∀ Proof Writing ∃ This Reference Book

A Student's Guide to Intermediate Mathematical Proofs

Kiddo Kidolezi

David Molk

Maurice Opara

Dan Shea

Winter Term 2002

Introduction

Maurice C. Opara

Mathematics, as we know it today, is not about scribbling numbers and sketching geometric shapes. Much of the beauty of a mathematical argument or proof lies in the manner in which it is presented. Besides, an argument would not be convincing if it were not presentable. A proof is basically a series of logical steps, used to verify a theorem or an argument. Usually, mathematics students encounter the bulk of proof reading and writing in the intermediate and higher-level portions of their college career. However, some of these students go into these classes without prior knowledge of the techniques of proper proof writing, and as such, they may find it difficult to express mathematical arguments as logically and concisely as is required of them. Other students might have some background in proof reading and writing, but need some brushing up. To save professors from digressing for too long from the main subject of the course in order to explain proof reading and writing techniques to their students, it is necessary for students to have a reference on mathematical proofs which is accessible to them and easy to understand.

This handbook focuses on writing mathematical proofs, and offers help with reading proofs as well. It starts off with an introduction to logic and how to understand logical statements, and continues with a series of examples of proofs. Examples are drawn from a range of topics including Basic Number Theory and Linear Algebra. Generally, it is geared towards a student just coming from a linear algebra class, although anyone who is sufficiently conversant with concepts in mathematics could also find this handbook useful. It is the hope of the authors of this handbook that it may prove helpful, not only as a reference, but also as a short text that can be read on its own.

Some Mathematical Symbols

We present here some notations we've seen in our mathematics courses. You will find a few of them in the later parts of this handbook.

$\in$	is an element of
$\notin$	is not an element of
$\Rightarrow$	implies
$\Leftrightarrow$	if and only if
iff	if and only if
$\therefore$	therefore
϶	such that
$\cap$	intersect
$\cup$	union
$\subset$	is a subset of; is contained in (but not equal to)
$\subseteq$	is a subset of (and possibly equal to)
$\exists$	there exists
$\forall$	for all
$\neg$	not
$\Rightarrow\Leftarrow$	contradiction
$\sum_{k=1}^{n} f(k)$	the sum f(1) + f(2) + …+ f(n)
$\prod_{k=1}^{n} g(k)$	the product g(1) · g(2) · … · g(n)
$\{x : P(x)\}$	the set of all values of x such that the statement P(x) is true
$\{(x,y) : P(x,y)\}$	the set of all ordered pairs (x,y) such that P(x,y) is true
R	the set of all real numbers
Z	the set of all integers
Q	the set of all rational numbers; i.e., $\left\{\frac{a}{b} : a,b \in Z; b \neq 0\right\}$.
C	the set of all complex numbers; i.e., $\{a + bi : a,b \in R\}$. (Here $i^2 = -1$.)

An Introduction to Logic

Maurice Opara

Consider the statement,

"John ate a banana for breakfast."

At a glance, the above statement makes sense and is understandable even as it stands on its own. However, in theoretical and practical English language, a lot of information that is necessary to truly understand the statement is not included. For instance, who is John? Did he eat the banana whole or did he cut it up? Did John eat it for breakfast yesterday, or the day before yesterday, or 10 years ago? And so forth. However, including all this extra information would stretch a point that can be expressed in just one line into a long essay, and may prove difficult to understand.

In a precision-dependent subject such as Mathematics, there is no room for ambiguity. In addition, excess detail does not allow for neatness and precision, which are desired qualities in mathematical presentations. Thus, it is necessary to develop a language that would express a mathematical argument accurately and concisely. In Logic, formal laws of reasoning are explored and used, together with special abbreviations and symbols, to properly present arguments and ideas.

In 1854, George Boole (1815-1864)[*] came up with [Boolean] Propositional Logic, which is a branch of First-Order Logic. The following are general explanations of some concepts used in Propositional Logic, which may be important for understanding the rest of this handbook.

The Conditional Statement

"If I am hungry, then I will eat my popcorn."

We can split this sentence into two propositions:

If **I am hungry** then **I will eat my popcorn**

[*] More information on George Boole can be found at:
http://homepages.enterprise.net/rogerp/george/boole.html

In the case where I am not hungry, it follows that I will not eat my popcorn. Nevertheless, the fact that I pop a few into my mouth every now and then does not necessarily mean that I am always hungry. As such, the sentence is still true when I'm not hungry and eating my popcorn. One the other hand, it would not be true if I am hungry and I'm not eating my popcorn, because then I would be starving myself and there is no indication in the original sentence that I intend to do so.

Let P signify "I am hungry," and Q signify "I will eat my popcorn." "If P then Q" in the notation of propositional logic would be written as:

$$P \Rightarrow Q$$

This is an example of a conditional statement or implication. It is read as "P implies Q," or "if P then Q," and the arrow $\Rightarrow$ is the implication operator. The proposition P is called the hypothesis, while Q is called the conclusion. As pointed out in the above example, conditional statements are only false when the conclusion is false AND the hypothesis is true.

When dealing with conditional statements, one may come across the following:

- The converse of the statement $P \Rightarrow Q$, written as $Q \Rightarrow P$.
- The contrapositive of the statement $P \Rightarrow Q$, written as not $Q \Rightarrow$ not P. The contrapositive may also be written as $\neg Q \Rightarrow \neg P$ or $\sim Q \Rightarrow \sim P$.

The Biconditional Statement.

"I will go to the dinner meeting if and only if Nancy will come with me."

Let us split the above statement into two sub-statements, or propositions:

I will go to the dinner meeting if and only if Nancy will come with me.

Notice that the above sentence will not be valid if I go to the dinner meeting without Nancy, or if Nancy agrees to come with me and I still do not go to the dinner meeting. However, the statement is not violated if I do not go to the dinner meeting, and Nancy will not come with me. In other words, the whole statement is only true when both propositions constituting the statement are true, or both false.

If we let P represent the proposition "I will go to the dinner meeting," and Q represent the proposition "Nancy will come with me," we can re-write

the statement " P if and only if Q" in Propositional Logic notation. It will look like this:

$$P \Leftrightarrow Q$$

This is an example of a biconditional statement. The arrow $\Leftrightarrow$ is used to represent the biconditional property of the statement. As stated earlier, $P \Leftrightarrow Q$ is true when both P and Q are either true or false.

In the case where $P \Leftrightarrow Q$ is always true, we say that P and Q are logically equivalent. For example, the propositions "I will go to the dinner meeting" and "Nancy will come with me" are logically equivalent if I go to the dinner meeting AND Nancy comes with me, or if I do not go to the dinner meeting AND Nancy does not come with me.

It is a proven fact that a conditional statement and its contrapositive are logically equivalent. Look again at the statement, "If I am hungry, then I will eat my popcorn." The reader can verify that its contrapositive, "If I do not eat my popcorn, then I am not hungry," is true if and only if the conditional statement itself is true. The reader should verify the case for other forms of the statement, including its false form (recall that a conditional statement is false when its hypothesis is true AND its conclusion is false).

However, note that a conditional statement and its converse are not always logically equivalent. Consider, for instance, the statement: "If a pig gets hit by a train, then it will die." It is very obvious that its converse, "If a pig dies, then it will get hit by a train," is false when the conditional statement itself is true.

Universal and Existential Quantifiers

Predicate Logic, the second branch of first-order logic, extends propositional logic with the treatment of "quantifiers," all (universal) and some (existential). Before defining these terms, here is a brief definition of the concept of a universe.

A Universe is basically "a set that contains all elements relevant to a particular discussion or problem."[1] Examples of universes include a collection of one-penny coins, and the set of positive integers.

1. The Universal Quantifier ($\forall$) is used in propositional logic when a statement is being made concerning all the objects in a particular universe. For instance, if we are dealing with the universe of all blue marbles, and we let x represent a marble in this universe, we could write: $\forall$ x (x is blue). In other words, "For all marbles x, x is blue."

2. The Existential Quantifier ($\exists$) is used in propositional logic when a statement is being made concerning some particular object in the universe. Going back to our universe of blue marbles, if there happens to be a red marble y among the blue marbles, we can write: $\exists$ y (y is red). In other words, "There exists some marble y such that y is red."

It is also important to know the definition of the symbol $\in$. This means "is an element of" or "belongs to". For example, if M represent the set of all integers divisible by 2, and x = 16, the statement $x \in M$ means "x is an element of M" or "x belongs to M". The symbol for the opposite, i.e. "is not an element of", is $\notin$.

Writing proofs in mathematics, first of all, entails understanding the statement that is being proved. A statement could be in the form of biconditional or conditional statement; it may be the converse or the contrapositive of a conditional statement. Furthermore, it may refer to the set of all real numbers, or restricted to a particular real number/numbers with a particular property. Knowledge of these concepts in logic gives one an edge in understanding mathematical statements and their proofs.

[1] Merriam-Webster Online Collegiate Dictionary

Proofs of Basic Integer Properties

Kiddo Kidolezi

The following problems deal with methods of proving some characteristics of integers and a few arithmetic operations. Most of these properties seem to be obvious and straightforward but they require the reader's familiarity with the definitions of the various integer properties. As in any other mathematical proofs, it is necessary to have in mind what the final answer at the end of the proof is supposed to look like.

Example I: Let x and y be integers. Prove that

(a) ***if x and y are even, then x + y is even.***

PROOF:

Assume that x and y are even. Then x = 2m and y = 2n for some integers m and n.

Adding $x + y = 2m + 2n$

$= 2(m + n)$.

Since the sum of two integers (in this case m + n) is also an integer, then x + y is even. //

(b) ***if x and y are even, then xy is divisible by 4.***

(An integer n is divisible by 4 if there exist an integer q such that $n = 4q$.)

PROOF:

Suppose x and y are even. As in question (a),

Multiplying $xy = (2m)(2n)$

$= 4mn$.

Since the product of integers is also an integer, xy is divisible by 4. //

(c) *if x is even and y is odd, then x + y is odd.*

PROOF:

Assume y is odd; then y = 2t + 1 where t is an integer. We can use x as in the previous question.

Adding x + y = 2m + (2t +1)

= 2(m + t) + 1

Since the sum of integers is also an integers, x + y is odd. //

(d) ***if x is even and y is odd, then xy is even.***

PROOF:

Let $x = 2m$ and $y = 2n + 1$

Then xy = (2m)(2n + 1)

= 4mn + 2

= 2(2*mn* + 1)

But $2mn + 1$ is an integer because the product and sum of integers is also an integer. Therefore *xy* is even. //

Example II: Suppose a, b and c are positive integers. Prove that

(a) if a divides b and b divides c, then a divides c.

PROOF:

Suppose a divides b; then ap = b and bq = c for some integers p and q.

Substituting b = ap into bq = c gives (ap)q = c

⇒ a(pq) = c.

Since the product of integers is also an integer, a divides c. //

(b) if a divides b and b divides a, then a = b.

PROOF:

By definition, a divides b if ar = b and b divides a if bs = a for some integers r and s.

Substituting b = ar into bs = a gives ars = a , so

$$rs = 1 \text{ (since } a \neq 0).$$

So r = s = 1 or r = s = -1. But a > 0 and b > 0

$$\Rightarrow \quad r = s = 1.$$

Hence b = a (1) = a and a = b (1) = b. //

(c) if ac divides bc, then a divides b.

PROOF:

Suppose ac divides bc; then acq = bc for some integer q.

In dividing on both sides of acq = bc by c (c > 0), we get

$$aq = b$$

Since q is an integer, a divides b. //

One Theorem, Many Proofs

Dan Shea

Don't let the variety of techniques for writing mathematical proofs we have described lead you to think that for each theorem, there is one and only one method of proving. This is not at all true: certain kinds of proofs work best with certain theorems, but in general, there is no one way to prove a theorem. Some of the proving techniques we have encountered in this primer include the direct proof, the proof by contradiction, and the proof by contraposition.

We shall demonstrate that more than one of these methods can be used to prove the

Theorem: If A and B are nonsingular matrices, then the matrix AB is also nonsingular.

Notes: (In order to give sufficient background; these notes will be used in the proof)

- The n x n matrix C is invertible if and only if the determinant of C (written $|C|$) does not equal zero. (This is a truth that can be proved using the definition of invertibility.)
- The determinant of the n x n matrix CD, where D is some n x n matrix multiplied to the right-hand side of C, is equal to the determinant of C times the determinant of D. (That is, $|CD| = |C||D|$.)

i. **Proof** (We will first prove this theorem by Direct Proof):
Assume the n x n matrices A and B are nonsingular; then their determinants must be nonzero, i.e., $|A| \neq 0$ and $|B| \neq 0$. Multiplying B to the right-hand side of A to make AB, we see its determinant is $|AB| = |A||B|$. Since $|A| \neq 0$ and $|B| \neq 0$, then $|AB| \neq 0$. By definition, AB is nonsingular; i.e., AB is invertible. //.

Explanation: This proof relied heavily on two simple truths: the definition of invertible matrices being one, and the other, a property of determinants. The first step, always an important one to take when writing a proof, was to

become aware of a definition – in this case, we are trying to prove the invertibility of a matrix, so we look to the definition of invertibility. Having found a useful mathematical fact as a direct consequence of this definition, we applied the "fact" to both parts of the conditional statement: to the "if" part, which dealt with A and B separately (and here we saw that both would have nonzero determinants), then to the "then" part (and here we know that the determinant must be nonzero). Knowing this last bit – that the determinant of AB must be nonzero – it is easy to see which property of determinants will help us finish the proof.

ii. **Proof** by contradiction:
Suppose the matrix AB, where A and B are n x n matrices, is singular. Then the determinant of AB = |AB| = 0. Now, we know that |AB| = |A||B|. Since A and B are invertible n x n matrices, |A| and |B| must be nonzero integers. Therefore, |A||B| is not equal to zero, and, since AB has a nonzero determinant, it cannot be singular. No such AB, then, as initially surmised, exists. //.

Explanation: We used the same "notes," the same ingredients to prove our theorem by contradiction as we did to prove it directly. The same thought process is utilized for each type of proof, essentially, although the direct proof clearly suits this particular theorem better. The proof by contradiction is done by supposing the opposite of what is said in the theorem (in a conditional statement, it is the "then" part). By reducing this supposition to an absurdity, the theorem can be proved.

iii. **Proof** by contraposition: (Revised theorem: If both A and B are not both invertible, then AB is not invertible):
If one (or both) of the n x n matrices A and B is not invertible, then either |A| or |B| equals zero. Therefore, when we multiply B to the right-hand side of A, we get a determinant, |AB|, which will equal zero. Since (NOT) A and B are invertible implies AB is (NOT) invertible, we have shown that when A and B are invertible n x n matrices, AB will be an invertible

n x n matrix. //.

Explanation: The proof by contraposition uses that bit of logic which holds that in a conditional statement, when If NOT S, then NOT R can be shown, the original statement -- If R, then S – is also true. We saw earlier that a conditional statement is always logically equivalent to its contrapositive. Because we have proved in the foregoing proof that the contrapositive statement is true, we know that the original statement is correct. Again, we have used the same "notes" that we have relied upon all along, and we see that the direct proof is still the best, easiest proof for this theorem, but that any of three methods can be used.

Finally, we will show that the converse of this statement, as converses sometimes are, is also true:

Theorem: If the *n x n* matrix AB is invertible, then the *n x n* matrices A and B are also invertible.

Proof: Assume the n x n matrix AB is invertible, where AB is the product of the n x n matrices A and B. Then the determinant of AB will, by definition, be nonzero: $|AB \neq 0$. Because we can rewrite $|AB|$ as $|A||B|$, we see that neither A nor B can have a determinant equal to zero. Therefore, both A and B are invertible. //.

Explanation: Once again, the same few notes get us through the proof. This shows importance of finding a workable definition for the condition that is to be proved, applying it to the theorem, and then using any helpful properties to complete the proof. Here, the converse of the proof is true, but the reader must be warned: this is by no means the case universally.

Mathematical Pig and Train

David Molk

One interesting aspect of the nature of proofs is that the validity of the statement "if P, then Q" does not necessitate the truth of the converse, "if Q, then P." Let's examine such an example.

Statement: If the n by n matrix A is similar to B, then A and B have the same characteristic polynomial.

Opening notes: Well, if one matrix is similar to another, then by definition $A=P^{-1}BP$ for some invertible matrix P. The characteristic matrix is the determinant of the matrix $A-\lambda I$. The matrix has both a variable lambda (λ) and numbers, so the computed determinant will contain powers of λ in addition to numbers. Let's proceed.

Proof: We are given that $A=PBP^{-1}$ for some invertible matrix P.
Then $\det(A-\lambda I)=\det(PBP^{-1}-\lambda I)=\det(PBP^{-1}-\lambda PIP^{-1})=\det(PBP^{-1}-P\lambda IP^{-1})$.
We then obtain $\det(P(B-\lambda I)P^{-1})=\det(P)\det(B-\lambda I)\det(IP^{-1})$.
Then we get $\det(A-\lambda I)=\det(B-\lambda I)$.

QED

Concluding notes: I chose a direct approach to this proof because we had a simple "if P, then Q" statement. I began with the definition of similar matrices and started manipulating it because I knew that I eventually wanted to end up with
$\det(A-\lambda I)=\det(B-\lambda I)$. A simple substitution for matrix A in the expression of its characteristic polynomial that related A to B and a few manipulations of P and its inverse led to the answer. In this proof, I found it helpful to write down what I knew and then what I was trying to show on my scrap paper, then work to equate the two.

Now let's examine the converse of our first proof and see that the converse is false, even though we showed the original statement to be true.

<u>Statement:</u> If the n by n matrices A and B have the same characteristic polynomial, then they are similar.

<u>Opening notes</u>: We will most likely be using the same information that we used from the original proof. Since we know that "if P, then Q" does not imply the validity of "if Q, then P," we should continue with caution and do a few examples before deciding how to start the proof. A little investigation yields the result that the converse is false. With that in mind, we are now trying to show that the statement to be proven is false. The most effective way to accomplish this end is to provide a counterexample where the statement breaks down; this method will work because our "if Q, then P" statement is a blanketing statement. It implies that all matrices have this property. Let us then find two matrices that do not have the property of the statement and our work will be done. Recall that we cannot prove by example. One may only disprove through example.

<u>Proof that the statement is false:</u> Let us consider for example the matrix $A=\begin{bmatrix}2 & 0\\ 3 & 2\end{bmatrix}$ and the matrix $B=\begin{bmatrix}2 & 0\\ 0 & 2\end{bmatrix}$. Matrix A has a characteristic polynomial of

$\det(A-\lambda I)=\begin{vmatrix}2-\lambda & 0\\ 3 & 2-\lambda\end{vmatrix}=(2-\lambda)^2$ and B has a characteristic polynomial of

$\det(B-\lambda I)=\begin{vmatrix}2-\lambda & 0\\ 0 & 2-\lambda\end{vmatrix}=(2-\lambda)^2$.

Now suppose, for contradiction, that there exists an invertible matrix P with $A=P^{-1}BP$.

Then $PA=BP$, so $\begin{bmatrix}p_{11} & p_{12}\\ p_{21} & p_{22}\end{bmatrix}\begin{bmatrix}2 & 0\\ 3 & 2\end{bmatrix}=\begin{bmatrix}2 & 0\\ 0 & 2\end{bmatrix}\begin{bmatrix}p_{11} & p_{12}\\ p_{21} & p_{22}\end{bmatrix}$.

Now $\begin{bmatrix}2p_{11}+3p_{12} & 2p_{12}\\ 2p_{21}+3p_{22} & 2p_{22}\end{bmatrix}=\begin{bmatrix}2p_{11} & 2p_{12}\\ 2p_{21} & 2p_{22}\end{bmatrix}\Rightarrow p_{12}=p_{22}=0.$

This statement implies that P is not invertible $\Rightarrow\Leftarrow$.

QED

Concluding notes: A little scratch work allowed us to find two matrices that will serve as a counterexample. I started the proof by defining my matrices and writing the resulting characteristic polynomials, showing that the two matrices had the same polynomial. Since I was trying to show that the statement was false, I decided to do a proof by contradiction at that point and assume the statement to be true. This method was effective because we were again dealing with a yes-or-no possibility; if the invertible matrix P could not exist, which we intended to show, then the statement would crumble accordingly. As a result, we assumed the opposite of what we wanted to show and showed that such an assumption leads irreversibly to a contradiction. In this case, we showed that the condition PA=BP leads to the statement $p_{12} = p_{22} = 0$. This means that the determinant of P must be zero, but invertible matrices have nonzero determinants. This contradiction means that matrix P cannot exist, which in turn leads to the breakdown of the statement. Thus the statement is false. Consequently, the truth of a statement neither implies nor insures the validity of its converse.

Introduction to Induction

David Molk

The next few proofs that we will introduce all require the use of a proving method called "proof by induction." Mathematicians commonly define two principles of induction. The first method involves the so-called forward domino effect. In short, we first show that a statement applies to the initial case. We then show that whenever it's true for the n^{th} case, it must be true for the next case. The validity of each case, or "domino," knocks the next domino over (shows the next case to be true), which continues down the chain of cases in a cascade of mathematical truth.

First Principle of Mathematical Induction: Let S be a set of integers containing some element a. Suppose S has the property that, whenever some integer n ≥ a belongs to S, then n+1 also belongs to S. Then S contains every integer greater than or equal to a.

Example

Kiddo Kidolezi

Task: Prove that, for any integer *n≥1*,

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

(It may be useful to first analyze this task in words. By definition of the summation sign Σ,

the problem asks for a proof that the sum of consecutive positive integers up to n is given by $\frac{n(n+1)}{2}$, where n is any positive intege.r)

Proof by Induction on n:

Step I: This statement is true for the lowest value of n; that is, when n = 1:

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

Step II: Let's assume that the statement is true for n = t, where t is a positive integer.

Then we would have $\sum_{k=1}^{t} k = \frac{t(t+1)}{2} = 1 + 2 + 3 + \ldots + (t-1) + t.$

Now we want to show that the statement would be true for a positive integer t + 1.

Starting with $\sum_{k=1}^{t+1} k = 1 + 2 + 3 + \ldots\ldots\ldots\ldots + (t-1) + t + (t+1)$

$$= \frac{t(t+1)}{2} + (t + 1)$$

$$= \frac{t(t+1) + 2(t+1)}{2}$$

$$= \frac{(t+1)(t+2)}{2}$$

$$= \frac{(t+1)([t+1]+1)}{2}.$$

Therefore $\sum_{k=1}^{t+1} k = \frac{(t+1)([t+1]+1)}{2}.$ //

Example

David Molk

Statement: Prove that, for every integer $n \geq 5$, $2^n > n^2$.

Opening notes: We will use the method of proof by induction to tackle this problem. The statement "for every integer" tips us off as to which proving method should be used. Recall that such blanketing statements usually signify a good opportunity to try to prove the statement using induction. Remember that we start a proof by induction by showing that the statement applies to the base case, or first case. Next, we assume that the statement holds for the nth case and then show that it follows that it holds for the n+1 case.

Proof: For the base case, n=5, we get $2^5=32$ and $5^2=25$. Clearly the statement holds for the base case. Now we assume that the statement holds true for the n=j case, let's show that it holds true for j+1.
We know $2^j>j^2$ so $2*2^j>2*j^2$, or $2^{j+1}>j^2+j^2$. Note that $j^2>2j+1$ for all $j\geq5$.
Then $2^{j+1}> j^2+2j+1$ so $2^{j+1}>(j+1)^2$.

Concluding notes: We switched variables from n to j in the interest of clarity. Some proofs involving summations get tricky when considering the summation from, say, 1 to n of some function of variable n. We wanted to show that when we manipulated the left side to an expression of order j+1 instead of j that we get the proper expression on the right side of the inequality. That is, we want to manipulate one side to an expression for j+1 and have the other side show the corresponding change, in this case from n^2 to $(n+1)^2$. The statement "Note that $j^2>2j+1$ for all $j\geq5$" can be verified through the use of the quadratic formula on the equation $j^2 -2j -1 = 0$, which gives roots of $1+2^{1/2}$ and $1-2^{1/2}$, both of which are less than 5.

The Second Principle of Mathematical Induction

Dan Shea

We have shown the way in which we prove by the first principle of mathematical induction. There is, however, another principle. This one differs slightly from the first, and it is also used to prove the truth of a theorem. The second principle is stated as follows:

Second Principle of Mathematical Induction: Let S be a set of integers containing a. Suppose S has the property that n belongs to S whenever every integer less than n and greater than or equal to a belongs to S. Then S contains every integer greater than or equal to n.

Example: Theorem: Every integer $n \geq 2$ has a prime factor.

Notes: - If an integer p is divisible by an integer q, then there exists an integer k such that qk = p. (We call q and k factors of p.)

- A prime number is an integer that is divisible only by itself and one.

Proof by induction:

(i) Base Case: Since 2 is a prime number, the theorem is true for n = 2.

(ii) Suppose that every integer that is greater than or equal to 2, and less than n, has a prime factor. If n is prime, then we have proved the theorem. If n is not prime, then n is certainly the product of lesser integers. Thus, n = pq, where $p,q < n$. Therefore, for some prime integers a and b, aj = p and bi = q, where j and i are integers not necessarily prime. Then n = (aj)(bi) = a(jbi). Therefore, n also has a prime factor, and by the second principle of induction, every integer $n \geq 2$ has a prime factor. //.

Explanation: The second principle of mathematical induction is a somewhat strangely-worded statement. However, it provides a more than sufficient framework for proving a theorem: the second principle draws lines very clearly that determine the course of the proof, and the mathematician need

only follow them. So, in the above proof, all we had to do was to show that n is the product of two factors – either of only itself and one, or of other numbers, too. Yet, we know that any integers less than n are either prime, or have some prime factors. The tricky part of this proof (for me) was to separate n and 2: the second principle requires two numbers, n and a. However, in this theorem, we are given an n that is greater than or equal to 2. Although the proof sets up this relation, we must take n and 2 as separate from each other, as n and a. Once this was done, the path was clear.

References

Anton, Howard Elementary Linear Algebra. New York: John Wiley & sons, 1994.

Arnold, Jimmy T., Johnson, Lee W., Riess, R. Dean Introduction to Linear Algebra. Reading, Massachussetts: Addison-Wesley Co., 1993.

Edwards, Bruce H., Larson, Roland E. Elementary Linear Algebra. Lexington, Massachusetts: D.C. Heath and Co., 1991.

Factasia – Logic http://www.rbjones.com/rbjpub/logic/index.htm [20 Jan. 2002]

Harrison, Eileen. George Boole – the Lincoln Genius http://homepages.enterprise.net/rogerp/george/boole.html. [31 Jan. 2002]

Merriam-Webster Online www.m-w.com [20 Jan. 2002]

Rosen, Kenneth. Discrete Mathematics and its Applications (Fourth Edition) McGraw-Hill 1999.