Your first assignment is to understand the following notes, solve the Exercises and submit mathematically rigorous solutions. Due date: **Friday, Sept 8.**

In class **you should read the Exercises first**, then come back and read the notes and try to recreate the proof as in the examples. This way you won't spend the entire class time reading and will actually get to discuss some problems. You're free and in fact encouraged to discuss the problems with other students and/or the instructor.

Introduction to Proofs

Proofs are the heart of mathematics. 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

- An assumption or
- 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 p 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. Infact, by dividing out the common multiple if neccessary, 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 factoriztion 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.

∎

Direct Proofs

Let's start with an example.

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.

∎

If P, Then Q

Most theorems that you want to prove are either explicitly or implicity 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".

$$P \rightarrow \ldots \rightarrow Q$$

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

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

∎

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

One-to-One Functions

A function f:X->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->Y and g:Y->Z are two functions then the composition gf:X->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 $p(x) = x^2 + b x + c$, 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 $r_1 r_2 = c$.

∎

Exercises

Prove each of the following.

1. If a divides b and a divides c then a divides b + c. (Here a, b, and c are positive natural numbers and the definition of divisibility is given above.)
2. If a is an integer, divisible by 4, then a is the difference of two perfect squares.
3. If a and b are real numbers, then $a^2 + b^2 >= 2 a b$.
4. The sum of two rational numbers is a rational number.
5. If two onto functions can be composed then their composition is onto. (A function f:X->Y is called **onto** if for every b in Y there is an element a in X such that f(a) = b.)
6. If r_1, r_2, r_3 are three distinct (no two the same) roots of the polynomial $p(x) = x^3 + b x^2 + c x+ d$, then $r_1 r_2 + r_1 r_3 + r_2 r_3 = c$.

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: $p_1, p_2 ..., p_n$. Consider the number $q = p_1 p_2 ... p_n + 1$. The number q is either prime or composite. If we divided any of the listed primes p_i into q, there would result a remainder of 1 for each i = 1, 2, ..., n. Thus, q cannot be composite. We conclude that q is a prime number, not among the primes listed above, contradicting our assumption that **all** primes are in the list $p_1, p_2 ..., p_n$.

∎

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 $a x^3 + b ^2 c x + d = 0$, that is more complicated than the qaudratic 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

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

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 posssible 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 its mine." It should be clear from this example that there is no guarantee that the converse of a true stement is true.

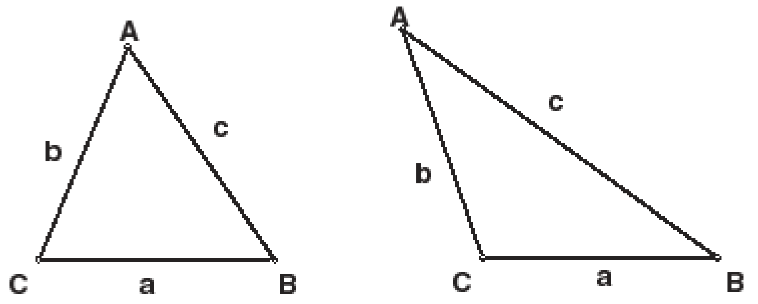
Proof by Contradiction is often the most natural way to prove the converse of an already proved theorem.

The Converse of the Pythagorean Theorem

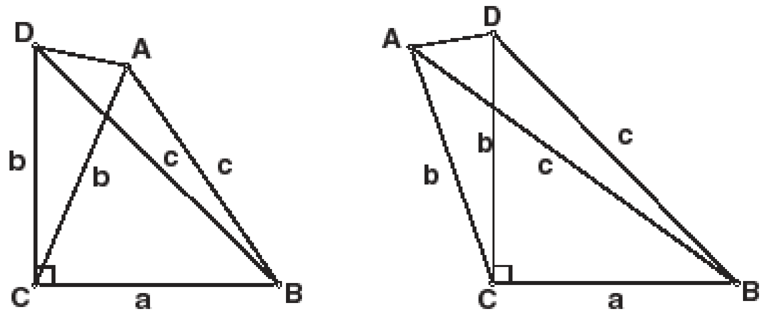
The Pythagorean Theorem tells us that in a right triangle, there is a simple relation between the two leg lengths (a and b) and the hypotenuse length, c, of a right triangle: $a^2 + b^2 = c^2$. Perhaps you don't know that the converse is also true.

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 possibilites 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).

∎

Exercises

Use the method of Proof by Contradiction to prove each of the following.

1. The cube root of 2 is irrational.
2. There are no positive integer solutions to the diophantine equation $x^2 - y^2 = 10$.
3. There is no rational number solution to the equation $x^5 + x^4 + x^3+x^2+ 1 = 0$.
4. If a is a rational number and b is an irrational number, then a+b is an irrational number.

Proof by Contrapositive

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, **n mod(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, 127 mod(29) = 11 since 29 will go into 127 4 times with a remainder of 11 (or, in other words, $127 = (4)(29) + 11$). Determining whether or not a positve 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 mod(4) = 3. Then use this theorem:

Theorem. If n is a positive integer such that n mod(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 mod(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 mod(4) = 0, then k = 4q, for some integer q. Then, $n = k^2 = 16\ q^2 = 4(4\ q^2)$, i.e. n mod(4) = 0.
2. If k mod(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 mod(4) = 1.
3. If k mod(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 mod(4) = 0.
4. If k mod(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 mod(4) = 1.

∎

Exercises

Prove each of the following by the contrapositive method.

1. If x and y are two integers whose product is even, then at least one of the two must be even.

2. If x and y are two integers whose product is odd, then both must be odd.

3. If a and b a real numbers such that the product a b is an irrational number, then either a or b must be an irration number.

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.

∎

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 = sqrt(2) + 1, where sqrt means the square root, and b = - sqrt(2). Neither a nor b are rational numbers, but a + b = 1, which is rational.

∎

Exercises

1. State the converse of "If a and b are even integers then a+b is an even integer". Show that the converse is not true by producing a counter example.
2. State the converse of "If a, b and c are real numbers such that a + b = c, then (a+b) ^{2} = c^2". Show that the converse is not true by producing a counter example.
3. State the converse of "If a, b and c are integers such that a divides b, then a divides the product bc." Show that the converse is not true by producing a counter example.
4. State the converse of "If a and b are rational numbers, then so is the product ab". Show that the converse is not true by producing a counter example.

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 <= 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 divide15 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 divisble 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 divisble 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 divisble by 3." This means "If a is not evenly divisible by 3, then a^2 -1 is evenly divisble 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.

∎

Sometimes you can prove an "If, and Only If" assertion without explicitly dividng 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 divisble by 3 if the sum of the digits of n is divisble by 3. For example, 2620461 is evenly divisble by 3 since 2 + 6 + 2 + 0 + 4 + 6 + 1 = 21 = (3)(7). In fact, 2620461 = (3)(873487). This condition is realy necessary and sufficient.

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

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

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

∎

Exercises

Prove each of the following.

1. If a is an integer, then a is not evenly divisible by 5 if, and only if, $a^4 - 1$ is evenly divisble by 5.
2. For two integers a and b, a+b is odd if, and only if, exactly one of the integers, a or b, is odd.
3. For two integers a and b, the product ab is even if and only if at least one of the integers, a or b, is even.
4. A postive integer n is evenly divisible by 9 if, and only if, the sum of the digits of n is divisble by 9.
5. A postive integer n is evenly divisible by 11 if, and only if, the difference of the sums of the digits in the even and odd positions in n is divisible by 11.

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 = 7 q + 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 $n^2 + n + 1 = (7q + 2)^2 + (7q+2) + 1 = 49 q^2 + 35 q + 7$ is clearly divisible by 7.

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

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

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

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

■

Exercises

Prove each of the following using a case by case analysis.

1. The "Triangle Inequality" for real numbers, $|a + b|$ is less than or equal to $|a| + |b|$. (The cases coorespond to the signs (plus or minus) of a and b.)