1 What is number theory?

Coming soon....
2 Intro to proofs: Propositional logic

A *proposition* is a statement that has a well-defined truth value, either true or false. We will use capital letters $P$, $Q$, $R$, ... to denote propositions.

**Example 1.**

\[
P = \text{It is raining.}
Q = \text{I brought an umbrella to school.}
R = \text{I ate cereal for breakfast today.}
\]

We can combine propositions with logical connectors, such as *and*, *or*, *not*, and *implies* (or “if-then”). This produces a *propositional expression*. The truth values of the propositions $P$ and $Q$ determine the truth value of a propositional expression such as $P$ or $Q$ in fairly obvious ways: $P$ or $Q$ is true if either $P$ is true, or $Q$ is true, or both, and is false otherwise (if both $P$ and $Q$ are false).

There are standard symbols for all of these logical connectors, as follows:

- $P \land Q$ means $P$ and $Q$
- $P \lor Q$ means $P$ or $Q$
- $\neg P$ means not $P$ (or equivalently, “$P$ is false”)
- $P \implies Q$ means $P$ implies $Q$ (or equivalently, “if $P$, then $Q$”)
- $P \iff Q$ means $P$ if and only if $Q$

Parentheses are often used in propositional expressions as well, such as in the expression

\[(P \land Q) \lor (\neg P \land \neg Q)\]

A simple way to understand the meanings of these logical connectors is using *truth tables*. For example, here is the truth table for $P \lor Q$:
Here are the truth tables for the other logical connectors:

\[
\begin{array}{c|c|c|c|c}
\hline
P & Q & P \lor Q \\
\hline
F & F & F \\
F & T & T \\
T & F & T \\
T & T & T \\
\hline
\end{array}
\]

Perhaps the one of these which is the least obvious is the truth table for \( P \rightarrow Q \). Certainly if \( P \) is true and \( Q \) is false, then \( P \rightarrow Q \) must be false, and it makes sense that if both \( P \) and \( Q \) are true, then \( P \rightarrow Q \) is true. But in the other cases, when \( P \) is false, the statement \( P \rightarrow Q \) says nothing about whether \( Q \) should be true or false. So if \( P \) is false, then no matter what truth value \( Q \) has, we say that \( P \rightarrow Q \) is true.

If that’s confusing, think about this with some actual statements in place of \( P \) and \( Q \), such as the statements from Example 1 above. Suppose I make a declaration that “if it is raining, then I bring an umbrella to school”. That is, let’s pretend that in my life, this statement is always true. What does this say about whether or not I bring an umbrella on days when it’s not raining? Perhaps I always bring an umbrella, regardless. Perhaps I never bring an umbrella when it’s not raining. Perhaps when it’s not raining, I flip a coin.
and decide whether or not to bring my trusty umbrella. In any of those cases, the statement “if it is raining, then I bring an umbrella to school” is still true. The one way it would be false is if there were a day when it did rain, and I did not bring an umbrella.

We say that two propositional expressions are equivalent (or logically equivalent) if they have the same truth value for all possible truth values of the propositional variables in each formula. For example, $P \leftrightarrow Q$ is logically equivalent to the formula

$$(P \land Q) \lor (\neg P \land \neg Q) \tag{1}$$

mentioned earlier. We can see why by looking at the truth table for each formula. Here is a truth table for expression (1), built up step by step from left to right:

<table>
<thead>
<tr>
<th>$P$</th>
<th>$Q$</th>
<th>$P \land Q$</th>
<th>$\neg P$</th>
<th>$\neg Q$</th>
<th>$\neg P \land \neg Q$</th>
<th>$(P \land Q) \lor (\neg P \land \neg Q)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>F</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>F</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>T</td>
</tr>
</tbody>
</table>

Note that the last column is exactly the same as the column for $P \leftrightarrow Q$ in the truth tables above. This shows that these two propositional expressions are logically equivalent.

**Theorem 2.1.** Each of the following is true:

1. $P \rightarrow Q$ is logically equivalent to $\neg Q \rightarrow \neg P$.
2. $P \leftrightarrow Q$ is logically equivalent to $(P \rightarrow Q) \land (Q \rightarrow P)$.
3. $\neg(P \lor Q)$ is logically equivalent to $\neg P \land \neg Q$.
4. $\neg(P \land Q)$ is logically equivalent to $\neg P \lor \neg Q$.
5. $\neg(\neg P)$ is logically equivalent to $P$.

**Proof.** 1. (Proof by Faith T.)
<table>
<thead>
<tr>
<th>P</th>
<th>Q</th>
<th>¬Q</th>
<th>¬P</th>
<th>¬Q → ¬P</th>
<th>P → Q</th>
</tr>
</thead>
<tbody>
<tr>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>T</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
</tr>
</tbody>
</table>

The last two columns are the same.

2. (Proof by Maddie Y.)

<table>
<thead>
<tr>
<th>P</th>
<th>Q</th>
<th>P → Q</th>
<th>Q → P</th>
<th>(P → Q) ∧ (Q → P)</th>
<th>P ↔ Q</th>
</tr>
</thead>
<tbody>
<tr>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
</tbody>
</table>

The last two columns are the same.

3. (Proof by Aidan S.)

<table>
<thead>
<tr>
<th>P</th>
<th>Q</th>
<th>¬P</th>
<th>¬Q</th>
<th>P ∧ Q</th>
<th>¬P ∧ ¬Q</th>
<th>¬(P ∨ Q)</th>
</tr>
</thead>
<tbody>
<tr>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>T</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>T</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>F</td>
<td>F</td>
</tr>
</tbody>
</table>

The last two columns are the same.

4. (Proof by Christine D.)

<table>
<thead>
<tr>
<th>P</th>
<th>Q</th>
<th>¬P</th>
<th>¬Q</th>
<th>P ∧ Q</th>
<th>¬P ∨ ¬Q</th>
<th>¬(P ∧ Q)</th>
</tr>
</thead>
<tbody>
<tr>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>F</td>
<td>F</td>
</tr>
</tbody>
</table>

The last two columns are the same.
5. (Proof by Leilani D.)

\[
\begin{array}{ccc}
P & \neg P & \neg(\neg P) \\
F & T & F \\
T & F & T \\
\end{array}
\]

The first and last columns are the same.

\[\square\]

**Remark.**

- In part (1), the if-then statement $\neg Q \rightarrow \neg P$ is called the *contrapositive* of the if-then statement $P \rightarrow Q$. Part (1) shows that a statement and its contrapositive are always logically equivalent. This will be a useful proof technique in some situations: instead of proving $P \rightarrow Q$ directly, you might instead prove $\neg Q \rightarrow \neg P$.

- Part (2) shows that to prove an if-and-only-if statement $P \leftrightarrow Q$, you can prove $P \rightarrow Q$ and $Q \rightarrow P$. Indeed, this is the standard strategy for proving an if-and-only-if statement.

- Parts (3) and (4) are called De Morgan’s Laws, named after the 19th-century British mathematician Augustus De Morgan. They give the standard way to negate a statement involving $\lor$ or $\land$.

- Part (5) is fairly obvious, but it says that a double negative $\neg \neg$ can be removed from a propositional expression.

**Exercise 1.** Find a propositional expression using only $\land$, $\lor$, and $\neg$ that is equivalent to $P \rightarrow Q$. Use this (and perhaps the rules from the previous theorem) to find a simple expression, again using only $\land$, $\lor$, and $\neg$, that is logically equivalent to $\neg(P \rightarrow Q)$.

**Solution.** (Solution of first part by Wei C.)
The third and last columns are the same.

(Solution of second part by Omar H.) The following expressions are all logically equivalent:

\[
\begin{align*}
\neg(P \rightarrow Q) \\
\neg(\neg P \lor Q) & \quad \text{(from the first part)} \\
\neg(\neg P) \land \neg Q & \quad \text{(by De Morgan’s Law for } \lor) \\
P \land \neg Q & \quad \text{(by Theorem 1 (5))}
\end{align*}
\]

Remark. This exercise shows that to disprove an if-then statement $P \rightarrow Q$, it is enough to find a situation where $P$ is true but $Q$ is false. This is referred to as finding a counterexample. (This is particularly true in the case where this if-then is preceded by a “For all . . .”. See the next section for more on that.)
3 Intro to proofs: Existential and universal quantifiers

**Definition 3.1.** A *propositional function* is a function of one or more variables whose output is always a proposition. Given a propositional function of some variable \( x \), the *universal set* for \( x \) (or just the *universe* of \( x \)) is the set of all values of \( x \) that can be used as inputs to this function. That is, if the propositional function is a function of a single variable, then the universal set for that variable is just the domain of the propositional function.

**Examples.**

\[
\begin{align*}
P(x) &= "x^2 + 1 > 0" & \text{Universe: } x \in \mathbb{R} \\
Q(a, b) &= "(a < b) \lor (b < a)" & \text{Universe: } a \in \mathbb{Z}, b \in \mathbb{Z} \\
R(x, y) &= "x \text{ loves } y" & \text{Universe: } x, y \in \{ \text{people} \}
\end{align*}
\]

This means that \( P(5) \) is the proposition “\( 5^2 + 1 > 0 \)”, and \( P(-42) \) is the proposition “\( (-42)^2 + 1 > 0 \)”. Note that here we are just plugging values into a function, without worrying yet about whether or not the resulting proposition is true. For example, \( R(\text{Professor Conley, Donald Trump}) \) is the proposition “Professor Conley loves Donald Trump”. This proposition is certainly false! But we can still plug these two values into the function \( R \) to produce a valid proposition, regardless of its truth value.

If \( P(x) \) is a propositional function of a variable \( x \), and *every* element in the universe of the variable \( x \) yields a proposition that is True, then we say that the statement

\[
\forall x \ P(x)
\]

is true. Of course, we have some notation for this:

\[
\forall x \ P(x) \quad \text{means} \quad \text{For all } x, \ P(x)
\]

The symbol \( \forall \) is called the *universal quantifier*, but you can just read it as “for all”, “for each”, “for any”, or “for every”.

If \( P(x) \) is a propositional function of a variable \( x \), and there is *some* element in the universe of the variable \( x \) for which the proposition \( P(x) \) is
True, then we say that the statement

\[ \text{There exists } x \text{ such that } P(x) \]

is true. Once again, we have some notation for this as well:

\[ \exists x \ P(x) \quad \text{means} \quad \text{There exists } x \text{ such that } P(x) \]

The symbol \( \exists \) is called the existential quantifier, but you can just read it as “there exists” or “for some”.

**Examples.**

1. Universal set for \( x \): \( \mathbb{R} \)
   \[ P(x) = "x^2 + 1 > 0" \]
   \( \forall x \ P(x) \) is True.

2. Universal set for \( x \): \( \mathbb{R} \)
   \[ Q(x) = "x^2 = -1" \]
   \( \exists x \ Q(x) \) is False.

Note that the universal set matters! If in both of the preceding examples, we change the universe from \( \mathbb{R} \) to \( \mathbb{C} \), the truth values of the statements both change:

3. Universal set for \( x \): \( \mathbb{C} \)
   \[ P(x) = "x^2 + 1 > 0" \]
   \( \forall x \ P(x) \) is now False. (Consider \( x = i \), for example.)

4. Universal set for \( x \): \( \mathbb{C} \)
   \[ Q(x) = "x^2 = -1" \]
   \( \exists x \ Q(x) \) is now True. (Again, \( x = i \) works.)

**Note.** As the examples above show, the choice of the universal set often matters too much to be just guessed from the context of the statement. So, although formal languages in the subject of mathematical logic usually prescribe these notations strictly as \( \forall x \ P(x) \) and \( \exists x \ P(x) \), most of the time in regular usage, mathematicians specify the universal set for each variable immediately after the quantifier, as in the following examples:

1. \( \forall x \in \mathbb{R} \quad x^2 + 1 > 0 \)
2. \( \exists x \in \mathbb{R} \quad x^2 = -1 \)

3. \( \forall x \in \mathbb{C} \quad x^2 + 1 > 0 \)

4. \( \exists x \in \mathbb{C} \quad x^2 = -1 \)

As before, these statements are (1) True, (2) False, (3) False, and (4) True.

Note that, in a statement with a mix of existential and universal quantifiers, the order of the quantifiers matters! For example, let \( \mathcal{H} \) be the set of all people, and let \( R(x, y) = "x \text{ loves } y" \). Think about what each of the following statements means. Do any of them have the same meaning? Are they all true or all false, or a mix of true and false statements?

1. \( \forall x \in \mathcal{H} \quad \exists y \in \mathcal{H} \quad x \text{ loves } y \)
2. \( \exists y \in \mathcal{H} \quad \forall x \in \mathcal{H} \quad x \text{ loves } y \)
3. \( \forall y \in \mathcal{H} \quad \exists x \in \mathcal{H} \quad x \text{ loves } y \)
4. \( \exists x \in \mathcal{H} \quad \forall y \in \mathcal{H} \quad x \text{ loves } y \)

**Negating a statement with quantifiers**

To negate a quantified statement, consider the following:

\[
\neg (\forall x \ P(x))
\]

means that it is *not* true that for every \( x \) in its universe, the proposition \( P(x) \) holds. That means that there must be some \( x \) for which \( P(x) \) is False. But this is the new statement

\[
\exists x \ \neg P(x)
\]

Similarly, the statement

\[
\neg (\exists x \ P(x))
\]

means that it is *not* true that there is some \( x \) in its universe for which the proposition \( P(x) \) holds. That is, there is no element \( x \) in the universe for
which \( P(x) \) is True, or in other words, \( P(x) \) is False for every possible \( x \) in the universe. This is the new statement

\[
\forall x \neg P(x)
\]

So we have the following theorem.

**Theorem 3.2.**

- The statement \( \neg(\forall x P(x)) \) is logically equivalent to the statement \( \exists x \neg P(x) \).
- The statement \( \neg(\exists x P(x)) \) is logically equivalent to the statement \( \forall x \neg P(x) \).

**Example.** To negate a statement such as

\[
\forall a \in \mathbb{Z} \ \exists n \in \mathbb{N} \ \forall x \in \mathbb{R} \quad \text{blah blah blah...}
\]

we have the following sequence of statements, each of which is logically equivalent to the one before it by the previous theorem:

\[
\neg(\forall a \in \mathbb{Z} \ \exists n \in \mathbb{N} \ \forall x \in \mathbb{R} \quad \text{blah blah blah...})
\]
\[
\exists a \in \mathbb{Z} \ \neg(\exists n \in \mathbb{N} \ \forall x \in \mathbb{R} \quad \text{blah blah blah...})
\]
\[
\exists a \in \mathbb{Z} \ \forall n \in \mathbb{N} \ \neg(\forall x \in \mathbb{R} \quad \text{blah blah blah...})
\]
\[
\exists a \in \mathbb{Z} \ \forall n \in \mathbb{N} \ \exists x \in \mathbb{R} \quad \neg(\text{blah blah blah...})
\]

Note the idea here: at each step, we are “moving the \( \neg \) inside a quantifier”, and each time we do so, we switch the quantifier to the other type: \( \forall \) becomes \( \exists \), and \( \exists \) becomes \( \forall \).

You will use this idea regularly in any setting where you must write proofs. However, one area of mathematics where this becomes especially crucial is the subject of real analysis. (Real analysis is the name that mathematicians have given to the subject “calculus, but starting from scratch and rigorously proving everything as you go.” You’ll study this in Math 131A, and perhaps also 131B and 131C, if you take those classes in the future.) As an example where you can see this sort of thing immediately rearing its head, recall the formal definition of the limit of a function, which you probably saw in some previous calculus class:
**Definition.** Definition: Let $a \in \mathbb{R}$, and let $X$ be a set of real numbers containing an open interval around $a$, except for possibly $a$ itself. Let $f: X \to \mathbb{R}$ be a function. We say that

$$\lim_{x \to a} f(x) = L$$

if for all $\varepsilon > 0$, there exists $\delta > 0$ such that for all $x \in X$,

$$|x - a| < \delta \implies |f(x) - L| < \varepsilon.$$

In this type of definition, it is implied that $\varepsilon$ and $\delta$ are real numbers, so we can take the universal set for each of them to be the set of positive real numbers. So let $\mathbb{R}_+$ denote the set of all positive real numbers. Then we can rewrite this definition in symbols as follows: $\lim_{x \to a} f(x) = L$ means

$$\forall \varepsilon \in \mathbb{R}_+ \exists \delta \in \mathbb{R}_+ \forall x \in X \ (|x - a| < \delta \implies |f(x) - L| < \varepsilon).$$

**Exercise 1.** Figure out what it means to say that $\lim_{x \to a} f(x) \neq L$.

You probably want to start by writing this in symbols, as above. But you should also be able to write it in words, more like in the original definition.

**Solution.** (Provided by Wei C.)

$$\lim_{x \to a} f(x) \neq L$$

means that

$$\exists \varepsilon \in \mathbb{R}_+ \forall \delta \in \mathbb{R}_+ \exists x \in X \ (|x - a| < \delta \land |f(x) - L| \geq \varepsilon).$$

**Exercise 2.** Figure out what it means to say that $\lim_{x \to a} f(x)$ does not exist.

Again, be able to state this in symbols or in words.
**Solution. (Provided by Aidan S.)**

\[
\lim_{x \to a} f(x) \text{ does not exist}
\]

means that

\[
\forall L \in \mathbb{R} \quad \exists \varepsilon \in \mathbb{R}_+ \quad \forall \delta \in \mathbb{R}_+ \quad \exists x \in X \quad (|x - a| < \delta \wedge |f(x) - L| \geq \varepsilon)
\]

\(\square\)

**Exercise 3 (Extra challenge).** Let \(f(x) = \cos(\pi x)\). See if you can use what you came up with for exercise 2 to prove that

\[
\lim_{x \to 0} f(x) \text{ does not exist}.
\]

(Hints: The only thing you really need to know about this function \(f\) to prove this is that \(f(\frac{1}{n}) = \pm 1\) for every whole number \(n\), and more specifically \(f(\frac{1}{n}) = 1\) if \(n\) is even, and \(f(\frac{1}{n}) = -1\) if \(n\) is odd. Also, to prove a statement of the form

\[
\forall L \in \mathbb{R} \quad P(L)
\]

start by just assuming that \(L\) is any arbitrary element of \(\mathbb{R}\). We usually do this by writing simply “Let \(L \in \mathbb{R}\.” Then prove \(P(L).\)
4 Intro to proofs: Basic proof techniques (direct, contrapositive, contradiction)

Proving a universally quantified (“for all. . .”) statement

To prove a statement about all numbers, or all functions, or all bears, the simplest way to start is to choose an arbitrary one of these things (an arbitrary number, any function, any bear). Then if you can deduce some fact about this thing, you will have proved that this fact must be true for all such things. The way we usually do this is simply by saying “Let $x$ be a number”, or “Assume $f$ is a function”, etc. As a silly example:

**Theorem.** All bears are brown.

**Proof.**
Let $b$ be a bear.

[Insert the real content of the proof here: Use cleverness and ingenuity to deduce things about $b$, concluding with . . .]

Therefore $b$ is brown.
Since $b$ was chosen arbitrarily among all bears, and we showed $b$ was brown, we have proved that all bears are brown.

Proving an if-then statement: direct proof

To prove a logical implication $P \rightarrow Q$, that is, any statement of the form “If $P$ then $Q$”, the direct method is to assume that $P$ (the hypothesis) is true, and use this to deduce that $Q$ (the conclusion) is true. Once again, the simplest way to do this is to just state “Assume $P$”. Here is a real example, that also demonstrates the technique for “for all” statements.

Recall first that an integer $n$ is called even if there exists an integer $k$ such that $n = 2k$; and $n$ is called odd if there exists $k \in \mathbb{Z}$ such that $n = 2k + 1$. As you know, any integer is either even or odd, and cannot be both.

**Theorem 4.1.** For all integers $n$, if $n$ is even then $n^2$ is even.
Proof.
Let \( n \in \mathbb{Z} \).  
[Deal with the “For all…”]
Assume \( n \) is even.  
[Assume the hypothesis.]
Then there exists \( k \) such that \( n = 2k \).
(Note: We want to show at this point that \( n^2 \) is even, which means that we need to show that there exists an integer \( l \) such that \( n^2 = 2l \).)

Therefore \( n^2 = (2k)^2 = 4k^2 = 2(2k^2) \).  
[So \( 2k^2 \) is the \( l \).]
Therefore \( n^2 \) is even.  
[The conclusion!]
We have proved that if \( n \) is even, then \( n^2 \) is even.
Since \( n \) was chosen to be an arbitrary integer, this is true for all integers \( n \).  
\( \Box \)

Proving an if-then statement: proof by contrapositive

Another way to prove a statement of the form \( P \rightarrow Q \) is to use the contrapositive. Recall that the contrapositive of \( P \rightarrow Q \) is the statement \( \neg Q \rightarrow \neg P \), and you proved in Theorem 2.1 (1) that these two are always logically equivalent. So proving \( \neg Q \rightarrow \neg P \) is equivalent to proving \( P \rightarrow Q \). This means that you start by assuming \( \neg Q \), and then deduce \( \neg P \) from that.

Here is an example. Note the difference between this proof and the previous one.

**Theorem 4.2.** For all integers \( n \), if \( n^2 \) is even then \( n \) is even.

**Proof.**
Let \( n \in \mathbb{Z} \).  
[Deal with the “For all…”]
Assume \( n \) is not even.  
[Assume \( \neg Q \).]
Then \( n \) must be odd.
Then there exists \( k \) such that \( n = 2k + 1 \).
(Note: We want to show at this point that \( n^2 \) is not even, hence is odd, which means that we need to show that there exists an integer \( l \) such that \( n^2 = 2l + 1 \).)

Therefore \( n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 \)
\[= 2(2k^2 + 2k) + 1. \]  
[So \( 2k^2 + 2k \) is the \( l \).]
Therefore \( n^2 \) is odd.  
[Deduced \( \neg P \)!]
We have proved that if $n$ is not even, then $n^2$ is not even.
Now by contrapositive, if $n^2$ is even, then $n$ is even.
Since $n$ was chosen to be an arbitrary integer, this is true for all integers $n$.

\[ \square \]

\section*{Proof by contradiction}

Finally, another common proof technique, that’s related to proof by contrapositive but is not quite the same, is proof by contradiction. Suppose you are trying to prove some conclusion $Q$. To construct a proof by contradiction, start by assuming that $Q$ is false. (That is, assume $\neg Q$.) Then use this to deduce a contradiction: a statement that is obviously false, or that directly contradicts something you’ve already proved. If assuming $Q$ is false leads to a contradiction, then certainly $Q$ must be true!\footnote{Actually, there are some mathematicians who do not accept this premise. So-called “constructivist” or “intuitionist” logic disallows proof by contradiction. At the most basic level, this comes from rejecting a logical concept known as the Law of the Excluded Middle. However, most working mathematicians are perfectly okay with proofs by contradiction.}

Here is a classic example of a proof by contradiction, which uses the previously proved theorem as a small step along the way. Note the distinction between this type of proof and a proof by contrapositive: here we assume $\neg Q$ just as before, but the conclusion we arrive at is not the negation of some hypothesis $P$. Rather, the conclusion we come to is a statement that contradicts something we’ve already concluded within the proof.

**Theorem 4.3.** $\sqrt{2}$ is not a rational number.

\section*{Proof.}
Assume that $\sqrt{2}$ is a rational number. \[ Assume \ \neg Q. \]
Then there exist integers $a$ and $b$, with $b \neq 0$, for which $\sqrt{2} = \frac{a}{b}$. Furthermore, if $a$ and $b$ had any common factor, we could divide both by that common factor to get a fraction in lowest terms. Therefore, \textit{we may assume without loss of generality} that $a$ and $b$ have no common factor.

Squaring both sides gives $2 = \frac{a^2}{b^2}$, so $a^2 = 2b^2$.
This means that $a^2$ is even.
By Theorem 4.2, $a$ must be even.
So there exists $k \in \mathbb{Z}$ such that $a = 2k$.
Then $a^2 = 2b^2$ becomes $4k^2 = 2b^2$.
Dividing by 2 yields $b^2 = 2k^2$, which means that $b^2$ is even.
Therefore by Theorem 4.2 again, $b$ is even.
But now $a$ and $b$ are both even, meaning they have a common factor of 2. This contradicts the assumption we made earlier that $a$ and $b$ have no common factor. [Contradiction!]
Therefore our assumption that $\sqrt{2}$ is rational must have been false.
So $\sqrt{2}$ is not a rational number.

\[ \square \]
5 Divisibility

It is finally time for us to start doing a little bit of number theory! To begin with, we recall a bit of notation.

Since number theory is the study of the natural numbers, we will let \( \mathbb{N} \) denote the set of all natural numbers:

\[
\mathbb{N} = \{1, 2, 3, 4, 5, \ldots \}.
\]

Note that we are defining the natural numbers to exclude the number 0, however this is just a convention. Some other textbooks (and other classes/instructors) define the natural numbers exactly as we have here, but others define the natural numbers to start from 0. *There is no definitive standard for this!* Fortunately, in practice, it won’t matter much whether 0 is included or not. But for the precise statements of theorems and definitions, do make sure you know what convention is being followed in any textbook or other source that you’re reading.

Much of what we say about the natural numbers will also be true of all integers. And it will just be useful to refer to the integers now and then. So we recall that

\[
\mathbb{Z} = \{\ldots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \ldots \}.
\]

Fortunately, unlike the natural numbers, this definition and notation is completely standard. There is never any ambiguity in what mathematicians mean when they refer to the set \( \mathbb{Z} \).

Although we won’t use them as much throughout this text, three other sets that have a standard notation similar to the above are the set of rational numbers, \( \mathbb{Q} \), the set of all real numbers, \( \mathbb{R} \), and the set of complex numbers, \( \mathbb{C} \).

**Definition 5.1.** Let \( a \) and \( b \) be integers. We say \( b \) divides \( a \) if there exists \( k \in \mathbb{Z} \) such that \( a = bk \). We write \( b \) divides \( a \) as

\[
b | a.
\]

**Remark.**
1. The notation $b \mid a$ is very unfortunate, because this notation is perfectly symmetric looking, but the relationship that it describes is not at all symmetric! For example, it is true that $5 \mid 20$ (that is, 5 divides 20), but it is not true that $20 \mid 5$ (that is, 20 does not divide 5). Since the symbol $\mid$ is symmetric, it might be hard to remember at first which way it’s supposed to go.

2. When $b$ divides $a$, we can also say that $b$ is a divisor of $a$, or $b$ is a factor of $a$, or that $a$ is a multiple of $b$. These all mean the same thing.

3. If $b$ does not divide $a$, we can write $b \nmid a$.

Examples.

1. $4 \mid 12$, since $12 = 4 \cdot 3$.

2. For any integer $n$, $(n + 1) \mid (n^2 - 1)$, because $n^2 - 1 = (n + 1) \cdot (n - 1)$, and if $n$ is an integer, $n - 1$ will be an integer as well.

For now, we collect a few basic theorems about divisibility.

**Theorem 5.2.** Let $a, b, c \in \mathbb{Z}$. If $c \mid a$ and $c \mid b$, then $c \mid (a + b)$.

*Proof.* (By Shehan F.)

Suppose $c \mid a$ and $c \mid b$.

Then, $\exists k \in \mathbb{Z}$ and $\exists l \in \mathbb{Z}$

$$a = ck \quad \text{and} \quad b = cl$$

Thus, $a + b = ck + cl = (k + l)c$.

Therefore, $c \mid (a + b)$. \hfill $\square$

**Theorem 5.3.** Let $a, b, c \in \mathbb{Z}$. If $c \mid a$ and $c \mid b$, then $c \mid (a - b)$.

*Proof.* (By Laetitia W.)

Suppose $c \mid a$ and $c \mid b$.

$c \mid a$ means $xc = a$ for some $x \in \mathbb{Z}$. 

$c \mid b$ means $yc = a$ for some $y \in \mathbb{Z}$.

Subbing in values for $a$ and $b$:

\[
\begin{align*}
    a - b &= xc - yc \\
    a - b &= c(x - y)
\end{align*}
\]

Therefore, $c \mid (a - b)$.

**Theorem 5.4.** Let $a, b, c \in \mathbb{Z}$. If $c \mid a$ and $c \mid b$, then $c \mid ab$.

**Proof.** (By Lucas M.)

Suppose $c \mid a$ and $c \mid b$.

$c \mid a \iff \exists k \in \mathbb{Z} \ a = ck, c \mid b \iff \exists n \in \mathbb{Z} \ b = cn$

Multiplying the equations, $ab = c^2nk = c(cn)$

$\exists k \in \mathbb{Z} \ x = cnk$

$ab = cx \rightarrow c \mid ab$  

**Remark.** Can you come up with a simpler version of Theorem 5.4? It should be a “stronger” theorem. Why? What do I mean by “stronger” here?

**Solution.** (By Aidan S.)

You don’t need to assume both $c \mid a$ and $c \mid b$. Just assuming one or the other is enough:

**Theorem.** Let $a$, $b$, and $c$ be integers. If $c \mid a$, then $c \mid ab$.

**Proof.** Assume $c \mid a$. So $\exists k \in \mathbb{Z}$ s.t. $a = kc$.

So $ab = kcb = (kb)c$. Since $kb \in \mathbb{Z}$, we have $c \mid ab$.

This is a “stronger” theorem because we are not assuming as many things, but we reach the same conclusion as before.

Another way of saying this is that we have “weakened the hypothesis”. When you can state a theorem with a weaker hypothesis (i.e. not assuming as many things) but the same conclusion, you have stated a stronger theorem.

**Theorem 5.5.** Let $a$, $b$, and $c$ be integers. If $c \mid a$ and $c \mid b$, then $c \mid (ax + by)$ for any $x, y \in \mathbb{Z}$.  

20
Proof. (By Maddie Y.)
Assume \( c \mid a \) and \( c \mid b \).
\[ \exists k \in \mathbb{Z} \text{ s.t. } a = ck. \]
\[ \exists m \in \mathbb{Z} \text{ s.t. } b = cm. \]
Let \( x \in \mathbb{Z} \) and \( y \in \mathbb{Z} \).
\[ ax + by = c(kx + my) \text{ by substitution.} \]
\[ ax + by = (kx + my)c \]
\[ kx + my \in \mathbb{Z} \]
So \( c \mid (ax + by) \).
Since \( x \) and \( y \) were chosen arbitrarily from \( \mathbb{Z} \), we have shown that for all \( x, y \in \mathbb{Z} \), \( c \mid (ax + by) \).

Theorem 5.6. Let \( a, b \in \mathbb{N} \). If \( b \mid a \) then \( b \leq a \).

Proof. (By Mien T., Christine D.)
Assume that \( b \mid a \) is true.
\( b \) divides \( a \) iff there exists some integer \( k \) such that \( a = bk \).
\[ b = \frac{a}{k} = \frac{1}{k} \cdot a \]
\[ k \in \mathbb{N} \quad k \geq 1 \quad \frac{1}{k} \leq 1 \quad \frac{1}{k} - 1 \leq 0 \]
\[ b - a = \frac{1}{k} \cdot a - a = \frac{1}{k} \cdot (a - 1) \]
\[ b - a \leq 0 \]
\[ b \leq a \]

Theorem 5.7. Let \( a \) and \( b \) be natural numbers. If \( b \mid a \) and \( a \mid b \) then \( a = b \).

Proof. (By Samanda H.)
Assume that \( b \mid a \) and \( a \mid b \).
Since \( b \mid a \), \( b \leq a \).
Since \( a \mid b \), \( a \leq b \).
Therefore \( a = b \).

Having now defined divisors, we can proceed to define what is perhaps the most important concept in all of number theory:
Definition 5.8. A natural number \( n \) is called a *prime number* if the only positive integers that divide \( n \) are 1 and \( n \).

Prime numbers are a theme that will come up over and over again in this course. But for now, just knowing the definition will suffice.
The Division-with-Remainder Theorem

**Theorem 6.1** (The Division-with-Remainder Theorem\(^2\)). Let \(a\) and \(b\) be integers, with \(b > 0\). Then there exist unique integers \(q\) and \(r\) such that

\[
a = bq + r \quad \text{and} \quad 0 \leq r < b.
\]

**Proof.** (Existence) We’ll do this on Wednesday.

(Uniqueness) (By Wei C., Aidan S.)

Assume there exist \(q_1, r_1, q_2, r_2 \in \mathbb{Z}\) such that \(a = b \cdot q_1 + r_1\) with \(0 \leq r_1 < b\) and \(a = b \cdot q_2 + r_2\) with \(0 \leq r_2 < b\).

\[
q_1 \cdot b + r_1 = q_2 \cdot b + r_2
\]

\[
b(q_1 - q_2) = r_2 - r_1
\]

\[
b \mid (r_2 - r_1)
\]

\(-b < r_2 - r_1 < b\) \quad \text{Why?}

The only integer in this range that is a multiple of \(b\) is 0, so we must have \(r_2 - r_1 = 0\).

\[
r_1 = r_2
\]

\[
q_1 = q_2 \quad \text{Why?}\]

\[\Box\]

**Remark.** The idea of this theorem is something you probably learned many years ago: you are trying to divide \(a\) by \(b\). The number \(q\) that you get is called the **quotient**, and the number \(r\) is called the **remainder**.

**Examples.**

- \(a = 22, b = 5\): \(22 = 5 \cdot 4 + 2\)
- \(a = 9374, b = 38\): \(9374 = 38 \cdot 246 + 26\)
- \(a = -26, b = 6\): \(-26 = 6 \cdot (-5) + 4\)

Note that in this example, we didn’t use \(q = -4\) and \(r = -2\), which would also give the correct calculation \((-26 = 6 \cdot (-4) + -2\)), because the theorem requires the remainder \(r\) to be nonnegative.

\(^2\)This theorem is also known as The Division Algorithm, even though it’s not an algorithm. The concept is also sometimes called Euclidean Division, although Euclid had nothing to do with it, and may not have even known this theorem.
Theorem 6.2. Let $a,b \in \mathbb{Z}$ with $b > 0$. Assume that $q$ and $r$ are integers such that $a = b \cdot q + r$ and $0 \leq r < b$, as given by the Division-with-Remainder Theorem. Then

1. $b \mid a$ if and only if $r = 0$.
2. If $c \mid a$ and $c \mid b$, then $c \mid r$.
3. If $c \mid b$ and $c \mid r$, then $c \mid a$.

Proof. To be completed by you! 

Exercise 1. With the same hypotheses as the above theorem, is it true that if $c \mid a$ and $c \mid r$, then $c \mid b$? Prove or give a counterexample.

Solution. To be completed by you!
7 Greatest common divisors and the Euclidean Algorithm

Definition 7.1. Let \( a \) and \( b \) be integers, not both 0. The greatest common divisor of \( a \) and \( b \) is a positive integer \( d \) satisfying the following two properties:

(i) \( d \mid a \) and \( d \mid b \)

(ii) For all \( c \in \mathbb{Z} \), if \( c \mid a \) and \( c \mid b \), then \( c \leq d \)

We write \( \gcd(a,b) \) for the greatest common divisor of \( a \) and \( b \).

Remark. Although in this class, we will write \( \gcd(a,b) \) for the greatest common divisor of \( a \) and \( b \), in many number theory textbooks and papers, the standard way of writing the greatest common divisor of \( a \) and \( b \) is the (rather ambiguous) notation \( (a,b) \).

Examples.

- \( \gcd(75,45) = 15 \)
- \( \gcd(84,34) = 2 \)
- \( \gcd(-60,24) = 12 \)
- \( \gcd(-35,-57) = 1 \)