Recall from last week this definition and the following theorem.

**Definition.**

A prime number is a number that can only be divided evenly by 1 or itself.

**Fundamental Theorem of Arithmetic.**

Any integer greater than 1 is either a prime number, or can be written as a unique product of prime numbers (ignoring the order).

1 Proof by Contradiction - More Examples

**Theorem.**

There are an infinite number of primes.

**Proof.**

Q. How can we prove this directly? How can we show a set is infinite?

A. Not easy in this case.
We will prove that there are an infinite number of primes using *proof by contradiction*. Assume that there are a *finite* number \( n \) of primes. Therefore, we can list them all:

\[
p_1, p_2, p_3, \ldots, p_n
\]

Consider the number \( p_1 \cdot p_2 \cdot p_3 \cdots p_n + 1 \).

By the *Fundamental Theorem of Arithmetic* there exists a unique prime factorization of this number.

Consider any prime number \( p_i \). Does this number divide \( p_1 \cdot p_2 \cdot p_3 \cdots p_n + 1 \)?

No, there is always a remainder of 1.

Therefore, none of our \( n \) primes is a factor of \( p_1 \cdot p_2 \cdot p_3 \cdots p_n + 1 \) so by definition of a prime number, \( p_1 \cdot p_2 \cdot p_3 \cdots p_n + 1 \) is prime.

Therefore there are now \( n + 1 \) prime numbers contradicting our assumption that there are \( n \). Therefore there are an infinite number of prime numbers.

**Summary:**

---

**Proof by Contradiction.**

Claim: \( P \)

Assume \( \neg P \).

Derive a *false* statement.

Conclude the assumption was wrong. Therefore \( P \).

---

**Q.** Suppose our claim \( P \) above is of the form \( \forall x \in X, a(x) \rightarrow b(x) \). What is \( \neg P \)?

**A.**

\[
\neg P
\]

\[
\iff \neg (\forall x \in X, a(x) \rightarrow b(x))
\]

\[
\iff \exists x \in X, \neg (\neg a(x) \vee q(x))
\]

\[
\iff \exists x \in X, a(x) \land \neg b(x).
\]

Usually we still use proof by contrapositive, but in some instances, it may be helpful to look at proof by contradiction of an implication.
1.1 Proof by Contradiction and Contrapositive Practice

Prove the following claims using proof by contrapositive or proof by contradiction.

**Claim:** $\forall n \in \mathbb{Z}, n^2$ is even $\rightarrow$ $n$ is even.

**Proof.**

First restate the claim by taking the contrapositive.

$\forall n \in \mathbb{Z}, n$ is odd $\rightarrow$ $n^2$ is odd.

Since $n$ is odd, exists a $k$ such that $n = 2k + 1$ and then $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1 = \text{even} + 1 = \text{odd}$.

**Claim:** The difference of any rational number and any irrational number is irrational.

**Proof.**

First restate the claim and then for a proof by contradiction, take the negation.

We are saying for all real numbers $x$ and $y$, if $x$ is rational and $y$ is irrational then $x - y$ is irrational.

$$\forall x \in \mathbb{R}, \forall y \in \mathbb{R}, (x \in \mathbb{Q} \land y \notin \mathbb{Q}) \rightarrow (x - y) \notin \mathbb{Q}.$$ 

Negating gives:

$$\exists x \in \mathbb{R}, \exists y \in \mathbb{R}, (x \in \mathbb{Q} \land y \notin \mathbb{Q}) \land (x - y) \in \mathbb{Q}$$

Suppose $x$ is rational so $\exists a \in \mathbb{Z}, \exists b \in \mathbb{Z}^+, x = \frac{a}{b}$ and that $x - y$ is rational so $\exists c \in \mathbb{Z}, d \in \mathbb{Z}^+, x - y = \frac{c}{d}$.

Then $x - y = \frac{c}{d} = \frac{a}{b} - y$ and $y = \frac{a}{b} - \frac{c}{d} = \frac{ad - bc}{bd}$. Since $b, d \in \mathbb{Z}^+$ so is $bd$ and similarly by closure of the integers under multiplication, $ab \in \mathbb{Z}$ and $bc \in \mathbb{Z}$. Therefore $y \in \mathbb{Q}$. Now, $y \notin \mathbb{Q} \land y \in \mathbb{Q}$, which is a contradiction. Therefore by contradiction,

$$\forall x \in \mathbb{R}, \forall y \in \mathbb{R}, (x \in \mathbb{Q} \land y \notin \mathbb{Q}) \rightarrow (x - y) \notin \mathbb{Q}.$$ 

**Claim:** $\sqrt{5}$ is irrational.

**Proof.**

First restate the claim by taking the negation.

This is the same proof as for $\sqrt{2}$. 

3
2 Proof by Cases - aka Proof by Exhaustion

Claim. Prove that if \( n \in \mathbb{Z} \), then \( 3n^2 + n + 14 \) is even.

Proof.

Two cases:

Case 1: \( n \) is even. So \( \exists k \in \mathbb{N}, 2k = n \). So

\[
3(2k)^2 + 2k + 14 = 12k^2 + 2k + 14 = 2(6k^2 + k + 7)
\]

and \( 3n^2 + n + 14 \) is even.

Case 2: \( n \) is odd. So \( \exists k \in \mathbb{N}, 2k + 1 = n \). So

\[
3(2k + 1)^2 + (2k + 1) + 14 = 3(4k^2 + 2k + 1) + 2k + 1 + 14
\]

\[
= 12k^2 + 6k + 2k + 18 = 2(6k^2 + 4k + 9)
\]

So \( 3n^2 + n + 14 \) is even.

---

Proof by Cases.

Claim: \( \forall x \in D, p(x) \rightarrow q(x) \)

Split the domain \( D \) into disjoint sets \( S_1, S_2, \ldots, S_k \) such that their union equals \( D \).

For each set \( S_i \) show that \( \forall x \in S_i, p(x) \rightarrow q(x) \).

Since \( \bigcup_i S_i = D \), conclude that \( \forall x \in D, p(x) \rightarrow q(x) \).
More Practice - All proof techniques.

Claim. Prove for every prime number \( p > 3 \), \( p = 6n + 1 \) or \( p = 6n + 5 \). First write the statement using quantifiers and logic and then prove it’s correctness.

\[
\forall p \in \mathbb{N}, (\text{prime}(p) \land p > 3) \rightarrow p = 6n + 1 \lor p = 6n + 5
\]

We can prove this using contrapositive:

\[
\forall p \in \mathbb{N}, (p \neq 6n + 1 \land p \neq 6n + 5) \rightarrow \neg \text{prime}(p) \lor p \leq 3
\]

Let \( p \) be a natural number and suppose \( p \neq 6n + 1 \) and \( p \neq 6n + 5 \),

then \( p = 6n + i \) for \( i = 0, 2, 3, 4 \).

Notice that for \( n > 0 \), for each \( i \) we can factor \( 6n + i \) by 2 or 3 which means that \( p \) is not prime.

If \( n = 0 \), then \( p = 0, 2, 3 \) or 4.

Since \( p \leq 3 \) for \( p = 0, 2, 3 \) and \( p = 4 \) is not prime we have shown \( \neg \text{prime}(p) \lor p \leq 3 \).

And

\[
\forall p \in \mathbb{N}, (p \neq 6n + 1 \land p \neq 6n + 5) \rightarrow \neg \text{prime}(p) \lor p \leq 3
\]

and by contrapositive we have shown

\[
\forall p \in \mathbb{N}, (\text{prime}(p) \land p > 3) \rightarrow p = 6n + 1 \lor p = 6n + 5
\]

Claim.

\[
\forall a \in \mathbb{Z}, a \equiv_6 3 \rightarrow a \not\equiv_3 2
\]

Prove the statement.

Proof.

Turns out the contrapositive is not the best way to write the proof! Try it.

\[
\forall a \in \mathbb{Z}, a \equiv_6 3 \rightarrow a \not\equiv_3 2
\]

Let \( a \) be in \( \mathbb{Z} \). Suppose \( a \equiv_6 3 \).

Notice that if \( a \equiv_6 3 \) then \( a = 6q + 3 \)

Then consider \( a \mod 3 = 6q + 3 \mod 3 = 0 \). Since \( a \equiv_3 0 \not\equiv_3 2 \)

Therefore \( a \not\equiv_3 2 \).

Proof by Induction

After all the proof practice we have done, proof by induction is the easiest to set up. The reason is that individually we know how to do all the steps already and the set up follows a standard format.
Proof by Induction: Claim $\forall n \in \mathbb{N}, S(n)$.

**Base Case:** The part where we prove $S(n)$ is true for one or more smallest values of $n_0$.

**Inductive Hypothesis.** Assume that $S(k)$ is true for an arbitrary natural number $k \geq n_0$.
(Optional depending on how carefully you prove the Inductive Step).

**Inductive Step:** The part where we prove $\forall k \in \mathbb{N}, (k \geq n_0 \land S(k)) \rightarrow S(k + 1)$. Notice that we know how to prove statements of this form!!

When we prove a statement of the form

$$(k \geq n_0 \land S(k)) \rightarrow S(k + 1),$$

we assume that $k \geq n_0$ and $S(k)$ is true and prove that $S(k + 1)$ is therefore true.

The assumption that $S(k)$ is true is called the **Inductive Hypothesis**. Often to make it clear for which values of $k$ we are assuming $S()$ holds for we explicitly state the hypothesis as follows:

**Induction Hypothesis.** Assume that for arbitrary natural number $k \geq n_0$, $S(k)$ holds.

When we use the assumption that $S(k)$ holds, we need to refer to it...and say “by the induction hypothesis. Let’s try it!

**Exercise 1.** Prove that the sum of the first $n$ odd natural numbers equals $n^2$.

**Solution.**

Let $S(n)$ be:

The sum of the first $n$ odd natural numbers equals $n^2$, ie. $\sum_{i=0}^{n-1} 2i + 1 = n^2$.

**Base Case** $n=1$ then $1 = 1^2$.

**I.H.** Let $k \in \mathbb{N}$. Assume that $S(k)$ holds, ie, that $\sum_{i=0}^{k-1} 2i + 1 = k^2$.

**i.S** Prove $S(k + 1)$. Consider the left hand side:

$$\sum_{i=0}^{k} 2i + 1 = 2k + 1 + \sum_{i=1}^{k-1} 2i + 1$$

$$= 2k + 1 + k^2 \text{ by I.H.}$$

$$= (k + 1)^2$$

**Exercise 2.** Prove for all natural numbers $n$, $3^n - 1$ is a multiple of 2.
Let $P(n)$ be:
\[ \exists m \in \mathbb{N}, 3^n - 1 = 2m \]

Prove $P(n)$ for all $n \in \mathbb{N}$.

**Base Case** $n=0$. $3^0 - 1 = 0$ Let $m = 0$ and we are done.

**I.H.** Assume $P(k)$ holds for arbitrary $k \in \mathbb{N}$.

**I.S.** Prove $P(k + 1)$.
\[
3^{k+1} - 1 = 3 \cdot 3^k - 1 \\
= (2 + 1)3^k - 1 \\
= (2 \cdot 3^k) + 3^k - 1 \\
= 2 \cdot 3^k + 2m \text{ by induction hypothesis} \\
= 2(3^k + m)
\]

Therefore there exists a natural number $m^*$ equal to $3^k + m$ such that
\[ 3^{k+1} - 1 = 2 \cdot m^* \]

**Exercise 3.** Use mathematical induction to prove that for all integers $n \geq 1$, $n^3 - n$ is divisible by 3.

**Solution.** Let $S(n)$ be $\exists b \in \mathbb{Z}, 3b = n^3 - n$. Prove $\forall n \in \mathbb{Z}^+, S(n)$.

**Base Case.** $n = 1$. Then $1^3 - 1 = 0$. Let $k = 0$ and $3k = n^3 - n$.

**I.H.** Assume for arbitrary $k \in \mathbb{Z}$, $k \geq 1$ that $S(k)$ holds.

**I.S.** Prove that $S(k) \implies S(k + 1)$.
Assume $S(k)$ holds. Then $\exists b \in \mathbb{Z}, k^3 - k = 3b$.
Consider $S(k+1)$. We need to show there exists $b' \in \mathbb{Z}$ such that $(k+1)^3 - (k+1) = 3b'$.
\[
(k+1)^3 - (k+1) = k^3 + 3k^2 + 3k + 1 - k - 1 = k^3 + 3k^2 + 2k = k^3 - k + (3k^2 + 3k) = 3b + 3(k^2 + k) \text{ by the induction hypothesis} \\
3b' = b + k^2 + k.
\]
Therefore there exists $b' \in \mathbb{Z}$ such that $(k + 1)^3 - k = 3b'$ and $S(k + 1)$ holds.

Therefore by induction $\forall n \in \mathbb{Z}^+, S(n)$.

**Exercise 4** We define a line map in the following way:

**Base.** A blank rectangle is a line map (this is the case where the number of lines is 0).

**Recursion.** Drawing a straight line all the way across a line map creates a new line map (this is how we increase the number of lines by 1).
Prove that any line map can be 2-coloured.

Note: This type of proof is a little trickier.

In the induction step, you cannot assume that the claim holds for \( k \) lines and then add a line to get \( k + 1 \) lines.

Instead assume the claim holds for \( k \) lines, then consider an arbitrary set up with \( k + 1 \) lines. Now consider removing a line and then putting it back....you should understand why the first way doesn’t work.

Sample Soln.

Let \( P(n) \) be: a line map on \( n \) lines admits a 2-colouring.

Prove \( \forall n \in \mathbb{N}, P(n) \).

**Base Case.** \( n = 0 \). Then the empty rectangle can be coloured with 1 colour which is a 2-colouring.

**I.H.** Assume that for arbitrary \( k \geq 0 \), \( P(k) \).

**I.S.** Prove \( P(k) \rightarrow P(k + 1) \).

Consider a line map with \( k + 1 \) lines. Remove any one line. The line map that remains has \( k \) lines and by I.H. \( P(k) \) holds so there exists a 2-colouring.

Add back the removed line \( L \). \( L \) splits the rectangle into two pieces. Reversing the colours on the regions created by adding \( L \) back creates a valid 2-colouring.
Triangles $\triangle acf, \triangle bcd, \triangle def, \triangle abe$ are formed by four lines.

Remember this problem?!!

Let $S(n)$ represent the following:

Given $n$ lines in the plane such that no two are parallel and no three intersect in a single point. These $n$ lines form $\binom{n}{3}$ triangles.

Claim. $\forall n \in \mathbb{N} \geq 3, S(n)$.

Proof.

Base Case.

$n = 3$. Then there is 1 triangle and $1 = \binom{3}{3}$.

I.H. Assume for arbitrary $3 \leq k$ that $S(k)$ holds.

I.S. Prove that $S(k) \rightarrow S(k + 1)$.

Consider $k + 1$ lines in the plane. Choose any of the $k + 1$ lines. Remove this line and the remaining $k$ lines, by I.H., $S(k)$ holds so there are $\binom{k}{3}$ triangles.

Consider adding the $k + 1$ line back. Each time this $k + 1^{st}$ line intersects any pair of lines, it creates a new triangle. Therefore the $k + 1^{st}$ line creates $\binom{k}{2}$ new triangles. So the total number of triangles is:

\[
\binom{k}{3} + \binom{k}{2} = \frac{k!}{(k-3)!3!} + \frac{k!}{(k-2)!2!} = \frac{(k-2)!k! + 3k!}{(k-2)!3!} = \frac{k \cdot k! - 2k! + 3k!}{(k+1-3)!3!} = \frac{(k+1)k!}{((k+1)-3)!3!} = \frac{(k+1)!}{((k+1)-3)!3!} = \binom{k+1}{3}
\]
**Challenge – Stamp Example – Simple Induction**

Try this! We will see an easier way to prove this next week.
Given an *unlimited supply* of 4-cent and 7-cent stamps, prove that there exists a *combination* of stamps to make any *amount* of *postage* that is *18-cents or more*.

Define $S(n)$, what we are proving:

In English: Postage of exactly $n$ cents can be made using only 4-cent and 7-cent stamp.

Formally: $S(n) : \exists a \in \mathbb{N}, \exists b \in \mathbb{N}, n = 4a + 7b$

**Prove**: $\forall n \in \mathbb{N}^{\geq 18}, S(n)$.

**Steps**

1. **Base Case**:
   
   $n = 18$

   $18 = 1 \cdot 4 + 2 \cdot 7$ so pick $a = 1$ and $b = 2$.

2. **Inductive Hypothesis (IH)**

   Let $k \in \mathbb{N}, k \geq 18$, suppose $S(k)$.

   i.e., there exists $i, j \in \mathbb{N}$ such that $i$ represents the number of 4 cent stamps and $j$ represents the number of 7 cent stamps and $k = 4i + 7j$

3. **Inductive Step (IS)**: Prove for $k \geq 18$, $S(k) \rightarrow S(k + 1)$ holds.