Chapter 2

Quantifiers and Written Proofs

Here are two assertions in mathematics: "*Every non-zero number x has a multiplicative inverse y*" and "*There is a a number x such that $x^2 = -1$*".

It is not possible to know the truth value of the either assertion unless you know what sort of numbers can be used to replace x and y. If they must be integers, then both assertions are false. If they can be real numbers, then the first assertion is true and the second one is false. If they can be complex numbers, then both assertions are true.

2.1 Open Statements

An *open statement* is an assertion that contains one or more variables. Usually the truth value of such a statement can not be determined until the values of the variables are known. An example is "*x is a root of $x^2 + 5x + 6$*". This statement is true if $x = 3$, and false if $x = 1$. It is never true if x is required to be a negative real number, and (as we've seen) can be true if x is required to be a positive real number.

We will drop the qualifier "open", and refer to assertions that contain one or more variables as *statements*.

It is also the case that we can't tell if a statement containing variables is ever true, or always true, unless we know what sort of values can replace the variables. An example is $x^2 = 2$. If x can be any real number, then this statement is true when $x = \sqrt{2}$ and when $x = -\sqrt{2}$. If x must be an integer,

then it is never true.

The point to remember about statements involving variables is that once the variables are assigned values (that they are allowed to have), then the resulting statement has a truth value. Before the variables have values it is only possible to know the truth value of such a statement if it is always true, or always false, no matter which of the allowed values are assigned to the variables.

The Laws of Logic apply to statements involving variables because they apply once values are given to the variables (in exactly the same way each time). Thus, for example, if $p(x)$ and $q(x)$ are statements involving the variable x, the contrapositive of $p(x) \to q(x)$ is $\neg q(x) \to \neg p(x)$, and these statements have the same truth value for any x, so either one can replace the other whenever it occurs. Similarly, for every x we have that $\neg(p(x) \vee q(x))$ has the same truth value as $\neg p(x) \wedge \neg q(x)$, so either one can replace the other whenever it occurs, and so on.

2.2 Quantifiers

When we make an assertions like "*if* $x^2+3x+2=0$ *then* $x=-1$ *or* $x=-2$", the intention is to convey that the assertion holds for every real number x. Similarly, an assertion like "*some rectangles are squares*" is intended to convey that at least one rectangle is a square.

If an assertion contains one or more variables, it isn't possible to know its truth value until something about the variables is known. There are two options:

1. If values are given to the variables, then the assertion will be either true or false for those particular values. Giving different values to the variables might result in a different truth value for the assertion.

2. Specify the quantity (that is, number) of allowed replacements for each variable that result in the assertion being true. This specification is an assertion that is either true or false, that is, it is a statement.

The goal of this section is to consider the second option. It will be helpful to keep the first possibility in mind when doing that.

The *universe* of a variable is the collection of values it is allowed to take.

The *universal quantifier* $\forall$ asserts that the given assertion is true *for all* allowed replacements for a variable. Think of the upside-down "A" as representing "All". Synonyms for "*for all*", include "*all*", "*every*" and "*for each*".

An example of using a universal quantifier is: "*for all integers n, the integer $n(n+1)$ is even*". We could take a first step towards a symbolic representation of this statement by writing "$\forall n, n(n+1)$ *is even*", and specifying that the universe of n is the integers. (This statement is true.)

The *existential quantifier* $\exists$ asserts that *there exists* at least one allowed replacement for a variable for which the given assertion is true. Think of the backwards "E" as representing "exists". Synonyms for "*there exists*" include "*there is*", "*there are*", "*some*", and "*at least one*".

An example of using an existential quantifier is "*there exists an integer n such that $n^2 - n + 1 = 0$*". A symbolic representation of this statement is obtained by writing $\exists n, n^2 - n + 1 = 0$, and specifying that the universe of n is the integers. (This statement is false.)

We can completely write the statement "$\forall n, n(n+1)$ *is even*" in symbols by remembering the definition of an even integer. An integer k is *even* when there is an integer t such that $k = 2t$. Symbolically, k is even when $\exists t, k = 2t$, where the universe of t is the integers. With this in mind "$\forall n, n(n+1)$ *is even*" becomes "$\forall n, \exists t, n(n+1) = 2t$".

Let $s(x)$ denote a statement involving the variable x. Observe that if $\forall x, s(x)$ is true, then so is $\exists x, s(x)$, provided the universe contains a non-zero number of elements: if an assertion is true for all x is the universe, then it is true for at least one x (provided there is one). If the universe contains no elements, then $\forall x, s(x)$ is always true, and $\exists x, s(x)$ is never true (why?). Of course, the truth of $\exists x, s(x)$ tells us nothing about the truth of $\forall x, s(x)$.

Both universal and existential quantifiers can be (unintentionally) hidden, as in the example used to begin this section. Another example is the statement "if $(a \neq 0)$ and $(ax^2 + bx + c = 0)$ then

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a},$$

is meant to apply to all real numbers x. If the universal quantifier were made explicit, it would read "for all real numbers $x \ldots$". Similarly, "a real

number can have more than one decimal expansion" is intended to assert the existence of one or more such numbers. If the existential quantifier were made explicit, it would read "there is a real number x such that x has more than one decimal expansion".

When quantifiers are nested, they are read in order from left to right. For example, if x and y are understood to be numbers, "$\forall x, \exists y, x + y = 0$" is read as follows: *for all x, the statement "$\exists y, x + y = 0$" is true.* No matter the value of x, the number y can be chosen to be its negative. Hence, $\exists y, x + y = 0$ is true for any x. Consequently, $\forall x, \exists y, x + y = 0$ is true.

The order of quantifiers is important. The statement "$\exists x, \forall y, x + y = 0$" says that there is a real number x such that, for every real number y, the quantity $x + y = 0$, which is false.

2.3 Negating Statements Involving Quantifiers

The negation of a universally quantified statement is an an existentially quantified statement. If it is not the case that a statement is true for all allowed replacements in the universe, then it is false for at least one allowed replacement.

For example "$\neg\forall n \geq 0, n^2 - n + 41$ *is prime*" says "it is not the case that for every positive integer n the number $n^2 - n + 41$ is prime", or in other words "there exists a positive integer n such that $n^2 - n + 41$ is not prime".

In symbols, if $s(x)$ is an assertion involving the variable x (and maybe some other variables and quantifiers) $\neg\forall x, s(x)$ is the same is $\exists x, \neg s(x)$.

The negation of an existentially quantified statement is a universally quantified statement. If it is not the case that a statement is true for at least one allowed replacement in the universe, then it is false for all allowed replacements.

For example "$\neg\exists a, b, \frac{a}{b} = \sqrt{2}$" says "it is not the case that there exists (integers) a and b such that $\frac{a}{b} = \sqrt{2}$", or in other words "for all (integers) a and b, $\frac{a}{b} \neq \sqrt{2}$", that is, "$\sqrt{2}$ is irrational".

In symbols, if $s(x)$ is an assertion involving the variable x (and maybe

some other variables and quantifiers) $\neg\exists x, s(x)$ is the same is $\forall x, \neg s(x)$.

Using what we've done above, the statement $\neg\exists x, \forall y, x + y = 0$ is the same as $\forall x, \neg\forall y, x+y = 0$ (take $s(x)$ to be $\forall y, x+y = 0$). In turn, this is the same as $\forall x, \exists y, \neg(x + y = 0)$, or equivalently $\forall x, \exists y, x + y \neq 0$. The latter statement is easily seen to be true. No matter number x is, we can choose y to be any number different than $-x$, and $x + y \neq 0$.

2.4 The Division Algorithm

Something everyone learns in elementary school is that when one integer is divided by another there is a unique quotient and a unique remainder. For example, when 65 is divided by 17 the quotient is 3 and the remainder is 14. That is, $65 = 3 \times 17 + 14$. What about when 65 is divided by -17? We have $65 = (-3) \times (-17) + 14$, and we also have $65 = (-4) \times (-17) - 3$. Should the remainder be 14 or -3? The convention is that *the remainder is always non-negative* when dividing by a negative number.

The fact that there is a unique quotient and a unique remainder is a theorem. It bears the name "The Division Algorithm" because the proof tells you how to find the quotient and the remainder when an integer a is divided by an integer b – keep subtracting multiples of b from a until what's left is a number r between 0 and $|b|-1$ (inclusive). The total number of times b was subtracted from a is the quotient, and the number r is the remainder. That is, $a = bq + r,\ 0 \leq r < |b|$.

Theorem 2.4.1 The Division Algorithm *Let $a, b \in \mathbb{Z}$, with $b \neq 0$. Then there exist unique integers q and r so that $a = bq + r$ and $0 \leq r < |b|$.*

The integers q and r in The Division Algorithm are the *quotient* and *remainder* when a is divided by b, respectively. The integer b is the *divisor*, and (for completeness we will note that) the integer a is the *dividend*.

Instead of proving the Division Algorithm, we illustrate the proof with the example below below where 2024 is divided by 75. First, ten 75s are subtracted, leaving 1274. Then, ten more 75s are subtracted, leaving 524. From this number five 75s are subtracted, leaving 149. And finally, one 75 is subtracted leaving 74 (the remainder). The quotient is the total number of 75s subtracted, which is 26. Thus $2024 = 26 \times 75 + 74$.

$$
\begin{array}{rr|l}
75\ ) & 2024 & 10 \\
 & -750 & \\
\hline
 & 1274 & 10 \\
 & -750 & \\
\hline
 & 524 & 5 \\
 & -375 & \\
\hline
 & 149 & 1 \\
 & -75 & \\
\hline
 & 74 & 26
\end{array}
$$

2.5 Some Examples of Written Proofs

Suppose you want to write a proof in words for a statement of the form "if p then q". That is, you wish to establish the theorem $p \Rightarrow q$. There are many techniques (methods) that can be tried. There is no guarantee of which method will work best in any given situation. Experience is a good guide, however. Once a person has written a few proofs, s/he gets a sense of the best thing to try first in any given situation.

To use the method of *direct proof* to show p logically implies q, *assume p is true* and then *argue using definitons, known implications and equivalences that q must be true.* The reason for assuming p is true comes from the definition of logical implication. In this case the first line of the proof is "*Assume p.*" and the last says, essentially, "*q is true*". What comes in between depends on p and q.

In the following example of a direct proof, we use the definition of an even integer: An integer n is *even* if there exists an integer k so that $n = 2k$. Put differently, the integer n is even if it leaves remainder 0 on division by 2. An integer n is *odd* if it leaves remainder 1 on division by 2, that is, if $n = 2k + 1$ for some integer k. By the Division Algorithm, every integer is either even or odd, and not both.

Proposition 2.5.1 *If the integer n is even, then n^2 is even.*

Proof. Suppose that the integer n is even. Hence, there exists an an integer k so that $n = 2k$. Then, $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$. Since $2k^2$ is an integer,

n^2 is even. □

It is customary in mathematics to use a box to indicate the end (or absence) or an argument.

Another proof technique is to *prove the contrapositive*. That is, assume q is false, and argue using the same things as above that p must also be false. This works since $p \to q \Leftrightarrow \neg q \to \neg p$. In this case the first line of the proof is "*Assume* $\neg q$." and the last is, essentially, "$\neg p$ *is true*". This method is sometimes called giving an *indirect proof*. The motivation for the name comes from the fact that the logical implication is proved indirectly, by its contrapositive.

Proposition 2.5.2 *If the integer n^2 is even, then n is even.*

Proof. We will prove the contrapositive that if n is not even, then n^2 is not even.

Suppose that the integer n is not even, that is, it is odd. We want to show that n^2 is odd. Since n is odd, there exists an an integer k so that $n = 2k + 1$. Then, $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$. Since $2k^2 + 2k$ is an integer, n^2 is odd. □

Yet another technique is *proof by contradiction*. Such a proof begins by assuming q is false and, again proceeding as above, until deriving a statement which is a (logical) contradiction. This enables you to conclude that q is true. In such a situation, the first line of the proof is "Suppose $\neg q$." and the proof ends with " We have obtained a contradiction. Therefore q."

Here is a classic example of proof by contradiction. It uses the definition of a rational number: a number x is *rational* if there exist integers a and b so that $x = a/b$. A number is *irrational* if it is not rational.

Put slightly differently, x is rational if it is a ratio of two integers. There are many ratios of integers that equal a given number. In particular, there is always one where the fraction a/b is in *lowest terms*, meaning that a and b have no common factors other than one.

Proposition 2.5.3 *$\sqrt{2}$ is not rational.*

Proof. Suppose $\sqrt{2}$ is rational. Then there exist integers a and b so that $\sqrt{2} = a/b$. The integers a and b can be chosen so that the fraction a/b is in lowest terms, so that a and b have no common factor other than 1. In particular, a and b are not both even.

Since $\sqrt{2} = a/b$, we have that $2 = (a/b)^2 = a^2/b^2$. By algebra, $2b^2 = a^2$. Therefore a^2 is even. By Proposition 2.5.2, a is even. Thus there exists an integer k so that $a = 2k$. It now follows that $2b^2 = a^2 = (2k)^2 = 4k^2$, so that $b^2 = 2k^2$. Therefore b^2 is even. By Proposition 2.5.2, b is even.

We have now derived the contradiction (a and b are not both even) and (a and b are both even). Therefore, $\sqrt{2}$ is not rational. □

Sometimes the hypotheses lead to a number of possible situations, and it is easier to consider each possibility in turn. In the method of *proof by cases*, one lists the cases that could arise (being careful to argue that all possibilities are taken into account), and then shows that the desired result holds in each case. It could be that different cases are treated with different proof methods. For example, one could be handled directly, and another by contradiction.

In the following example we make use the fact that, by the Division Algorithm, every integer n can be uniquely written in the form $3k+r$, where k is an integer and r equals 0, 1, or 2. When the remainder, r, equals 0 we have $n = 3k$, so that n is a multiple of 3.

Proposition 2.5.4 *If the integer n^2 is a multiple of 3, then n is a multiple of 3.*

Proof. We prove the contrapositive: if n is not a multiple of 3, then n^2 is not a multiple of 3. Suppose n is not a multiple of 3. Then the remainder when n is divided by 3 equals 1 or 2. This leads to two cases:

Case 1. The remainder on dividing n by 3 equals 1.

Then, there exists an integer k so that $n = 3k+1$. Hence $n^2 = (3k+1)^2 = 9k^2 + 6k + 1 = 3(3k^2 + 2k) + 1$. Since $(3k^2 + 2k)$ is an integer, the remainder on dividing n^2 by 3 equals 1. Therefore n^2 is not a multiple of 3.

Case 2. The remainder on dividing n by 3 equals 2.

Then, there exists an integer k so that $n = 3k+2$. Hence $n^2 = (3k+2)^2 = 9k^2 + 12k + 4 = 3(3k^2 + 4k + 1) + 1$. Since $(3k^2 + 4k + 1)$ is an integer, the remainder on dividing n^2 by 3 equals 1. Therefore n^2 is not a multiple of 3.

Both cases have now been considered. In each of them, we have shown that n^2 is not a multiple of 3. It now follows that if n is not a multiple of 3, then n^2 is not a multiple of 3. This completes the proof. □

2.6 Divisibility

If a and b are integers, we say that a *divides* b, and write $a|b$, if there is an integer k such that $ak = b$. When this happens, we also say

- a *is a divisor of* b,
- b *is divisible by* a, or
- b *is a multiple of* a.

Equivalently, a divides b when the remainder when b is divided by a equals 0, so that b is a times some other integer.

Although it is true that if a divides b then b/a is an integer, notice that there is no discussion of fractions. Everything taking place involves only integers and multiplication.

According to the definition,

- $5|30$ because $5 \times 6 = 30$,
- $-7|28$ because $(-7) \times (-4) = 28$,
- $10|-100$ because $10 \times (-10) = -100$ and
- $-4|-12$ because $(-4) \times 3 = 12$.

Which numbers divide zero? If a is any integer, then $a \times 0 = 0$ so $a|0$. In particular, $0|0$. (However, zero does not divide any other integer.)

It is clear from the definition that, for any integer b, we have $1|b$ (because $1 \times b = b$), and also $b|b$ (because $b \times 1 = b$). The second of these say that the relation "divides" on $\mathbb{Z}$ is reflexive. It also turns out to be a transitive relation on $\mathbb{Z}$ (see below), but not an anti-symmetric relation on $\mathbb{Z}$. (However, it is an anti-symmetric relation on $\mathbb{N}$.)

Divisibility is defined in terms of the existential quantifier "there exists" (the definition requires that *there exists k such that ...*), so proofs of divisibility involve demonstrating how such an integer k can be found. This is what was happening in the previous paragraph, and also what will happen in the proofs of the propositions below.

We know, for example, that $6|12$ (because $6 \times 2 = 12$). Hence any multiple of 12, say $12k$, is also a multiple of 6 because $12k = 6 \times (2k)$. The same factoring argument works when 6 and 12 are replaced by any two numbers a and b such that $a|b$. This fact, and its proof, are the next proposition.

Proposition 2.6.1 *Let $a, b, c \in \mathbb{Z}$. If $a|b$ and $b|c$, then $a|c$*

Proof. Suppose $a|b$ and $b|c$. The goal is to find an integer k so that $ak = c$. Since $a|b$, there is an integer m so that $am = b$. Since $b|c$, there is an integer n so that $bn = c$. Therefore, $c = bn = amn = a(mn)$. Since $mn \in \mathbb{Z}$, we have that $a|c$. □

In a manner similar to what's above, we know that since $6|12$ and $6|18$, then for any integers x and y we have $6|12x + 18y = 6 \times (2x) + 6 \times 3y = 6 \times (2x + 3y)$. As before, this factoring argument works whenever 6, 12 and 18 are replaced by numbers a, b and c such that $a|b$ and $a|c$.

Proposition 2.6.2 *Let $a, b, c \in \mathbb{Z}$. If $a|b$ and $a|c$, then $a|bx + cy$ for any integers x and y.*

Proof. Suppose $a|b$ and $a|c$. Let $x, y \in \mathbb{Z}$. The goal is to find an integer k so that $ak = bx + cy$. Since $a|b$, there is an integer m so that $am = b$. Since $a|c$, there is an integer n so that $an = c$. Therefore, $bx + cy = amx + any = a(mx + ny)$. Since $mx + ny \in \mathbb{Z}$, we have that $a|bx + cy$. □

By taking $y = 0$ in the proposition above, we obtain the result that if a divides b, then it divides any integer multiple of b.

The previous proposition can be generalized so that $bx + cy$ is replaced by a sum involving more than two terms, each of which has a factor divisible by a.

What could we say about the integers a and b if we have both $a|b$ and $b|a$? Let's look at an example. Take $b = 6$. If $a|6$, then a is one of the numbers $\pm 1, \pm 2, \pm 3, \pm 6$. The only numbers in this collection that are also divisible by 6 are -6 and 6. After checking out a couple more examples, one is led to the next proposition.

Proposition 2.6.3 *Let $a, b \in \mathbb{Z}$. If $a|b$ and $b|a$, then $a = \pm b$.*

Proof. Since $a|b$, there is an integer m so that $am = b$. Since $b|a$, there is an integer n so that $bn = a$. Therefore, $a = bn = amn$, so that $mn = 1$. Since m and n are integers, either $m = n = 1$ or $m = n = -1$. If $n = 1$ then $a = b$ and if $n = -1$ then $a = -b$. □

2.7 Prime Numbers

An integer $p > 1$ is called *prime* if its only positive divisors are 1 and itself. An integer $n > 1$ which is not prime is called *composite*.

That is, an integer n is composite if there are integers a and b with $1 < a \leq b < n$ such that $n = ab$.

The integer 1 is neither prime nor composite. It is just a unit. The Greeks thought of numbers as lengths. Every length $n \geq$ is made up of n unit lengths. A length was regarded as prime if it was not a multiple of some length other than the unit, and composite if it was.

Proposition 2.7.1 *Every integer $n > 1$ has a prime divisor (possibly itself).*

Proof. Let $n > 1$ be an integer. Since n is divisible by 1 and itself, it has at least two positive divisors. Let b be the smallest divisor of n which is greater than 1.

We claim that b must be prime. Let a be a positve integer such that $a|b$. Then $a \leq b$. We will argue that $a = 1$ or $a = b$, so that the only positive

divisors of b are 1 and itself. We have $a|b$ and $b|n$, thus $a|n$. Since b is the smallest divisor of n which is greater than 1, it follows that $a = 1$ or $a = b$. Therefore, b is prime. This completes the proof. □

A collection of objects is *finite* if it contains exactly n objects for some integer $n \geq 0$. A collection of objects is *infinite* if it is not finite. That is, a collection of object is *infinite* if it contains more than n objects for any integer $n \geq 0$. To show that there are infinitely many of something, it is enough to show that, given a collection of n of them, there is always at least one more that does not belong to the collection.

The Greeks knew that there were infinitely many prime numbers. There is a remarkable proof in Euclid's *Elements*, published about 300BC. There is a temptation to think of this book only as a classic treatise on geometry (which it is). But, it also contains some very nice results in number theory. Euclid's argument uses proof by contradiction to show that there are more than n primes for any integer n; hence there are infinitely many primes.

Theorem 2.7.2 [Euclid, $\approx$ 300BC] *There are infinitely many prime numbers.*

Proof. Suppose not, and let $p_1, p_2, \ldots, p_n$ be the collection of all prime numbers. Consider the number $N = p_1 p_2 \ldots p_n + 1$. The number N has a prime divisor (possibly itself). But none of $p_1, p_2, \ldots, p_n$ divide N: each leaves a remainder of 1 when divided into N. Therefore there is a prime number not in the collection, a contradiction. □

While it is tempting to thing that the number N in Euclid's proof is prime, this is not always true. Try the first few possible values and see for yourself. It does not take too long to get to an N that's composite.

The *Sieve of Eratosthenes*.is a method for generating all of the prime numbers less than or equal to n.

1. Write the numbers $2, 3, 4, \ldots, n$ in a line. Circle the number 2.

2. Cross out all multiples of the number just circled. Circle the first number in the list which is neither circled nor crossed out. If the number just circled is less than $\sqrt{n}$, repeat this step using the newly circled number.

3. If the number just circled is greater than $\sqrt{n}$, then circle all remaining numbers that are neither already circled nor crossed out.

4. The collection of circled numbers is the collection of primes less than or equal to n.

So why does this work? The first number to be circled is prime, and each subsequent number circled in step 2 is not a multiple of a smaller prime, hence it must be prime. It remains to explain why the process can be "short circuited" after a number greater than $\sqrt{n}$ has been circled. That's because of the proposition below.

Proposition 2.7.3 *If $n > 1$ is composite, then it has a prime divisor p such that $2 \leq p \leq \sqrt{n}$.*

Proof. Suppose $n > 1$ is composite. Then there are integers a and b such that $1 < a \leq b < n$ and $n = ab$. If both a and b are greater than $\sqrt{n}$, then $n = ab > \sqrt{n}\sqrt{n} = n$, a contradiction. Thus $a \leq \sqrt{n}$. Any prime divisor of a is both less than or equal to a (and hence $\sqrt{n}$) and a divisor of n (because $p|a$ and $a|n$). Thus n has a prime divisor p such that $2 \leq p \leq \sqrt{n}$. □

2.8 Quantifiers and Written Proofs Questions

1. Determine if each statement below is true or false, and explain your reasoning.

   (a) The negation of "*Every golf shot is a hook or a slice*" is "*Some golf shots are hooks and slices*".

   (b) The negation of "*All enforcers skate slowly and pass badly*" is "*Some enforcers skate fast and pass well*".

   (c) When the statement "*There is no largest integer.*" is written is symbols, both of the quantifiers $\forall$ and $\exists$ appear.

   (d) For integers m and n, arguing that if mn is odd then m and n are odd proves that if m or n is even then mn is even.

   (e) For the universe of real numbers, $\forall x, \exists y, xy = 1$ is false.

2. Consider the following (correct) argument in which all variables represent integers.

   Suppose n and k are odd.
   Then $n = 2t + 1$ for some integer t, and $k = 2\ell + 1$ for some integer ℓ.
   Hence, $nk = (2t + 1)(2\ell + 1) = 4t\ell + 2t + 2\ell + 1$.
   Therefore, nk is odd.

   (a) Write the implication proved by the argument in plain English.

   (b) Write the contrapositive of the implication in plain English. Is it also proved by the argument?

   (c) Write the converse of your statement in (a). Is it also proved by the argument?

3. Consider the following. All variables represent integers.

   Proposition: If n^2 is a multiple of 8, then n is a multiple of 8.
   Proof: Let $n = 8m$. Then $n^2 = 64m^2 = 8(8m^2)$, which is a multiple of 8, as desired. $\square$.

   Why does the given argument not prove the proposition? Either give a correct proof, or give an example to show that the proposition is false.

4. Explain what is wrong with the following argument which "shows" that *If n is both a multiple of 2 and a multiple of 3, then n is a multiple of 6.*

   Suppose n is a multiple of 6. Then $n = 6k$ for some integer k. Since $6 = 2 \times 3$ we have that $n = 2 \times (3k)$ so it is a multiple of 2, and $n = 3 \times (2k)$, so it is a multiple of 3.

5. Determine if each statement below is true or false, and explain your reasoning.

   (a) When the statement "*There is no largest integer.*" is written is symbols, both of the quantifiers $\forall$ and $\exists$ appear.

   (b) For the universe of real numbers, $\forall x, \exists y, xy = 1$ is false.

   (c) For the universe of integers, $\exists x, (x^2 < 0) \rightarrow (x > 10)$ is true.

6. Let $(0, 1)$ denote the open interval consisting of the real numbers x such that $0 < x < 1$. Consider the statement $\mathcal{A} : \exists x \in (0, 1), \forall y \in (0, 1),\ y \leq x$.

(a) Write $\mathcal{A}$ in English without using symbols except $x,\ y,\ (0,1)$.

(b) Write down the negation of statement $\mathcal{A}$ in symbols without using either of $\neg$ and $\not\leq$.

(c) Show that $\mathcal{A}$ is false.

7. Write each statement in plain English. Do not use any symbols except the letters that denote elements of the universe.

(a) $\forall x, \forall y, (x \neq -y) \rightarrow (x + y) \neq 0$, where the universe is the real numbers.

(b) $\exists s, \forall t, p(s) \wedge [(t \neq s) \rightarrow \neg p(t)]$, where the universe of s and t is the collection of all students who completed Math 122 last fall, and $p(s)$ is the assertion "s got 100% on the final exam".

8. Suppose the universe of m and n is $\{-1, 0, 1\}$. Then, for example,

$$\exists n, n^2 + n > 0 \Leftrightarrow ((-1)^2 + (-1) > 0) \vee (0^2 + 0 > 0) \vee (1^2 + 1 > 0).$$

For each of the following statements,

(*i*) write a compound statement involving neither quantifiers nor variables that is logically equivalent to the given quantified statement,

(*ii*) determine whether the statement is TRUE or FALSE, and

(*iii*) write the negation of the quantified statement in symbols, with quantifiers, and without using negation ($\neg$) or any negated mathematical symbols like $\neq$ or $\not<$.

(a) $\forall n, n^3 - n = 0$

(b) $\exists n, \forall m, n + m < 1$.

9. Write each statement in plain English.

(a) $\neg[\exists x, (p(x) \wedge \neg(q(x)))]$, where the universe of x is all Canadian citizens, $p(x)$ is the statement "x is eligible to vote in a municipal election" and $q(x)$ is the statement "x is 18 years old or older."

(b) $\forall x, [(x \neq \text{ Quebec}) \rightarrow v(x)] \wedge \neg v(\text{Quebec}$, where the universe of x is the collection of all major Canadian cities, and $v(x)$ is the assertion "Gary has visited x."

(c) $\exists s, \forall t, p(s) \wedge [(t \neq s) \rightarrow \neg p(t)]$, where the universe of s and t is the collection of all students who completed Math 122 last fall, and $p(s)$ is the assertion "s got 100% on the final exam."

10. (a) Let n be in integer. Explain what is wrong with the following argument which "shows" that *if n is a multiple of 2 and a multiple of 3, then n is a multiple of 6.*

> Suppose n is a multiple of 6. Then $n = 6k$ for some integer k. Since $6 = 2 \times 3$, we have that $n = 2 \times (3k)$, so it is a multiple of 2, and $n = 3 \times (2k)$, so it is a multiple of 3. $\square$

(b) Give a correct proof of the assertion.

11. (a) Suppose that m and n are integers. It is claimed that the argument below proves that *if mn is odd, then m and n are both odd.* Does it? Explain your reasoning.

Suppose that the integers m and n are both even. Then there exists an integer k such that $m = 2k$, and there exists an integer ℓ such that $n = 2\ell$. Thus,

$$mn = (2k)(2\ell) = 2(2k\ell).$$

Since $2k\ell$ is an integer, mn is even.

12. Write each statement in plain English.

(a) $\forall x, [(x \neq \text{"Quebec"}) \rightarrow v(x)] \wedge \neg v(\text{"Quebec"})$, where the universe of x is the collection of all major Canadian cities, and $v(x)$ is the assertion "Gary has visited x".

(b) $\exists s, \forall t, p(s) \wedge [(t \neq s) \rightarrow \neg p(t)]$, where the universe of s and t is the collection of all students who completed Math 122 last fall, and $p(s)$ is the assertion "s got 100% on the final exam".

13. Suppose the collection of allowed replacements for the variables is the integers. Let $p(n)$ be "*n is even*" and $q(n)$ be "*n is odd*''. Determine the truth value of each statement and provide a brief explanation of your reasoning.

    (a) $\forall n, p(n) \vee q(n)$

    (b) $[\exists n, p(n)] \wedge [\exists n, q(n)]$

    (c) $\exists n, p(n) \rightarrow q(n)$

    (d) $[\forall n, p(n)] \wedge [\forall n, q(n)]$

    (e) $\forall n, \exists m, n + m = 0$

    (f) $\exists n, \forall m, n + m = 0$

14. According to Robert Plant, the original first line of the Led Zepplen song *Stairway to Heaven* was "*There's a lady who knows all is glitters, is gold, and she is buying a stairway to heaven.*" Explain why, when this statement is written in symbols, either 3 or 4 quantifier appear, and the two formulations are logically equivalent.

15. Suppose that the collecton of allowed replacements for the variable p is $\{$*Gary*, *Christi*$\}$ and the collection of allowed replacements for the variable c is $\{$*Whitehorse*, *Ottawa*, *Halifax*$\}$. Let $v(p, c)$ be the statement "p has visited c". Write each statement in symbolic form without quantifiers.

    (a) Christi has visited every city.

    (b) There is a city Gary has not visited.

    (c) For every person there is a city which they have visited.

16. Suppose that the integer a is a multiple of 3, and the integer b is a multiple of 4. Give a direct proof that ab is a multiple of 12.

17. Prove that if the integer n^2 is a multiple of 5, then the integer n is a multiple of 5. (Hint: prove the contrapositive using a proof by cases; there are 4 cases.)

18. Prove that $\sqrt{5}$ is irrational. Can you use essentially the same argument to show that $\sqrt{p}$ is irrational for any prime number p?

19. Let $a, b, c, d \in \mathbb{Z}$. Prove that if $a|b$ and $c|d$, then $ac|bd$.

20. Let $a, b, d \in \mathbb{Z}$. Prove that if $d|a$ and $d|b$, then $d^2|ab$.

21. Let $a, b, c, d \in \mathbb{Z}$, and suppose that $a + b = c$. Prove that if d divides and two of a, b, c, then it also divides the third of these.

22. Prove that if $a|b$, then $\frac{b}{a}|b$. Make sure you are using the definition of the statement "a divides b".

23. For a positive integer n, define n *factorial* to be the integer $n(n-1)(n-2)\cdots 1$.

    (a) Suppose $1 \leq k \leq n$. What are the quotient and remainder when $N = n! + 1$ is divided by k?

    (b) Explain why part (a) implies that N has a prime divisor greater than n.

    (c) Explain why part (b) implies that there are infinitely many prime numbers. (Note that of there are only finitely many prime numbers, then there is a largest prime.)

24. (a) What are the possible remainders when an odd prime number is divided by 4?

    (b) Show that if $a = 4k + 1$ and $b = 4\ell + 1$, then the remainder when ab is divided by 4 equals 1.

    (c) Use part (b) to explain why a number that leaves remainder 3 when divided by 4 must have a positive divisor that leaves remainder 3 when divided by 4. (Note: such a number is odd, so all of its divisors are odd.)

    (d) Suppose $p_1, p_2, \ldots, p_t$ are prime numbers different from 3. For $i = 1, 2, \ldots, t$, what is the remainder when $N = 4p_1p_2\cdots p_t + 3$ is divided by p_i? (It is the same answer in each case.)

    (e) Use (c) and (d) above, and the same ideas as in Euclid's proof of the infinitude of primes, to show that there are infinitely many primes that leave remainder 3 when divided by 4.

25. Let $a, b, d \in \mathbb{Z}$. Suppose that $d|ab$. Is it always true that $d|a$ or $d|b$? Give a proof or counterexample, as appropriate.