

HOW TO READ AND DO PROOFS (some notes)

Proofs are the heart of mathematics. If you are a math major, then you must come to terms with proofs--you must be able to read, understand and write them. What is the secret? What magic do you need to know? The short answer is: there is no secret, no mystery, no magic. All that is needed is some common sense and a basic understanding of a few trusted and easy to understand techniques.

The Structure of a Proof

The basic structure of a proof is easy: it is just a series of statements, each one being either (A) an assumption or (B) a conclusion, clearly following from an assumption or previously proved result.

And that is all. Occasionally there will be the clarifying remark, but this is just for the reader and has no logical bearing on the structure of the proof.

A well written proof will flow. That is, the reader should feel as though they are being taken on a ride that takes them directly and inevitably to the desired conclusion without any distractions about irrelevant details. Each step should be clear or at least clearly justified. A good proof is easy to follow.

When you are finished with a proof, apply the above simple test to every sentence: is it clearly (a) an assumption or (b) a justified conclusion? If the sentence fails the test, maybe it doesn't belong in the proof.

An Example: The Irrationality of the Square Root of 2

In order to write proofs, you must be able to read proofs. See if you can follow the proof below. Don't worry about how you would have (or would not have) come up with the idea for the proof. Read the proof with an eye towards the criteria listed above. Is each sentence clearly an assumption or a conclusion? Does the proof flow? Was the theorem in fact proved?

Before we begin the proof, let's recall a few definitions. A real number is called **rational** if it can be expressed as the ratio of two integers: p/q . The ancient Greeks thought that all numbers were rational. A number that is not rational would be called **irrational**. You probably believe that π is irrational. (It might surprise you that this is not easy to prove.) When the Greeks proved that the square root of 2 is not a rational number, the very foundations of arithmetic were called into question. This is one of the reasons that Greek geometry subsequently flourished--all numbers could be treated geometrically without reference to rationality.

Another fact that we will need is the **Fundamental Theorem of Arithmetic**. This exciting sounding theorem is nothing more than the fact that every positive integer has a

unique representation as a product of prime numbers. The technique of proof we will use is proof by **contradiction**. You do not need any specialized knowledge to understand what this means. It is very simple. We will assume that the square root of 2 is a rational number and then arrive at a contradiction. Make sure you understand every line of the proof.

Theorem. The square root of 2 is an irrational number.

Proof. Let's represent the square root of 2 by s . Then, by definition, s satisfies the equation

$$s^2 = 2.$$

If s were a rational number, then we could write

$$s = p/q$$

where p and q are a pair of integers. In fact, by dividing out the common multiple if necessary, we may even assume p and q have no common multiple (other than 1). If we now substitute this into the first equation we obtain, after a little algebra, the equation

$$p^2 = 2 q^2 .$$

But now, by the Fundamental Theorem of Arithmetic, 2 must appear in the prime factorization of the number p^2 (since it appears in the same number $2 q^2$). Since 2 itself is a prime number, 2 must then appear in the prime factorization of the number p . But then, 2^2 would appear in the prime factorization of p^2 , and hence in $2 q^2$. By dividing out a 2, it then appears that 2 is in the prime factorization of q^2 . Like before (with p^2) we can now conclude 2 is a prime factor of q . But now we have p and q sharing a prime factor, namely 2. This violates our assumption above (see if you can find it) that p and q have no common multiple other than 1.

Example: Divisibility is Transitive

If a and b are two natural numbers, we say that **a divides b** if there is another natural number k such that $b = a k$. For example, 2917 divides 522143 because there is a natural number k (namely $k = 179$) such that $522143 = 2917 k$.

Theorem. If a divides b and b divides c then a divides c .

Proof. By our assumptions, and the definition of divisibility, there are natural numbers k_1 and k_2 such that

$$b = a k_1 \text{ and } c = b k_2.$$

Consequently,

$$c = b k_2 = a k_1 k_2.$$

Let $k = k_1 k_2$. Now k is a natural number and $c = a k$, so by the definition of divisibility, a divides c .

q

If P, Then Q

Most theorems (homework or test problems) that you want to prove are either explicitly or implicitly in the form "If P, Then Q". In the previous example, "P" was "If a divides b and b divides c " and "Q" was " a divides c ". This is the standard form of a theorem (though it can be disguised). A direct proof should be thought of as a flow of implications beginning with "P" and ending with "Q".

$$P \rightarrow \dots \rightarrow Q$$

Most proofs are (and should be) direct proofs. Always try direct proof first, unless you have a good reason not to.

It Seems Too Easy

If you find a simple proof, and you are convinced of its correctness, then don't be shy about. Many times proofs are simple and short.

In the theorem below, a **perfect square** is meant to be an integer in the form a^2 where a itself is an integer and an **odd integer** is any integer in the form $2a+1$ where a is an integer.

Theorem. Every odd integer is the difference of two perfect squares.

Proof. Suppose $2a+1$ is an odd integer, then

$$2a+1 = (a+1)^2 - a^2.$$

q

Where's the proof? It's there. It's just very short.

Another Simple Example

Recall that a natural number is called **composite** if it is the product of other natural numbers all greater than 1. For example, the number 39481461 is composite since it is the product of 15489 and 2549.

Theorem. The number $100\dots01$ (with $3n-1$ zeros where n is an integer larger than 0) is composite.

Proof. We can rewrite our number as $100\dots01 = 10^{3n} + 1$ where n is an integer larger than 0. Now use the identity $a^3 + b^3 = (a+b)(a^2 - ab + b^2)$ with $a = 10^n$ and $b = 1$, to get

$$(10^n)^3 + 1 = (10^n + 1)(10^{2n} - 10^n + 1).$$

We will be done once we have shown that both factors $(10^n + 1)$ and $(10^{2n} - 10^n + 1)$ are greater than 1. In the first case, this is clear since $10^n > 0$ when $n > 0$. In the second case, $10^{2n} - 10^n = 10^n(10^n - 1) > 0$, when $n > 0$. This completes the proof.

q

Make sure you understand why it was necessary to discuss the two cases at the end.

One-to-One Functions

A function $f: X \rightarrow Y$ is called **one-to-one** if for any pair a, b in X such that $f(a) = f(b)$ then $a = b$. Also, if $f: X \rightarrow Y$ and $g: Y \rightarrow Z$ are two functions then the composition $gf: X \rightarrow Z$ is the function defined by $gf(a) = g(f(a))$ for every a in X . Note that the composition gf is only defined if the domain of f is contained in the range of g .

Theorem. If two one-to-one functions can be composed then their composition is one-to-one.

Proof. Let a and b be in X and assume $gf(a) = gf(b)$. Thus, $g(f(a)) = g(f(b))$, and since g is one-to-one we may conclude that $f(a) = f(b)$. Finally, since f is one-to-one, $a = b$.

Roots of Polynomials

A number r is called a **root** of the polynomial $p(x)$ if $p(r) = 0$.

Theorem. If r_1 and r_2 are distinct roots of the polynomial $p(x) = x^2 + bx + c$, then $r_1 + r_2 = -b$ and $r_1 r_2 = c$.

Proof. It follows from our assumptions that $p(x)$ will factor

$$p(x) = (x - r_1)(x - r_2)$$

If we expand the right hand side we get

$$p(x) = x^2 - (r_1 + r_2)x + r_1 r_2.$$

Compare the coefficients above with those of $p(x) = x^2 + b x + c$ to get $r_1 + r_2 = -b$ and $r_1 r_2 = c$.

Proof by Contradiction

In a proof by contradiction we assume, along with the hypotheses, the **logical negation** of the result we wish to prove, and then reach some kind of contradiction. That is, if we want to prove "If P, Then Q", we assume P and Not Q. The contradiction we arrive at could be some conclusion contradicting one of our assumptions, or something obviously untrue like $1 = 0$. Read the proof of the irrationality of the square root of 2 in the [introduction](#) for an example.

Here are a few more examples.

Infinitely Many Primes

One of the first proofs by contradiction is the following gem attributed to Euclid.

Theorem. There are infinitely many prime numbers.

Proof. Assume to the contrary that there are only finitely many prime numbers, and all of them are listed as follows: p_1, p_2, \dots, p_n . Consider the number $q = p_1 p_2 \dots p_n + 1$. This number is not divisible by any of the listed primes since if we divided p_i into q , there would result a remainder of 1 for each $i = 1, 2, \dots, n$. Well then, we must conclude that q is a prime number, not among the primes listed above, contradicting our assumption that **all** primes are in the list p_1, p_2, \dots, p_n .

Proof by contradiction is often used when you wish to prove the impossibility of something. You assume it is possible, and then reach a contradiction. In the examples below we use this idea to prove the impossibility of certain kinds of solutions to some equations.

Example: A Diophantine Equation

A **Diophantine equation** is an equation for which you seek integer solutions. For example, the so-called pythagorean triples (x, y, z) are positive integer solutions to the equation $x^2 + y^2 = z^2$. Here is another.

Theorem. There are no positive integer solutions to the diophantine equation $x^2 - y^2 = 1$.

Proof. (Proof by Contradiction.) Assume to the contrary that there is a solution (x, y) where x and y are positive integers. If this is the case, we can factor the left side: $x^2 - y^2 = (x-y)(x+y) = 1$. Since x and y are integers, it follows that either $x-y = 1$ and $x+y = 1$ or $x-y = -1$ and $x+y = -1$. In the first case we can add the two equations to get $x = 1$ and $y = 0$, contradicting our assumption that x and y are positive. The second case is similar, getting $x = -1$ and $y = 0$, again contradicting our assumption.

Example: Rational Roots

There is a formula for solving the general cubic equation $ax^3 + bx^2 + cx + d = 0$, that is more complicated than the quadratic equation. But in this example, we wish to prove there is no rational root to a particular cubic equation without have to look at the general cubic formula.

Theorem. There are no rational number solutions to the equation $x^3 + x + 1 = 0$.

Proof. (Proof by Contradiction.) Assume to the contrary there is a rational number p/q , in reduced form, with p not equal to zero, that satisfies the equation. Then, we have $p^3/q^3 + p/q + 1 = 0$. After multiplying each side of the equation by q^3 , we get the equation

$$p^3 + pq^2 + q^3 = 0$$

There are three cases to consider. (1) If p and q are both odd, then the left hand side of the above equation is odd. But zero is not odd, which leaves us with a contradiction. (2) If p is even and q is odd, then the left hand side is odd, again a contradiction. (3) If p is odd and q is even, we get the same contradiction. The fourth case-- p even and q even--is not possible because we assumed that p/q is in reduced form. This completes the proof.

The Converse of a Theorem

The **Converse** of "If P , Then Q " is the assertion "If Q , Then P ". For example, the converse of "If it is my car, it's red" is "If the car is red, then it's mine." It should be clear from this example that there is no guarantee that the converse of a true statement is true.

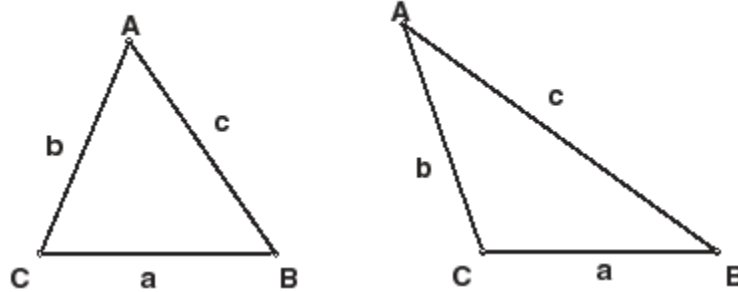
Proof by Contradiction is often the most natural way to prove the converse of an already proved theorem.

The Converse of the Pythagorean Theorem

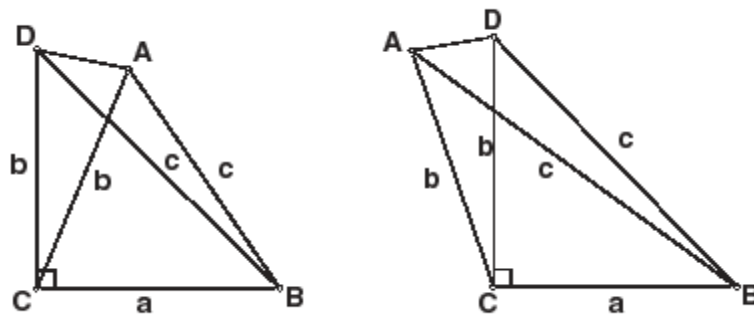
The Pythagorean Theorem tells us that in a right triangle, there is a simple relation between the two leg lengths (a and b) and the hypotenuse length, c , of a right triangle: $a^2 + b^2 = c^2$. Perhaps you don't know that the converse is also true.

The Converse of the Pythagorean Theorem. If the (nonzero) three side lengths of a triangle-- a , b and c --satisfy the relation $a^2 + b^2 = c^2$, then the triangle is a right triangle. (Assume the Pythagorean Theorem has already been proved.)

Proof. (Proof by Contradiction.) Suppose the triangle is not a right triangle. Label the vertices A, B and C as pictured. (There are two possibilities for the measure of angle C: less than 90 degrees (left picture) or greater than 90 degrees (right picture).)



Erect a perpendicular line segment CD as pictured below.



By the Pythagorean Theorem, $BD^2 = a^2 + b^2 = c^2$, and so $BD = c$. Thus we have isosceles triangles ACD and ABD. It follows that we have congruent angles $CDA = CAD$ and $BDA = DAB$. But this contradicts the apparent inequalities (see picture) $BDA < CDA = CAD < DAB$ (left picture) or $DAB < CAD = CDA < BDA$ (right picture).

Proof by contrapositive takes advantage of the logical equivalence between "P implies Q" and "Not Q implies Not P". For example, the assertion "If it is my car, then it is red" is equivalent to "If that car is not red, then it is not mine". So, to prove "If P, Then Q" by the method of contrapositive means to prove "If Not Q, Then Not P".

Example: Parity

Here is a simple example that illustrates the method. The proof will use the following definitions.

Definitions.

1. An integer x is called **even** (respectively **odd**) if there is another integer k for which $x = 2k$ (respectively $2k+1$).
2. Two integers are said to have the same **parity** if they are both odd or both even.

For the purpose of this example we will assume as proved that each integer is either even or odd.

Theorem. If x and y are two integers for which $x+y$ is even, then x and y have the same parity.

Proof. The contrapositive version of this theorem is "If x and y are two integers with opposite parity, then their sum must be odd." So we assume x and y have opposite parity. Since one of these integers is even and the other odd, there is no loss of generality to suppose x is even and y is odd. Thus, there are integers k and m for which $x = 2k$ and $y = 2m+1$. Now then, we compute the sum $x+y = 2k + 2m + 1 = 2(k+m) + 1$, which is an odd integer by definition.

How Is This Different From Proof by Contradiction?

The difference between the Contrapositive method and the Contradiction method is subtle. Let's examine how the two methods work when trying to prove "If P , Then Q ".

- Method of Contradiction: Assume P and Not Q and prove some sort of contradiction.
- Method of Contrapositive: Assume Not Q and prove Not P .

The method of Contrapositive has the advantage that your goal is clear: Prove Not P . In the method of Contradiction, your goal is to prove a contradiction, but it is not always clear what the contradiction is going to be at the start.

A Test for Perfect Squares

In this example, we will need two notions. An integer n is called a **perfect square** if there is another integer k such that $n = k^2$. For example, 13689 is a perfect square since $13689 = 117^2$.

The second idea is the remainder and modular arithmetic. For two integers m and n , $\mathbf{n \bmod(m) = r}$ will be the remainder resulting when we divide m into n . This means that there is an integer q such that $n = mq + r$. For example, $107 \bmod(29) = 11$ since 29 will go into 107 4 times with a remainder of 11 (or, in other words, $107 = (4)(29) + 11$). Determining whether or not a positive integer is a perfect square might be difficult. For example, is 82,642,834,671 a perfect square? First we compute $82,642,834,671 \bmod(4) = 3$. Then use this theorem:

Theorem. If n is a positive integer such that $n \bmod(4)$ is 2 or 3, then n is not a perfect square.

Proof. We will prove the contrapositive version: "If n is a perfect square then $n \bmod(4)$ must be 0 or 1." (Do you understand why this is the contrapositive version?) Suppose $n = k^2$. There are four cases to consider.

1. If $k \bmod(4) = 0$, then $k = 4q$, for some integer q . Then, $n = k^2 = 16 q^2 = 4(4 q^2)$, i.e. $n \bmod(4) = 0$.
2. If $k \bmod(4) = 1$, then $k = 4q + 1$, for some integer q . Then, $n = k^2 = 16 q^2 + 8 q + 1 = 4(4 q^2 + 2 q) + 1$, i.e. $n \bmod(4) = 1$.
3. If $k \bmod(4) = 2$, then $k = 4q + 2$, for some integer q . Then, $n = k^2 = 16 q^2 + 16 q + 4 = 4(4 q^2 + 4 q + 1)$, i.e. $n \bmod(4) = 0$.
4. If $k \bmod(4) = 3$, then $k = 4q + 3$, for some integer q . Then, $n = k^2 = 16 q^2 + 24 q + 9 = 4(4 q^2 + 6 q + 2) + 1$, i.e. $n \bmod(4) = 1$.

If, and Only If

Many theorems are stated in the form "P, if, and only if, Q". Another way to say the same things is: "Q is necessary, and sufficient for P". This means two things: "If P, Then Q" and "If Q, Then P". So to prove an "If, and Only If" theorem, you must prove two implications.

Example: Division

In this example we will use a very useful fact about integers, the so called **Division Algorithm**: If n and m are integers, then there are two other integers q and r , where $0 \leq r < m$, and such that $n = qm + r$. For example, if $n = 103$ and $m = 15$, then $103 = (6)(15) + 13$. (That is, if we divide 15 into 103, we get a quotient of $q = 6$, with a remainder of $r = 13$.)

Theorem. If a is an integer, then a is not evenly divisible by 3 if, and only if, $a^2 - 1$ is evenly divisible by 3.

Proof. Since this is an "If, and Only If" theorem, we must prove two implications.

("If") We must prove " a is not evenly divisible by 3 if $a^2 - 1$ is evenly divisible by 3". So we assume that 3 evenly divides $a^2 - 1 = (a-1)(a+1)$. Since 3 is a prime number, 3 must evenly divide either $a-1$ or $a+1$. In either case, it should be apparent that 3 cannot evenly divide a .

("Only If"). We must prove " a is not evenly divisible by 3 only if $a^2 - 1$ is evenly divisible by 3." This means "If a is not evenly divisible by 3, then $a^2 - 1$ is evenly divisible by 3". This is where we use the division algorithm stated above. We can write $a = 3q + r$, where $r = 0, 1$ or 2 . Our assumption that a is not divisible by 3 implies r cannot be 0. If $r = 1$,

then $a-1 = 3q$ and so 3 evenly divides $a^2 - 1 = (a-1)(a+1)$. A similar argument works if $r = 2$.

q

Sometimes you can prove an "If, and Only If" assertion without explicitly dividing the proof into two parts. The next example illustrates how this might be done.

Example: A Division Rule

You probably learned in school that a positive integer n is evenly divisible by 3 if the sum of the digits of n is divisible by 3. For example, 2620461 is evenly divisible by 3 since $2 + 6 + 2 + 0 + 4 + 6 + 1 = 21 = (3)(7)$. In fact, $2620461 = (3)(873487)$. This condition is really necessary and sufficient.

Theorem. A positive integer n is evenly divisible by 3 if, and only if, the sum of the digits of n is divisible by 3.

Proof. Suppose n is a positive integer whose digit representation is $a_0a_1\dots a_k$. This means, $n = a_0 + a_1 10 + \dots + a_k 10^k$. The digit sum is $s = a_0 + a_1 + \dots + a_k$.

Now, $n - s = (a_0 + a_1 10 + \dots + a_k 10^k) - (a_0 + a_1 + \dots + a_k) = a_1 9 + a_2 99 + \dots + a_k (99\dots 9)$ (where the last term has k nines). So, clearly, $n - s$ is divisible by 3. It follows that n is divisible by 3 if, and only if, s is divisible by 3.

Let's begin with an example.

Example: A Sum Formula

Theorem. For any positive integer n , $1 + 2 + \dots + n = n(n+1)/2$.

Proof. (Proof by Mathematical Induction) Let's let $P(n)$ be the statement " $1 + 2 + \dots + n = n(n+1)/2$." (The idea is that $P(n)$ should be an assertion that for any n is verifiably either true or false.) The proof will now proceed in two steps: the **initial step** and the **inductive step**.

Initial Step. We must verify that $P(1)$ is True. $P(1)$ asserts " $1 = 1(2)/2$ ", which is clearly true. So we are done with the initial step.

Inductive Step. Here we must prove the following assertion: "If there is a k such that $P(k)$ is true, then (for this same k) $P(k+1)$ is true." Thus, we assume there is a k such that $1 + 2 + \dots + k = k(k+1)/2$. (We call this the **inductive assumption**.) We must prove, for this same k , the formula $1 + 2 + \dots + k + (k+1) = (k+1)(k+2)/2$.

This is not too hard: $1 + 2 + \dots + k + (k+1) = k(k+1)/2 + (k+1) = (k(k+1) + 2(k+1))/2 = (k+1)(k+2)/2$. The first equality is a consequence of the inductive assumption.

The Math Induction Strategy

Mathematical Induction works like this: Suppose you want to prove a theorem in the form "For all integers n greater than equal to a , $P(n)$ is true". $P(n)$ must be an assertion that we wish to be true for all $n = a, a+1, \dots$; like a formula. You first verify the **initial step**. That is, you must verify that $P(a)$ is true. Next comes the **inductive step**. Here you must prove "If there is a k , greater than or equal to a , for which $P(k)$ is true, then for this same k , $P(k+1)$ is true."

Since you have verified $P(a)$, it follows from the inductive step that $P(a+1)$ is true, and hence, $P(a+2)$ is true, and hence $P(a+3)$ is true, and so on. In this way the theorem has been proved.

Example: A Recurrence Formula

Math induction is of no use for deriving formulas. But it is a good way to prove the validity of a formula that you might think is true. Recurrence formulas are notoriously difficult to derive, but easy to prove valid once you have them. For example, consider the sequence a_0, a_1, a_2, \dots defined by $a_0 = 1/4$ and $a_{n+1} = 2 a_n(1-a_n)$ for $n > 0$.

Theorem. A formula for the sequence a_n defined above, is $a_n = (1 - 1/2^{2n})/2$ for all n greater than or equal to 0.

Proof. (By Mathematical Induction.)

Initial Step. When $n = 0$, the formula gives us $(1 - 1/2^{2n})/2 = (1 - 1/2)/2 = 1/4 = a_0$. So the closed form formula gives us the correct answer when $n = 0$.

Inductive Step. Our inductive assumption is: Assume there is a k , greater than or equal to zero, such that $a_k = (1 - 1/2^{2k})/2$. We must prove the formula is true for $n = k+1$.

First we appeal to the recursive definition of $a_{k+1} = 2 a_k(1-a_k)$. Next, we invoke the inductive assumption, for this k , to get

$a_{k+1} = 2 (1 - 1/2^{2k})/2 (1 - (1 - 1/2^{2k})/2) = (1 - 1/2^{2k})(1 + 1/2^{2k})/2 = (1 - 1/2^{2k+1})/2$. This completes the inductive step.

Unwinding Definitions (Getting Started)

One of the most often asked questions of students that are new to proofs is "How do I get started?" The answer is usually simple: **Unwind the definitions**. First, look at what you are being asked to prove. Does it involve a term that has been defined (in the lecture or in the text or in the problem)? Write out the definition. What about the assumptions? Do they involve definitions? If so, write those out. Sometimes there are Theorems that are relevant to your problem. If so, write those out. Do not be afraid to jot down everything you know about what you are trying to prove.

Example: The Greatest Common Divisor

The **greatest common divisor** of two positive integers a and b is the number $d = \gcd(a, b)$ that satisfies two properties: (1) d evenly divides a and b and (2) if d' is any other positive integer that evenly divides a and b , then $d > d'$. We can think of the gcd as a binary operation.

Theorem. The binary operation gcd is associative, that is, for any three positive integers a , b and c ,

$$\gcd(\gcd(a, b), c) = \gcd(a, \gcd(b, c)).$$

Strategy. What do we have to prove? Two gcd's are the same. Where do we start? Let d be one of these gcd's. Let's let $d = \gcd(\gcd(a, b), c)$. What does this mean? It means (1) d evenly divides $\gcd(a, b)$ and c and (2) if d' is any other positive integer that evenly divides $\gcd(a, b)$ and c , then $d > d'$. We must prove $d = \gcd(a, \gcd(b, c))$. What does this mean? We must prove two things: (1) d evenly divides a and $\gcd(b, c)$ and (2) if d' is some other positive integer that evenly divides a and $\gcd(b, c)$, then $d > d'$.

(1) Since d divides $\gcd(a, b)$, d must divide a and b . We know d divides c , so d must divide $\gcd(b, c)$. So the first part is easy.

(2) Now we suppose d' divides a and $\gcd(b, c)$. Then, d' divides b and c , so d' must divide $\gcd(a, b)$ too. But then by our assumption, $d > d'$. And this is all we needed to prove.

Proof. Let $d = \gcd(\gcd(a, b), c)$. Then d divides a , b and c , and hence divides a and $\gcd(b, c)$. If d' divides a and $\gcd(b, c)$, then d' must divide $\gcd(a, b)$ and c , and hence $d > d'$. Thus $d = \gcd(a, \gcd(b, c))$.

q

Example: Algebraic Numbers

A real number a is called an **algebraic number** if there is a nonzero polynomial $p(x)$ whose coefficients are all rational numbers such that $p(a) = 0$. An example would be the $\sqrt{2}$, the square root of 2. If we let $p(x) = x^2 - 2$, then $p(\sqrt{2}) = 0$, so $\sqrt{2}$ is an algebraic number. Pretty clearly any root of a rational number is an algebraic number.

Theorem. If a is an algebraic number and r is a rational number, then $a + r$ is an algebraic number.

Strategy. What do we have to prove? $a + r$ is an algebraic number. What does this mean? We must prove that there is a polynomial $p(x)$ with rational number coefficients such that $p(a+r) = 0$. What is our assumption? We assume (1) a is an algebraic number, that is, there is a polynomial $q(x)$ with rational number coefficients such that $q(a) = 0$ and (2) $r =$

s/t where s and t are integers. Where do we start? Start with the polynomial we have, $q(x)$, for which $q(a) = 0$. Can we modify $q(x)$ into a polynomial, $p(x)$, that does what we want: $p(a+r) = 0$? Yes! Let $p(x) = q(x-r)$. Then $p(a+r) = q(a) = 0$.

Proof. Let $q(x)$ be the nonzero polynomial with rational coefficients for which $q(a) = 0$. Then $p(x) = q(x-r)$ is also a polynomial with rational coefficients (since r is a rational number) and $p(a+r) = 0$. Hence $a + r$ is an algebraic number.

Constructive Versus Existential Proofs

Constructive Proofs

How would you prove $2^{99} + 1$ is a composite number? You would exhibit a factorization:

$$2^{99} + 1 = (2^{33})^3 + 1 = (2^{33} + 1)((2^{33})^2 - 2^{33} + 1).$$

In other words, to prove $2^{99} + 1$ is composite we constructed a factorization. Not surprisingly, we call such a proof **constructive**.

q

Example: Pythagorean Triples

A **Pythagorean triple** is a triple of positive integers (a, b, c) that satisfies the equation $a^2 + b^2 = c^2$. For example, $(3, 4, 5)$ is a Pythagorean triple since $3^2 + 4^2 = 5^2$. Are there more? Yes, there are infinitely more, just take multiples of $(3, 4, 5)$: $(3k, 4k, 5k)$ where k can be any positive integer. We call something like $(3k, 4k, 5k)$ a **one parameter** family of solutions. There is one parameter, namely k . Are there more solutions? Yes.

Theorem. There is a two parameter family of Pythagorean triples.

Proof. (We construct the solution.) Let $a = u^2 - v^2$ and $b = 2 u v$ where u and v are positive integers with $u > v$. Then $a^2 + b^2 = (u^2 - v^2)^2 + (2uv)^2 = u^4 - 2 u^2 v^2 + v^4 + 4 u^2 v^2 = u^4 + 2u^2 v^2 + v^4 = (u^2 + v^2)^2$. Thus, $(u^2 - v^2, 2 u v, u^2 + v^2)$, for $u > v$, is two parameter family of Pythagorean triples.

Existential Proofs

Sometimes it is possible to prove the existence of something mathematical without actually constructing it. Why would you want to do this? Well, it could be that you just cannot think of a constructive proof, or that a constructive proof is very long and tedious. In any case, existential proofs are another valuable technique in proofs. Let's look at a familiar example from the calculus.

An Example from Calculus

First let's recall the Intermediate Value and Mean Value Theorems:

Intermediate Value Theorem. If a real valued function f is continuous on the closed interval $[a, b]$ and if N is a number strictly between $f(a)$ and $f(b)$, then there exists a number c in (a, b) such that $f(c) = N$.

Mean Value Theorem. If a real valued function f is continuous on the closed interval $[a, b]$ and f is differentiable on the open interval (a, b) then there is a number c in (a, b) such that $f'(c) = (f(b) - f(a))/(b-a)$. We can use the Mean Value Theorem to prove that certain polynomials do not have more than one real root. (A root of a polynomial $p(x)$ is a number c such that $p(c) = 0$.)

Theorem. The polynomial $p(x) = x^3 + x - 1$ has exactly one real root.

Proof. The proof is in two parts.

Part 1. (Direct Existential Proof.) First we will prove $p(x)$ has one real root. We appeal to the Intermediate Value Theorem with $a = 0$ and $b = 1$: $p(0) = -1 < 0$ and $p(1) = 1 > 0$. Since 0 ($N = 0$) is between -1 ($=p(0)$) and 1 ($=p(1)$), we may conclude that there is a real number c , between 0 and 1 , for which $p(c) = 0$.

Part 2. (Proof by Contradiction.) Now we will prove that $p(x)$ has only one root. Assume to the contrary that $p(x)$ has more than one root. Let's suppose two distinct roots c_1 and c_2 , so $p(c_1) = p(c_2) = 0$. Then by appealing to the Mean Value Theorem, there must be a number c between c_1 and c_2 for which $p'(c) = (p(c_2) - p(c_1))/(c_2 - c_1) = 0$. But a direct calculation shows that $p'(x) = 3x^2 + 1$, which can never be zero since $x^2 \geq 0$ for all real numbers x . The contradiction completes the proof.

Example: Continuous Motion

Here is an example where we appeal to the Mean Value Theorem to obtain the existence of something.

Theorem. If an object is traveling in a straight line with a differentiable position function $s(t)$, where t denotes the time variable, for t between a and b , then there is a time t_0 , between a and b where the instantaneous velocity at $t = t_0$ is equal to the average velocity over the entire path.

Proof. The velocity function is the derivative of the position function $v(t) = s'(t)$. According to the Mean Value Theorem, there is a value $t = t_0$ between a and b where $v(t_0) = s'(t_0) = (s(b) - s(a))/(b-a) =$ average velocity over the path.

Counter Examples

Counter examples play an important role in mathematics. Whereas a complicated proof may be the only way to demonstrate the validity of a particular theorem, a single counter example is all that is need to refute the validity of a proposed theorem. For example, numbers in the form $2^{2^n} + 1$, where n is a positive integer, were once thought to be prime. These numbers are prime for $n = 1, 2, 3$ and 4 . But when $n = 5$, we get

$$2^{2^5} + 1 = 4294967297 = (641)(6700417)$$

a composite number. Conclusion: When faced with a number in the form $2^{2^n} + 1$, we are not allowed to assume it is either prime or composite, unless we know for sure for some other reason.

A natural place for counter examples to occur is when the converse of a known theorem comes into question. The **converse** of an assertion in the form "If P, Then Q" is the assertion "If Q, Then P".

Example: From Calculus

In Calculus you learn that if a function is differentiable at a point, then it is continuous at that point. What would the converse assert? It would say that if a function is continuous at a point, then it is differentiable at that point. But you know this is false. The counter example is $f(x) = |x|$. This function is continuous at $x = 0$, but it is not differentiable at $x=0$. This one counter example is all we need to refute the converse.

q

Example: Rational & Irrational Numbers

If a and b are rational numbers, then so is $a+b$. The proof is very simple. By definition of a rational number, $a = p/q$ and $b = s/t$ for some quadruple of integers $p, q, s,$ and t and such that q and t are nonzero. The sum $a+b = p/q + s/t = (p t + q s)/(q t)$, a rational number by definition. What would the converse say? It would assert "If a and b are real numbers such that $a + b$ is a rational number, then a and b are rational numbers." But this is false. Just let $a = \text{sqrt}(2) + 1$, where sqrt means the square root, and $b = - \text{sqrt}(2)$. Neither a nor b are rational numbers, but $a + b = 1$, which is rational. Proof by Exhaustion (Case by Case)

Sometimes the most straight forward, if not the most elegant, way to construct a proof is by checking cases.

Example: Divisibility

Theorem. If n is a positive integer then $n^7 - n$ is divisible by 7.

Proof. First we factor $n^7 - n = n(n^6 - 1) = n(n^3 - 1)(n^3 + 1) = n(n-1)(n^2 + n + 1)(n+1)(n^2 - n + 1)$. Now there are 7 cases to consider, depending on $n = 7q + r$ where $r = 0, 1, 2, 3, 4, 5, 6, 7$.

Case 1: $n = 7q$. Then $n^7 - n$ has the factor n , which is divisible by 7.

Case 2: $n = 7q + 1$. Then $n^7 - n$ has the factor $n-1 = 7q$.

Case 3: $n = 7q + 2$. Then the factor $n^2 + n + 1 = (7q + 2)^2 + (7q+2) + 1 = 49q^2 + 35q + 7$ is clearly divisible by 7.

Case 4: $n = 7q + 3$. Then the factor $n^2 - n + 1 = (7q + 3)^2 - (7q+3) + 1 = 49q^2 + 35q + 7$ is clearly divisible by 7.

Case 5: $n = 7q + 4$. Then the factor $n^2 + n + 1 = (7q + 4)^2 + (7q+4) + 1 = 49q^2 + 63q + 21$ is clearly divisible by 7.

Case 6: $n = 7q + 5$. Then the factor $n^2 - n + 1 = (7q + 5)^2 - (7q+5) + 1 = 49q^2 + 63q + 21$ is clearly divisible by 7.

Case 7: $n = 7q + 6$. Then the factor $n + 1 = 7q + 7$ is clearly divisible by 7.

What does "Well Defined" Mean?

Sooner or later you will have to prove that something is "well defined". So what does this mean? Let's look at an example.

Example: Congruence Arithmetic

For integers a and b and a positive integer m , we say that **a is congruent to b modulo m** , written $a \equiv b \pmod{m}$, if $a - b$ is evenly divisible by m . Another way of saying this is there is another integer k such that $a = b + km$. For example, $1749 \equiv 15 \pmod{17}$ because $1749 = 15 + (102)(17)$. We like to think of a and b as representing the same "number" modulo m . So there are m "numbers" in this system and they are $0, 1, 2, \dots, m-1$. For example, $m = 0 \pmod{m}$ so we don't have to list 0.

It turns out that we can do arithmetic with these new "numbers". For example, we can define addition modulo m by standard addition. But there is a potential problem. What if

$a = b \pmod{m}$ and $c = d \pmod{m}$, we should get the same result, modulo m , by adding $a + b$ or $c + d$.

Theorem. Addition is **well defined** modulo m , that is, if $a = b \pmod{m}$ and $c = d \pmod{m}$, then $(a+c) = (b+d) \pmod{m}$.

Strategy. What do we have to prove? $(a+c) = (b+d) \pmod{m}$. What does this mean? It means we must show there is an integer k such that $a+c = (b+d) + k m$. What are we assuming? $a = b \pmod{m}$ and $c = d \pmod{m}$. This means there are integers k_1 and k_2 such that $a = b + k_1 m$ and $c = d + k_2 m$. What do we do? We can add these last two equations together to get: $(a+c) = (b+d) + (k_1+k_2)m$. So if we were to let $k = k_1 + k_2$, we would have what we want. Now we see what to do. So we write the proof.

Proof. By our assumption, there are integers k_1 and k_2 such that $a = b + k_1 m$ and $c = d + k_2 m$. Adding these two equations together gives us $(a+c) = (b+d) + (k_1+k_2)m$, which, by definition, means $(a+c) = (b+d) \pmod{m}$.

So "well defined" means that the definition being made has no internal inconsistencies and is free of contradictions. To better understand this idea, let's look at an example where a definition turns out not to be well defined.

Example: Not Well Defined

Using modular arithmetic, consider division. For integers it makes sense to talk about $x/2$ when x is even. Does this make sense modulo 2? For example, let $x = 2$. In mod (2) arithmetic, the "number" $2/2$ should be the unique solution (y) to the equation $2y = 2 \pmod{2}$. But, as you can see, any integer y will satisfy this equation. That is, $x/2$ is not well defined.

Example: Functions Modulo m

In the previous two examples, we looked at the "numbers" modulo m . In this system there are only m "numbers", represented by $0, 1, \dots, m-1$. It is traditional to call this set Z_m . For example, Z_4 has 4 elements, represented by $0, 1, 2, 3$. Remember, all other integers are just other names for these 4. For example, $13 = 1 \pmod{4}$ and $-13 = 3 \pmod{4}$.

Theorem. The function $f:Z_4 \rightarrow Z_4$, given by $f(x) = 2x+1$ is well defined.

Strategy. It is easy to see that $f(0) = 1$, $f(1) = 3$, $f(2) = 5 = 1 \pmod{4}$ and $f(3) = 7 = 3 \pmod{4}$. What do we need to prove? We need to prove that $f(a) = f(b) \pmod{4}$. That is, $f(a) - f(b)$ is evenly divisible by 4, that is, $(2a+1) - (2b+1) = 2(a - b)$ is evenly divisible by 4. What is our assumption? We are assuming $a = b \pmod{4}$. What does this mean? It

means that $a - b$ is evenly divisible by 4. We can see immediately that our assumption implies $2(a - b)$ is divisible by 4, which is what we wanted.

Proof. If $a = b \pmod{m}$, then $(a - b)$ is divisible by 4. Hence so is $(2a + 1) - (2b + 1)$, that is $f(a) = f(b) \pmod{m}$.

The Pigeon Hole Principle

The so called **pigeon hole principle** is nothing more than the obvious remark: if you have fewer pigeon holes than pigeons and you put every pigeon in a pigeon hole, then there must result at least one pigeon hole with more than one pigeon. It is surprising how useful this can be as a proof strategy.

Example

Theorem. Among any N positive integers, there exists 2 whose difference is divisible by $N-1$.

Proof. Let a_1, a_2, \dots, a_N be the numbers. For each a_i , let r_i be the remainder that results from dividing a_i by $N - 1$. (So $r_i = a_i \pmod{N-1}$ and r_i can take on only the values $0, 1, \dots, N-2$.) There are $N-1$ possible values for each r_i , but there are N r_i 's. Thus, by the pigeon hole principle, there must be two of the r_i 's that are the same, $r_j = r_k$ for some pair j and k . But then, the corresponding a_i 's have the same remainder when divided by $N-1$, and so their difference $a_j - a_k$ is evenly divisible by $N-1$.

Example

Theorem. For any N positive integers, the sum of some of these integers (perhaps one of the numbers itself) is divisible by N .

Proof. Consider the N numbers $b_1 = (a_1) \pmod{N}$, $b_2 = (a_1 + a_2) \pmod{N}$, $b_3 = (a_1 + a_2 + a_3) \pmod{N}$, ..., $b_N = (a_1 + \dots + a_N) \pmod{N}$. If one of these numbers is zero, then we are done. Otherwise, only the $N-1$ numbers $1, 2, \dots, N-1$ are represented in this list, and so two of them must be the same, $b_i = b_j$ (say $i < j$). This would then imply that $(a_{i+1} + \dots + a_j) \pmod{N} = 0$, proving our claim.

In mathematics we make assertions about a system whether it be a number system or something more abstract such as a group or linear space. An assertion not known to be true or false is called a *hypothesis* or *conjecture*. Prior to 1995, a famous conjecture was Fermat's Last Theorem. It stated that for an integer $n \geq 3$ there are no positive integer solutions to the equation $x^n + y^n = z^n$. The process of establishing the truth of an assertion is called a *proof*. Once a conjecture has been shown to be a true statement we label it as a *lemma*, *theorem* or *corollary*. We think of a lemma as a result which is used primarily to prove a more important result (i.e. a theorem), and a corollary as a special case or

consequence of a theorem. For example in calculus, we could think of Maclaurin's Theorem as a corollary to Taylor's Theorem.

In these notes we are concerned with techniques that may be used to prove a result and provide a tonic to the student's malady on proofs namely "I don't know where to start". It is probably impossible to teach how to prove something and the best one can offer is a catalog of types of proof along with examples. By reading proofs, the student can often gain insight as to how to prove their own particular result. Once they have gained some experience, they might then be ready for more complicated proofs. What is certain is that there is no cook book solution to obtaining a proof.

How to Read and Do Proofs : An Introduction to Mathematical Thought Processes (Paperback)

by [Daniel Solow](#) "The objective of mathematicians is to discover and to communicate certain truths..." (very good reference)