The Induction Principle and Properties of Integers

Three Principles

Most (if not all) discrete structures studied in computer science have infinitely many objects, but fortunately, there are usually systematic techniques to investigate the properties about these structures. The single most important such technique is based on an important property of natural numbers known as \textit{the induction principle}.

The set of natural numbers, \( N = \{0, 1, 2, \ldots\} \), consists of all non-negative integers. There are two operations, \( + \) (add) and \( \cdot \) (multiply), defined on \( N \) which satisfy the usual algebra laws (closure, commutative, associative, distributive, and identity elements). In addition, and at a more fundamental level, mathematicians have sought after the definition of natural numbers, e.g., what is zero, one, etc. One important outcome of this investigation is the following principle, characterizing the infinite yet simple nature of \( N \):

\textbf{The Induction Principle:} Let \( A \subseteq N \) denote a subset that satisfies the following two properties:

(1) \( 0 \in A \); and

(2) if \( k \in A \), then \( k + 1 \in A \).

Then \( A = N \).

Since this is a principle, it is intended to state an obvious fact for which no proof is required. The principle effectively says that starting with the number 0, every natural number can be reached by repeatedly adding 1 for enough times.
A similar and equivalent principle is the following:

**The Strong Induction Principle:** Let \( A \subseteq N \) denote a subset that satisfies the following two properties:

1. \( 0 \in A \); and
2. if \( 0, 1, \ldots, k \in A \), then \( k + 1 \in A \).

Then \( A = N \).

Again, this principle should be obviously true. For example, if set \( A \subseteq N \) satisfies the two properties, Property (1) implies \( 0 \in A \). Applying (2) with \( k = 0 \), we conclude \( 1 \in A \). Then since both \( 0, 1 \in A \), applying (2) again with \( k = 1 \) implies \( 2 \in A \), etc. Thus, we can conclude \( A = N \). (Of course, this argument is not considered a proof.)

There is another (lesser-known) principle of natural numbers, stated as follows:

**The Well-Ordering Principle:** Let \( B \subseteq N \) be a subset of natural numbers, and \( B \neq \emptyset \). Then \( B \) has a smallest element (that is, there is a number \( s \in B \) such that \( s \leq b \) for every \( b \in B \)).

The reason that set \( B \) in the Principle has a smallest element is that the set of natural numbers \( N \) has 0 as its lower bound, preventing its subset \( B \) from finding smaller and smaller elements forever. It turns out that any of the preceding principles can be used to prove the others.
**Theorem.** The following three principles are equivalent: (a) the Induction Principle; (b) the Strong Induction Principle; and (c) the Well-Ordering Principle.

**Proof:** It suffices to prove (a) ⇒ (b), (b) ⇒ (c), and (c) ⇒ (a).

Proof of (a) ⇒ (b): Let $A \subseteq N$ and $A$ satisfies the two properties: (1) $0 \in A$; and (2) if $0, 1, \ldots, k \in A$, then $k + 1 \in A$. We need to prove $A = N$. Define $C = \{m | m \in N$ and $0, 1, \ldots, m \in A\}$. Thus, $C \subseteq A \subseteq N$ ---- (3). Since $0 \in A$ by (1), $0 \in C$ by its definition. Also, if $k \in C$, that is, $0, 1, \ldots, k \in A$ by the definition of $C$, then $k + 1 \in A$ by (2), which implies $k + 1 \in C$ because now, $0, 1, \ldots, k + 1 \in A$. Thus, set $C$ satisfies the two properties of the Induction Principle, so $C = N$. Therefore, $A = N$ because of (3).

Proof of (b) ⇒ (c): Assume $B \subseteq N$ and $B \neq \emptyset$ ------ (4). Suppose the Well-Ordering Principle is false, that is, suppose $B$ doesn’t have a smallest element ---- (5). Then we want to show this leads to a contradiction. Let $A = N - B$ ------ (6). By (5), $0 \notin B$ because $B$ doesn’t have a smallest element; thus, $0 \in A$ because of (6). If the numbers $0, 1, \ldots, k \in A$, then these numbers don’t belong to $B$, so $k + 1 \notin B$, because if it were, $k + 1$ would be a smallest number in $B$, contradicting to (5). Thus, $k + 1 \in A$. Thus, by the Strong Induction Principle, $A = N$, which implies $B = \emptyset$ by (6), contradicting to (4). So (c) is proved.

Proof of (c) ⇒ (a): Let $A \subseteq N$ and $A$ satisfies the two properties: (7) $0 \in A$; and (8) if $k \in A$, then $k + 1 \in A$. We need to prove $A = N$. Let $B = N - A$; it suffices to prove $B = \emptyset$ ---- (9). Suppose $B \neq \emptyset$. The Well-ordering Principle (c) implies $B$ has a smallest element, call it $s$ ---- (10). Note that $s \neq 0$ because (7). So $s > 0$, and $s - 1 \in N$ (being $\geq 0$). Note that $s - 1 \in A$, because $s$ is the smallest element of $B$ and $s - 1 < s$. But then (8) implies $(s - 1) + 1 = s \in A$, contradicting to (10). This contradiction proves (9).
Typically, the two induction principles are used in proving that a statement $P(n)$ holds true for all natural numbers $n$. Let us consider a few examples.

**Theorem.** The expression $n(n + 1)$ is an even number for all $n \in N$.

**Proof:** We will first prove this fact by setting it up for using the Induction Principle. We then will show a simplified proof which is what people usually do, but which is still based on the Induction Principle.

( Longer Version) Define a set $A = \{n \mid n \in N \text{ and } n(n + 1) \text{ is even}\}$. Thus, proving the theorem is equivalent to proving $A = N$, which consists of proving

(1) $0 \in A$; and (2) if $k \in A$, then $k + 1 \in A$,

according to the Induction Principle.

To prove (1), which is known as the **Induction Basis Step**, we verify that when $n = 0$, the expression $0(0 + 1)$ is even. This is true because $0(0 + 1) = 0$, an even number.

To prove (2), we assume $k \in A$, that is, assume $k(k + 1) = 2m$, an even number (this is known as the **Induction Hypothesis**), we then need to prove $k + 1 \in A$, that is, prove $(k + 1)(k + 1 + 1) = (k + 1)(k + 2)$ is even (known as the **Induction Step**).

Note that $(k + 1)(k + 2) = (k + 1)k + (k + 1)2 = 2m + (k + 1)2 = 2(m + k + 1)$, by applying the Induction Hypothesis (and other algebra laws). Thus, since $(m + k + 1)$ is an integer by the closure property of addition, we have proved $(k + 1)(k + 2)$ is even, i.e., $k + 1 \in A$. By the Induction Principle, we have proved $A = N$, i.e., $n(n + 1)$ is even for all $n \in N$. 
(Proof cont’d) (Shorter Version) To prove \( n(n + 1) \) is even for all \( n \geq 0 \), we use induction on \( n \).

(Basis Step) Consider \( n = 0 \). In this case, the expression \( n(n + 1) = 0(0 + 1) = 0 \), is an even number. So the Basis Step is proved.

(Induction Hypothesis) Consider \( n = k \). Assume \( k(k + 1) \) is an even number, where \( k \geq 0 \) is a natural number. Thus, \( k(k + 1) = 2m \) for some integer \( m \), by the definition of even.

(Induction Step) Consider \( n = k + 1 \). We want to prove \( n(n + 1) = (k + 1)(k + 1 + 1) = (k + 1)(k + 2) \) is even. Note that

\[
(k + 1)(k + 2) = (k + 1)k + (k + 1)2, \text{ by distributive law}
\]

\[
= 2m + (k + 1)2, \text{ by Induction Hypothesis}
\]

\[
= 2(m + k + 1), \text{ by distributive law.}
\]

Thus, since \( (m + k + 1) \) is an integer by the closure property of integer addition, the expression \( (k + 1)(k + 2) \) is even, and we have proved \( n(n + 1) \) is even for \( n = k + 1 \).

By (mathematical) induction, we have proved \( n(n + 1) \) is even for all \( n \geq 0 \).

Thus, the shorter version of an induction proof can be applied to proving the truth of a statement \( P(n) \), for \( n \geq 0 \). The proof consists of three steps: (Basis Step) Prove \( P(0) \) is true; (Induction Hypothesis) Assume \( P(k) \) is true, for some \( k \in \mathbb{N} \); and (Induction Step) Prove \( P(k + 1) \) is true. As a result, we conclude that \( P(n) \) is true, for all \( n \geq 0 \).
Notice that an induction problem may not start with \( n = 0 \), but the Induction Principle still applies with a slight modification. Sometimes, the Strong Induction Principle needs to be used, because proving the case of the Induction Step (i.e., when \( n = k + 1 \)) requires the truth for all the preceding values (i.e., when \( n = 0, 1, \ldots, k \)).

**Theorem (Fundamental Theorem of Arithmetic, Part I).** Let \( n \geq 2 \) denote an integer. Then there exists prime numbers \( p_1, p_2, \ldots, p_k \), not necessarily distinct, such that \( n = p_1 p_2 \ldots p_k \); that is, any integer \( n \geq 2 \) can be factored as a product of prime numbers.

**Proof:** We use strong induction on \( n \geq 2 \).

(Basis Step) Consider \( n = 2 \). In this case, since 2 is a prime, \( n = 2 \) is a prime factorization.

(Induction Hypothesis) Assume the theorem is true for all values of \( n = 2, 3, \ldots, k \), i.e., assume each number \( n \) in the range \( 2 \leq n \leq k \), for some \( k \geq 2 \), has a prime factorization.

(Induction Step) Consider \( n = k + 1 \). There are two cases, either \( n \) is itself a prime, in which case the theorem is immediately proven because \( n = n \) is a prime factorization; or, if \( n \) is not a prime. In the latter case, \( n = ab \), where \( 1 < a, b < n \), by the definition of non-prime. By the Induction Hypothesis, both \( a \) and \( b \) have their prime factorizations,

\[
a = p_1 p_2 \ldots p_k \quad \text{and} \quad b = q_1 q_2 \ldots q_h , \quad \text{where} \quad k, h \geq 1, \quad \text{and all} \quad p_i \quad \text{and} \quad q_j \quad \text{are primes.}
\]

Thus, \( n = ab = p_1 p_2 \ldots p_k q_1 q_2 \ldots q_h \), which is a prime factorization for \( n \). Thus, we proved the Induction Step.

By strong induction, the theorem is true (i.e., \( n \) has a prime factorization) for all \( n \geq 2 \).
We now illustrate how the Well-Ordering Principle can be applied. We first state a simple fact about prime numbers without proving it (it is proved on page 3-27).

**Theorem.** Let $p$ denote a prime. If $p \mid ab$, where $a$, $b$ are two integers, then $p \mid a$ or $p \mid b$.

(For example, 3 is a prime and $3 \mid 24 = 12 \cdot 2$. Note $3 \mid 12$.)

**Theorem (Fundamental Theorem of Arithmetic, Part II).** Let $n \geq 2$ denote an integer. Then the prime factorization of $n$, $n = p_1 p_2 \ldots p_k$, is unique except for possible rearrangement of the prime factors.

**Proof:** We use the method of proof by contradiction. Assume the theorem is false, that is, there exists some integer which has non-unique prime factorization. By the Well-Ordering Principle, there is a smallest such integer, which we call it $m$. That is, $m \geq 2$ has two distinct prime factorizations, and $m$ is the smallest such integer.

Let $m = p_1 p_2 \ldots p_k = q_1 q_2 \ldots q_h$ (1), be the two factorizations.

Since $p_1$ is a prime, and $p_1 \mid m = q_1 q_2 \ldots q_h$, then $p_1 \mid q_i$, by the theorem stated above. Without loss of generality, we assume $p_1 \mid q_1$.

Since both $p_1$ and $q_1$ are primes, we must have $p_1 = q_1$. Therefore, canceling $p_1$ and $q_1$ from (1) yields

$$m' = m/p_1 = p_2 \ldots p_k = q_2 \ldots q_h$$

which gives two distinct factorizations of a number $m' < m$, a contradiction to the fact $m$ is the smallest such integer. Thus, we proved the truth of the theorem.
Sequences and Series

A sequence refers to a list of objects, for example, the sequence of prime numbers are

2, 3, 5, 7, 11, ...

and the sequence of positive odd integers are

1, 3, 5, 7, ...

More generally, a sequence of \( n \) objects is denoted by the following notations:

\[ a_1, a_2, \ldots, a_n. \]

A sequence such as \( a_1, a_2, \ldots, a_n \) can be formally defined as a function whose domain is the set of natural numbers, or a subset of it possibly missing some initial integers. That is, the sequence \( a_1, a_2, \ldots, a_n \) is basically a function:

\[ f: \{1, 2, \ldots, n\} \rightarrow A, \text{ for some co-domain } A, \]

and we simply use the notations \( a_1, a_2, \ldots, a_n \) to represent, respectively, \( f(1), f(2), \ldots, f(n) \).

Typically, a sequence’s index (subscript) starts at 1 or 0. Very often, a sequence consists of numbers which are given by a formula, for example,

\[ a_k = 2k - 1, \text{ for } 1 \leq k \leq n, \text{ defines the sequence of the first } n \text{ odd integers}; \]

\[ b_k = k^2, \text{ for } 1 \leq k \leq n, \text{ defines the sequence of the first } n \text{ squares}. \]
A series refers to a sum of the numbers in a sequence. Thus, the following is a series which consists of the terms in the sequence $a_1, a_2, \ldots, a_n$:

$$a_1 + a_2 + \ldots + a_n.$$ 

The above series can be abbreviated using the summation notation as follows:

$$\sum_{k=1}^{n} a_k$$

Thus, the summation term $a_k$ is used to represent each of the terms in the series, and the range of the summation index $k$ is from $k = 1$ to $n$.

**Examples.** The following are summation notations for the corresponding series:

$$\sum_{k=1}^{n} (2k - 1) = 1 + 3 + \ldots + (2n - 1)$$

$$\sum_{k=1}^{n} k^2 = 1 + 4 + \ldots + n^2$$

$$\sum_{k=1}^{n} (-1)^{k-1} k = 1 - 2 + 3 - \ldots + (-1)^{n-1} n$$

$$\sum_{i=1}^{n} i = 1 + 2 + \ldots + n$$

Note that the name of the summation index is only a dummy variable; thus,

$$\sum_{i=1}^{n} i = \sum_{k=1}^{n} k = \sum_{j=0}^{n-1} (j + 1)$$
The induction method is often used to prove properties about sequences and series. First, we review some basic rules and laws of Algebra.

**Properties of +, −, •, and /:**

(Commutative) $a + b = b + a$; $a \cdot b = b \cdot a$. (Associative) $(a + b) + c = a + (b + c)$; $(a \cdot b) \cdot c = a \cdot (b \cdot c)$. (Distributive) $a \cdot (b + c) = a \cdot b + a \cdot c$. (Additive inverse) $a - b = a + (-b)$; $a + (-a) = 0$. (Multiplicative inverse) $a / b = a \cdot (1/b)$ if $b \neq 0$; $a \cdot (1/a) = 1$, if $a \neq 0$. (Identity elements) $a + 0 = a$; $a \cdot 1 = a$.

**Laws of exponent and Logarithm:**

If $a > 0$, $a^x \cdot a^y = a^{x+y}$; $(a^x)^y = a^{xy}$; $a^x / a^y = a^{x-y}$; $a^{-x} = 1/(a^x)$;

If $b > 0$ and $b \neq 1$, $\log_b(xy) = \log_b x + \log_b y$; $\log_b(x/y) = \log_b x - \log_b y$; $\log_b(x^p) = p \log_b x$.

**Rules of inequalities:**

$a > b \iff a + c > b + c$; if $c > 0$, then $a > b \iff a \cdot c > b \cdot c$; if $a > b$ and $b > c$, then $a > c$; if $a > b$ and $c > d$, then $a + c > b + d$.

**Useful algebra rules:**

$ab = 0 \iff a = 0$ or $b = 0$; if $bd \neq 0$, then $a/b = c/d \iff ad = bc$;

$(a + b)^2 = a^2 + 2ab + b^2$; $(a + b)(a - b) = a^2 - b^2$. 
**Example.** Prove the following summation formula using the induction method.

\[ \sum_{i=1}^{n} i = 1 + 2 + \ldots + n = \frac{n(n+1)}{2}, \text{ for } n \geq 1. \]

**Proof:** We use induction on \( n \geq 1. \)

(Basis Step) Consider \( n = 1. \) In this case, the summation \( \sum_{i=1}^{1} i = 1. \) The formula on the RHS (right-hand side) of the identity \( = 1(1 + 1)/2 = 2/2 = 1. \) So, LHS = RHS, the Basis Step is proved.

(Induction Hypothesis) Consider \( n = k. \) Assume the identity holds for \( n = k, \) that is,

\[ \sum_{i=1}^{k} i = \frac{k(k+1)}{2}, \text{ for some } k \geq 1. \]

(Induction Step) Consider \( n = k + 1. \) We need to prove the following identity:

\[ \sum_{i=1}^{k+1} i = \frac{(k+1)(k+1+1)}{2} = \frac{(k+1)(k+2)}{2} \quad \text{--- (1).} \]

Notice that the LHS = \( \sum_{i=1}^{k} i + (k+1), \) by the definition of summation

\[ = \frac{k(k+1)}{2} + (k+1), \text{ by the Induction Hypothesis} \]

\[ = \frac{(k + 1)(k + 2)}{2}, \text{ by distributive law.} \]

Thus, identity (1) of the Induction Step is proved. Therefore, by mathematical induction, we have proved the summation formula of the theorem for all \( n \geq 1. \)
Example. Prove the following summation formula using the induction method.
\[ \sum_{i=1}^{n} (2i - 1) = n^2, \] for \( n \geq 1 \).

Proof: We use induction on \( n \geq 1 \).

(Basis Step) Consider \( n = 1 \). In this case, the summation = \( \sum_{i=1}^{1} (2i - 1) = (2 - 1) = 1 \). The formula on the RHS = \( 1^2 = 1 \) = LHS. Thus, the Basis Step is proved.

(Induction Hypothesis) Consider \( n = k \). Assume the identity holds for \( n = k \), that is,
\[ \sum_{i=1}^{k} (2i - 1) = k^2, \] for some \( k \geq 1 \).

(Induction Step) Consider \( n = k + 1 \). We need to prove the following identity:
\[ \sum_{i=1}^{k+1} (2i - 1) = (k + 1)^2 \] (1).

Note that the summation on the LHS of (1) is
\[ \sum_{i=1}^{k+1} (2i - 1) = \sum_{i=1}^{k} (2i - 1) + (2(k + 1) - 1), \] by the definition of summation
= \( k^2 + (2k + 1) \), by the Induction Hypothesis
= \( (k + 1)^2 \), by the algebra rule \((a + b)^2 = a^2 + 2ab + b^2\).

Thus, the identity (1) of the Induction Step is proved. Therefore, by mathematical induction, we have proved the summation formula for all \( n \geq 1 \).
Example. Prove the following summation inequality using the induction method.

$$\sum_{i=1}^{n} \frac{1}{n+i} > \frac{13}{24}, \text{ for } n \geq 2.$$ 

Proof: We use induction on \( n \geq 2 \).

(Basis Step) Consider \( n = 2 \). The summation on the LHS =

$$\sum_{i=1}^{2} \frac{1}{2+i} = \frac{1}{2+1} + \frac{1}{2+2} = \frac{1}{3} + \frac{1}{4} = \frac{7}{12} > \frac{13}{24} = \text{ RHS}.$$ 

(Induction Hypothesis) Consider \( n = k \). Suppose the summation inequality holds, i.e.,

suppose  $$\sum_{i=1}^{k} \frac{1}{k+i} > \frac{13}{24}, \text{ for some } k \geq 2.$$ 

(Induction Step) Consider \( n = k + 1 \). We need to prove

$$\sum_{i=1}^{k+1} \frac{1}{(k+1)+i} > \frac{13}{24} \quad - - - - (1).$$

Note that the summation on the LHS of (1) =

$$\sum_{i=1}^{k+1} \frac{1}{(k+1)+i} = \frac{1}{k+1+1} + \frac{1}{k+1+2} + \cdots + \frac{1}{k+1+k+1}, \text{ by expanding summation}$$

$$= \left( \frac{1}{k+1} + \frac{1}{k+2} + \cdots + \frac{1}{k+k} \right) + \frac{1}{k+1} + \frac{1}{k+k+1} + \frac{1}{k+k+2}, \text{ by rearranging terms}$$

$$= \sum_{i=k+i}^{k} + \left( \frac{1}{2k+1} + \frac{1}{2k+2} - \frac{1}{k+1} \right) \quad - - - (2) \text{ by the definition of summation}$$

Since the summation in (2) is the LHS of the Induction Hypothesis, and since the second expression in (2) is,

$$\frac{1}{2k+1} + \frac{1}{2k+2} - \frac{1}{k+1} = \frac{1}{2k+1} + \frac{1}{2k+2} - \frac{2}{2k+2} = \frac{1}{2k+1} - \frac{1}{2k+2} > 0,$$

substituting this into (2) implies the expression of (2) \( > 13/24 \), by the Induction Hypothesis. So the Induction Step is proved. By induction, we have proved the theorem for all \( n \geq 2 \).
Example. Prove by induction that $n! > 2^n$ for all $n \geq 4$. (Note: $n! = n(n-1)\cdots \cdot 1$, for $n \geq 1$; $0! = 1$ by convention.)

Proof: We use induction on $n \geq 4$.

(Basis Step) Consider $n = 4$. In this case,

$$n! = 4! = 4 \cdot 3 \cdot 2 \cdot 1 = 24,$$

and

$$2^n = 2^4 = 16 < 24.$$ So the Basis Step is proved.

(Induction Hypothesis) Consider $n = k$. Suppose $k! > 2^k$ for some $k \geq 4$.

(Induction Step) Consider $n = k + 1$. We need to prove $(k + 1)! > 2^{k+1}$ \hspace{1cm} (1).

Note that the LHS of (1) = $(k + 1)! = (k + 1) \cdot k \cdots 2 \cdot 1$, by the definition of $(k + 1)!$

$$= (k + 1) \cdot k!, \text{ by the definition of } k!$$

$$> (k + 1) \cdot 2^k, \text{ by the Induction Hypothesis}$$

$$> 2 \cdot 2^k, \text{ because } k + 1 \geq 5 > 2$$

$$= 2^{k+1}.$$ Thus, we have proved Inequality (1) of the Induction Step.

By induction, we have proved the inequality $n! > 2^n$ for all $n \geq 4$. 
Example. Prove by induction that the expression $11^{n+2} + 12^{2n+1}$ is divisible by 133 for all $n \geq 0$.

Proof: We use induction on $n \geq 0$.

(Basis Step) Consider $n = 0$. In this case, the expression

$$11^{n+2} + 12^{2n+1} = 11^2 + 12^1 = 121 + 12 = 133,$$

which is divisible by 133. So the Basis Step is proved.

(Induction Hypothesis) Consider $n = k$. Suppose $11^{k+2} + 12^{2k+1}$ is divisible by 133 for some $k \geq 0$, that is, $11^{k+2} + 12^{2k+1} = 133m$, for some integer $m$.

(Induction Step) Consider $n = k + 1$. We need to prove the expression

$$11^{n+2} + 12^{2n+1} = 11^{(k+1)+2} + 12^{2(k+1)+1} = 11^{k+3} + 12^{2k+3}$$

is divisible by 133.

Note that this expression $11^{k+3} + 12^{2k+3} = 11 \cdot 11^{k+2} + 12^2 \cdot 12^{2k+1}$

$$= 11 \cdot (11^{k+2} + 12^{2k+1}) + (12^2 - 11) \cdot 12^{2k+1}$$

$$= 11 \cdot 133m + (144 - 11) \cdot 12^{2k+1},$$

by the Induction Hypothesis

$$= 133 \cdot (11m + 12^{2k+1}),$$

which is divisible by 133. Thus, we proved the Induction Step.

By induction, we have proved that $11^{n+2} + 12^{2n+1}$ is divisible by 133 for all $n \geq 0$. 
Inductively (Recursively) Defined Objects

The induction principles can be used to define structures in terms of themselves, usually “smaller” in size. We first consider recursively defined functions. For example, to define the Factorial function \( n! \), where \( n \) is a natural number,

we first define the case with \( n = 0 \), as \( 0! = 1 \); and

we then define \( n! \) for \( n > 0 \), in terms of \( (n - 1)! \), by a recursive (inductive) formula: \( n! = n \cdot (n - 1)! \).

Thus, to compute \( 1! \), we use the recurrence relation (by letting \( n = 1 \)) which says

\[
1! = 1 \cdot (1 - 1)! = 1 \cdot 0! = 1 \cdot 1 = 1.
\]

Similarly, \( 2! = 2 \cdot (2 - 1)! = 2 \cdot 1! = 2 \cdot 1 = 2 \); and \( 3! = 3 \cdot (3 - 1)! = 3 \cdot 2! = 6 \), etc.

It can be seen that by applying the induction principle, \( n! \) is defined for all \( n \in N \). That is, we could apply the recurrence relation repeatedly which eventually leads to the case of \( 0! \), in order to compute the value of \( n! \) for any \( n \).

More generally, a recursively (or inductively) defined function \( f(n) \) for \( n \geq 0 \) consists of the initial value \( f(0) \), and a recurrence relation which relates the value of \( f(n) \) in terms of the preceding value \( f(n - 1) \) for \( n \geq 1 \). Minor variations of this recursive definition include a starting value different than 0, several starting values and a recurrence relating the function value to several of the preceding values.
When a function is defined by a recurrence, the most natural way to prove the properties about the function is by using induction.

**Example.** Consider a sequence \( f(n) \), \( n \geq 0 \), defined by the following recurrence:

\[
    f(0) = 0; \text{ and } f(n) = 2f(n-1) + 1 \text{ for } n \geq 1.
\]

Prove that \( f(n) = 2^n - 1 \), for \( n \geq 0 \). (Thus, we are proving a *closed-form* formula or *closed-form* solution for the function \( f(n) \).)

**Proof:** We prove that \( f(n) = 2^n - 1 \) using induction on \( n \geq 0 \).

(Basis Step) Consider \( n = 0 \). In this case, the formula \( 2^n - 1 = 2^0 - 1 = 1 - 1 = 0 \), which is equal to the initial value \( f(0) = 0 \). So the Basis Step is proved.

(Induction Hypothesis) Consider \( n = k \). Suppose \( f(k) = 2^k - 1 \) for some \( k \geq 0 \).

(Induction Step) Consider \( n = k + 1 \). We need to prove \( f(k + 1) = 2^{k+1} - 1 \) ------ (1).

Note that \( f(k + 1) = 2f((k + 1) - 1) + 1 \), by applying the recurrence since \( k + 1 \geq 1 \)

\[
    = 2f(k) + 1 = 2(2^k - 1) + 1, \text{ by the Induction Hypothesis}
\]

\[
    = 2^{k+1} - 2 + 1 = 2^{k+1} - 1 = \text{RHS of (1)}.
\]

Thus, we have proved (1) of the Induction Step.
By mathematical induction, we have proved \( f(n) = 2^n - 1 \), for all \( n \geq 0 \).

**Note:** The recurrence given in this example arises from the Tower of Hanoi puzzle, see [http://www.cut-the-knot.com/recurrence/hanoi.shtml](http://www.cut-the-knot.com/recurrence/hanoi.shtml) for a detailed description.
Sometimes, there are more than one initial value in defining a recurrence for a function. In such cases, proving properties about the function using induction requires verification of all the initial values in the basis step, and requires a strong induction proof.

**Example.** Given the following recurrence for a sequence \( a_n, n \geq 1 \):

\[
a_1 = 4, \quad a_2 = 10, \quad \text{and} \quad a_n = 3a_{n-1} - 2a_{n-2} \quad \text{when} \quad n \geq 3.
\]

Prove that \( a_n = 3 \cdot 2^{n-2} \) for \( n \geq 1 \).

**Proof:** We use strong induction on \( n \geq 1 \) to prove the formula \( a_n = 3 \cdot 2^{n-2} \).

**(Basis Step)** Consider \( n = 1 \). By the formula, \( a_1 = 3 \cdot 2^1 - 2 = 6 - 2 = 4 \), which is equal to the given initial value of \( a_1 \). Also, consider \( n = 2 \). By the formula, \( a_2 = 3 \cdot 2^2 - 2 = 12 - 2 = 10 \), which is also equal to the given initial value of \( a_2 \). Thus, the Basis Step is proved.

**(Induction Hypothesis)** Suppose the formula \( a_n = 3 \cdot 2^{n-2} \) holds for all \( n \) in the range \( 1 \leq n \leq k \), for some \( k \geq 2 \).

**(Induction Step)** Consider \( n = k + 1 \). We need to prove \( a_{k+1} = 3 \cdot 2^{k+1} - 2 \) ------ (1).

Note that \( a_{k+1} = 3 \ a_{(k+1)-1} - 2 \ a_{(k+1)-2} \) by applying the recurrence since \( k + 1 \geq 3 \)

\[
= 3 \ a_k - 2 \ a_{k-1} = 3 (3 \cdot 2^k - 2) - 2 (3 \cdot 2^{k-1} - 2) \quad \text{by applying the Induction Hypothesis to both} \ a_k \text{ and} \ a_{k-1}
\]

\[
= 3(3 \cdot 2^k) - 6 - 3 \cdot 2^k + 4 = 2(3 \cdot 2^k) - 2 = 3 \cdot 2^{k+1} - 2 = \text{RHS of (1)}.
\]

Thus, the Induction Step is proved. By induction, we have proved the formula for all \( n \geq 1 \).