example 2.4 - 10 we showed that there was *at most one* additive identity for ordinary arithmetic, using an argument that required nothing more than the rules for identity. Our argument here proves that there is *at least one* additive identity. Together they provide a rigorous demonstration that 0 is the unique additive identity for *Peano Arithmetic*, something we concluded already in Example 2.4 - 10 by assuming the result we have just proved.

Looking at the result of the last proposition in a slightly different light, we can say that 0 *commutes* with all natural numbers. Showing that any two natural numbers commute will be left as an exercise (see Exercise 11). As a second step on the road toward getting that result, though, we will show that 1 also commutes with everything. This result turns out to be needed to prove the general case.

PROPOSITION* 3.3 - 3: *Commutativity of 1

$\forall m(1 + m = m + 1)$

***Proof*:**

We will again argue by mathematical induction, making use of the proposition just proved.

1) *Anchor step*

$1 + 0 = 1 = 0 + 1$	Propn 2, UI ($m = 1$)

2) *Induction step*

Suppose that $1 + k = k + 1$.	Indn Hyp
Then $\quad 1 + (k + 1) = (1 + k) + 1$	Defn of Addn, Eqn b
$\qquad\qquad\qquad\quad = (k + 1) + 1$	Sub

3) *Conclusion*

Thus, $\quad \forall m(1 + m = m + 1)$.	PMI ■

These last two propositions begin to show how recursive definitions are used in conjunction with *PMI* to prove the fundamental computational laws of arithmetic. In the way we have presented them, they look rather trivial. However, in developing an axiomatic theory from scratch, the subject matter doesn't tell you *when* you have to prove *what*. It may well be that in trying to prove a certain result, you run stuck and so decide it would be better to prove another result first so you can use that one in your proof. This is what would have happened if we had tried to deduce *Proposition* 3 before *Proposition* 2. This sort of confusion occurs on a grander scale when you know quite a few true results in a given theory and you want to organize them deductively into a series of propositions. For instance, if you were now to try to prove the commutative law, having already done two special cases in the above propositions, you would discover that your proof could make good use of still other results that haven't been proved (see Exercise 11b). Constructing proofs completely on your own, you would quickly sense that the various computational laws of arithmetic are logically intertwined and that the order in which you try to prove them will probably make some difference. Once the order of the results is determined by someone who has figured out a way to proceed through the results, the proofs become more straightforward. Whenever this turns out to be the case, though, you should suspect that a good deal of work went on behind the scene to arrange the results so that they could be readily demonstrated one after the other.

We will finish exploring addition by proving the associative law (which, as our proof makes clear, could have been done before *Proposition* 2); equation b in the recursive definition of addition is a special instance of this law. Other results on addition are in the Exercise Set.

PROPOSITION* 3.3 - 4: *Associative Law for Addition
$\forall l \forall m \forall n((l+m)+n = l+(m+n))$

***Proof*:**
We will use *Mathematical Induction* on n and *UG* on the first two variables.

1) *Anchor step*

$$\begin{aligned} (l+m)+0 &= l+m && \text{Defn of Addn, Eqn } a \\ &= l+(m+0) && \text{Defn of Addn, Eqn } a \end{aligned}$$

2) *Induction step*

Suppose that $(l+m)+k = l+(m+k)$. — Indn Hyp

$$\begin{aligned} \text{Then} \quad (l+m)+(k+1) &= ((l+m)+k)+1 && \text{Defn of Addn, Eqn } b \\ &= (l+(m+k))+1 && \text{Sub} \\ &= l+((m+k)+1) && \text{Defn of Addn, Eqn } b \\ &= l+(m+(k+1)) && \text{Defn of Addn, Eqn } b \end{aligned}$$

3) *Conclusion*

Hence, $\forall n((l+m)+n = l+(m+n))$. — PMI

And so by *UG*, we may conclude $\forall l \forall m \forall n((l+m)+n = l+(m+n))$. ■

Peano Arithmetic: Multiplication

Having shown how to proceed with addition, we will now briefly introduce multiplication. As with addition, multiplication is defined recursively. We will define it in terms of addition.

DEFINITION* 3.3 - 4: *Multiplication of Natural Numbers (Standard Version)
Let m be an arbitrary natural number. Then

a) $m \cdot 0 = 0$
b) $m \cdot (k+1) = m \cdot k + m$

This defines $m \cdot n$ for any two natural numbers m and n. It stipulates that all multiples of 0 are 0, and it defines the multiple of any successor to be the sum of the same multiple of the predecessor with m itself.

Based on this definition, the recursive definition of addition, the definition of 1, and the above propositions for addition, results analogous to the ones we just argued for addition can be proved for multiplication:

$$\forall m(m \cdot 0 = 0 = 0 \cdot m)$$
$$\forall m(m \cdot 1 = m = 1 \cdot m)$$

Having just given detailed proofs of propositions similar to these, the proofs for these and other results involving multiplication will be left for your enjoyment (see Exercises 13 – 18).

EXERCISE SET 3.3

***NOTE*:** In proving propositions of *Peano Arithmetic* below, be sure *not* to use any result you know to be true, no matter how elementary you think it is, *unless* it is one of the *Peano Postulates*, part of a definition, or has already been proved. Put your proof into a two-column format as was done for the propositions in the text; that will help keep you honest. Also, be careful to group binary operation results by means of parentheses; any regrouping must be justified by some result gotten earlier.

Problems 1 - 2: Baby-Steps Arithmetic

Prove the following basic arithmetic results.

*1. Using the definitions $2 = \mathcal{S}(\mathcal{S}(0))$ and $4 = \mathcal{S}(\mathcal{S}(\mathcal{S}(\mathcal{S}(0))))$ along with the recursive definition for addition, show that $2 + 2 = 4$.

*2. Using the definitions and result of Exercise 1 along with properties for addition and the recursive definition for multiplication, show that $2 \cdot 2 = 4$.

Problems 3 - 6: Natural Numbers, Successors, and Sums

*Use the **successor version of PMI** along with the Peano Postulates to prove the following results.*

*3. No natural number is its own successor: $\forall n(\mathcal{S}(n) \neq n)$.

*4. No natural number is the sum of a non-zero natural number with itself: $\neg\exists m\exists n(m + n = n \ \wedge \ m \neq 0)$. *Hint*: using what you know about negating quantified sentences, put the result in its best equivalent form, and then use induction on n to prove that result.

EC 5. All non-zero natural numbers are successors of unique natural numbers: $\forall n(n \neq 0 \rightarrow \exists! m(n = \mathcal{S}(m)))$.

6. A sum is zero only if both addends are zero: $\forall m\forall n(m + n = 0 \rightarrow m = 0 \wedge n = 0)$. *Hint*: use induction on n, remembering when conditional sentences are true.

Problems 7 - 10: True or False

Are the following statements true or false? Explain your answer.

7. Arithmetic was axiomatized already in ancient times by the Greeks.

*8. The *Axiom of Induction* is needed in order to justify *Proof by Mathematical Induction.*

9. The *Peano Postulates* were demonstrated by Dedekind before Peano formulated them as postulates for arithmetic.

*10. Calculus is easy; it's elementary arithmetic that's hard!

Problems 11 - 12: Properties of Addition

Prove the following laws holding for addition.

*11. *Commutative Law for Addition*

*a. Using any definitions and propositions from the lesson, prove that addition is commutative: $\forall m\forall n(m + n = n + m)$. *Hint*: use induction on n and *UG* on m.

b. Examine your proof that addition is commutative in part *a*. Did you use the associative law (*Proposition* 4) in your proof? Can the commutative law be proved without making use of the full associative law? Why or why not? Be careful: a certain degree of associativity is already guaranteed by the recursive definition of addition, equation *b*.

12. *Cancellation Laws for Addition*

Prove that both cancellation laws hold for addition, using any results mentioned up to this point, but without using subtraction of equals (since subtraction has not been defined and this result has not been proved). Which, if any, of these two laws can be proved without assuming commutativity of addition?

a. $\forall l\forall m\forall n(l + n = m + n \rightarrow l = m)$

b. $\forall l\forall m\forall n(l + m = l + n \rightarrow m = n)$

Problems 13 - 18: Properties of Multiplication

Prove the following laws holding for multiplication.

*13. *Multiplicative Properties of* 0

*a. Prove that 0 annihilates all natural numbers under multiplication: $\forall m(m \cdot 0 = 0 = 0 \cdot m)$.

b. Prove that 0 is a factor of any 0 product: $\forall m \forall n(m \cdot n = 0 \rightarrow m = 0 \ \vee \ n = 0)$.

14. Prove that 1 is an identity for multiplication: $\forall m(1 \cdot m = m = m \cdot 1)$. Is 1 the unique multiplicative identity? Why?

*15. *Distributive Laws*

Prove that multiplication distributes over addition from both sides.

a. $\forall l \forall m \forall n(l \cdot (m + n) = l \cdot m + l \cdot n)$

*b. $\forall l \forall m \forall n((l + m) \cdot n = l \cdot n + m \cdot n)$

16. *Associative Law for Multiplication*

Prove that multiplication is associative: $\forall l \forall m \forall n((l \cdot m) \cdot n = l \cdot (m \cdot n))$.

17. *Commutative Law for Multiplication*

Prove that multiplication is commutative: $\forall m \forall n(m \cdot n = n \cdot m)$.

18. *Cancellation Laws for Multiplication*

Prove, if possible, that both cancellation laws hold for multiplication of non-zero natural numbers.

a. $\forall l \forall m \forall n(l \neq 0 \wedge l \cdot m = l \cdot n \rightarrow m = n)$

b. $\forall l \forall m \forall n(l \neq 0 \wedge m \cdot l = n \cdot l \rightarrow m = n)$

Problems 19 - 30: Ordering Properties of the Natural Numbers

The order relation $\leq$ is defined for the natural numbers as follows: $\forall m \forall n(m \leq n \leftrightarrow \exists d(m + d = n))$. Prove the following results for $\leq$. Some of them, but not all, require inductive proofs. Do not use any result you are familiar with unless it is justified by the definition or a previously proved proposition.

19. $\forall m(m \leq m)$

20. $\forall l \forall m \forall n(l \leq m \wedge m \leq n \rightarrow l \leq n)$

21. $\forall m(m \leq m + 1)$

22. $\forall n(0 \leq n)$

23. $\forall n(n \leq 0 \rightarrow n = 0)$

24. $\forall l \forall m \forall n(l \leq m \wedge m \leq n \rightarrow l \leq n)$

25. $\forall m \forall n(m \leq n \wedge n \leq m \rightarrow m = n)$

EC 26. $\forall m \forall n(m \leq n \vee n \leq m)$ *Hint*: Take cases in your induction step and use Exercise 5.

EC 27. $\forall n(n \leq 1 \rightarrow n = 0 \vee n = 1)$ *Hint*: use Exercise 6.

EC 28. $\forall m \forall n(m \leq n \ \wedge \ n \leq m + 1 \rightarrow n = m \ \vee \ n = m + 1)$

29. $\forall l \forall m \forall n(l \leq m \rightarrow l + n \leq m + n)$

30. $\forall l \forall m \forall n(l \leq m \rightarrow l \cdot n \leq m \cdot n)$

Problems 31 - 36: Metalogical Exporation of the Peano Postulates

Work the following problems related to models of the Peano Postulates. Recall that a model needs to identify a universe of discourse and interpret the constant and function symbols involved in the axioms.

EC 31. Locate a model of the first two axioms of *Peano Arithmetic* in which there are numbers besides 0 that are not successors of another number.

EC 32. Locate a model of the first two axioms of *Peano Arithmetic* in which all numbers except 0 are successors of some number but in which not every number can be gotten as the eventual successor of 0.

EC 33. Locate a model N of the first two axioms of *Peano Arithmetic* that has a subset P containing 0 as well as the successor of every element it contains, yet which is not N. What does this say about the truth of the *Axiom of Induction* for N? What does it say about the relation of Axiom 3 to Axioms 1 and 2?

34. Using the method of models/interpretations, show that Axiom 1 is not logically implied by Axioms 2 and 3.

35. Using the method of models/interpretations, show that Axiom 2 is not logically implied by Axioms 1 and 3.

36. Can a finite set be a model of the first two axioms of *Peano Arithmetic*? Why or why not?

Problems 37 - 38: Mathematical Induction and Well-Ordering

Prove the following equivalences.

EC 37. Symbolically formulate the *Well-Ordering Principle* for the natural numbers: every non-empty subset S of the natural numbers $\mathbb{N}$ has a least element. Then prove it using some form of *Mathematical Induction*.

38. Assuming the *Well-Ordering Principle* (see part a), prove the *Axiom of Mathematical Induction* (without using *Proof by Mathematical Induction*, of course).

Problems 39 - 40: The Axiom of Induction and Variants of Mathematical Induction

Prove the following results about variants of PMI.

39. Formulate and prove a *Modified Axiom of Induction*, using the *Axiom of Induction*.

40. Formulate and prove a *Strong Axiom of Induction*, using the *Axiom of Induction*.

HINTS TO STARRED EXERCISES 3.3

1. Proving this simple equation involves patient substitution of equals, using the definitions of 2 and 4 along with the recursive definition of addition (successor version), mostly the second part.

2. This is similar to Problem 1, only this time using the recursive definition of multiplication. You can also use the result of Problem 1.

3. Use the *successor version* of *PMI* here. Axiom 2 also plays a role.

4. Use the *successor version* of *PMI* here, too. Also, see the hint given in the book. For the induction step, use an *EO* strategy to prove the "or" statement you get when you move the negation past the quantifiers.

8. [No hint.]

10. Go with your gut reaction here. (Thanks to T Vis for this comment.)

11. a. This is a fairly straight-forward application of *PMI* in the form you learned in Section 3.1 (***read the bottom of page 7***), but you'll need to use Propositions 2, 3, and 4 for different parts of the proof.

13. a. One half of this double equation is easy; the other half is a fairly straight-forward induction argument, using *PMI* in its standard form.

15. b. Do induction on n. You may use anything proved up to this point, including both propositions and problems.