3 Theorems and Proofs

A *theorem* is any mathematical statement, such as a formula of first-order logic, that has been proved true. When you are about to prove a theorem, you call it theorem as a way of promising that a proof is about to be produced.

3.1 What is a proof?

There are many different precise definitions of a proof. But most mathematicians accept an informal definition: a proof is a clear and unambiguous argument that a mathematical statement is true that any sufficiently knowledgeable person can check. The key is that a reader must be able to check that each step is correct.

Students who are just learning to do proofs make many different kinds of mistakes, but most fall into one of the following two categories.

1. **The student does not check his or her own work.** The reason can vary from lack of time to lack of understanding to fear of failure.

   A student might take a proof of something else from a book or from notes and make some modifications to it, and then *hope* that the modifications have produced a correct proof, without checking whether that is true. The student who has a lack of understanding cannot check the proof. The student who is afraid of failure will not check the proof out of fear that it might turn out to be incorrect.

   Regardless of your reason for not checking your proof, you can be sure that an unchecked proof is incorrect, for the same reasons that an untested computer program does not work. You will need to find a way to motivate yourself to check your proofs carefully.

2. Mathematics relies on precise definitions. When you do a proof, it is essential for you to use definitions wherever appropriate. **Students often get stuck in a proof because they have forgotten to use definitions**. Any time you cannot see how to proceed, ask yourself if using a definition will help. We will do many examples of that.

3.2 Forward proofs

A *forward proof* reasons from what you know to what you can conclude. Each new conclusion relies on prior knowledge or conclusions.

You have probably been taught a different approach in an algebra class. In a *backwards proof*, you write down what you want to show and then perform some manipulations on it, working backwards to a statement that you already know is true.

In this class, we will do forward proofs, with minor excursions using backwards reasoning. **I expect you to use forward proofs as well.** At least for this class, put aside the backwards proofs that you have learned in algebra.

In this section, I do proofs at two different levels of detail. One of the proof works in small steps and shows everything that you know after each step. The other proof is more typical of what you would write, and what I want to see from you.

3.3 Some definitions

Definition 3.1. Integer n is *even* if there exists an integer m such that $n = 2m$. For example, 6 is even because $6 = (2)(3)$.

Definition 3.2. Integer n is *odd* if there exists an integer m such that $n = 2m + 1$. We will also make use of the fact that, for every n, n is odd if and only if n is not even.

Definition 3.3. Integer n is a *perfect square* if there exists an integer m such that $n = m^2$.

Definition 3.4. Real number x is *rational* if there exist integers n and m where $m \neq 0$ such that $x = n/m$.

3.4 Proof techniques

The remaining subsections discuss common ways of proving particular kinds of first-order formulas.

3.5 Proving $A \to B$

To prove $A \to B$, assume that A is true and show that B is true.

Theorem 3.1. If n is even then n^2 is even.

Detailed Proof.

1. Suppose that n is even.

Known variables:	n
Know:	n is even.
Goal:	n^2 is even.

2. By the definition of an even integer, there exists an integer m such that $n = 2m$.

Known variables:	n, m
Know:	n is even.
Know:	$n = 2m$.
Goal:	n^2 is even.

3. Since $n = 2m$, $n^2 = (2m)^2 = 4m^2 = 2(2m^2)$.

Known variables:	n, m
Know:	n is even.
Know:	$n = 2m$.
Know:	$n^2 = 2(2m^2)$.
Goal:	n^2 is even.

4. So $n^2 = 2(x)$ where $x = 2m^2$. Using the definition of an even number again, n^2 is even.

♢———————————————————————————————♢

Typical Proof. Suppose n is even. By the definition of an even integer, there is an integer m such that $n = 2m$. So

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

By the definition of an even integer, n^2 is even.

♢———————————————————————————————♢

Theorem 3.2. If n and m are perfect squares then nm is a perfect square.

Detailed Proof.

1. Suppose that n and m are perfect squares.

Known variables:	n, m
Know:	n is a perfect square.
Know:	m is a perfect square.
Goal:	nm is a perfect square.

2. By the definition of a perfect square, there exist integers x and y such that $n = x^2$ and $m = y^2$.

Known variables:	n, m, x, y
Know:	$n = x^2$.
Know:	$m = y^2$.
Goal:	nm is a perfect square.

3. Replacing n by x^2 and m by y^2, $nm = x^2y^2 = (xy)^2$.

Known variables:	n, m, x, y
Know:	$n = x^2$.
Know:	$m = y^2$.
Know:	$nm = (xy)^2$.
Goal:	nm is a perfect square.

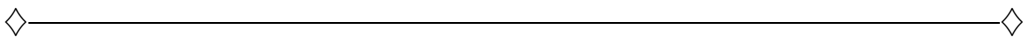
4. So $nm = z^2$ where $z = xy$. Using the definition of a perfect square again, nm is perfect square.

♢———————————————————————————————♢

Typical Proof. Suppose that n and m are perfect squares. By the definition of a perfect square, there exist integers x and y such that $n = x^2$ and $m = y^2$. Replacing n by x^2 and m by y^2,

$$nm = x^2y^2 = (xy)^2.$$

So nm is a perfect square.



3.5.1 Using the contrapositive

You can prove any theorem by proving an equivalent mathematical statement. For example, you can prove $A \to B$ by proving equivalent formula $\neg B \to \neg A$, which is called the *contrapositive* of $A \to B$. Here is an example.

Theorem 3.3. Suppose n is an integer. If $3n + 2$ is odd, then n is odd.

Detailed Proof. We prove the contrapositive: If n is not odd then $3n + 2$ is not odd.

1. We know that an integer x is even if and only if x is not odd. So what we want to prove is equivalent to: If n is even then $3n + 2$ is even.

Known variables:	n
Goal:	If n is even then $3n + 2$ is even.

2. Suppose that n is even.

Known variables:	n
Know:	n is even.
Goal:	$3n + 2$ is even.

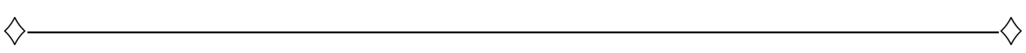
3. By the definition of an even integer, there exists an integer m such that $n = 2m$.

Known variables:	n, m
Know:	$n = 2m$.
Goal:	$3n + 2$ is even.

4. $3n + 2 = 3(2m) + 2 = 6m + 2 = 2(3m + 1)$.

Known variables:	n, m
Know:	$n = 2m$.
Know:	$3n + 2 = 2(3m + 1)$.
Goal:	$3n + 2$ is even.

5. Using the definition of an even integer again, $3n + 2$ is even because $3n + 2 = 2z$ where $z = 3m + 1$.

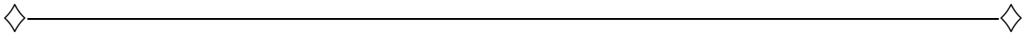


Typical Proof. We prove the contrapositive: If n even then $3n + 2$ is even.

Suppose n is even. Then there exists an integer m such that $n = 2m$.

$$3n + 2 = 3(2m) + 2 = 6m + 2 = 2(3m + 1).$$

Since $3n + 2$ is twice an integer, $3n + 2$ is even.



3.6 Proving and using $A \wedge B$

To prove $A \wedge B$, prove A and prove B.

If you know that $A \wedge B$ is true, then you know that A is true and you know that B is true.

3.7 Proving and using $\neg(A)$

To prove $\neg(A)$, you typically use DeMorgan's laws and the laws for negating quantified formulas to push the negation inward. For example, to prove $\neg(A \wedge B)$, you prove equivalent formula $\neg A \vee \neg B$. To prove $\neg(\forall x A)$, you prove equivalent formula $\exists x(\neg A)$.

The same principle applies when you already know $\neg(A)$. For example, if you know $\neg(A \to B)$, you can conclude equivalent formula $A \wedge \neg B$. You write that down as an additional known fact.

3.8 Proving and using $A \vee B$

To prove $A \vee B$, you usually prove one of the equivalent formulas $\neg A \to B$ or $\neg B \to A$.

Suppose that you know that $A \vee B$ is true and you want to use that to show that C is true. That is, you want to show that $A \vee B \to C$ is true. You typically prove equivalent formula

$$A \to C \ \wedge \ B \to C.$$

That is called *proof by cases*. First, you assume that A is true and show that C is true. Next, you assume that B is true and show that C is true. See Section 3.

3.9 Proving and using $\exists x A$

To prove that something exists, produce it.

Theorem 3.4. There exists an integer n where n is even and n is prime.

Proof. Choose $n = 2$. Notice that n is even and n is prime.

♢———————————————————————————♢

3.9.1 Using existential knowledge

Sometimes, instead of needing to prove $\exists x P(x)$, you already know $\exists x P(x)$. What do you do? You ask somebody else to give you a value x so that $P(x)$ is true. It is not necessary for you to say how to find x. We will encounter many examples of that.

3.10 Proving $\forall x A$

To prove $\forall x P(x)$, prove $P(x)$ for an *arbitrary* value of x.

That does not mean that you can choose the value of x. Rather, someone else chooses x and you must prove that $P(x)$ is true for that value of x. Think of it as a challenge. You say to someone else, give me any value of x that you

like. I will prove that $P(x)$ is true. In mathematics, *arbitrary* always means a value chosen by someone else.

We have actually used this idea above. When the statement of a theorem involves unbound variables, it is assumed to be saying that the statement is true for all values of those variables. Here is the first proof above with the quantifier explicit. The universe of discourse is the set of all integers.

Theorem 3.5. $\forall n(n \text{ is even} \to n^2 \text{ is even})$.

Detailed Proof.

1. Ask someone else to select an arbitrary integer n. (We cannot assume anything about n except that it belongs to the universe of discourse.) We must prove: (n is even $\to n^2$ is even) for that n.

Known variables:	n
Goal:	n is even $\to n^2$ is even.

2. Suppose that n is even.

Known variables:	n
Know:	n is even.
Goal:	n^2 is even.

3. By the definition of an even integer, there exists an integer m such that $n = 2m$.

Known variables:	n
Know:	$\exists m(n = 2m)$.
Goal:	n^2 is even.

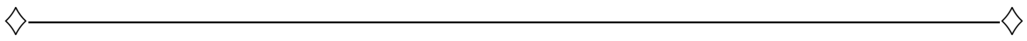
4. Ask someone else to provide the integer m that is asserted to exist.

Known variables:	n, m
Know:	$n = 2m$.
Goal:	n^2 is even.

5. Since $n = 2m$, $n^2 = (2m)^2 = 4m^2 = 2(2m^2)$.

Known variables:	n, m
Know:	$n = 2m$.
Know:	$n^2 = 2(2m^2)$.
Goal:	n^2 is even.

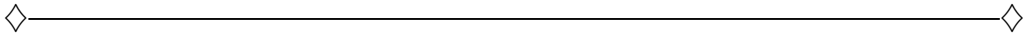
6. So $n = 2(x)$ where $x = 2m^2$. Using the definition of an even number again, n is even.



Typical Proof. Let n be an arbitry even integer. By the definition of an even integer, there exists an integer m such that $n = 2m$. So

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

Evidently, n^2 is even.



3.10.1 Proof by contradiction

You can prove any theorem by proving an equivalent theorem. We have seen propositional tautology

$$P \equiv (\neg P \to \mathbf{F}).$$

That is, to prove P, assume that P is false and prove that **F** is true. That is called *proof by contradiction*. Let's use proof by contradition to reprove a theorem that we proved above.

Theorem 3.6. For every integer n, if $3n + 2$ is odd, then n is odd.

Detailed Proof.

1. Reasoning by contradiction, we can assume the theorem is false and prove **F**. That is:

Know:	$\neg\forall n(3n + 2$ is odd $\to n$ is odd$)$.
Goal:	**F**.

2. We can push the negation across the quantifier using valid formula $\neg\forall x A \equiv \exists x(\neg A))$.

Know:	$\exists n(\neg(3n+2 \text{ is odd } \rightarrow n \text{ is odd}))$.
Goal:	**F**.

3. Now use the tautology that $\neg(P \rightarrow Q) \equiv P \wedge \neg Q)$.

Know:	$\exists n(3n+2 \text{ is odd } \wedge n \text{ is even})$.
Goal:	**F**.

4. Ask somebody else to select an integer n such that $3n+2$ is odd and n is even.

Known variables:	n
Know:	$3n+2$ is odd.
Know:	n is even.
Goal:	**F**.

5. By the definition of an even integer, saying that n is even is equivalent to saying that there exists an integer m such that $n = 2m$. (Existential information is useful because it allows you to get something in hand, as is done in the next step. So you often want to exploit existential information.)

Known variables:	n
Know:	$3n+2$ is odd.
Know:	$\exists m(n = 2m)$.
Goal:	**F**.

6. Since we know that an integer m exists such that $n = 2m$, we can ask somebody else to give us such an m. Let's do that.

Known variables:	n, m
Know:	$3n+2$ is odd.
Know:	$n = 2m$.
Goal:	**F**.

7. Since we know that $n = 2m$, it seems reasonable to substitute $2m$ for n in expression $3n + 2$ to see what we get. Doing that gives

$$3n + 2 = 3(2m) + 2 = 6m + 2 = 2(3m + 1).$$

So $3n + 2$ is even. Recording that:

Known variables:	n, m
Know:	$3n + 2$ is odd.
Know:	$n = 2m$.
Know:	$3n + 2$ is even.
Goal:	**F**.

8. But $3n + 2$ cannot be both even and odd. Formula ($3n + 2$ is odd $\wedge$ $3n + 2$ is even) is equivalent to **F**. So we have concluded that **F** is true and we are done.

♢———————————————————————————♢

Typical Proof. By contradiction. Assume there exists an n such that $3n+2$ is odd but n even) Since n is even, there exists an integer m so that $n = 2m$. So

$$3n + 2 = 3(2m) + 2 = 6m + 2 = 2(3m + 1).$$

That means $3n + 2$ is even, contradiction the assumption that $3n + 2$ is odd.

♢———————————————————————————♢

3.11 Proving $\forall x(\exists y A)$

It is common to encounter theorems whose general form is $\forall x(\exists y P(x, y))$. The proof usually involves finding an algorithm. For any x, the algorithm must find a y so that $P(x, y)$ is true. Here is an example.

Theorem 3.7. For all real numbers x and y, if x and y are both rational numbers then $x + y$ is also a rational number.

Detailed Proof.

1. Ask someone else to select arbitrary real numbers of x and y.

Known variables:	x, y
Goal:	If x and y are rational then $x + y$ is rational.

2. Assume that x and y are rational.

Known variables:	x, y
Know:	x is rational.
Know:	y is rational.
Goal:	$x + y$ is rational.

3. Our knowledge involves the term *rational*. We need to know what that means. From the definition of a rational number, there must exist integers a and b where $b \neq 0$ and $x = a/b$; and there must exist integers c and d where $d \neq 0$ and $y = c/d$.

Known variables:	x, y, a, b, c, d
Know:	a, b, c and d are integers.
Know:	$b \neq 0$.
Know:	$d \neq 0$.
Know:	$x = a/b$.
Know:	$y = c/d$.
Goal:	$x + y$ is rational.

4. Since the goal is to show that $x + y$ is rational, let's replace x by a/b and replace y by c/d in expression $x + y$.

$$x + y = a/b + c/d = ad/bd + bc/bd = (ad + bc)/bd.$$

Known variables:	x, y, a, b, c, d
Know:	a, b, c and d are integers.
Know:	$b \neq 0$.
Know:	$d \neq 0$.
Know:	$x = a/b$.
Know:	$y = c/d$.
Know:	$x + y = (ad + bc)/bd$.
Goal:	$x + y$ is rational.

5. But we have shown that $x + y$ is the ratio of integers $ad + bc$ and bd. Since neither b nor d is 0, bd cannot be 0. So $x + y$ is rational, by the definition of a rational number.

♢———————————————————————————♢

Typical Proof. Let x and y be arbitrary rational numbers. By the definition of a rational number, there exists integers a, b, c and d ($b \neq 0$ and $d \neq 0$) such that $x = a/b$ and $y = c/d$. Then

$$x + y = a/b + c/d = ad/bd + bc/bd = (ad + bc)/bd.$$

Since $x + y$ is the ratio of two integers, $x + y$ is rational. (You can observe that $bd \neq 0$ since the product of two nonzero numbers is nonzero.)

3.12 Proving $A \equiv B$ or $A \leftrightarrow B$

There are two commonly used ways of proving $A \equiv B$.

3.12.1 Using direct equivalences

You can treat $\equiv$ in a way similar to the way you treat $=$ in algebraic equations, performing equivalence-preserving manipulations. Let's use that approach to prove the law of the contrapositive.

Theorem 3.8. $P \to Q \ \equiv \ \neg Q \to \neg P$.

Proof.

$$\begin{array}{lcll} \neg Q \to \neg P & \equiv & \neg(\neg Q) \vee \neg P & \text{(defn of } \to\text{)} \\ & \equiv & Q \vee \neg P & \text{(double negation)} \\ & \equiv & \neg P \vee Q & \text{(commutative law of } \vee\text{)} \\ & \equiv & P \to Q & \text{(defn of } \to\text{)} \end{array}$$

3.12.2 Proving two implications

Sometimes it is preferable to use the definition of $P \leftrightarrow Q$, namely $P \to Q \wedge Q \to P$.

Theorem 3.9. For every integer n, n is odd if and only if n^2 is odd.

Detailed Proof.

1. It suffices to prove

   $$\forall n(n \text{ is odd } \to n^2 \text{ is odd } \wedge\ n^2 \text{ is odd } \to n \text{ is odd}).$$

   That gives two goals. We use tautology $\forall x(A \wedge B) \equiv \forall x A \wedge \forall x B$ and change the variable names so that we can look at the two parts separately without variables from one interfering with the other.

Goal (1):	$\forall n(n \text{ is odd } \to n^2 \text{ is odd}).$
Goal (2):	$\forall m(m^2 \text{ is odd } \to m \text{ is odd}).$

2. Ask someone else to choose arbitrary values of m and n.

Known variables:	n, m
Goal (1):	n is odd $\to n^2$ is odd.
Goal (2):	m^2 is odd $\to m$ is odd.

3. Goal (2) is equivalent to its contrapositive, m is even $\to m^2$ is even. We proved that as Theorem 3.1. That only leaves Goal (1). (We know goal (2), but we can always discard known things to simplify.)

Known variables:	n
Goal (1):	n is odd $\to n^2$ is odd.

4. To prove Goal (1), assume that n is odd.

Known variables:	n
Know:	n is odd.
Goal (1):	n^2 is odd.

5. Since n is odd, there exists an integer k so that $n = 2k + 1$.

Known variables:	n
Know:	$\exists k(n = 2k + 1)$.
Goal (1):	n^2 is odd.

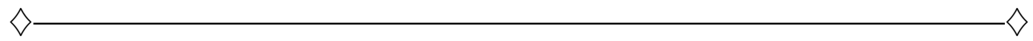
6. Ask someone else to provide a value k such that $n = 2k + 1$.

Known variables:	n, k
Know:	$n = 2k + 1$.
Goal (1):	n^2 is odd.

7. Since $n = 2k + 1$,

$$n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1.$$

Since $n^2 = 2z + 1$ for $z = 2k^2 + 2k$, it is evident that n^2 is odd.



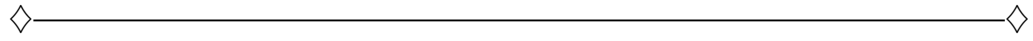
Typical Proof.

(a) (n is odd $\rightarrow$ n^2 is odd) Assume that n is odd. By the definition of an odd integer, there is an integer k such that $n = 2k + 1$. So

$$n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1.$$

By the definition of an odd integer, n^2 is odd.

(b) (n^2 is odd $\rightarrow$ n is odd) This is equivalent to (n is even $\rightarrow$ n^2 is even), which we profed earlier as Theorem 3.1.



3.13 Proof by cases

Proof by cases involves proving two or more implications. You must be careful that assumptions made during one of those cases are not still in place when proving another one. Think of this is similar to calling a function in a program. Each time a function is called, a new frame is created, so that calling $f(3)$ does not interfere with a later call to $f(4)$.

Theorem 3.10. For every integer n, $n^2 \geq n$.

Detailed Proof.

1. Ask someone to select an arbitrary integer n.

Known variables:	n
Know:	n is an integer
Goal:	$n^2 \geq n$.

2. Let's break proving the goal into three cases: $n = 0$, $n > 0$ and $n < 0$.

Known variables:	n
Know:	n is an integer
Goal (1):	$n = 0 \to n^2 \geq n$.
Goal (2):	$n > 0 \to n^2 \geq n$.
Goal (3):	$n < 0 \to n^2 \geq n$.
Goal (4):	$n^2 \geq n$.

3. Goal (1) is clearly true since $0^2 \geq 0$. Let's record it among the known facts.

Known variables:	n
Know:	n is an integer
Know (1):	$n = 0 \to n^2 \geq n$.
Goal (2):	$n > 0 \to n^2 \geq n$.
Goal (3):	$n < 0 \to n^2 \geq n$.
Goal (4):	$n^2 \geq n$.

4. Goal (2) is an implication, so we should assume that $n > 0$ and prove that $n^2 \geq n$. But let's prove that as a separate subproof. Knowledge and goals that are local to the proof of goal (2) is numbered 2.1, 2.2, etc., and they can only be used to establish goal (2).

Known variables:	n
Know:	n is an integer
Know (1):	$n = 0 \to n^2 \geq n.$
Goal (2):	$n > 0 \to n^2 \geq n.$
Goal (3):	$n < 0 \to n^2 \geq n.$
Goal (4):	$n^2 \geq n.$
Know (2.1):	$n > 0$
Goal (2.1):	$n^2 \geq n$

5. Since $n > 0$ is an integer, it must be the case that $n \geq 1$.

Known variables:	n
Know:	n is an integer
Know (1):	$n = 0 \to n^2 \geq n.$
Goal (2):	$n > 0 \to n^2 \geq n.$
Goal (3):	$n < 0 \to n^2 \geq n.$
Goal (4):	$n^2 \geq n.$
Know (2.1):	$n \geq 1$
Goal (2.1):	$n^2 \geq n$

Multiplying both sides of fact (2.1) by n preserves the inequality because $n > 0$. That gives $n \cdot n \geq n \cdot 1$, or equivalently, $n^2 \geq n$.

Known variables:	n
Know:	n is an integer
Know (1):	$n = 0 \to n^2 \geq n.$
Goal (2):	$n > 0 \to n^2 \geq n.$
Goal (3):	$n < 0 \to n^2 \geq n.$
Goal (4):	$n^2 \geq n.$
Know (2.1):	$n \geq 1$
Know (2.2):	$n^2 \geq n$
Goal (2.1):	$n^2 \geq n$

6. We have succeeded in proving goal (2). Notice that fact (2.2) cannot be used to establish goal (4) since it depends on the assumption that $n > 0$.

   We can move goal (2) into our knowledge. But we must also throw out parts that were local to the proof of goal (2).

Known variables:	n
Know:	n is an integer
Know (1):	$n = 0 \to n^2 \geq n.$
Know (2):	$n > 0 \to n^2 \geq n.$
Goal (3):	$n < 0 \to n^2 \geq n.$
Goal (4):	$n^2 \geq n.$

7. Now we need to prove goal (3). Assume that $n < 0$. But the square of any number is nonnegative. It follows that $n^2 \geq 0 > n$, and we can move goal (3) into what we know.

Known variables:	n
Know:	n is an integer
Know (1):	$n = 0 \to n^2 \geq n.$
Know (2):	$n > 0 \to n^2 \geq n.$
Know (3):	$n < 0 \to n^2 \geq n.$
Goal (4):	$n^2 \geq n.$

8. Propositional formula

$$((P \to S) \wedge (Q \to S) \wedge (R \to S)) \to ((P \vee Q \vee R) \to S)$$

is a tautology. That means known facts (1), (2) and (3) imply

$$(n = 0 \vee n > 0 \vee n < 0) \to n^2 \geq n.$$

But we know that $(n = 0 \vee n > 0 \vee n < 0)$ is true, and $\mathbf{T} \to S$ is equivalent to S. So we have demonstrated goal (4).

♢———————————————————————————————♢

Typical Proof. The proof is by cases ($n = 0$, $n > 0$ and $n < 0$).

Case 1 ($n = 0$). Then $n^2 \geq n$ because $0^2 \geq 0$.

Case 2 ($n > 0$). The smallest positive integer is 1, so $n > 0$ implies $n \geq 1$. Multiplying both sides of inequality $n \geq 1$ by positive number n gives $n^2 \geq n$.

Case 3 ($n < 0$). $n^2 \geq 0$ for all numbers n. Since, in this case, n is negative, clearly $n^2 \geq n$.

♢———————————————————————————————♢

prev **next**