Proofs

A proof is an essay that will persuade a logical reader that a mathematical theorem is true.
Some Vocabulary related to Mathematical Theorems and Proofs

A mathematical proof is a valid argument that demonstrates that a mathematical statement is true. A proof usually starts by restating the premises and ends with the conclusion.

A true mathematical statement is called a theorem, though in practice, the term is usually reserved for “important” true mathematical statements.

Less important true mathematical statements are called propositions.

A theorem that is needed as a stepping stone to prove a greater theorem is called a lemma.

A theorem that is an immediate consequence (and perhaps special case) of another theorem is called a corollary.

An axiom is an elementary mathematical truth that is assumed self-evident and not in need of proof. For example, the commutative, associative and distributive laws for real numbers are axioms. They cannot be justified as consequences of even more basic laws.
Formal Vs. Informal Proofs

A **formal proof** is a proof, written mostly in symbolic language, in which the argument is broken down to the level of basic rules of inference as discussed in the previous presentation. Formal proofs are usually excessively long and difficult to read. They are suitable for areas such as research into artificial intelligence and automated theorem proving, not for communication between mathematicians.

Mathematicians almost exclusively write informal proofs. An **informal proof** is a natural-language essay in which the writer addresses imagined readers and leads them through the argument, from the assumptions to the conclusions. Steps that are considered “obvious” to the intended audience are omitted, and basic rules of inference are used without identifying them. What is “obvious” or not cannot be objectively defined and requires subjective judgment. An informal proof is given in the same format as any other essay: continuous text organized into paragraphs of suitable lengths, written in complete, grammatically correct sentences including correct punctuation. It is **not** to be presented as a numbered or bullet-point list of statements.

A good informal proof is concise. Purely pedagogical elements and explanations how you came up with ideas do not belong in either a formal or an informal proof. A **proof is not a teaching device**.

We will only write informal proofs in this class.
Some rules you may use and treat as “obvious” in proofs

• The laws of arithmetic for real numbers, in particular, the commutative, associative and distributive laws.
• The order properties among real numbers: $1 < 2.5$, $3.9 < 4$, etc.
• The closure properties of the integers: sums and products of integers are again integers.
• The sign properties of real numbers: products of two positive numbers are positive, as are products of two negative numbers; a positive number times a negative number is negative.
• Adding a number to an equation, or multiplying an equation by a nonzero number, transforms the equation into an equivalent equation.
• Adding a number to an inequality, or multiplying the inequality by a positive number, transforms the inequality into an equivalent inequality.
• Multiplying an inequality by a negative number and flipping the inequality symbol transforms the inequality into an equivalent inequality.
Direct vs. Indirect Proofs

A mathematical statement of the form $p \rightarrow q$ can be proved in various ways:

- Directly: we assume the premise $p$ and then use definitions, axioms, theorems that have already been proved and valid rules of inference to show that the conclusion $q$ must be true.
- By contraposition: we give a direct proof of the contrapositive $\neg q \rightarrow \neg p$. This is sufficient to prove $p \rightarrow q$ because the contrapositive is logically equivalent to $p \rightarrow q$.
- By contradiction: we assume the premise $p$ and the negation of the desired conclusion, $\neg q$. We then construct an argument that concludes with a contradiction. Therefore, the premise $p \land \neg q$ was false, which by De Morgan means $\neg p \lor q$. Since the original premise $p$ cannot be false by assumption, $q$ must be true.

The last two types of proofs are known as indirect proofs. We will first spend some time studying direct proofs.
Even and Odd Numbers

We will practice some proof writing on simple theorems involving even and odd numbers. We first need to give exact definitions of these concepts.

Informally, an even number is an integer that can be expressed as two times some other integer.

Definition: A number $n$ is **even** iff there exists an integer $m$ such that $n = 2m$.

We could define an odd number as an integer that is not even, but it is more useful to give a direct definition. An odd number is an integer that can be expressed as an even number plus one.

Definition: A number $n$ is **odd** iff there exists an integer $m$ such that $n = 2m + 1$.

Important: do not assume that every proof we will write will be about even and odd numbers. Do not try to shoehorn every proof into an “even or odd” type situation.
First Example of a Direct Proof

Proposition: the product of any even number and any integer is even.

Proof:

Suppose \( n \) is an arbitrary even number and \( k \) is an arbitrary integer. By definition of an even number, there exists an integer \( m \) such that \( n = 2m \).

Therefore, \( nk = (2m)k = 2(mk) \). Since \( mk \) is again an integer, we have shown that \( nk \) satisfies the definition of an even number: it is equal to two times an integer.

Since \( n \) and \( k \) were arbitrary, we have shown that the product of any even number and any integer is even.

The “explanation of the proof” on the right is not part of the proof and only supplied for the benefit of the student. In proof writing assignments, you do not write pedagogical commentary like that, only the proof itself.
Avoid “variable name literalism”

The variable name \( m \) in the definition of even and odd numbers on the previous page is arbitrary. Any other letter could have been used to give the definition:

A number \( n \) is even iff there exists an integer \( k \) such that \( n = 2k \).

The variable \( n \), too, is just a placeholder, and changing its name in the definition does not change the definition itself. We can change both variable names and still retain the meaning of the definition:

A number \( p \) is even iff there exists an integer \( q \) such that \( p = 2q \).

Being even has absolutely nothing to do with the letters “n” or “m”.

If you assume, because of the given definition of even number, that every and any integer \( m \) in a statement involving an integer \( n \) must satisfy \( n = 2m \), then you are practicing the fallacy of “variable name literalism”, and are in danger of writing nonsensical proofs. Here is an example:

Prove that if \( n = 2 \), you can find a number \( m \) so that \( n + m = 8 \).

Correct Proof: Given \( n = 2 \), the number \( m = 6 \) satisfies \( n + m = 8 \).

Incorrect Proof: Since \( n \) is even, \( n = 2m \) for some \( m \), so \( n = 2 \) implies \( m = 1 \). Thus \( n + m = 8 \).
Second Example of a Direct Proof

Theorem: The product of any two odd numbers is odd.

Proof: suppose \( n \) and \( k \) are arbitrary odd integers. By definition of odd integer, this means that \( n = 2p + 1 \) and \( k = 2q + 1 \) for some integers \( p \) and \( q \). Then \( nk = (2p + 1)(2q + 1) = 4pq + 2p + 2q + 1 = 2(2pq + p + q) + 1 \). This shows that \( nk \) satisfies the definition of an odd number.

[Variable name literalism is again a danger here. If you apply the definition of odd number literally in terms of variable names and conclude that \( n = 2m + 1 \) and \( k = 2m + 1 \) for a single integer \( m \), then you are assuming that \( n \) and \( k \) are actually the same integer. Two different odd numbers have different “\( m \)’s”. You therefore have to use different letters for them.]
Example of a Proof by Contraposition

Proposition: for an integer $n$, if $n^2$ is odd, so is $n$.

Proof:

We will show the contrapositive: if $n$ is even, so is $n^2$. So suppose $n$ is an even integer.

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

Therefore, $n^2 = 2m \cdot 2m = 2(2m^2)$. Since $2m^2$ is again an integer, we have shown that $n^2$ satisfies the definition of an even number: it is equal to two times an integer.

Explanation of the proof

We start by explaining the type of proof we are doing and stating the premise.

We appeal to the definition of an even number.

We exploit the definition of an even number to derive an equation that gives us the desired conclusion.
Rational and Irrational Numbers

A number is called rational if it is equal to a quotient of integers.

Definition: a number $x$ is rational iff there exist integers $p$ and $q$ such that $x = \frac{p}{q}$. (It is implied in the definition that $q$ cannot be zero.)

A real number that is not rational is called irrational. Examples of irrational numbers are $\sqrt{2}$, $\pi$ and $e$.

Integers are special rational numbers.
Example 1 of a Proof by Contradiction

Proposition: the sum of a rational and an irrational number is irrational.

Proof:

Suppose $x$ is an arbitrary rational number and $y$ is an arbitrary irrational number. Further assume, for the purpose of obtaining a contradiction, that $x + y$ is rational.

By definition of a rational number, there must be integers $p$ and $q$ such that $x = \frac{p}{q}$. There must also be integers $n$ and $m$ such that $x + y = \frac{n}{m}$.

Therefore, $y = (x + y) - x = \frac{n}{m} - \frac{p}{q}$. But $\frac{n}{m} - \frac{p}{q} = \frac{nq - mp}{mq}$ is again a rational number, which contradicts the irrationality of $y$. Thus, $x + y$ must be irrational.

Explanation of the proof

We start with the premise and introduce variable names. We also assume the negation of the conclusion and make it clear that this is for giving a proof by contradiction.

We appeal to the definition of a rational number.

We exploit the equations for $x$ and $x + y$ to derive an equation for $y$ that represents a contradiction.
Avoid “Fake” Proofs by Contradiction (I)

Proving by contradiction is very attractive because one has more premises to work with than in a direct proof or in a proof by contraposition. One has the original premise, and the negation of the conclusion.

Some students therefore yield to the temptation to write proofs by contradiction by default, even when a simple direct proof is available. They usually end up writing a direct proof anyway, but wrap it inside an unnecessary packaging of contradiction. This results in what could be called “fake” proofs by contradiction. We first look at an example to illustrate the idea.

**Theorem**: there is an integer n so that $2n = 6$.

**Correct (direct) proof**: pick $n = 3$. Then $2n = 6$. It follows that $2n = 6$ has an integer solution.

**Fake proof by contradiction**: suppose that no integer solution of $2n = 6$ exists. Pick $n = 3$. Then $2n = 6$. Thus $2n = 6$ has an integer solution. This contradicts our assumption that $2n = 6$ does not have an integer solution. Therefore, our assumption that $2n = 6$ does not have an integer solution is false. This proves that $2n = 6$ has an integer solution.
Avoid “Fake” Proofs by Contradiction (II)

The following is a more formal analysis of what makes a proof by contradiction that \( p \) implies \( q \) “fake”.

1. Assume \((p \text{ and } \neg q)\)
2. Show that since \( p \) is true, \( q \) is also true
3. Observe that \( q \) contradicts \( \neg q \)
4. Therefore, the assumption \((p \text{ and } \neg q)\) must have been false, and its negation, \((\neg p \text{ or } q)\) must be true. Since it is the given premise of the theorem that \( p \) is true, we conclude that \( q \) must be true.

This is a technically valid proof by contradiction that encapsulates a direct proof of (if \( p \) then \( q \)) in its second step. Only that second step was necessary.

A second type of “fake” proof by contradiction is the following:

1. Assume \((p \text{ and } \neg q)\)
2. Show that since \( \neg q \) is true, \( \neg p \) is also true
3. Observe that \( \neg p \) contradicts \( p \)
4. Therefore, the assumption \((p \text{ and } \neg q)\) must have been false, and its negation, \((\neg p \text{ or } q)\) must be true. Since it is the given premise of the theorem that \( p \) is true, we conclude that \( q \) must be true.

This is again a technically valid proof by contradiction. Its heart is a proof of (if \( p \) then \( q \)) by contraposition in step 2. Only step 2 was necessary.
Example 2 of a Proof by Contradiction

**Theorem:** given a finite collection of real numbers, at least one of them must be greater than or equal to their average.

This makes sense – how could they all be less than their average? The intuition that that ought to be impossible lends itself naturally to the following

**Proof by Contradiction:** suppose \( x_1, x_2, \ldots, x_n \) are arbitrary real numbers and \( \bar{x} \) is their average. Suppose further, to get a contradiction, that \( x_k < \bar{x} \) for all integers \( k \) with \( 1 \leq k \leq n \). By adding all these inequalities, we get

\[
x_1 + x_2 + \cdots + x_n < n\bar{x}.
\]

Dividing by \( n \), we get

\[
\frac{x_1 + x_2 + \cdots + x_n}{n} < \bar{x}.
\]

Since the left side is the definition of the average, we have shown \( \bar{x} < \bar{x} \). That is a contradiction. Hence, \( x_k \geq \bar{x} \) for at least one integers \( k \) with \( 1 \leq k \leq n \).
Theorem: given 8 people, there must be two who were born on the same day of the week.

Proof by Contradiction: suppose that in our group of 8 people, for each week day, there is at most one person who was born on that day. Since there are 7 week days, and at most one person on each day, we have at most 7 people. This contradicts the fact that we have 8 people.
One common type of statement we may have to prove is the universal statement *for all x in some universal set, something is true.*

Formally, the type of statement we are discussing here is $\forall x P(x)$, where $P(x)$ is a statement that depends on $x$.

We prove such a statement directly by assuming that some arbitrary $x$ is given, and for this (generic) $x$, we show that $P(x)$ is true.

Example: Prove that for all positive integers $n$, $n(n + 1) > n^2$.

Proof: Suppose $n$ is an arbitrary positive integer. We know that $n + 1 > n$, and that we can multiply an inequality by a positive quantity. Multiplying the inequality $n + 1 > n$ by the positive quantity $n$ produces $n(n + 1) > n^2$. 
How *Not* To Prove Universal Statements: “Proof by Example”

You cannot prove universally quantified statements about infinitely many objects by example.

Consider the following example:

**Proposition:** if $n$ is any integer, then $n(n + 1)$ is even.

**Attempted proof:** For $n = 1$, $n(n + 1) = 2$ which is even. For $n = 2$, $n(n + 1) = 6$ which is also even, etc.

This argument only shows that the statement that $n(n + 1)$ is even is true for at least two values of $n$, for $n = 1$ and for $n = 2$. It does not show that it is true for any other values of $n$, regardless of the suggestion implied in the word “etc”. There are infinitely many values of $n$. A correct proof must show that $n(n + 1)$ is even for all of them, not just finitely many of them.

**Correct proof:** Assume that $n$ is an arbitrary integer. Then either $n$ is even, or it is odd. If $n$ is even, then $n + 1$ is odd, and if $n$ is odd, then $n + 1$ is even. This means that one of the two numbers $n$ and $n + 1$ is always even. Since the product of an even number and an integer is even, that means that $n(n + 1)$ is always even.

Note: existential statements can in principle be proved by supplying an example.
Proving Existential Statements

While we cannot generally prove universal statements by example, we can prove existential statements by producing an example of the type of object whose existence is being claimed.

Theorem: There is an integer \( n \) that satisfies \( 2n + 1 = 3 \).

Proof: Let \( n = 1 \). Then \( 2n + 1 = 3 \).

If you think that this is “too easy”, then you may still be thinking that a proof is a teaching device and that part of the proof is showing how you found your answer. Existential proofs don’t care how you found the answer. If you show a unicorn, that proves that unicorns exist. You don’t have to tell the story of how you caught the unicorn.

The most common mistake in existential proofs is to assume existence:

Incorrect Proof: Suppose \( n \) is an integer that satisfies \( 2n + 1 = 3 \). Then \( n = 1 \).

This argument cannot prove existence because it started with the assumption of existence. It doesn’t show that \( n = 1 \) is a solution and that therefore a solution exists. It only shows that if a solution exists, it must be \( n = 1 \). The incorrect proof therefore only shows uniqueness of solutions: you can’t have more than one solution, but it leaves open the question of whether a solution exists in the first place.

If you think that this is sophistry, study the next two pages particularly carefully.
Assuming Existence Cannot Prove Existence (I)

Starting an argument for existence with the assumption of existence can “prove” false statements. Here is an example of a false statement:

**False Statement:** There exists a positive real number \( x \) such that \( x^2 = -1 \).

In fact, no such real number exists because squares of real numbers are never negative. Nevertheless, if we start with the assumption of existence, we can derive a value for \( x \).

**Invalid Proof:** suppose \( x^2 = -1 \) for some positive real number \( x \). By squaring both sides of the equation, we get \( x^4 = 1 \). By taking the fourth root, and using the algebraic fact that \( \sqrt[4]{x^4} = x \) for every non-negative real number \( x \), we get \( x = 1 \). Therefore, a positive solution \( x \) of \( x^2 = -1 \) exists.

This proof pretends to show not only that a positive solution \( x \) of \( x^2 = -1 \) exists, but that this solution is in fact \( x = 1 \). This is not a solution though because for this \( x \), \( x^2 = 1 \), not \(-1\).

What the invalid proof actually showed is that if a positive solution of \( x^2 = -1 \) exists, then it must be \( x = 1 \). That’s a true statement, but it is only true because its premise is false. A conditional statement with a false premise is true by default.

The following is a similarly true statement: if **humans have 6 fingers on each hand**, then each human has **12 fingers total**.
Assuming Existence Cannot Prove Existence (II)

If we had treated the reasoning of the invalid proof on the previous page as what it truly is, just scratch work, and then attempted to write a correct proof based on that, one that does not assume existence, we would have quickly realized our mistake. Let’s repeat the false statement for the record one more time.

**False Statement:** There exists a positive real number $x$ such that $x^2 = -1$.

For our scratch work, just like on the previous page, we provisionally assumed existence of such a solution and convinced ourselves that if the solution exists, it can only be $x = 1$. Based on this, we write our

**Attempted Correct Proof:** let $x = 1$. Then $x^2 = -1$.

We realize immediately that this proof is invalid because $x^2 = 1$.

This lesson cannot be over-emphasized. While it is legitimate to assume existence in your scratch work for an existence proof, to find the candidate solution(s), the actual proof cannot proceed from the assumption of existence. It must present the candidates you found in your scratch work and show that they meet the requirements.

(Non-existence can be proved by assuming existence and deriving a contradiction.)
Proving the negation of a universally quantified statement

The negation of a universally quantified statement is the existential quantification of the negation. Formally, \( \neg \forall x P(x) \) is equivalent to \( \exists x \neg P(x) \). Therefore, to prove that a universally quantified statement is false, you have to write an existential proof of the negated statement.

Put differently, to show that something is not true for all objects, you just have to find one exception.

**Theorem:** Not all integers have a square that is greater than zero.

**Proof:** select \( n = 0 \). Then \( n \) is an integer, and its square is zero.
Proving the negation of an existentially quantified statement (I)

We have learned that to show that an object with certain properties exists, all you need to do is to produce such an object. To review the technique, here is another existential statement.

**Proposition:** there is a number whose square is greater than 10.

Proof: let \( n = 4 \). Then \( n^2 = 16 > 10 \). We have shown that a number exists whose square is greater than 10.

The **negation** of an existentially quantified statement is the universal quantification of the negation, which **cannot** be proved by producing an example.

**Proposition:** there is no positive integer whose square is 3.

Incorrect proof: \( 1^2 \) is 1, which is too small, and \( 2^2 \) is 4, which is too large.

The proof is incorrect because it gives no “hard” reason why the square of some other integer that is not 1 or 2 could not be 3. It is a mere appeal to the intuition – the reader is asked to agree with the intuitive picture that since the sequence of squares seems to skip the 3, 3 isn’t a square. This idea is useful as inspiration for a rigorous proof, but by itself, it is not a rigorous proof.

The incorrect proof will convince a friendly audience that wants to believe you, but not a hostile jury. A correct proof must convince a hostile (but reasonable) jury.

Correct proof: Let \( n \) be an arbitrary positive integer. Then \( n = 1 \) or \( n > 1 \). If \( n = 1 \), then \( n^2 = 1 \), thus \( n^2 \) cannot be 3. If on the other hand \( n > 1 \), then \( n \geq 2 \), since \( n \) is an integer. Therefore, \( n^2 \geq 4 \), which again means that \( n^2 \) cannot be 3. We have shown that in either case, \( n^2 \) cannot be 3.
Proving the negation of an existentially quantified statement (II)

On the previous page, we proved *directly* that the square of every positive integer is not 3, which is logically equivalent to the statement that there is no positive integer whose square is 3. Often, it is convenient to prove negations of existential statements by contradiction instead: assume existence and show that it leads to a contradiction.

**Theorem:** There is no integer solution of $2x + 1 = 4$.

**Proof by Contradiction:** Assume there is an integer $x$ such that $2x + 1 = 4$. Then $2x = 3$, and $x = 3/2$. Since $3/2$ is not an integer, we have arrived at a contradiction. That means that there can be no integer solution of $2x + 1 = 4$.

We can still prove the theorem directly though, by showing that for all integers $x$, $2x + 1 \neq 4$.

**Direct Proof:** Suppose $x$ is an integer. Then either $x \geq 2$, or $x \leq 1$. We now multiply both equalities by 2 and then add 1. If $x \geq 2$, then $2x + 1 \geq 5$, and if $x \leq 1$, then $2x + 1 \leq 3$. Either way, $2x + 1 \neq 4$.

It is an interesting question whether one of these proofs is superior to the other. The proof by contradiction seems easier to follow – we assume that a solution exists, and derive a necessary condition for it. If the solution exists, it can only be $3/2$, but that is not an integer.

A logical purist would find the direct proof superior because it uses fewer assumptions. It works solely within the realm of the integers and their properties, and would make sense to someone who has never heard of fractions. The proof by contradiction implicitly assumes that the reader is familiar with fractions and their properties.
# An Overview of Common Proof Techniques for Quantified Statements

<table>
<thead>
<tr>
<th></th>
<th>Direct</th>
<th>By Contradiction</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\forall x P(x)$</td>
<td>Assume that an arbitrary $x$ is given. Show that $P(x)$ must be true.</td>
<td>Assume that $P(x)$ is false for at least one $x$, derive a contradiction.</td>
</tr>
<tr>
<td>$\neg \forall x P(x) \equiv \exists x \neg P(x)$</td>
<td>Produce an $x$ for which $P(x)$ is false.</td>
<td>Assume that $P(x)$ is true for all $x$, derive a contradiction.</td>
</tr>
<tr>
<td>$\exists x P(x)$</td>
<td>Produce an $x$ for which $P(x)$ is true.</td>
<td>Assume that $P(x)$ is false for all $x$, derive a contradiction.</td>
</tr>
<tr>
<td>$\neg \exists x P(x) \equiv \forall x \neg P(x)$</td>
<td>Assume that an arbitrary $x$ is given. Show that $P(x)$ must be false.</td>
<td>Assume that $P(x)$ is true for at least one $x$, derive a contradiction.</td>
</tr>
</tbody>
</table>
Many theorems combine universal and existential quantification and therefore require us to combine what we learned about universal and existential proofs on the previous pages.

Here we study the statement where for every object, the existence of some other object with a certain relationship to the original object is asserted. An abstract version of this type of statement is $\forall a \exists b P(a, b)$.

Examples of statements that follow this format:

*Every pot has a lid. For every person, there is the perfect job. Every house has an owner.*

In fact, our very first proof example in this lecture was a *for all, there is..* type statement. It said that for any even number and any arbitrary integer, the product is even. Being even is really an existential statement in disguise, because $n$ being even means that there exists an integer $m$ with $n = 2m$.

Formally, we could have written the theorem as follows:

$$\forall n \text{ even}, k \text{ integer}(\exists m \text{ integer such that } nk = 2m)$$
“For All, There Is” Type Statements (II)

Being able to prove “For All, There Is” type statements is relevant for computer science. If we are to write a function in a program that takes an input $a$ and is supposed to produce a specific output $b$ that is somehow related to $a$, we should prove first that it is possible to do that. That means we have to prove that for each $a$, the corresponding $b$ actually exists.

We cannot take this for granted. For example, if you write a square root function that takes a real number as an input (or, rather, it’s closest programming equivalent, a floating point number), then this function will malfunction if you call it with a negative input. That’s because the statement

\[
\text{for every real number } a, \text{ there is a real number } b \text{ such that } b^2 = a
\]

is **false**. It is false because for any real number $b$, $b^2 \geq 0$. Therefore, the equation $b^2 = a$ cannot be true if $a < 0$.

We will now study examples.
“For All, There Exists” Type Theorems (III)

Theorem: for every integer \( n \), there is an integer \( k \) such that \( n + k = 1 \).

Observe that the theorem does not assert that we can find integers \( n \) and \( k \) whose sum is 1. It asserts something more subtle: *that no matter what integer \( n \) is given, one can find another integer \( k \) so that their sum will be 1*. There is no single \( k \) that works for all \( n \). Rather, for each \( n \), there is an individual \( k \).

This can be thought of as a challenge-response game: someone gives you the integer \( n \). You have no control whatsoever over that. Your job is to respond with an integer \( k \) of your own. You win the game if your \( k \), plus the \( n \) you were given, add up to 1. Can you always win this game?

A little scratch work will immediately convince you that you can always win this game. You want to achieve \( n + k = 1 \). Solving for \( k \), you get \( k = 1 - n \). If \( n \) is an integer, \( 1 - n \) will always be an integer as well. Therefore, you can always win the game by responding to \( n \) with the quantity \( k = 1 - n \). We summarize our thinking with the following

Proof of the Theorem: suppose \( n \) is an integer. Pick \( k = 1 - n \). Then \( k \) is also an integer, and \( n + k = 1 \).
Many students who learn how to write proofs for the first time will write the following incorrect proof of the theorem:

Incorrect Proof of the Theorem: suppose \( n \) is an integer and suppose \( k \) is an integer such that \( n + k = 1 \). Then \( k = 1 - n \). This proves that for every integer \( n \), an integer \( k \) exists with \( n + k = 1 \).

This argument proves no such thing. It starts with the assumption that a suitable \( k \) exists. **Assuming that a solution exists and then reverse-engineering its value cannot prove that a solution exists. To make this argument is what is called circular reasoning.**

This is not just a mathematical issue. It is a general life lesson. If you start with a preconceived assumption, and work backwards from this unquestioned assumption, you can justify all kinds of wrong-headed ideas.
“For All, There Exists” Type Theorems (V)

A Proof is not a Computer Program

The following is another incorrect proof of the theorem that for every integer n, there is an integer k such that $n + k = 1$:

Incorrect Proof of the Theorem: Suppose n and k are integers. Pick $k = 1 - n$. Then $n + k = 1$. This proves that for every integer n, an integer k exists with $n + k = 1$.

A proof is not a computer program. Variables do not need to be declared before they are used. “Suppose n and k are integers” does not “declare” n and k for later use, as in, “the symbols n and k will be used to represent integers, but we haven’t decided yet what their values will be”. Rather, it means that we are assuming that n and k are arbitrary selected integers and will make no further assumptions about them. By making this statement, we are preparing to prove something about all integers n and k, which is different than showing that for all integers n, a specific k exists.

The proof above assumes that k is an arbitrary integer and then immediately contradicts itself by changing the definition of k to a specific integer, namely, the integer $1 - n$.

But isn’t $1 - n$ “arbitrary” because n was arbitrary? It’s true that n was arbitrarily selected, but once it’s selected, it’s no longer arbitrary, and nor is $1 - n$.

Think of this as a challenge-response game: once your opponent has made their opening move and selected the n, n is a specific number, and it requires a specific response from you in the form of $k = 1 - n$. No other number will let you win the game.
“For All, There Exists” Type Theorems (VI)

Let’s look at another example, and study an incorrect proof first.

**Proposition:** \( \forall x \exists y (y > x) \).

**Incorrect proof:** Suppose \( x \) is an arbitrary number. Since you can always find a bigger number than any given number, there is a number \( y \) such that \( y > x \).

The heart of this “proof” lies in the statement that for any number, you can find a bigger number. But that is what the original proposition is saying. We “proved” the proposition *by affirmatively declaring it to be true*. This is not proof, it is circular reasoning. We assumed the conclusion to justify the conclusion. This we cannot do.

A correct proof must *show constructively* that this bigger number exists:

**Correct proof:** Suppose \( x \) is an arbitrary number. Define \( y = x + 1 \). Then \( y > x \). We have shown that for any arbitrary number \( x \), there is a number \( y \) that is bigger.

Remember to think of this as a challenge-response game. In this game, someone hands you an arbitrary number, and you win the game if you counter with an even bigger number. To convince me that you can always win this game, you can’t just bluff and merely declare that you can always find a bigger number. You have to tell me how you find it. You have to tell me your winning strategy.
“For All, There Exists” Type Theorems (VII)

We summarize the general theory. We wish to give a direct proof of

$$\forall a \exists b P(a, b).$$

A direct proof of this type of statement always has the same logical framework. We start by assuming that we have an arbitrary $a$, to set up a universal generalization. We must not make any additional assumptions about $a$. In particular, we must not choose an example for $a$. Then, for this arbitrary $a$, we must explicitly show that a $b$ exists so that $P(a, b)$ is true. It is insufficient to simply claim its existence; that would be making the error of assuming the conclusion or “proof by affirmation”. We must say exactly how we pick $b$ based on $a$.

Once we have shown the existence of the $b$, universal generalization yields the truth of the statement $\forall a \exists b P(a, b)$ since $a$ was arbitrary.

Therefore, such a proof has the following logical structure:

Assume we have an $a$, arbitrary. Then choose $b$ suitable in response to $a$ so that $P(a, b)$ is true. [How you pick $b$ may require scratch work that is NOT to be included in the proof. ] Since $a$ was arbitrary, conclude that $\forall a \exists b P(a, b)$ is true.
“For All, There Exists” Type Theorems (VIII)

If you decide to finish your proof by making a concluding statement that repeats the theorem that you have proved, then you must do it correctly. The following is an example of what NOT to do, using the example of the theorem that for every integer $n$, there is an integer $k$ such that $n + k = 1$:

Incorrect Proof of the Theorem: Suppose $n$ is an integer. Pick $k = 1 - n$. Then $n + k = 1$. This proves that for every integer $n$, an integer $k$ exists.

Sure. When someone gives you an integer, it’s always possible to tell them an integer in return. They say 3, you say 4. They say 11, you say 33. That is not the point of the theorem though. The theorem doesn’t say that you can always respond to an integer with an integer. It says that you can always respond to an integer with another integer so that the two will add up to 1.

You don’t have to write a concluding statement that repeats the theorem, but if you do, you must quote the actual theorem, not a caricature of the theorem.