Method of proof

Part 1

Assumptions

- In this text we assume a familiarity with the laws of basic algebra.
- We also use the three properties of equality: For all objects *A*, *B*, and *C*,
  (1) $A = A$,
  (2) if $A = B$, then $B = A$, and
  (3) if $A = B$ and $B = C$, then $A = C$.
- And we use the principle of substitution: For all objects *A* and *B*, if $A = B$, then we may substitute *B* wherever we have *A*.
- In addition, we assume that there is no integer between 0 and 1 and that the set of all integers is closed under addition, subtraction, and multiplication. This means that sums, differences, and products of integers are integers.

Definition:

An integer n is ***even*** if, and only if, n equals twice some integer. An integer n is ***odd*** if, and only if, n equals twice some integer plus 1.

Symbolically, if n is an integer, then

$$n \text{ is even} \Leftrightarrow \exists \text{ an integer } k \text{ such that } n = 2k.$$

$$n \text{ is odd} \Leftrightarrow \exists \text{ an integer } k \text{ such that } n = 2k + 1.$$

Definition:

An integer n is ***prime*** if, and only if, $n > 1$ and for all positive integers r and s, if $n = rs$, then either r or s equals n.

An integer n is ***composite*** if, and only if, $n > 1$ and $n = rs$ for some integers r and s with $1 < r < n$ and $1 < s < n$.

In symbols:

n is prime $\Leftrightarrow$ $\forall$ positive integers r and s, if $n = rs$ then either r = 1 and s = n or r = n and s = 1.

n is composite $\Leftrightarrow$ $\exists$ positive integers r and s such that $n = rs$ and $1 < r < n$ and $1 < s < n$.

Is every integer greater than 1 either prime or composite?

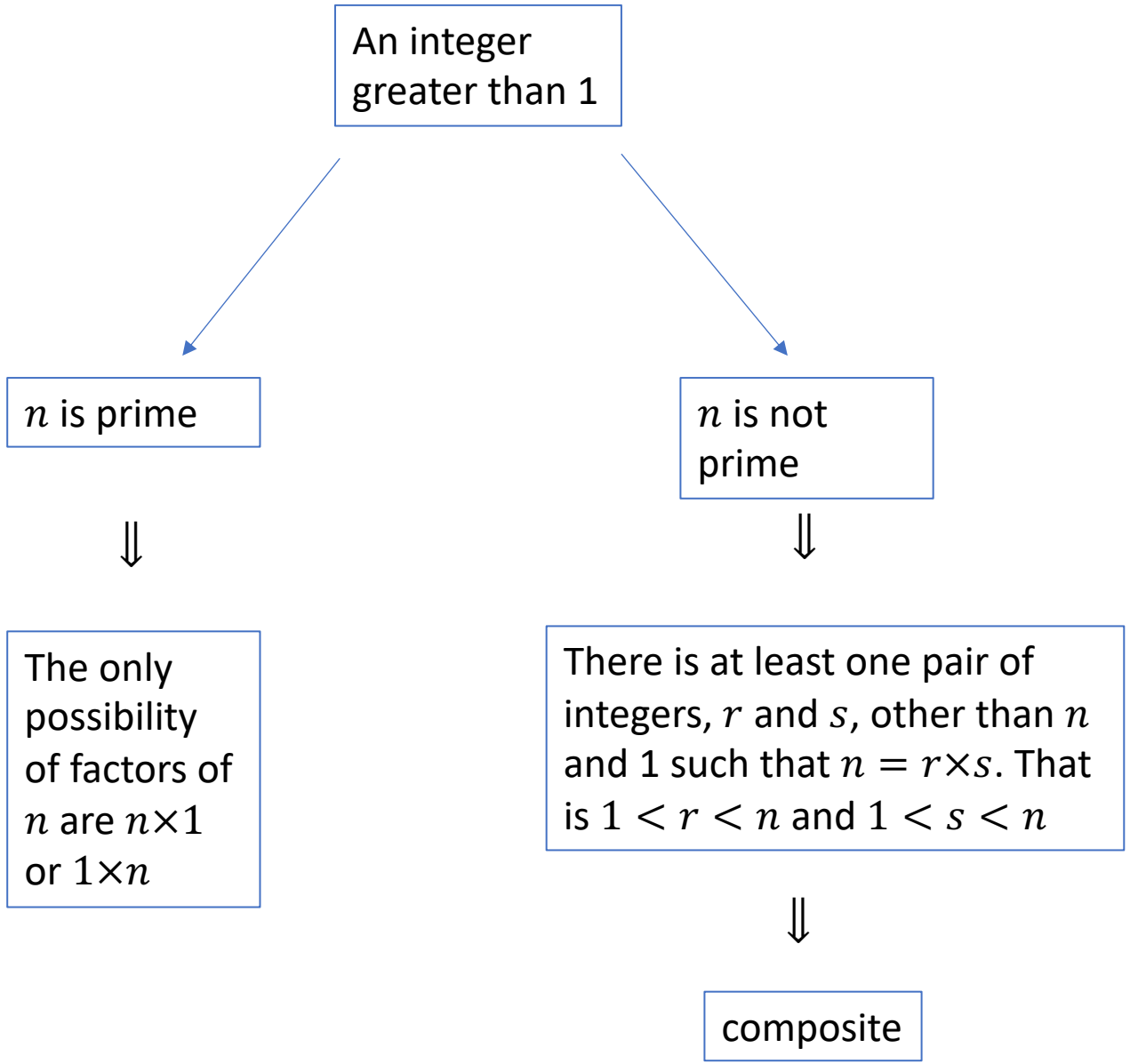
Yes. Let n be any integer that is greater than 1. Consider all pairs of positive integers r and s such that $n=rs$. There exist at least two such pairs, namely,

$$r=n \text{ and } s=1$$

and

$$r=1 \text{ and } s=n.$$

Moreover, since $n=rs$, all such pairs satisfy the inequalities $1 \leq r \leq n$ and $1 \leq s \leq n$. If n is prime, then these two pairs are the only ways to write n as rs. Otherwise, there exists a pair of positive integers r and s such that $n=rs$ and neither r nor s equals either 1 or n. Therefore, in this case $1<r<n$ and $1<s<n$, and hence n is composite.


An integer greater than 1
n is prime
n is not prime
The only possibility of factors of n are $n \times 1$ or $1 \times n$
There is at least one pair of integers, r and s, other than n and 1 such that $n = r \times s$. That is $1 < r < n$ and $1 < s < n$
composite

Proving Existential Statements

A statement in the form

$$\exists x \in D \text{ such that } Q(x)$$

is true if, and only if,

$$Q(x) \text{ is true for at least one } x \text{ in } D.$$

There are two methods of proving an existential statement,

1) constructive proofs of existence, and
2) non-constructive proofs of existence.

1) Constructive proofs of existence

- One way to prove this is to find an x in D that makes $Q(x)$ true.
- Another way is to give a set of directions for finding such an x.

Both methods are called constructive proofs of existence.

Example

Prove the following:

∃ an even integer n that can be written in two ways as a sum of two prime numbers.

Solution

Let $n = 10$. Then $10 = 5 + 5 = 3 + 7$ and $3,\ 5$, and 7 are all prime numbers.

Example:

Suppose that r and s are integers. Prove the following:

$$\exists \text{ an integer } k \text{ such that } 22r + 18s = 2k.$$

Solution:

Let $k = 11r + 9s$. Then k is an integer because it is a sum of products of integers; and by substitution, $2k = 2(11r + 9s)$, which equals $22r + 18s$ by the distributive law of algebra.

2) Non-constructive proof of existence

A nonconstructive proof of existence involves showing either

(a) that the existence of a value of x that makes $Q(x)$ true is guaranteed by an axiom or a previously proved theorem or

(b) that the assumption that there is no such x leads to a contradiction.

Example:

Consider the function $f(x) = x^3 - 2x - 4$. Prove that there exists a real number r such that $2 < r < 3$ and $f(r) = 0$.

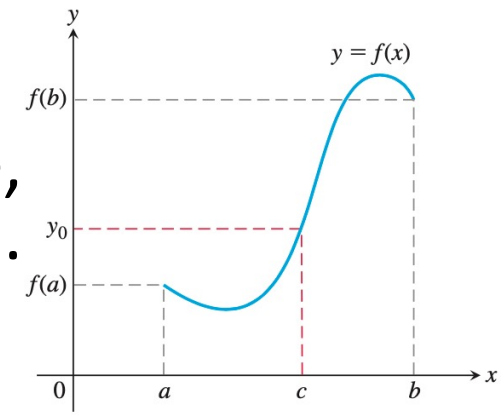
Solution

The intermediate value theorem states the following:

Consider an interval $I = [a, b]$ in $\mathbb{R}$ and a continuous function $f: I \to \mathbb{R}$. Then

$\forall\ u$ a number between $f(a)$ and $f(b)$, $\exists$ is a $c \in (a, b)$ such that $f(c) = u$.

Since, $f(2) = -4$ and $f(3) = 5$, $0 \in [f(2), f(3)]$. Therefore, intermediate value theorem, $\exists\ r \in (2, 3)$ such that $f(r) = 0$.



Disproving Universal Statements by Counterexample

To disprove a statement of the form

$$\text{“}\forall x \in D\text{, if } P(x) \text{ then } Q(x)\text{,”}$$

find a value of x in D for which the hypothesis $P(x)$ is true and the conclusion $Q(x)$ is false. Such an x is called a counterexample. This means, there must be an example proving the negation of the statement, that is

$$\exists x \in D \text{ such that } P(x) \text{ and not } Q(x)$$

Example: Disproof by Counterexample

Disprove the following statement by finding a counterexample:

$$\forall \text{ real numbers } a \text{ and } b, \text{ if } a^2 = b^2 \text{ then } a = b.$$

Proving Universal Statements

Most mathematical statements to be proved are universal. In discussing how to prove such statements, it is helpful to imagine them in a standard form:

$$\forall x \in D, \text{ if } P(x) \text{ then } Q(x).$$

1) Method of exhaustion

When D is finite or when only a finite number of elements satisfy $P(x)$, such a statement can be proved by the *method of exhaustion*.

Example:

Use the method of exhaustion to prove the following statement:

$\forall n \in Z$, if n is even and $4 \leq n \leq 26$, then n can be written as a sum of two prime numbers.

Solution

4 = 2+2, 6 = 3+3, 8 = 3 + 5, 10 = 5 + 5, $P(x) \rightarrow Q(x)$
12=5+7, 14=11+3, 16=5+11, 18=7+11,
20=7+13, 22=5+17, 24=5+19, 26=7+19.

2) Method of Generalizing from the Generic Particular

The most powerful technique for proving a universal statement is one that works regardless of the size of the domain over which the statement is quantified. It is called *the method of generalizing from the generic particular*.

To show that every element of a set satisfies a certain property, suppose x is a particular but arbitrarily chosen element of the set, and show that x satisfies the property.

Example:

The difference of the squares of any two consecutive integers is odd.

Proof:

The formal version of the statement is,

$$\forall x \in \mathbb{Z}, x^2 - (x+1)^2 \text{ is odd.}$$

Let x be a particular but arbitrarily chosen integer, then

$$x^2 - (x+1)^2 = x^2 - x^2 - 2x - 1 = -2x - 1 = 2(-x-1) + 1 = 2k + 1,$$

where $k \in \mathbb{Z}$ because sum and product of int is int. Therefore $x^2 - (x+1)^2$ is an odd integer.

3) The Method of Direct Proof

When the method of generalizing from the generic particular is applied to a property of the form

"If $P(x)$ then $Q(x)$,"

the result is the method of direct proof.

Method of Direct Proof

1. Express the statement to be proved in the form "$\forall x \in D$, if $P(x)$ then $Q(x)$." (This step is often done mentally.)
2. Start the proof by supposing x is a particular but arbitrarily chosen element of D for which the hypothesis $P(x)$ is true. (This step is often abbreviated "Suppose $x \in D$ and $P(x)$.")
3. Show that the conclusion $Q(x)$ is true by using definitions, previously established results, and the rules for logical inference.

Example: The sum of any two even integers is even.

Proof:

$$\forall\, m, n \in \mathbb{Z}, \text{if } m \text{ and } n \text{ are even then } m + n \text{ is even}$$

Suppose m and n are [particular but arbitrarily chosen] even integers. [We must show that $m + n$ is even.] By the definition of even, $m = 2r$ and $n = 2s$ for some integers r and s. Then

$$m + n = 2r + 2s \qquad \text{by substitution}$$

$$= 2(r + s) \qquad \text{by factoring out a 2.}$$

Let $t = r + s$. Note that t is an integer because it is a sum of integers. Hence $m + n = 2t$ where t is an integer.

It follows by the definition of even that $m + n$ is even.

Showing That an Existential Statement Is False

Recall that the negation of an existential statement is universal. It follows that to prove an existential statement is false, you must prove a universal statement (its negation) is true.

Example: Disproving an Existential Statement

Show that the following statement is false:

There is a positive integer n such that $n^2 + 3n + 2$ is prime.

Solution

Proving that the given statement is false is equivalent to proving its negation is true. The negation is

For all positive integers n, $n^2 + 3n + 2$ is not prime.

Because the negation is universal, it is proved by generalizing from the generic particular.

Claim: The statement "There is a positive integer n such that $n^2 + 3n + 2$ is prime" is false.

Example: Disproving an Existential Statement

Claim: The statement "There is a positive integer n such that $n^2 + 3n + 2$ is prime" is false.

Proof:

Suppose n is any [particular but arbitrarily chosen] positive integer. [We will show that $n^2 + 3n + 2$ is not prime.]

We can factor $n^2 + 3n + 2$ to obtain $n^2 + 3n + 2 = (n + 1)(n + 2)$. We also note that $n + 1$ and $n + 2$ are integers (because they are sums of integers) and that both $n + 1 > 1$ and $n + 2 > 1$ (because $n \geq 1$). Thus $n^2 + 3n + 2$ is a product of two integers each greater than 1, and so $n^2 + 3n + 2$ is not prime. ■

Directions for Writing Proofs of Universal Statements

Over the years, the following rules of style have become fairly standard for writing the final versions of proofs:

1. Copy the statement of the theorem to be proved on your paper.
2. Clearly mark the beginning of your proof with the word Proof.
3. Make your proof self-contained.
4. Write your proof in complete, grammatically correct sentences.
5. Keep your reader informed about the status of each statement in your proof.
6. Give a reason for each assertion in your proof.
7. Include the “little words and phrases” that make the logic of your arguments clear.
8. Display equations and inequalities.

Common Mistakes

The following are some of the most common mistakes people make when writing mathematical proofs.

1) Arguing from examples.

Looking at examples is one of the most helpful practices a problem solver can engage in and is encouraged by all good mathematics teachers. However, it is a mistake to think that a general statement can be proved by showing it to be true for some special cases. A property referred to in a universal statement may be true in many instances without being true in general.

1) Arguing from examples.

Looking at examples is one of the most helpful practices a problem solver can engage in and is encouraged by all good mathematics teachers. However, it is a mistake to think that a general statement can be proved by showing it to be true for some special cases. A property referred to in a universal statement may be true in many instances without being true in general.
Example:
It is an incorrect "proof" of the fact that the sum of any two even integers is even.
"This is true because if $m = 14$ and $n = 6$, which are both even, then $m + n = 20$, which is also even."
In this example, it is not sufficient to show that the conclusion "$m + n$ is even" is true for $m = 14$ and $n = 6$. You must give an argument to show that the conclusion is true for any even integers m and n.

2) Using the same letter to mean two different things.

Some beginning theorem provers give a new variable quantity the same letter name as a previously introduced variable.

2) Using the same letter to mean two different things.

Some beginning theorem provers give a new variable quantity the same letter name as a previously introduced variable. Consider the following "proof" fragment:
Suppose m and n are any odd integers. Then by definition of odd,

$m = 2k + 1$ and $n = 2k + 1$ for some integer k.

2) Using the same letter to mean two different things.

Some beginning theorem provers give a new variable quantity the same letter name as a previously introduced variable. Consider the following "proof" fragment:

Suppose m and n are any odd integers. Then by definition of odd,

$m = 2k + 1$ and $n = 2k + 1$ for some integer k.

This is incorrect. Using the same symbol, k, in the expressions for both m and n implies that $m = 2k + 1 = n$. It follows that the rest of the proof applies only to integers m and n that equal each other. This is inconsistent with the supposition that m and n are arbitrarily chosen odd integers. For instance, the proof would not show that the sum of 3 and 5 is even.

3) Jumping to a conclusion.

To jump to a conclusion means to allege the truth of something without giving an adequate reason. Consider the following “proof” that the sum of any two even integers is even.

3) Jumping to a conclusion.

To jump to a conclusion means to allege the truth of something without giving an adequate reason. Consider the following “proof” that the sum of any two even integers is even.

Suppose m and n are any even integers. By definition of even, $m = 2r$ and

$n = 2s$ for some integers r and s. Then

$$m + n = 2r + 2s.$$

So $m + n$ is even.

3) Jumping to a conclusion.

To jump to a conclusion means to allege the truth of something without giving an adequate reason. Consider the following "proof" that the sum of any two even integers is even.

Suppose m and n are any even integers. By definition of even, $m = 2r$ and

$n = 2s$ for some integers r and s. Then

$$m + n = 2r + 2s.$$

So $m + n$ is even.

The problem with this "proof" is that the crucial calculation $2r + 2s = 2(r + s)$ is missing. The author of the "proof" has jumped prematurely to a conclusion.

4) Circular reasoning.

To engage in circular reasoning means to assume what is to be proved; it is a variation of jumping to a conclusion. As an example, consider the following “proof” of the fact that the product of any two odd integers is odd:

4) Circular reasoning.

To engage in circular reasoning means to assume what is to be proved; it is a variation of jumping to a conclusion. As an example, consider the following “proof” of the fact that the product of any two odd integers is odd:
Suppose m and n are any odd integers. When any odd integers are multiplied, their product is odd. Hence mn is odd.

5) Confusion between what is known and what is still to be shown.

A more subtle way to engage in circular reasoning occurs when the conclusion to be shown is restated using a variable. Here is an example in a “proof” that the product of any two odd integers is odd:

5) Confusion between what is known and what is still to be shown.

A more subtle way to engage in circular reasoning occurs when the conclusion to be shown is restated using a variable. Here is an example in a "proof" that the product of any two odd integers is odd:
Suppose m and n are any odd integers. We must show that mn is odd. This means that there exists an integer s such that

$$mn = 2s + 1.$$

Also by definition of odd, there exist integers a and b such that
$m = 2a + 1 \; and \; n = 2b + 1$. Then

$$mn = (2a + 1)(2b + 1) = 2s + 1.$$

So, since s is an integer, mn is odd by definition of odd.

5) Confusion between what is known and what is still to be shown.

A more subtle way to engage in circular reasoning occurs when the conclusion to be shown is restated using a variable. Here is an example in a "proof" that the product of any two odd integers is odd:
Suppose m and n are any odd integers. We must show that mn is odd. This means that there exists an integer s such that

$$mn = 2s + 1.$$

Also by definition of odd, there exist integers a and b such that
$m = 2a + 1 \; and \; n = 2b + 1$. Then

$$mn = (2a + 1)(2b + 1) = 2s + 1.$$

So, since s is an integer, mn is odd by definition of odd.
In this example, when the author restated the conclusion to be shown (that mn is odd), the author wrote "there exists an integer s such that $mn = 2s + 1$." Later the author jumped to an unjustified conclusion by assuming the existence of this s when that had not, in fact, been established. This mistake might have been avoided if the author had written "This means that we must show that there exists an integer s such that $mn = 2s + 1$.

5) Confusion between what is known and what is still to be shown.

A more subtle way to engage in circular reasoning occurs when the conclusion to be shown is restated using a variable. Here is an example in a "proof" that the product of any two odd integers is odd:
Suppose m and n are any odd integers. We must show that mn is odd. This means that there exists an integer s such that

$$mn = 2s + 1.$$

Also by definition of odd, there exist integers a and b such that
$m = 2a + 1 \; and \; n = 2b + 1$. Then

$$mn = (2a + 1)(2b + 1) = 2s + 1.$$

So, since s is an integer, mn is odd by definition of odd.
In this example, when the author restated the conclusion to be shown (that mn is odd), the author wrote "there exists an integer s such that $mn = 2s + 1$." Later the author jumped to an unjustified conclusion by assuming the existence of this s when that had not, in fact, been established. This mistake might have been avoided if the author had written "This means that we must show that there exists an integer s such that $mn = 2s + 1$.
An even better way to avoid this kind of error is not to introduce a variable into a proof unless it is either part of the hypothesis or deducible from it.

6) Use of any rather than some.

There are a few situations in which the words any and some can be used inter-changeably. For instance, in starting a proof that the square of any odd integer is odd, one could correctly write “Suppose m is any odd integer” or “Suppose m is some odd integer.” In most situations, however, the words any and some are not interchangeable. Here is the start of a “proof” that the square of any odd integer is odd, which uses any when the correct word is some:

6) Use of any rather than some.

There are a few situations in which the words any and some can be used inter-changeably. For instance, in starting a proof that the square of any odd integer is odd, one could correctly write “Suppose m is any odd integer” or “Suppose m is some odd integer.” In most situations, however, the words any and some are not interchangeable. Here is the start of a “proof” that the square of any odd integer is odd, which uses any when the correct word is some:
Suppose m is a particular but arbitrarily chosen odd integer. By definition of odd, $m = 2a + 1$ for any integer a.

6) Use of any rather than some.

There are a few situations in which the words any and some can be used inter-changeably. For instance, in starting a proof that the square of any odd integer is odd, one could correctly write "Suppose m is any odd integer" or "Suppose m is some odd integer." In most situations, however, the words any and some are not interchangeable. Here is the start of a "proof" that the square of any odd integer is odd, which uses any when the correct word is some:

Suppose m is a particular but arbitrarily chosen odd integer. By definition of odd, $m = 2a + 1$ for any integer a.

In the second sentence it is incorrect to say that "$m = 2a + 1$ for any integer a" because a cannot be just "any" integer; in fact, solving $m = 2a + 1$ for a shows that the only possible value for a is $(m - 1)/2$. The correct way to finish the second sentence is, "$m = 2a + 1$ for some integer a" or "there exists an integer a such that $m = 2a + 1$."

7) Misuse of the word if.

Another common error is not serious in itself, but it reflects imprecise thinking that sometimes leads to problems later in a proof. This error involves using the word if when the word because is really meant. Consider the following proof fragment:

7) Misuse of the word if.

Another common error is not serious in itself, but it reflects imprecise thinking that sometimes leads to problems later in a proof. This error involves using the word if when the word because is really meant. Consider the following proof fragment:
Suppose p is a prime number. If p is prime, then p cannot be written as a product of two smaller positive integers.

7) Misuse of the word if.

Another common error is not serious in itself, but it reflects imprecise thinking that sometimes leads to problems later in a proof. This error involves using the word if when the word because is really meant. Consider the following proof fragment:
Suppose p is a prime number. If p is prime, then p cannot be written as a product of two smaller positive integers.
The use of the word if in the second sentence is inappropriate. It suggests that the primeness of p is in doubt. But p is known to be prime by the first sentence. It cannot be written as a product of two smaller positive integers because it is prime. Here is a correct version of the fragment:

7) Misuse of the word if.

Another common error is not serious in itself, but it reflects imprecise thinking that sometimes leads to problems later in a proof. This error involves using the word if when the word because is really meant. Consider the following proof fragment:
Suppose p is a prime number. If p is prime, then p cannot be written as a product of two smaller positive integers.
The use of the word if in the second sentence is inappropriate. It suggests that the primeness of p is in doubt. But p is known to be prime by the first sentence. It cannot be written as a product of two smaller positive integers because it is prime. Here is a correct version of the fragment:
Suppose p is a prime number. Because p is prime, p cannot be written as a product of two smaller positive integers.

Fill in the Blanks for a Proof

Theorem: For all integers r and s, if r is even and s is odd then $3r + 2s$ is even

Proof: Suppose r and s are any *[particular but arbitrarily chosen]* integers such that r is even and s is odd.

[We must show that $3r + 2s$ is even.]

By_____ , $r = 2m$ and $s = 2n + 1$ for some integers m and n.

Then

$$3r + 2s = 3(2m) + 2(2n + 1) \quad \text{by } \_\_\_\_\_$$

$$= 6m + 4n + 2 \quad \text{by multiplying out}$$

$$= 2(3m + 2n + 1) \quad \text{by factoring out 2}$$

Let $t = 3m + 2n + 1$.

Then t is an integer because *m*, *n*, 3, 2, and 1 are integers and because _____. Hence $3r + 2s = 2t$, where t is an integer, and so by_____, $3r + 2s$ is even *[as was to be shown].*

Prove or disprove the following:

1. For every integer p, if p is prime then $p^2 + 1$ is even.

2. For every integer n, if n is odd then $\frac{n^2-1}{2}$ is odd.

3. There is a perfect square that can be written as a sum of two other perfect squares.

Disprove:∃ an integer n, such that, $6n^2 + 27$ is prime.

Negation is

Disprove:∃ an integer n, such that, $6n^2 + 27$ is prime.

Negation is

$$\forall \text{ integer } n, 6n^2 + 27 \text{ is not prime.}$$

Disprove:∃ an integer n, such that, $6n^2 + 27$ is prime.

Negation is

$$\forall \text{ integer } n, 6n^2 + 27 \text{ is not prime.}$$

Factorize:

$$6n^2 + 27 = 3(2n^2 + 9)$$

For a particular but arbitrarily chosen integer n

Disprove:∃ an integer n, such that, $6n^2 + 27$ is prime.

Negation is

$$\forall \text{ integer } n, 6n^2 + 27 \text{ is not prime.}$$

Factorize:

$$6n^2 + 27 = 3(2n^2 + 9)$$

For a particular but arbitrarily chosen integer n

Then, $2n^2 + 9$ cannot be equal to 1.

Disprove:∃ an integer n, such that, $6n^2 + 27$ is prime.

Negation is

$$\forall \text{ integer } n, 6n^2 + 27 \text{ is not prime.}$$

Factorize:

$$6n^2 + 27 = 3(2n^2 + 9)$$

For a particular but arbitrarily chosen integer n

Then, $2n^2 + 9$ cannot be equal to 1. Because if so, then

$$2n^2 + 9 = 1$$

Which gives,

$$n^2 = -\frac{8}{2} = -4$$

Not possible.

Disprove:∃ an integer n, such that, $6n^2 + 27$ is prime.

Negation is

$$\forall \text{ integer } n, 6n^2 + 27 \text{ is not prime.}$$

Factorize:

$$6n^2 + 27 = 3(2n^2 + 9)$$

For a particular but arbitrarily chosen integer n

Then, $2n^2 + 9$ cannot be equal to 1. Because if so, then

$$2n^2 + 9 = 1$$

Which gives,

$$n^2 = -\frac{8}{2} = -4$$

Not possible.

Therefore, $6n^2 + 27$ is not prime for any integer n.

Example:

Prove that

For all integers n and m, if $n - m$ is even then $n^3 - m^3$ iseven.

Exercise:

1. Prove that the following statement is false
   ∃ an integer n, such that, $6n^2 + 27$ is prime.
2. Find counter example of the statement:
   "For all integers m and n, if $2m + n$ is odd then m and n both are odd."
3. There is an integer n such that $2n^2 - 5n + 2$ is prime.
4. There is an integer m and n such that $m > 1$ and $n > 1$ and $\frac{1}{m} + \frac{1}{n}$ is an integer.
5. There are distinct integers m and n such that $\frac{1}{m} + \frac{1}{n}$ is an integer.
6. Prove that for all integer n and m, if $n - m$ is even then $n^3 - m^3$ is even.

Example:

For every integer n, $n^2 - n + 11$ is a prime number.