

This entire course requires you to write proper mathematical proofs. All proofs should be written elegantly in a formal mathematical style. Complete sentences of explanation are required. Do not simply write an equation; you must explain what the equation is giving and/or why it is being used. Moreover, all equations must be properly aligned with *no scratch outs*. Always give a conclusion.

We will begin by reviewing several standard methods of proof using the following basic definitions and using the facts that the sum and product of integers are integers.

**Divisibility:** We say that  $a$  divides  $b$  if there exists an integer  $k$  such that  $b = ka$ . For example, 6 divides 18 because  $18 = 3 \times 6$ , where  $k = 3$  is an integer.

**Even Number:** An integer  $n$  is said to be *even* if it has the form  $n = 2k$  for some integer  $k$ . That is,  $n$  is even if and only if  $n$  divisible by 2.

**Odd Number:** An integer  $n$  is called *odd* if it has the form  $n = 2k + 1$  for some integer  $k$ .

**Prime Number:** A natural number  $n > 1$  is said to be *prime* if its only positive divisors are 1 and  $n$ . If  $n$  has other positive divisors, then  $n$  is called *composite*.

**Rational Number:** A real number  $x$  is called *rational* if  $x$  can be written as a fraction  $m/n$ , where  $m$  and  $n$  are integers with  $n \neq 0$ . Otherwise,  $x$  is called *irrational*.

### Direct Proof

Consider the statements  $S_1 \implies p \implies q$  and  $S_2 \implies x, p(x)$ . At times we may try to prove that these types of statements are true. To prove  $S_1$  directly, we assume  $p$  is true and then argue that  $q$  must also be true. To prove  $S_2$  is true, we pick an *arbitrary*  $x$  and argue that property  $p(x)$  must hold.

**Example 1.** Prove the following results directly:

- (a) If  $n$  is an odd integer, then  $n^2 + 1$  is even.
- (b) If  $a$  divides  $b$  and  $b$  divides  $c$ , then  $a$  divides  $c$ .
- (c) For all rational numbers  $x$  and  $y$ , the product  $xy$  is also a rational number.

*Proof.* (a) Assume  $n$  is an odd integer. Then  $n = 2k + 1$  for some integer  $k$ . We then have

$$\begin{aligned} n^2 + 1 &= (2k + 1)^2 + 1 \\ &= 4k^2 + 4k + 2 \\ &= 2(2k^2 + 2k + 1) \\ &= 2l, \end{aligned}$$

where  $l = 2k^2 + 2k + 1$  is still an integer because  $k$  is an integer. Thus,  $n^2 + 1$  has the form of an even number, and so  $n^2 + 1$  is even. QED

(b) Assume  $a$  divides  $b$  and  $b$  divides  $c$ . Then  $b = ka$  for some integer  $k$ , and  $c = jb$  for some integer  $j$ . Thus,

$$c = jb = j(ka) = (jk)a.$$

Because the product of integers  $jk$  is still an integer, we have that  $a$  divides  $c$ . QED

(c) Let  $x$  and  $y$  be rational numbers. Then  $x = m/n$  and  $y = j/k$  for some integers  $m$ ,  $n$ ,  $j$ , and  $k$ , with  $n \neq 0$  and  $k \neq 0$ . Then

$$xy = \frac{m}{n} \times \frac{j}{k} = \frac{mj}{nk}.$$

The products of integers  $m j$  and  $n k$  are still integers, and  $n k$  cannot be 0 because neither  $n$  nor  $k$  is 0. Thus,  $xy$  is in the form of a rational number and therefore  $xy$  is rational. QED

### Indirect Proofs

Given an implication  $S \implies p \implies q$ , its contrapositive is  $\sim q \implies \sim p$ , which is logically equivalent to the original implication. In order to prove that  $S$  is true, it might be easier to prove that the contrapositive is true. That is, we can assume that  $q$  is *not true*, and then argue that  $p$  is not true.

Another common method used to prove  $p \implies q$  is a proof by contradiction. In this case, we assume that  $p$  is true but that  $q$  is *not true*. We then argue that a mathematical contradiction occurs. We conclude that  $q$  in fact must be true.

#### Proof by Contrapositive

To prove  $p \implies q$ ,  
assume that  $q$  is not true,  
then argue that  $p$  is not true.

#### Proof by Contradiction

To prove  $p \implies q$ ,  
assume that  $p$  is true but  $q$  is not true.  
Then argue that a mathematical  
contradiction occurs.

**Notes:** (i) A logical statement is often a conjunction  $a \wedge b$  ( $a$  and  $b$ ) or a disjunction  $a \vee b$  ( $a$  or  $b$ ). We apply DeMorgan's Laws to obtain the negations of these statements as follows:

$$\sim(a \wedge b) = \sim a \wedge \sim b \qquad \sim(a \vee b) = \sim a \wedge \sim b$$

(ii) The negation of "one or the other but not both" is given by "both or neither".

(iii) A logical statement may be in terms of a quantifier such as "for every  $x$ , property  $p(x)$  holds." The negation is "there exists an  $x$  for which  $p(x)$  does not hold."

$$\text{Statement: } \forall x, p(x) \qquad \text{Negation: } \exists x, \sim p(x)$$

**Example 2.** Prove the following results:

- (a) If  $c$  is a non-zero rational number, then  $c^{\sqrt{2}}$  is irrational.
- (b) If  $m^3$  is even, then  $m$  is even.
- (c) For all real numbers  $x$  and  $y$ , if  $x + y > 0$ , then  $x > 0$  or  $y > 0$ .
- (d) If  $n^2$  is divisible by 3, then  $n$  is divisible by 3.
- (e) Let  $x$  be a real number. If  $|x| < \varepsilon$  for all  $\varepsilon > 0$ , then  $x = 0$ .

(a) *Proof.* (By contradiction) Let  $c$  be a non-zero rational number, and suppose that  $c^{\sqrt{2}}$  is rational. Then  $c^{\sqrt{2}} = m/n$ , where  $m, n$  are integers and  $n \neq 0$ . Moreover,  $c = j/k$ , where  $j, k$  are integers and  $k \neq 0$ , but also  $j \neq 0$  because  $c$  is non-zero. We then have

$$= \frac{1}{c} \times \frac{m}{n} = \frac{k}{j} \times \frac{m}{n} = \frac{km}{jn}.$$

The products of integers  $km$  and  $jn$  are still integers, and  $jn$  cannot be 0 because neither  $n$  nor  $j$  is 0. Thus,  $c^{\sqrt{2}}$  is in the form of a rational number, which is a contradiction because  $c^{\sqrt{2}}$  is irrational. Ergo,  $c^{\sqrt{2}}$  must be irrational. QED

(b) *Claim:* If  $m^3$  is even, then  $m$  is even. We shall prove the contrapositive instead; we shall assume that  $m$  is *not* even and show that  $m^3$  is *not* even. That is, we shall assume that  $m$  is *odd* and show that  $m^3$  is odd.

*Proof.* Assume that  $m$  is odd. Then  $m = 2k + 1$  for some integer  $k$ . Then,

$$\begin{aligned} m^3 &= (2k + 1)^3 \\ &= 8k^3 + 12k^2 + 6k + 1 \\ &= 2(4k^3 + 6k^2 + 3k) + 1 \\ &= 2l + 1, \end{aligned}$$

where  $l$  is the integer  $4k^3 + 6k^2 + 3k$ . Thus,  $m^3$  is odd because it is written in the form of an odd integer. By contrapositive, if  $m^3$  is even, then  $m$  is even. QED

(c) *Proof.* Let  $x$  and  $y$  be real numbers. Assume that  $x \leq 0$  and  $y \leq 0$ . Then by adding, we have  $x + y \leq 0 + 0 = 0$ . That is,  $x + y \leq 0$ . Hence,  $x > 0$  and  $y > 0$  implies that  $x + y > 0$ . By contrapositive, if  $x + y > 0$ , then  $x > 0$  or  $y > 0$ . QED

(d) Claim: If  $n^2$  is divisible by 3, then  $n$  is divisible by 3.

*Proof.* Assume  $n$  is not divisible by 3. We then can apply the Fundamental Theorem of Arithmetic to write  $n$  uniquely as a product of powers of primes as follows:

$$n = p_1^{r_1} \times p_2^{r_2} \times \dots \times p_k^{r_k},$$

where  $r_i$  are natural numbers and the  $p_i$  are distinct primes. Because  $n$  is not divisible by 3, then  $p_i \neq 3$  for  $1 \leq i \leq k$ . By squaring we obtain

$$n^2 = (p_1^{r_1} \times p_2^{r_2} \times \dots \times p_k^{r_k})^2 = p_1^{2r_1} \times p_2^{2r_2} \times \dots \times p_k^{2r_k},$$

which is a prime factorization of  $n^2$ . By uniqueness of prime factorization, the above  $p_i$  for  $1 \leq i \leq k$  are the only prime factors of  $n^2$ . Because none of the  $p_i$  equals 3, then  $n^2$  is not divisible by 3. By contrapositive, if  $n^2$  is divisible by 3, then  $n$  must also be divisible by 3. QED

-----  
**Note:** The preceding result can be generalized as follows:

Let  $p$  be prime and suppose  $k \geq 2$ . If  $n^k$  is divisible by  $p$ , then  $n$  is divisible by  $p$ .

(In the proof of (d), simply replace 3 with  $p$  and replace the exponent 2 with  $k$ .)

-----  
 (e) Claim: If  $|x| < \varepsilon$  for all  $\varepsilon > 0$ , then  $x = 0$ .

*Proof.* Suppose  $|x| < \varepsilon$  for all  $\varepsilon > 0$ . We must show that  $x = 0$ . So suppose that  $x \neq 0$ . Then  $x < 0$  or  $x > 0$ . In either case, we have  $|x| > 0$ . Now let  $\varepsilon = |x|/2 > 0$ . For this  $\varepsilon$ , we then have  $|x| > |x|/2 = \varepsilon$ , which contradicts the assumption. Thus we must have that  $x = 0$ . QED

**Note:** We also could have argued by contrapositive: Assume  $x \neq 0$ . Then we showed that there exists an  $\varepsilon > 0$  for which  $|x| < \varepsilon$  fails. So if  $x \neq 0$ , then it is not true that  $|x| < \varepsilon$  for all  $\varepsilon > 0$ . By contrapositive, if it is true that  $|x| < \varepsilon$  for all  $\varepsilon > 0$ , then  $x = 0$ .

### Double Implication

A double implication is of the form  $p \iff q$ , which is read “ $p$  if and only if  $q$ ”. This statement means  $p \implies q$  and  $q \implies p$  and both implications must be proven.

**Example 3.** Let  $n$  be an integer. Then  $n$  is even if and only if  $n^2$  is even.

*Proof.* Suppose first that  $n$  is even. Then  $n = 2k$ , for some integer  $k$ . So then

$$n^2 = (2k)^2 = 4k^2 = 2(2k^2).$$

Because  $2k^2$  is also an integer, we see that  $n^2$  must be even.

Next we must prove that if  $n^2$  is even, then  $n$  is even. But we shall prove the contrapositive instead. So assume that  $n$  is not even, i.e., that  $n$  is odd. Then  $n = 2k + 1$  for some integer  $k$ . We then have

$$n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1 = 2j + 1,$$

where  $j = 2k^2 + 2k$  is an integer. Hence,  $n^2$  is odd; that is,  $n^2$  is not even. We have proven that if  $n$  is not even, then  $n^2$  is not even. By contrapositive, if  $n^2$  is even, then  $n$  is even. From both directions, we now have that  $n$  is even if and only if  $n^2$  is even.

**QED**

**Note:** The second direction also follows from the generalization of Part (d) using the prime  $p = 2$ . In other words, if 2 divides  $n^2$  then 2 divides  $n$ .

**Theorem.**  $\sqrt{2}$  is irrational.

*Proof.* Assume  $\sqrt{2}$  is rational. Then we can write  $\sqrt{2} = m/n$ , where  $m$  and  $n$  are integers with  $n \neq 0$ . Furthermore, we can assume that the fraction is reduced so that  $m$  and  $n$  have no common divisors. Then by squaring the fraction, we have

$$2 = \frac{m^2}{n^2} \quad \text{or} \quad 2n^2 = m^2.$$

Thus,  $m^2$  is even because it is divisible by 2. It follows that the integer  $m$  must be even. So we may write  $m = 2k$  for some integer  $k$ . Then

$$2n^2 = m^2 = (2k)^2 = 4k^2 = 2(2k^2), \quad \text{which gives } n^2 = 2k^2.$$

Thus,  $n^2$  is even because it is divisible by 2. It follows that the integer  $n$  must be even. So both  $m$  and  $n$  are even and therefore both are divisible by 2. But this fact contradicts the assumption that we have chosen  $m$  and  $n$  to have no common divisors. This contradiction leads us to conclude that  $\sqrt{2}$  cannot be written as a fraction. Thus,  $\sqrt{2}$  is irrational.

**QED**

**Corollary.** For any prime  $p$ ,  $\sqrt{p}$  is irrational.

### Exercises

Prove the following results in a formal, elegantly written, mathematical style:

- (a) For all integers  $m$  and  $n$ , if  $m$  is even and  $n$  is odd, then  $m + n$  is odd.
- (b) Let  $a$  be an integer. If  $a$  divides  $b$ , then  $b$  is an integer and  $a$  divides  $b^2$ .
- (c) If  $x$  and  $y$  are rational numbers, then  $x + y$  is a rational number.
- (d) Let  $m$  and  $n$  be integers. If  $mn$  is even, then  $m$  is even or  $n$  is even.
- (e) Let  $m$  and  $n$  be integers. If  $m + n$  is odd, then  $m$  is odd or  $n$  is odd but not both.
- (f) Let  $x$  and  $y$  be real numbers. Then  $x = y$  if and only if  $|x - y| < \varepsilon$  for every  $\varepsilon > 0$ .
- (g) For any prime  $p$ ,  $\sqrt{p}$  is irrational.