2.1-2.3 Proofs

A mathematical proof is a logical argument that justifies that a certain conclusion must follow from certain hypotheses. All proofs start with assumptions, some of which are axioms: propositions that are assumed to be true.

All mathematical proofs involve some axiom(s).

A direct proof is a mathematical proof where the hypotheses lead directly to the conclusion.

Consider the following definitions: Let $f(x)$ be a real-valued function over the domain $\mathbb{R}$. The function $f$ is odd if $\forall x \in \mathbb{R}$, $f(-x) = -f(x)$. $f$ is even if $\forall x \in \mathbb{R}$, $f(-x) = f(x)$.

Let’s prove the following theorem (a proposition requiring proof):

**Theorem**: The composition of an odd function with an odd function is an odd function.

**Proof**: Let $f$ and $g$ be odd real-valued functions over the domain $\mathbb{R}$. Then $\forall x \in \mathbb{R}$, $f(-x) = -f(x)$ and $g(-x) = -g(x)$. Let $h = f \circ g$. Let $x \in \mathbb{R}$. Then it follows that $h(-x) = f(g(-x)) = f(-g(x)) = -f(g(x)) = -h(x)$ since $f, g$ are odd. Hence $h$ is odd □

**Theorem**: $\forall n \in \mathbb{N}$, $1 + 2 + \cdots + n = n(n+1)/2$.

**Proof**: Let $n \in \mathbb{N}$. Let $S = 1 + 2 + \cdots + n$. Then $S = n + (n-1) + \cdots + 1$. Adding these two equations cleverly yields

$$2S = (n + 1) + (n + 1) + \cdots + (n + 1) = n(n + 1).$$

So $S = n(n+1)/2$, which completes the proof □

Consider these definitions:

1. An integer $n$ is even if $\exists k \in \mathbb{Z}$ such that $n = 2k$.
2. An integer $n$ is odd if $\exists k \in \mathbb{Z}$ such that $n = 2k + 1$.
3. An integer $n$ is divisible by an integer $k$ if $\exists m \in \mathbb{Z}$ such that $n = km$. We call such $a$ $k$ a divisor of $n$.
4. An natural number $p$ is prime if $p \neq 1$ and the only positive integer divisors of $p$ are 1 and $p$.

Basic exercise left for you: Prove that the sum of two even integers is even and the sum of two odd integers is even.
Let’s prove the following theorem:

Theorem: For all sets $X, Y, Z$, if $X \cap Y = X \cap Z$ and $X \cup Y = X \cup Z$ then $Y = Z$.

Proof: Let $X, Y, Z$ be sets. Assume $X \cap Y = X \cap Z$ and $X \cup Y = X \cup Z$. We need to show that $Y$ and $Z$ are subsets of each other:

Let $y \in Y$. Then $y \in X \cup Y$. So $y \in X \cup Z$. That means $y \in X$ or $y \in Z$. So we have two cases ($y \in X$ or $y \in Z$). Suppose $y \in X$. Then $y \in X \cap Y$. So $y \in X \cap Z$. Then $y \in Z$. Thus both cases $y \in Z$. Hence $Y \subseteq Z$.

Reversing the argument should be obvious by symmetry (just swap the roles of $Y$ and $Z$). Therefore $Y = Z$ □

Here is a cute example:

Theorem: $\forall n \in \{10, 11, 12, \ldots\}$, the product of the digits of $n$ is less than $n$.

Proof: Let $n \in \{10, 11, 12, \ldots\}$. There exists $k \in \mathbb{N}$ such that $10^k \leq n < 10^{k+1}$. So we may write $n = \sum_{i=0}^{k} d_i 10^i$ where $d_0, d_1, \ldots, d_k$ are digits.

The product of digits $P = \prod_{i=0}^{k} d_i$ is a product of non-negative integers less than 10. Thus

$$P = d_k \prod_{i=0}^{k-1} d_i < d_k 10^k \leq d_k 10^k + d_{k-1} 10^{k-1} + \cdots + d_1 10 + d_0 = n \ □$$

An indirect proof is a proof of a proposition by proving an equivalent proposition.

There are two types (let $p, q$ represent propositions below):

(i) A proof by contrapositive shows that a conditional proposition $p \Rightarrow q$ is true by showing that the logically equivalent contrapositive $\neg q \Rightarrow \neg p$ is true.

(ii) A proof by contradiction shows that a proposition $p$ is true by showing that $\neg p \Rightarrow (q \land \neg q)$.

Note: The proposition $q \land \neg q$ is always false. Such a proposition is called a contradiction. A proposition that is always true is a tautology.

You should verify for yourself that $p \equiv \neg p \Rightarrow (q \land \neg q)$ using a truth table.
Here is a proof by contrapositive example:

**Theorem**: Suppose $a \in \mathbb{R}^+$ and $n \in \mathbb{N}$. If $a^n \notin \mathbb{Q}$ then $a \notin \mathbb{Q}$.

**Proof**: Let $a \in \mathbb{R}^+$ and $n \in \mathbb{N}$. We will prove the contrapositive of $a^n \notin \mathbb{Q} \Rightarrow a \notin \mathbb{Q}$:

$a \in \mathbb{Q} \Rightarrow a^n \in \mathbb{Q}$.

Suppose $a \in \mathbb{Q}$. Then $\exists p, q \in \mathbb{Z}$ with $q \neq 0$ such that $a = \frac{p}{q}$. From this we get

$$a^n = \left(\frac{p}{q}\right)^n = \frac{p^n}{q^n}.$$ 

Since $p^n, q^n \in \mathbb{Z}$ and $q^n \neq 0$ it follows that $a^n \in \mathbb{Q}$. □

Here is another:

**Theorem**: Suppose $a \in \mathbb{Z}$. If $a^2$ is even then $a$ is even.

**Proof**: Let $a \in \mathbb{Z}$. Assume $a$ is not even, which means it is odd (since the even and odd integers form a partition of $\mathbb{Z}$). Then $a = 2k + 1$ for some $k \in \mathbb{Z}$. Then $a^2 = 2(2k^2 + 2k) + 1$ is odd since $2k^2 + 2k \in \mathbb{Z}$. So $a^2$ is not even. We have proved that if $a$ is not even then $a^2$ is not even. This completes the proof by contrapositive □

A classic example of a proof by contradiction:

**Theorem**: $\sqrt{2} \notin \mathbb{Q}$.

**Proof**: Suppose that $\sqrt{2} \in \mathbb{Q}$. Then we can write $\sqrt{2} = \frac{p}{q}$ where $p, q \in \mathbb{Z}$ and $q \neq 0$.

Without loss of generality we may assume that $p, q$ are not both even (if they were we could cancel 2 until they weren’t any longer).

Then $p = q\sqrt{2}$ and hence $p^2 = 2q^2$. Then $p^2$ is even. That means $p$ is even, and thus $p = 2k$ for some $k \in \mathbb{Z}$. But then $p^2 = 2q^2$ becomes $4k^2 = 2q^2$ which reduces to $2k^2 = q^2$.

Then $q^2$ is even. That means $q$ is even. This contradicts the premise that $p, q$ are not both even □

Note: Any proof by contrapositive can always be reformatted into a proof by contradiction (by assuming $p$ is true at the start, followed by assuming $\neg q$).
More examples of a proof by contradiction:

**Theorem**: The sum of a rational and irrational is irrational.

**Proof**: Suppose otherwise. Then $\exists x, y \in \mathbb{R}$ such that $x \in \mathbb{Q}$ and $y \not\in \mathbb{Q}$, but $x + y \in \mathbb{Q}$. Then $\exists p_1, p_2, q_1, q_2 \in \mathbb{Z}$ with $q_1 \neq 0$ and $q_2 \neq 0$ such that

$$x = \frac{p_1}{q_1} \text{ and } x + y = \frac{p_2}{q_2}.$$

Then $y = (x + y) - x = \frac{p_2}{q_2} - \frac{p_1}{q_1} = \frac{p_2q_1 - p_1q_2}{q_1q_2}$ is in $\mathbb{Q}$ since $p_2q_1 - p_1q_2, q_1q_2 \in \mathbb{Z}$ and $q_1q_2 \neq 0$.

That contradicts the assumption that $y \not\in \mathbb{Q}$. ∎

**Theorem**: Suppose 15 non-negative integers sum to 100. Then at least two must be the same.

**Proof**: Suppose otherwise. That is, suppose there exists 15 non-negative integers $a_1, a_2, ..., a_{15}$ that are pairwise distinct and whose sum is 100. Without loss of generality assume they are in an increasing order. Then $a_i \geq i - 1$ and thus

$$100 = \sum_{i=1}^{15} a_i \geq \sum_{i=1}^{15} (i - 1) = \sum_{k=1}^{14} k = (14)(15)/2 = 105.$$

This contradiction completes the proof. ∎

An existence proof proves the existence of a mathematical object.

An existence proof is **constructive** if it exhibits such an object. Otherwise it is called **nonconstructive**.

Here is an example of a constructive existence proof:

**Theorem**: There exists a real-valued function over the domain $\mathbb{R}$ that is continuous over $\mathbb{R}$, but not differentiable over $\mathbb{R}$.

**Proof**: Consider $f(x) = |x|$. $f$ is continuous over $\mathbb{R}$, but not differentiable at $x = 0$. So $f(x) = |x|$ is such a function.
Here is another example of an existence proof:

**Theorem:** There exists two irrational real numbers \(a\) and \(b\) such that \(a^b\) is rational.

**Proof:** Let \(x = y = \sqrt{2}\). If \(x^y\) is rational then we are done since \(\sqrt{2}\) is irrational. Otherwise, \(x^y\) is irrational. Then by setting \(a = x^y\) and \(b = \sqrt{2}\) we have that \(a^b = (x^y)^b = x^{by} = (\sqrt{2})^{\sqrt{2} \sqrt{2}} = (\sqrt{2})^2 = 2\), which is rational \(\square\)

Do you see that this proof is non-constructive?

A uniqueness proof for a mathematical object that exists, shows that there is only one such object. We often use \(\exists!\) as a quantifier to denote that there exists a unique object. For example, consider the statement \(\exists!n \in \mathbb{N}, n^2 = 9\).

**Theorem:** The real-valued function \(y(x) = x^2 + 1\) over the domain \(\mathbb{R}\) is the unique real-valued differentiable function over the domain \(\mathbb{R}\) satisfying \(y'(x) = 2x, y(0) = 1\).

**Proof:** Let \(y(x) = x^2 + 1\). Then \(y'(x) = 2x\) and \(y(0) = 1\). Suppose \(f(x)\) is a real-valued differentiable function over the domain \(\mathbb{R}\) satisfying \(y'(x) = 2x, y(0) = 1\).

Then \((y(x) - f(x))' = y'(x) - f'(x) = 2x - 2x = 0\). So \(y(x) - f(x) = C\) for some constant \(C \in \mathbb{R}\). But evaluating at \(x = 0\) yields \(C = y(0) - f(0) = 1 - 1 = 0\). Hence \(y(x) = f(x)\). So the function \(y(x) = x^2 + 1\) is the unique function satisfying \(y'(x) = 2x, y(0) = 1\) \(\square\)

**THE PRINCIPLE OF MATHEMATICAL INDUCTION (WEAK FORM):**

Suppose \(S(n)\) is a propositional function over the domain \(D = \{n_0, n_0 + 1, n_0 + 2, \ldots\}\) where \(n_0 \in \mathbb{Z}\).

Suppose both of the following statements are true:

(i) \(S(n_0)\) is true.
   
   [The base case.]

(ii) For all \(n \in D\), if \(S(n)\) is true then \(S(n + 1)\) is true.
   
   [The inductive step; the hypothesis of the implication is the inductive hypothesis.]

Then \(S(n)\) is true for all \(n \in D\).
One nice analogy for the logical underpinning of this principle is the following:

Imagine an infinite set of dominos labeled 1, 2, 3, ... Suppose you can stack all the dominos in along a curve such that if domino \( i \in \mathbb{N} \) falls it will cause domino \((i + 1)\) to fall. Now imagine you knock over domino 1. What happens?

Let’s prove the following relatively simple fact...

**Theorem:** For all \( n \in \mathbb{N} \), \( 1 + 3 + \cdots + (2n - 1) = n^2 \).

**Proof:** Let start with the case \( n = 1 \). Then \( 1 + 3 + \cdots + (2n - 1) = 1 \) and \( n^2 = 1 \). That establishes the base case.

Let \( n \in \mathbb{N} \). Here is the inductive hypothesis: Assume \( 1 + 3 + \cdots + (2n - 1) = n^2 \).

We need to show that \( 1 + 3 + \cdots + (2n - 1) + (2(n + 1) - 1) = (n + 1)^2 \). Be careful not to assume that this is true [**].

Well,

\[
1 + 3 + \cdots + (2n - 1) + (2(n + 1) - 1) = 1 + 3 + \cdots + (2n - 1) + (2n + 1)
\]

\[
= [1 + 3 + \cdots (2n - 1)] + (2n + 1)
\]

\[
= [n^2] + (2n + 1)
\]

\[
= (n + 1)^2.
\]

This completes the proof by induction \( \square \)

[**] This is where many induction proofs go sour; do not assume the conclusion of the implication you must prove!

Let’s prove the following by induction...

**Theorem:** For all integers \( n > 1 \), \( \frac{1}{0!} + \frac{1}{1!} + \cdots + \frac{1}{n!} < 3 - \frac{2}{(n + 1)!} \).

**Proof:** Let’s start with the case \( n = 2 \). Then

\[
\frac{1}{0!} + \frac{1}{1!} + \cdots + \frac{1}{n!} = \frac{1}{0!} + \frac{1}{1!} + \frac{1}{2!} = 1 + 1 + \frac{1}{2} = \frac{5}{2}, \quad \text{and}
\]

\[
3 - \frac{2}{(n + 1)!} = 3 - \frac{2}{3!} = 3 - \frac{1}{3} = \frac{8}{3} > \frac{5}{2}
\]

So the base case holds.
Now let $n > 1$ be an integer and assume that \( \frac{1}{0!} + \frac{1}{1!} + \cdots + \frac{1}{n!} < 3 - \frac{2}{(n+1)!} \) (inductive hypothesis).

We must show that \( \frac{1}{0!} + \frac{1}{1!} + \cdots + \frac{1}{n!} + \frac{1}{(n+1)!} < 3 - \frac{2}{((n+1) + 1)!} \). Once again, we must not assume this.

\[
\begin{align*}
\frac{1}{0!} &+ \frac{1}{1!} + \cdots + \frac{1}{n!} + \frac{1}{(n+1)!} = \left[ \frac{1}{0!} + \frac{1}{1!} + \cdots + \frac{1}{n!} \right] + \frac{1}{(n+1)!} \\
&< 3 - \frac{2}{(n+1)!} + \frac{1}{(n+1)!} \\
&= 3 - \frac{1}{(n+1)!} \\
&< 3 - \frac{1}{(n+1)!} \cdot \frac{2}{n+2} \\
&= 3 - \frac{2}{(n+2)!} \\
&= 3 - \frac{2}{((n+1) + 1)!}
\end{align*}
\]

This completes the proof by induction $\square$. 
Here are some more proof by induction examples:

**Theorem:** \( \forall n \in \mathbb{N}, \prod_{i=1}^{n} \left( 1 + \frac{1}{i} \right) = n + 1. \)

**Proof:** Clearly \( \prod_{i=1}^{n} \left( 1 + \frac{1}{i} \right) = n + 1 \) when \( n = 1 \) as both sides simplify to 2. That establishes the base case.

Now let \( n \in \mathbb{N} \) and assume \( \prod_{i=1}^{n} \left( 1 + \frac{1}{i} \right) = n + 1 \) (inductive hypothesis).

We must show that \( \prod_{i=1}^{n+1} \left( 1 + \frac{1}{i} \right) = (n + 1) + 1 \). Don’t assume this!

Here we go...

\[
\prod_{i=1}^{n+1} \left( 1 + \frac{1}{i} \right) = \left[ \prod_{i=1}^{n} \left( 1 + \frac{1}{i} \right) \right] \cdot \left( 1 + \frac{1}{n+1} \right) = (n + 1) \left( 1 + \frac{1}{n+1} \right) = (n + 1) + 1.
\]

That completes the proof by induction \( \square \)

**Theorem:** \( \forall r \in \mathbb{C} \setminus \{1\}, \forall n \in \mathbb{N} \cup \{0\} = \mathbb{N}_0, \sum_{i=0}^{n} r^i = \frac{1 - r^{n+1}}{1 - r} \).

**Proof:** Let \( r \in \mathbb{C} \setminus \{1\} \). Consider the case \( n = 0 \). Then \( \sum_{i=0}^{n} r^i = \sum_{i=0}^{0} r^i = 1 \) and \( \frac{1 - r^n}{1 - r} = 1 \) by canceling \( 1 - r \neq 0 \). So the base case holds.

Let \( n \in \mathbb{N}_0 \) and assume that \( \sum_{i=0}^{n} r^i = \frac{1 - r^{n+1}}{1 - r} \).

Then \( \sum_{i=0}^{n+1} r^i = \left( \sum_{i=0}^{n} r^i \right) + r^{n+1} = \frac{1 - r^{n+1}}{1 - r} + r^{n+1} = \frac{1 - r^{n+1}}{1 - r} + r^{n+1} \left( \frac{1 - r}{1 - r} \right) = \frac{1 - r^{(n+1)+1}}{1 - r} \).

This completes the proof by induction \( \square \)

Now we get the following as a **corollary** (theorem that directly follows from a previous theorem):

**Corollary:** Let \( r \in \mathbb{C} \). The series \( \sum_{i=0}^{\infty} r^i \) converges iff \( |r| < 1 \). When \( |r| < 1 \), \( \sum_{i=0}^{\infty} r^i = \frac{1}{1 - r} \). \( \square \)
Let’s use induction to prove that a sequence decreases:

**Theorem**: The sequence defined by \( a_1 = 2 \), and \( a_{n+1} = \frac{a_n^2 + 5}{5} \) for \( n = 1, 2, ... \) is decreasing.

**Proof**: We want to show that \( a_{n+1} < a_n \) for all \( n \in \mathbb{N} \). Clearly \( a_2 = \frac{9}{5} < 2 = a_1 \). So the base case holds.

Note: Clearly \( a_1 > 0 \) implies \( a_2 > 0 \), which implies \( a_3 > 0 \), which implies \( a_4 > 0 \), and so on...

Let \( n \in \mathbb{N} \) and assume \( a_{n+1} < a_n \). Then \( a_{n+2} = \frac{a_{n+1}^2 + 5}{5} < \frac{a_n^2 + 5}{5} = a_{n+1} \).

That completes the proof by induction □

You have to be careful with induction. Can you find the flaw in the following argument?

**Claim**: All horses are the same color.

**Proof by induction on the number of horses**: 

Base case: One horse is trivially the same color as itself.

Let \( n \in \mathbb{N} \) and assume that any set of \( n \) horses consist of horses that are the same color (inductive hypothesis).

Now consider a set \( S \) of \( n + 1 \) horses, labeled from 1 to \( n \). Let \( S_1 \subset S \) consist of horse 1 through \( n \) and let \( S_2 \subset S \) consist of horse 2 through \( n + 1 \).

By the induction hypothesis, all horses in set \( S_1 \) are the same color and all horses in set \( S_2 \) are the same color.

Since horse 2 lies in both \( S_1 \) and \( S_2 \), it follows that all horses in \( S_1 \) and in \( S_2 \) are the same color, the color of horse 2. But then all horses in set \( S \) have are the same color. This purportedly completes the proof by induction...
Let’s prove the following theorem by induction:

**Theorem:** For all $n \in \mathbb{N}$, $H_{2^n} \geq 1 + \frac{n}{2}$ where $H_k = 1 + \frac{1}{2} + \cdots + \frac{1}{k}$.

**Proof:** Suppose $n = 1$. Then $H_{2^1} = H_2 = 1 + \frac{1}{2} = \frac{3}{2}$ and $1 + \frac{n}{2} = 1 + \frac{1}{2} = \frac{3}{2}$.

Let $n \in \mathbb{N}$. Assume $H_{2^n} \geq 1 + \frac{n}{2}$.

Then

$$H_{2^{n+1}} = 1 + \frac{1}{2} + \cdots + \frac{1}{2^{n+1}}$$

$$= \left(1 + \frac{1}{2} + \cdots + \frac{1}{2^n}\right) + \frac{1}{2^n+1} + \frac{1}{2^n+2} + \cdots + \frac{1}{2^n+2^n}$$

$$= H_{2^n} + \frac{1}{2^n+1} + \frac{1}{2^n+2} + \cdots + \frac{1}{2^n+2^n}$$

$$\geq 1 + \frac{n}{2} + \frac{1}{2^n+1} + \frac{1}{2^n+2} + \cdots + \frac{1}{2^n+2^n}$$

$$\geq 1 + \frac{n}{2} + \frac{1}{2^n+2^n} + \frac{1}{2^n+2^n} + \cdots + \frac{1}{2^n+2^n}$$

$$= 1 + \frac{n}{2} + 2^n \cdot \frac{1}{2(2^n)}$$

$$= 1 + \frac{n+1}{2}$$

That completes the proof by induction □

As consequence of this theorem above, $\sum_{k=1}^{\infty} \frac{1}{k} = \lim_{n \to \infty} \sum_{k=1}^{2^n} \frac{1}{k} = \lim_{n \to \infty} H_{2^n} \geq \lim_{n \to \infty} 1 + \frac{n}{2}$, which is $\infty$, proving the following corollary:

**Corollary:** The harmonic series $\sum_{k=1}^{\infty} \frac{1}{k}$ diverges □
THE PRINCIPLE OF MATHEMATICAL INDUCTION (STRONG FORM):

Suppose $S(n)$ is a propositional function over the domain $D = \{n_0, n_0 + 1, n_0 + 2, \ldots \}$ where $n_0 \in \mathbb{Z}$.

Suppose both of the following statements are true:

(i) $S(n_0), S(n_0 + 1), \ldots, S(n_0 + (\ell - 1))$ are true.
   
   [\ell base cases; \ell depends on the particular argument.]

(ii) For all $n \in \{n_0 + \ell, n_0 + \ell + 1, \ldots \}$, if $S(k)$ is true for all $k \in D$ where $k < n$ then

   $S(n)$ is true.

   [The inductive step; the hypothesis of the implication is the inductive hypothesis.]

Then $S(n)$ is true for all $n \in D$.

This example is fun:

\textit{Theorem}: A chocolate bar that consists of a $n$ squares ($n \in \mathbb{N}$) arranged in a rectangular pattern takes a minimum of $n - 1$ breaks (along lines between pieces) to completely separate into its $n$ individual squares.

\textit{Proof}: Suppose $n = 1$. A chocolate bar that consists of just one square obviously doesn’t take a break to separate, so it takes 0 breaks. Since $n - 1 = 0$ the base case holds.

Let $n \in \mathbb{N}$, $n \geq 2$ and assume any chocolate bar that consists of $k < n$ squares ($k \in \mathbb{N}$) arranged in a rectangular pattern takes a minimum of $k - 1$ breaks (along lines between pieces) to completely separate into its $k$ individual squares.

Consider a chocolate bar of $n$ squares arranged in a rectangular pattern. Break it! Then you get two chocolate bars with $n_1, n_2 \in \{1, 2, \ldots, n - 1\}$ squares respectively. Furthermore, $n_1 + n_2 = n$.

By the inductive hypothesis, it takes $(n_1 - 1) + (n_2 - 1) = n - 2$ breaks to completely separate these two bars. Putting this all together we have a total of $1 + (n - 2) = n - 1$ breaks, completing the proof by induction $\square$
Examples that requires more than a single base case:

**Theorem**: Let the sequence \( f_0, f_1, \ldots \) be given by the initial values \( f_0 = f_1 = 1 \) and the recurrence relation \( f_n = f_{n-1} + f_{n-2} \) for \( n = 2, 3, \ldots \) (this is called the Fibonacci sequence).

\( \forall n \in \{0, 1, 2, 3, \ldots \} \), we have \( f_n \geq \phi^{n-1} \) where \( \phi = \frac{1 + \sqrt{5}}{2} \) (the golden ratio).

**Proof**: Let \( \phi = \frac{1 + \sqrt{5}}{2} \) and \( f_0, f_1, \ldots \) be the Fibonacci sequence (as described above).

Suppose \( n = 0 \). Then \( f_n = f_0 = 1 \) and \( \phi^{n-1} = \phi^{-1} = \frac{2}{1 + \sqrt{5}} < 1 \), so \( f_n \geq \phi^{n-1} \). Suppose \( n = 1 \). Then \( f_n = f_1 = 1 \) and \( \phi^{n-1} = \phi^0 = 1 \), so \( f_n \geq \phi^{n-1} \). So the two base cases hold.

Let \( n \in \mathbb{N} \), \( n \geq 2 \). Assume \( f_k \geq \phi^{k-1} \) for \( k \in \{0, 1, \ldots, n-1\} \).

A quick calculation (this is left to you) shows that \( \phi \) is a root of \( x^2 - x - 1 \). Hence \( \phi^2 = \phi + 1 \).

Now consider that \( f_n = f_{n-1} + f_{n-2} \), so by induction,

\[
 f_n \geq \phi^{(n-1)-1} + \phi^{(n-2)-1} = \phi^{n-2} + \phi^{n-3} = \phi^{n-3} (\phi + 1) = \phi^{n-3} \phi^2 = \phi^{n-1}.
\]

This completes the proof by induction \( \square \).

So, why did we need two base cases? It’s because in order to justify the inductive step when \( n = 2 \) we need both cases (that is, we need two cases just to get the dominos to start falling...)

**Theorem**: Every amount of postage of 12 cents or more can be formed using 4-cent and 5-cent stamps.

**Proof**: We begin with four base cases. 12-cent postage can be made with three 4-cent stamps. 13-cent postage can be made with two 4-cent stamps and one 5-cent stamp. 14-cent postage can be made with one 4-cent stamp and two 5-cent stamps. 15-cent postage can be made with three 5-cent stamps.

Now let \( n \geq 16 \) be an integer. Assume \( k \)-cent postage can be formed using 4-cent and 5-cent stamps for any integer \( k \in \{12, 13, \ldots, n-1\} \).

Now let’s consider trying to make \( n \)-cent postage. Slap a 4-cent stamp on it. Then we have \( (n-4) \)-cent postage left to achieve. Since \( n-4 \in \{12, 13, \ldots, n-1\} \) we can form \( (n-4) \)-cent postage using 4-cent and 5-cent stamps. Thus we have \( n \)-cent postage, completing the proof by induction \( \square \).
THE PIGEONHOLE PRINCIPLE:

If more than \( n \) objects are placed into \( n \) categories then one category contains more than one object.

Let’s prove the following basic fact using this principle:

**Theorem:** Any three integers contains a pair whose sum is even.

**Proof:** Let \( a, b, c \in \mathbb{Z} \). There are two categories to consider: The category of even integers and the category of odd integers.

Since there are three integers, at least two of them fall into the same category (by the pigeonhole principle). That means either there is a pair \( u, v \in \{a, b, c\} \) of integers that are either both even or both odd.

Since the sum of two even integers is even and the sum of two odd integers is even, it follows that this pair has an even sum. That completes the proof □

Here is another example that takes advantage of the pigeonhole principle:

**Theorem:** Let \( N \in \mathbb{N} \). Any set of \( N \) non-negative integers contains a subset whose sum is a multiple of \( N \).

**Proof:** Let \( S = \{k_1, k_2, ..., k_N\} \) be non-empty set of non-negative integers. Set \( S_i = \{k_1, k_2, ..., k_i\} \) for each \( i = 1, 2, ..., N \).

Let \( r_i \) be the remainder when \( \sum_{x \in S_i} x \) is divided by \( N \). If \( \exists i \in \{1, 2, ..., N\} \) such that \( r_i = 0 \) then we are done as the sum of the elements of \( S_i \) would be a multiple of \( N \). Assume \( r_i \neq 0 \) for all \( i \in \{1, 2, ..., N\} \).

Then \( r_1, r_2, ..., r_N \in \{1, 2, ..., N - 1\} \). By the pigeonhole principle, \( \exists j, k \in \{1, 2, ..., N\} \) such that \( r_j = r_k \). Without loss of generality assume \( j < k \).

Then \( \sum_{x \in S_k} x = Na + r_k \) and \( \sum_{x \in S_j} x = Nb + r_j \) for some \( a, b \in \mathbb{Z} \).

Then \( n_{j+1} + n_{j+2} + \cdots + n_k = \sum_{x \in S_k} x - \sum_{x \in S_j} x = N(a - b) \) is a multiple of \( N \) □
STRONG FORM OF THE PIGEONHOLE PRINCIPLE:

Let \( m, n \in \mathbb{N} \). Suppose at least \( 1 + n(m - 1) \) objects are placed into \( n \) categories. Then at least one category has \( m \) objects or more.

Let’s figure out how to use this principle to justify the following:

**Theorem:** In a group of 25 people, at least 3 have a birthdate in the same month.

**Proof:** There are 25 people (objects) and 12 months in a year (categories). Since 25 = 1 + 12(3 - 1) it follows that at least one month contains at least 3 of the birthdays \( \square \)