Math 324 Summer 2012
Elementary Number Theory
Notes on Mathematical Induction

Principle of Mathematical Induction

Recall the following axiom for the set of integers.

Well-Ordering Axiom for the Integers

If B is a nonempty subset of $\mathbb{Z}$ which is bounded below, that is, there exists an $n \in \mathbb{Z}$ such that $n \leq b$ for all $b \in B$, then B has a smallest element, that is, there exists a $b_0 \in B$ such that $b_0 < b$ for all $b \in B$, $b \neq b_0$.

In particular, we have

Theorem. (Well-Ordering Principle for $\mathbb{N}$)

Every nonempty set of nonnegative integers has a least element.

Now we show that the Principle of Mathematical Induction and the Well-Ordering Principle for $\mathbb{N}$ are logically equivalent. First we state the induction principle.

- **Principle of Mathematical Induction:**

  If P is a set of integers such that

  (i) a is in P,

  (ii) for all $k \geq a$, if the integer k is in P, then the integer $k+1$ is also in P,

  then $P = \{x \in \mathbb{Z} \,|\, x \geq a\}$ that is, P is the set of all integers greater than or equal to a.

We need the following lemma which states that 1 is the smallest positive integer, and we need to be able to prove it using either well–ordering or induction.

Lemma. 1 is the smallest positive integer.

proof.

(i) Based on the Principle of Mathematical Induction.

Let S be the set of all positive integers. We have shown that $1 \in S$ using the order properties of the integers. If the integer k is in S, then $k > 0$, so that

$$k + 1 > k > 0$$

and so the integer $k+1$ is also in S. It follows from the principle of mathematical induction that S is the set of all integers greater than or equal to 1. Therefore, 1 is the smallest positive integer.

(ii) Based on the Well–Ordering Principle.

Suppose that 1 is not the smallest positive integer, since 1 is positive, from the Well–Ordering Principle, there is a smallest positive integer, say s, and $s < 1$. If we multiply the inequality

$$0 < s < 1$$

by s, then

$$0 < s^2 < s,$$

which implies that s is not the smallest positive integer. Because our assumption led to a contradiction, it must be false. Therefore, 1 is the smallest positive integer. □

The following lemma is true, assuming either the Well-Ordering Principle or the Principle of Mathematical Induction.

Lemma. If n is an integer, there is no integer strictly between n and $n+1$.

proof. Suppose that n is an integer and there exists an integer m such that $n < m < n+1$, then $p = m - n$ is an integer and satisfies the inequalities $0 < p < 1$, which contradicts the previous lemma. Therefore, given an integer n, there is no integer between n and $n+1$. □

Theorem. The principles of mathematical induction and well–ordering are logically equivalent.

proof.

I. Assume that the well–ordering principle holds. Let a be a fixed integer, and let S be a set of integers greater than or equal to a such that

(i) a is in S, and

(ii) for all $k \geq a$, if k is in S, then $k+1$ is also in S

We have to show that S is the set of all integers greater than or equal to a. Let

$$T = \{x \in \mathbb{Z} \,|\, x \geq a \quad \text{and} \quad x \notin S\},$$

that is, T is the set of all integers greater than or equal to a that are not in S. If T is nonempty, then it follows from the well–ordering principle that T has a smallest element, say $x_0 \in T$. Since $x_0 \geq a$ and $a \notin T$, then $x_0 > a$, and since there are no integers between $x_0 - 1$ and x_0, this implies that $x_0 - 1 \geq a$. Therefore, $x_0 - 1 \notin T$ since x_0 is the smallest element of T, and so $x_0 - 1$ must be in S. By the second property of S, we have $x_0 - 1 + 1 = x_0$ is also in S, which is a contradicton. Because our assumption that T is nonempty leads to a contradiction, it must be false. Therefore, T is empty and

$$S = \{x \in \mathbb{Z} \,|\, x \geq a\},$$

that is, S is the set of all integers greater than or equal to a, and the principle of mathematical induction holds.

II. Assume that the principle of mathematical induction holds, assume also that there exists a nonempty set S of integers which is bounded below by an integer a, and that S does not have a smallest element. Since $a \leq x$ for every $x \in S$, and S does not have a smallest element, then $a \notin S$ and therefore, $a < x$ for all $x \in S$.

Let
$$T = \{x \in \mathbb{Z} \,|\, x \geq a \text{ and } x < s \text{ for all } s \in S\},$$
that is, T is the set of all integers greater than or equal to a which are strictly less than every element of S. We have shown that a is in T. Now suppose that $k \geq a$ is in T, so that $k < s$ for all $s \in S$. If $k+1$ is in S, then since there is no integer between k and $k+1$, this implies that $k+1$ is the smallest element of S, which contradicts our assumption about S. Thus, if k is in T, then $k+1$ must also be in T. It follows from the principle of mathematical induction that T is the set of all integers greater than or equal to a, and so S is empty. Therefore, if S is a nonempty set of integers which is bounded below, then S has a smallest element, and the well–ordering principle holds. □

There is a variation of the principle of mathematical induction that, in some cases, is easier to apply:

- **Principle of Strong Mathematical Induction:**

  If P is a set of integers such that

  (i) a is in P,

  (ii) if all integers k, with $a \leq k \leq n$ are in P, then the integer $n+1$ is also in P,

  then $P = \{x \in \mathbb{Z} \,|\, x \geq a\}$ that is, P is the set of all integers greater than or equal to a.

Theorem. The principle of strong mathematical induction is equivalent to both the well–ordering principle and the principle of mathematical induction.

Proof.

I. Assume that the well–ordering principle holds. Let a be a fixed integer, and let S be a set of integers such that

(i) a is in S, and

(ii) if all integers k with $a \leq k \leq n$ are in S, then $n+1$ is also in S

We have to show that S is the set of all integers greater than or equal to a.

Let
$$T = \{x \in \mathbb{Z} \,|\, x \geq a \quad \text{and} \quad x \notin S\},$$
that is, T is the set of all integers greater than or equal to a that are not in S. If T is nonempty, then it follows from the well–ordering principle that T has a smallest element, say $x_0 \in T$. Since $x_0 \geq a$ and $a \notin T$, then $x_0 > a$. Since x_0 is the smallest element of T, then $k \in S$ for all integers k satisfying $a \leq k \leq x_0 - 1$. The first and second properties of the set S now imply that $x_0 = (x_0 - 1) + 1 \in S$ also, which is a contradiction. Therefore, T is empty and
$$S = \{x \in \mathbb{Z} \,|\, x \geq a\},$$
that is, S is the set of all integers greater than or equal to a, and the principle of strong mathematical induction holds.

II. Assume that the principle of strong mathematical induction holds. Let a be a fixed integer, and let S be a set of integers such that

(i) a is in S, and

(ii) for all $n \geq a$, if n is in S, then $n+1$ is also in S

We show that S is the set of all integers greater than or equal to a.

From the first property of S, we know that $a \in S$. Now suppose that $k \in S$ for all integers $a \leq k \leq n$, since $n \in S$, then the second property of S implies that $n+1 \in S$ also. By the principle of strong mathematical induction we must have

$$S = \{x \in \mathbb{Z} \,|\, x \geq a\}.$$

Therefore the principle of mathematical induction holds, and from the previous result the well–ordering principle holds. □

Finally, we give one version of double induction:

- **Principle of Double Induction:**

  If $P(m,n)$ is a doubly indexed family of statements, one for each $m \geq a$ and $n \geq b$ such that

  (i) $P(a,b)$ is true,

  (ii) For all $m \geq a$, if $P(m,b)$ is true, then $P(m+1,b)$ is true,

  (iii) For all $n \geq b$, if $P(m,n)$ is true for all $m \geq a$, then $P(m,n+1)$ is true for all $m \geq a$,

  then $P(m,n)$ is true for all $m \geq a$ and $n \geq b$.

The proof follows immediately from the usual statement of the principle of mathematical induction and is left as an exercise.

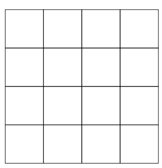
Examples Using Mathematical Induction

We now give some classical examples that use the principle of mathematical induction.

Example 1. Given a positive integer n, consider a square of side n made up of n^2 1×1 squares. We will show that the total number S_n of squares present is

$$S_n = \sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}. \qquad (*)$$

Solution. For example, if $n = 4$, then it is easily seen from the figure



that the total number of squares present is 30, since there are

$4^2 = 16$	1×1	squares
$3^2 = 9$	2×2	squares
$2^2 = 4$	3×3	squares
$1^2 = 1$	4×4	squares

for a total of 30.

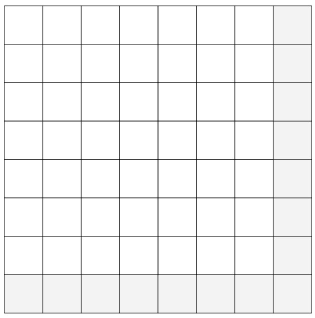
We will show that $(*)$ is true by induction on n.

Base Case: For $n = 1$, there is only 1 square, so that $S_1 = 1$, and

$$\sum_{k=1}^{1} k^2 = 1^2 = 1,$$

so that $(*)$ is true for $n = 1$.

Inductive Step: Let $n \geq 1$ be arbitrary and assume that $(*)$ is true for n. Consider an $(n+1) \times (n+1)$ square, where we have added $2n + 1$ unit squares along the bottom and right hand side of an $n \times n$ square, as shown in the figure.

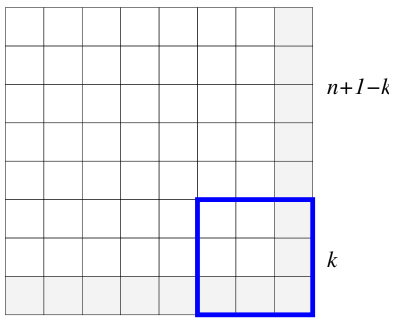


The only new squares that have been added are those that contain one of the new unit squares on the border, and we can count these as follows.

For each k with $1 \leq k \leq n + 1$, we have

$$2[n + 1 - (k - 1)] - 1 = 2(n + 2 - k) - 1$$

squares of side k,



and therefore we have added

$$\begin{aligned}\sum_{k=1}^{n+1}[2(n+2-k)-1] &= 2\sum_{k=1}^{n+1}(n+2-k)-(n+1)\\ &= 2\sum_{k=1}^{n+1}k-(n+1)\\ &= (n+1)(n+2)-(n+1)\\ &= (n+1)^2\end{aligned}$$

new squares.

From the inductive hypothesis, we have

$$S_{n+1} = S_n + (n+1)^2 = \sum_{k=1}^{n} k^2 + (n+1)^2 = \sum_{k=1}^{n+1} k^2$$

Therefore, by the Principle of Mathematical Induction, we have $S_n = \sum\limits_{k=1}^{n} k^2$ for all $n \geq 1$.

Example 2. Let $a_1, a_2, \ldots, a_n$ be positive real numbers. The *arithmetic mean* of these numbers is defined by

$$A = \frac{a_1 + a_2 + \cdots + a_n}{n},$$

and the *geometric mean* of these numbers is defined by

$$G = (a_1 \cdot a_2 \cdots a_n)^{\frac{1}{n}}.$$

The *Arithmetic-Geometric Mean Inequality* states that:

$$G \leq A \tag{$*$}$$

and equality holds if and only if $a_1 = a_2 = \cdots = a_n$.

Proof. We will give a proof of $(*)$ by induction on n. We note first that if we are given any positive real numbers

$$a_1,\ a_2,\ \ldots,\ a_n,$$

we may assume, by relabelling if necessary, that

$$a_1 \leq a_2 \leq \cdots \leq a_n.$$

If this is the case, then clearly

$$na_1 \leq a_1 + a_2 + \cdots + a_n \leq na_n,$$

so that $a_1 \leq A \leq a_n$, and $A - a_1 \geq 0$ and $a_n - A \geq 0$. Therefore,

$$(A - a_1)(a_n - A) = Aa_n + Aa_1 - A^2 - a_1 a_n \geq 0,$$

that is,

$$A(a_1 + a_n - A) \geq a_1 a_n. \tag{$**$}$$

Base Case: If $n = 1$, then

$$A = \frac{a_1}{1} = (a_1)^1 = G,$$

and $(*)$ is true for $n = 1$.

Inductive Step: Let n be an arbitrary positive integer with $n \geq 2$, and suppose that $(*)$ is true for any set of $n-1$ positive real numbers. Let $a_1, a_2, \ldots, a_n$ be a set of n positive real numbers, let A be their arithmetic mean and let G be their geometric mean. We may assume without loss of generality that

$$a_1 \leq a_2 \leq \cdots \leq a_n.$$

Now consider the set of $n-1$ positive real numbers

$$a_2,\ a_3,\ \ldots,\ a_{n-1},\ (a_1 + a_n - A),$$

the arithmetic mean of these $n-1$ numbers is

$$\begin{aligned}\frac{a_2 + a_3 + \cdots + a_{n-1} + (a_1 + a_n - A)}{n-1} &= \frac{(a_1 + a_2 + \cdots + a_n) - A}{n-1} \\ &= \frac{nA - A}{n-1} \\ &= A,\end{aligned}$$

that is, they have the same arithmetic mean as the original n integers.

By the inductive hypothesis,

$$A \geq \big(a_2 \cdot a_3 \cdots a_{n-1}(a_1 + a_n - A)\big)^{\frac{1}{n-1}},$$

so that

$$A^{n-1} \geq a_2 \cdot a_3 \cdots a_{n-1}(a_1 + a_n - A).$$

Muliplying this last inequality by A, we have from $(**)$,

$$A^n \geq a_2 \cdot a_3 \cdots a_{n-1} A(a_1 + a_n - A) \geq a_2 \cdot a_3 \cdots a_{n-1} \cdot a_1 \cdot a_n = G^n,$$

so that $G \leq A$, that is, $(*)$ is also true for n. This completes the proof of the inequality by induction.

We leave it as an exercise to show that equality holds if and only if $a_1 = a_2 = \cdots = a_n$ using the principle of mathematical induction. We give an alternate proof due to Besicovitch which uses the following fact (easily proven using calculus):

Lemma. For all real numbers x,

$$e^x \geq 1 + x$$

with equality if and only if $x = 0$.

Alternate Proof. Besicovitch's proof is very simple. Let $a_1, a_2, \ldots, a_n$ be n positive real numbers, and let A be their arithmetic mean, from the lemma, the following inequalities hold

$$e^{(a_k/A-1)} \geq \frac{a_k}{A} \quad \text{for} \quad k = 1, 2, \ldots, n.$$

Multiplying these inequalities together, we have

$$1 = e^0 = \prod_{k=1}^{n} e^{(a_k/A-1)} \geq \frac{a_1 \cdot a_2 \cdots a_n}{A^n},$$

so that $A^n \geq a_1 \cdot a_2 \cdots a_n$, and taking the n^{th} root, we have $A \geq G$ with equality if and only if $a_k = A$ for all $k = 1, 2, \ldots, n$. □

Example 3. For any positive integer $n > 2$, we have

$$\prod_{k=0}^{n} \binom{n}{k} < \left(\frac{2^n - 2}{n-1} \right)^{n-1}.$$

Proof. We apply the Arithmetic-Geometric Mean Inequality to the $n-1$ positive real numbers

$$\binom{n}{1}, \binom{n}{2}, \binom{n}{3}, \ldots, \binom{n}{n-1}$$

to obtain

$$\left(\prod_{k=1}^{n-1} \binom{n}{k} \right)^{\frac{1}{n-1}} < \frac{1}{n-1} \cdot \sum_{k=1}^{n-1} \binom{n}{k} = \frac{2^n - 2}{n-1},$$

and since $\binom{n}{0} = \binom{n}{n} = 1$, then

$$\prod_{k=0}^{n} \binom{n}{k} < \left(\frac{2^n - 2}{n-1} \right)^{n-1}.$$

□

Example 4.

(a) Let $\{a_n\}_{n \geq 0}$, be the unique solution to the discrete initial value problem

$$\begin{aligned} a_{n+2} &= a_{n+1} + a_n \qquad n \geq 0 \\ a_0 &= 0 \\ a_1 &= 1, \end{aligned}$$

that is, a_n is the n^{th} term in the Fibonacci sequence, then

$$a_n = \frac{1}{\sqrt{5}} \left[\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right]$$

for all $n \geq 0$. This is called *Binet's formula*, it was first discovered by DeMoivre, and later independently by Binet.

(b) Let $\alpha = \dfrac{1+\sqrt{5}}{2}$, then a_n is the nearest integer to $\dfrac{\alpha^n}{\sqrt{5}}$ for all $n \geq 0$.

Solution: We prove Binet's formula using the principle of mathematical induction later, here we solve the discrete initial value problem.

(a) Assuming a solution of the form $a_n = \lambda^n$, the characteristic equation becomes $\lambda^2 = \lambda + 1$, with two distinct real roots,

$$\lambda_1 = \frac{1+\sqrt{5}}{2} \qquad \text{and} \qquad \lambda_2 = \frac{1-\sqrt{5}}{2},$$

so the general solution is

$$a_n = A \cdot \left(\frac{1+\sqrt{5}}{2}\right)^n + B \cdot \left(\frac{1-\sqrt{5}}{2}\right)^n,$$

where the constants A and B are determined from the initial conditions

$$a_0 = A + B = 0 \qquad \text{and} \qquad a_1 = A \cdot \left(\frac{1+\sqrt{5}}{2}\right) + B \cdot \left(\frac{1-\sqrt{5}}{2}\right) = 1$$

to be

$$A = \frac{1}{\sqrt{5}} \qquad \text{and} \qquad B = -\frac{1}{\sqrt{5}},$$

so that

$$a_n = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right]$$

for all $n \geq 0$.

(b) Since $\dfrac{1}{\sqrt{5}} < \dfrac{1}{2}$, then

$$\left|\frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n\right| < \frac{1}{2},$$

so that

$$-\frac{1}{2} < -\frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n < \frac{1}{2}$$

and therefore, from Binet's formula, $\dfrac{1}{\sqrt{5}}\left(\dfrac{1+\sqrt{5}}{2}\right)^n - \dfrac{1}{2} < a_n < \dfrac{1}{\sqrt{5}}\left(\dfrac{1+\sqrt{5}}{2}\right)^n + \dfrac{1}{2}$. Equivalently, $\left|a_n - \dfrac{1}{\sqrt{5}}\left(\dfrac{1+\sqrt{5}}{2}\right)^n\right| < \dfrac{1}{2}$ so that a_n is the nearest integer to $\dfrac{1}{\sqrt{5}}\left(\dfrac{1+\sqrt{5}}{2}\right)^n$.

Example 5. Let $\{a_n\}_{n\geq 0}$ be a sequence of real numbers satisfying the recurrence relation and initial conditions below.

$$\begin{aligned} &a_n = a_{n-1} + 2a_{n-2} + 3a_{n-3} + \cdots + na_0 + 1, \quad n \geq 1 \\ &a_0 = 1. \end{aligned}$$

(a) Compute the next 5 terms of the sequence, that is, compute a_1, a_2, a_3, a_4, a_5.

(b) From part (a), make a conjecture as to the value of a_n for any positive integer n.

(c) Use the principle of mathematical induction to prove that your conjecture in part (b) is correct.

Solution:

(a) From the recurrence relation and the initial conditions we have

$$\begin{aligned}
a_0 &= 1 \\
a_1 &= 1 \cdot a_0 + 1 = 1 \cdot 1 + 1 = 2 \\
a_2 &= a_1 + 2 \cdot a_0 + 1 = 2 + 2 \cdot 1 + 1 = 5 \\
a_3 &= a_2 + 2 \cdot a_1 + 3 \cdot a_0 + 1 = 5 + 2 \cdot 2 + 3 \cdot 1 + 1 = 13 \\
a_4 &= a_3 + 2 \cdot a_2 + 3 \cdot a_1 + 4 \cdot a_0 + 1 = 13 + 2 \cdot 5 + 3 \cdot 2 + 4 \cdot 1 + 1 = 34 \\
a_5 &= a_4 + 2 \cdot a_3 + 3 \cdot a_2 + 4 \cdot a_1 + 5 \cdot a_0 + 1 = 34 + 2 \cdot 13 + 3 \cdot 5 + 4 \cdot 2 + 5 \cdot 1 + 1 = 89
\end{aligned}$$

(b) It appears that for all $n \geq 0$, we have $a_n = F_{2n+1}$, that is, the Fibonacci numbers with odd indices.

(c) We will show that the sequence $\{a_n\}_{n\geq 0}$ satisfies the same recurrence relation and initial conditions as the sequence $\{F_{2n+1}\}_{n\geq 0}$, and then an easy inductive argument shows that $a_n = F_{2n+1}$ for all $n \geq 0$.

First we note that for $n \geq 1$, we have

$$\begin{aligned}
F_{2n+3} &= F_{2n+2} + F_{2n+1} = (F_{2n+1} + F_{2n}) + F_{2n+1} = 2F_{2n+1} + F_{2n} \\
&= 2F_{2n+1} + (F_{2n+1} - F_{2n-1}) = 3F_{2n+1} - F_{2n-1},
\end{aligned}$$

and the sequence $\{F_{2n+1}\}_{n\geq 0}$ satisfies the discrete initial value problem

$$\begin{aligned}
F_{2n+3} &= 3F_{2n+1} - F_{2n-1},\ n \geq 1 \\
F_1 &= 1 \\
F_3 &= 2.
\end{aligned}$$

For the sequence $\{a_n\}_{n\geq 0}$, we have

$$\begin{aligned}
a_{n+1} &= 1 \cdot a_n + 2 \cdot a_{n-1} + 3 \cdot a_{n-2} + \cdots + (n-1) \cdot a_2 + n \cdot a_1 + (n+1) \cdot a_0 + 1 \\
a_n &= 1 \cdot a_{n-1} + 2 \cdot a_{n-2} + 3 \cdot a_{n-3} + \cdots + (n-1) \cdot a_1 + n \cdot a_0 + 1
\end{aligned}$$

and subtracting the second equality from the first, we have

$$a_{n+1} - a_n = a_n + a_{n-1} + \cdots + a_2 + a_1 + a_0,$$

that is,

$$a_{n+1} - a_n = \sum_{k=0}^{n} a_k. \qquad (*)$$

Therefore,

$$a_{n+1} - 2a_n = \sum_{k=0}^{n-1} a_k$$

for all $n \geq 1$.

However, from $(*)$ with n replaced by $n-1$, we get

$$a_{n+1} - 2a_n = \sum_{k=0}^{n-1} a_k = a_n - a_{n-1},$$

and therefore,

$$\begin{aligned}
a_{n+1} &= 3a_n - a_{n-1},\ n \geq 1 \\
a_0 &= 1 \\
a_1 &= 2,
\end{aligned}$$

and the sequence $\{a_n\}_{n\geq 0}$ satisfies exactly the same discrete initial value problem as $\{F_{2n+1}\}_{n\geq 0}$. To see that this implies that $a_n = F_{2n+1}$ for all $n \geq 0$, we define

$$b_n = a_n - F_{2n+1}$$

for $n \geq 0$, and note that the sequence $\{b_n\}_{n\geq 0}$ satisfies

$$\begin{aligned} b_{n+1} &= 3b_n - b_{n-1},\ n \geq 1 \\ b_0 &= 0 \\ b_1 &= 0, \end{aligned}$$

and now an easy inductive argument shows that $b_n = 0$ for all $n \geq 0$. □

Example 6. Let a be a positive real number such that

$$a + \frac{1}{a}$$

is an integer. Use the principle of strong mathematical induction to show that

$$a^n + \frac{1}{a^n} \tag{$*$}$$

is also an integer for all positive integers n.

Solution: Let a be a positive real number such that

$$a + \frac{1}{a}$$

is an integer.

Base Case: We will show that $(*)$ is also true for $n = 2$. We have

$$\left(a + \frac{1}{a}\right)^2 = a^2 + a \cdot \frac{1}{a} + \frac{1}{a^2} = a^2 + \frac{1}{a^2} + 1,$$

so that

$$a^2 + \frac{1}{a^2} = \left(a + \frac{1}{a}\right)^2 - 1.$$

Since the expression on the right side of this equality is an integer, then the expression on the left side is also an integer.

Inductive Step: Assume that $(*)$ is true for all integers k such that $1 \leq k \leq n$, we will show that this implies that $(*)$ is also true for $n+1$. We have

$$\left(a^n + \frac{1}{a^n}\right)\left(a + \frac{1}{a}\right) = a^{n+1} + a^n \cdot \frac{1}{a} + a \cdot \frac{1}{a^n} + \frac{1}{a^{n+1}} = a^{n+1} + \frac{1}{a^{n+1}} + a^{n-1} + \frac{1}{a^{n-1}}$$

so that

$$a^{n+1} + \frac{1}{a^{n+1}} = \left(a^n + \frac{1}{a^n}\right)\left(a + \frac{1}{a}\right) - \left(a^{n-1} + \frac{1}{a^{n-1}}\right).$$

From the inductive hypothesis, the expression on the right side of this equality is an integer, so that the expression on the left side is also an integer, and $(*)$ is true for $n+1$.

By the principle of strong mathematical induction the result is true for all positive integers n. □

Example 7. Let a_n be the number of strings of length n from the alphabet $\Sigma = \{0, 1, 2\}$ with no consecutive 0's.

(a) Find a_1, a_2, a_3, a_4.

(b) Give a simple counting argument to show that

$$a_n = 2a_{n-1} + 2a_{n-2}$$

for all $n \geq 3$.

(c) Use the principle of strong mathematical induction to show that

$$a_n = \frac{1}{4\sqrt{3}}\left[\left(1+\sqrt{3}\right)^{n+2} - \left(1-\sqrt{3}\right)^{n+2}\right]$$

for all $n \geq 0$.

Solution:

(a) For $n = 1$, every string of length 1 from the alphabet $\Sigma = \{0, 1, 2\}$ contains no consecutive 0's, and therefore $a_1 = 3$.

For $n = 2$, the total number of strings of length 2 is 3^2, and there is only one string with consecutive 0's, namely 0 0, and therefore, $a_2 = 3^2 - 1 = 8$.

For $n = 3$, there are only 5 strings of length 3 that contain consecutive 0's, namely,

$$000 \quad 100 \quad 200 \quad 001 \quad 002,$$

and the total number of strings of length 3 from the alphabet $\Sigma = \{0, 1, 2\}$ is 3^3, and therefore $a_3 = 3^3 - 5 = 22$.

For $n = 4$, given a string of length 4 from the alphabet $\Sigma = \{0, 1, 2\}$ with no consecutive 0's, it either starts with a 0, a 1, or a 2.

If it starts with a 0, the second element of the string must be either a 1 or a 2, and so there are $2a_2$ strings of length 4 with no consecutive 0's that start with a 0.

If it starts with a 1, then there are a_3 strings of length 4 with no consecutive 0's that start with a 1.

If it starts with a 2, then there are a_3 strings of length 4 with no consecutive 0's that start with a 2.

Since this accounts for all strings of length 4 with no consecutive 0's, and since these cases are mutually exclusive, then

$$a_4 = 2a_2 + 2a_3 = 2 \cdot 8 + 2 \cdot 22 = 60.$$

(b) We can use the method we used to determine a_4 to find a recurrence relation satisfied by a_n for all $n \geq 3$. Any string of length n with no consecutive 0's from the alphabet $\Sigma = \{0, 1, 2\}$ either starts with a 0, a 1, or a 2. Reasoning as above, there are $2a_{n-2}$ that start with a 0, a_{n-1} that start with a 1, and a_{n-1} that start with a 2. This accounts for all such strings of length n, and therefore

$$a_n = 2a_{n-1} + 2a_{n-2}$$

for all $n \geq 3$.

(c) If we want the formula $(*)$ below to hold for all $n \geq 0$, we need to define a_0, and we do this using the recurrence relation and the values of a_1 and a_2. We want

$$8 = a_2 = 2a_1 + 2a_0 = 6 + 2a_0,$$

so that we should define $a_0 = 1$. This makes sense, since there is only one string of length 0, namely, the empty string, and it has no consecutive 0's.

Now the recurrence relation

$$a_{n+2} = 2a_{n+1} + 2a_n$$

holds for all $n \geq 0$, and we will use this to show by the principle of strong mathematical induction that

$$a_n = \frac{1}{4\sqrt{3}}\left[\left(1+\sqrt{3}\right)^{n+2} - \left(1-\sqrt{3}\right)^{n+2}\right] \qquad (*)$$

is true for all $n \geq 0$.

Base Case: For $n = 0$, we have

$$\frac{1}{4\sqrt{3}}\left[\left(1+\sqrt{3}\right)^{2} - \left(1-\sqrt{3}\right)^{2}\right] = \frac{1}{4\sqrt{3}}\left[4+2\sqrt{3} - \left(4-2\sqrt{3}\right)\right] = 1 = a_0$$

and $(*)$ holds for $n = 0$.

Inductive Step: Let $n \geq 0$ be arbitrary and assume that $(*)$ holds for all integers k with $0 \leq k \leq n$, then from the recurrence relation we have

$$\begin{aligned}
a_{n+1} &= 2a_n + 2a_{n-1} \\
&= \frac{1}{2\sqrt{3}}\left[\left(1+\sqrt{3}\right)^{n+2} - \left(1-\sqrt{3}\right)^{n+2}\right] + \frac{1}{2\sqrt{3}}\left[\left(1+\sqrt{3}\right)^{n+1} - \left(1-\sqrt{3}\right)^{n+1}\right] \\
&= \frac{1}{2\sqrt{3}}\left[\left(1+\sqrt{3}\right)^{n+2} + \left(1+\sqrt{3}\right)^{n+1}\right] - \frac{1}{2\sqrt{3}}\left[\left(1-\sqrt{3}\right)^{n+2} + \left(1-\sqrt{3}\right)^{n+1}\right] \\
&= \frac{1}{2\sqrt{3}}\left[\left(2+\sqrt{3}\right)\left(1+\sqrt{3}\right)^{n+1}\right] - \frac{1}{2\sqrt{3}}\left[\left(2-\sqrt{3}\right)\left(1-\sqrt{3}\right)^{n+1}\right] \\
&= \frac{1}{2\sqrt{3}}\left[\frac{(1+\sqrt{3})^2}{2}\left(1+\sqrt{3}\right)^{n+1}\right] - \frac{1}{2\sqrt{3}}\left[\frac{(1-\sqrt{3})^2}{2}\left(1-\sqrt{3}\right)^{n+1}\right],
\end{aligned}$$

since

$$(1+\sqrt{3})^2 = 2(2+\sqrt{3}) \qquad \text{and} \qquad (1-\sqrt{3})^2 = 2(2-\sqrt{3}).$$

Therefore,

$$a_{n+1} = \frac{1}{4\sqrt{3}}\left[\left(1+\sqrt{3}\right)^{n+3} - \left(1-\sqrt{3}\right)^{n+3}\right],$$

and $(*)$ also holds for $n+1$.

Therefore, $(*)$ holds for all integers $n \geq 0$ by the principle of strong mathematical induction.

Example 8. Let $a_n,\ n \geq 1$, be the solution to the problem

$$\begin{aligned} a_{n+1} &= 1 + \frac{n}{a_n}, \quad n \geq 1 \\ a_1 &= 1. \end{aligned}$$

Show that

$$\sqrt{n} \leq a_n \leq \sqrt{n} + 1$$

for $n \geq 1$, and the inequalities are strict for all integers $n > 1$.

Solution: We will prove that $\sqrt{n} \leq a_n \leq \sqrt{n} + 1$ for $n \geq 1$ by induction on n. If $n = 1$, then

$$\sqrt{1} = 1 = a_1 \leq 2 = \sqrt{1} + 1$$

and the result is true for $n = 1$. Now suppose the result is true for some $n \geq 1$, then

$$\begin{aligned} a_{n+1} - \sqrt{n+1} &= 1 + \frac{n}{a_n} - \sqrt{n+1} \\ &= \frac{n}{a_n} - \left(\sqrt{n+1} - 1\right) \\ &= \frac{n}{a_n} - \frac{n}{\sqrt{n+1} + 1} \\ &= \frac{n\left(\sqrt{n+1} + 1 - a_n\right)}{a_n\left(\sqrt{n+1} + 1\right)} \\ &\geq \frac{n\left(\sqrt{n+1} - \sqrt{n}\right)}{a_n\left(\sqrt{n+1} + 1\right)} \\ &> 0 \end{aligned}$$

from the induction hypothesis, that is, $a_{n+1} > \sqrt{n+1}$. Also,

$$\begin{aligned} \sqrt{n+1} + 1 - a_{n+1} &= \sqrt{n+1} - \frac{n}{a_n} \\ &\geq \sqrt{n+1} - \frac{n}{\sqrt{n}} \\ &= \sqrt{n+1} - \sqrt{n} \\ &> 0 \end{aligned}$$

from the induction hypothesis, that is, $a_{n+1} < \sqrt{n+1} + 1$. Thus,

$$\sqrt{n+1} < a_{n+1} < \sqrt{n+1} + 1,$$

so we have shown that if the result is true for some $n \geq 1$, this implies that it is true for $n+1$ also. Therefore, by the principle of mathematical induction, the result is true for all $n \geq 1$.

Example 9. If F_n is the nth Fibonacci number, then

$$\lim_{n\to\infty} \frac{F_{n+1}}{F_n} = \frac{1+\sqrt{5}}{2}.$$

Solution. Recall that the *Fibonacci sequence* $\{F_n\}_{n\geq 0}$ is the unique solution to the discrete initial value problem

$$\begin{aligned} F_{n+2} &= F_{n+1} + F_n, \qquad n \geq 0 \\ F_0 &= 0 \\ F_1 &= 1. \end{aligned}$$

The first few terms of the sequence are:

$$0,\ 1,\ 1,\ 2,\ 3,\ 5,\ 8,\ 13,\ 21,\ 34,\ 55,\ 89,\ 144,\ \ldots$$

We proved *Cassini's Identity*:

$$F_{n+1}F_{n-1} - F_n^2 = (-1)^n$$

for all integers $n \geq 1$, by evaluating the determinant of the matrix

$$A^n = \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix},$$

where $A = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$, in two different ways.

Here we will use Cassini's identity to show that the sequence

$$\gamma_n = \left\{ \frac{F_n}{F_{n+1}} \right\}_{n\geq 1}$$

converges and that $\lim_{n\to\infty} \gamma_n = \frac{\sqrt{5}-1}{2}$.

After examining the terms

$$\frac{F_{2n}}{F_{2n+1}} - \frac{F_{2n-2}}{F_{2n-1}},$$

it appears that they are all positive, and that $F_{2n} \cdot F_{2n-1} - F_{2n+1} \cdot F_{2n-2} = 1$ for all $n \geq 1$. For example, if $n = 1$, we have

$$F_2 \cdot F_1 - F_3 \cdot F_0 = 1 \cdot 1 - 2 \cdot 0 = 1.$$

Lemma 1. For each $n \geq 1$,

$$F_{2n} \cdot F_{2n-1} - F_{2n+1} \cdot F_{2n-2} = 1, \qquad (*)$$

so that

$$0 < \gamma_{2n-2} = \frac{F_{2n-2}}{F_{2n-1}} < \frac{F_{2n}}{F_{2n+1}} = \gamma_{2n} < 1$$

for all $n \geq 2$. Therefore the sequence $\{\gamma_{2n}\}_{n\geq 1}$ is strictly increasing and bounded above, hence converges.

proof. If $n \geq 1$, then

$$\begin{aligned} F_{2n} \cdot F_{2n-1} - F_{2n+1} \cdot F_{2n-2} &= \left[F_{2n-1} + F_{2n-2}\right] \cdot F_{2n-1} - \left[F_{2n} + F_{2n-1}\right] \cdot F_{2n-2} \\ &= F_{2n-1}^2 + F_{2n-2} \cdot F_{2n-1} - F_{2n} \cdot F_{2n-2} - F_{2n-1} \cdot F_{2n-2} \\ &= F_{2n-1}^2 - F_{2n} \cdot F_{2n-2} \\ &= -(-1)^{2n-1} \\ &= 1 \end{aligned}$$

by Cassini's identity. Therefore, $(*)$ is true for all $n \geq 1$.

□

After examining the terms

$$\frac{F_{2n-1}}{F_{2n}} - \frac{F_{2n+1}}{F_{2n+2}},$$

it appears that they are all positive, and that $F_{2n+2} \cdot F_{2n-1} - F_{2n} \cdot F_{2n+1} = 1$ for all $n \geq 1$. For example, if $n = 1$, we have

$$F_4 \cdot F_1 - F_2 \cdot F_3 = 3 \cdot 1 - 1 \cdot 2 = 1.$$

Lemma 2. For each $n \geq 1$,

$$F_{2n+2} \cdot F_{2n-1} - F_{2n} \cdot F_{2n+1} = 1, \tag{$**$}$$

so that

$$0 < \gamma_{2n+1} = \frac{F_{2n+1}}{F_{2n+2}} < \frac{F_{2n-1}}{F_{2n}} = \gamma_{2n-1} < 1$$

for all $n \geq 2$. Therefore the sequence $\{\gamma_{2n-1}\}_{n\geq 1}$ is strictly decreasing and bounded below, hence converges.

proof. If $n = 1$, then

$$\begin{aligned} F_{2n+2} \cdot F_{2n-1} - F_{2n} \cdot F_{2n+1} &= \left[F_{2n+1} + F_{2n}\right] \cdot F_{2n-1} - F_{2n} \cdot \left[F_{2n} + F_{2n-1}\right] \\ &= F_{2n+1} \cdot F_{2n-1} + F_{2n} \cdot F_{2n-1} - F_{2n}^2 - F_{2n} F_{2n-1} \\ &= F_{2n+1} \cdot F_{2n-1} - F_{2n}^2 \\ &= (-1)^{2n} \\ &= 1 \end{aligned}$$

by Cassini's identity. Therefore, $(**)$ is true for all $n \geq 1$.

□

Now let

$$u = \lim_{n\to\infty} \gamma_{2n} \qquad \text{and} \qquad v = \lim_{n\to\infty} \gamma_{2n+1},$$

then from Cassini's identity, we have

$$F_{2n+1} \cdot F_{2n-1} - F_{2n}^2 = (-1)^{2n} = 1,$$

so that

$$\gamma_{2n-1} - \gamma_{2n} = \frac{F_{2n-1}}{F_{2n}} - \frac{F_{2n}}{F_{2n+1}} = \frac{(-1)^{2n}}{F_{2n} \cdot F_{2n+1}},$$

and letting $n \to \infty$, we have $v - u = 0$, that is, $u = v$.

Now, given $\epsilon > 0$, there exists an integer N_1 such that $|u - \gamma_{2n}| < \epsilon$ for all positive integers n such that $2n > N_1$, and there exists an integer N_2 such that $|v - \gamma_{2n+1}| < \epsilon$ for all positive integers n such that $2n+1 > N_2$. Let $N = \max\{N_1, N_2\}$, since $u = v$, we have $|u - \gamma_n| < \epsilon$ for all $n > N$. So we have shown that given any $\epsilon > 0$, there exists an integer N such that $|u - \gamma_n| < \epsilon$ whenever $n > N$, but this is exactly what we mean when we say $\lim\limits_{n\to\infty} \gamma_n = u$.

Now we know that the limit $u = \lim\limits_{n\to\infty} \gamma_n$ exists, but we still don't know its value. If we look at the difference equation for the Fibonacci numbers, $F_{n+2} = F_{n+1} + F_n$, and divide both sides by F_{n+1}, then we have

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

for all $n \geq 1$, that is,

$$\frac{1}{\dfrac{F_{n+1}}{F_{n+2}}} = 1 + \frac{F_n}{F_{n+1}}$$

for all $n \geq 1$, and letting $n \to \infty$, we get

$$\frac{1}{u} = 1 + u.$$

Therefore, u satisfies the quadratic equation $u^2 + u - 1 = 0$, with distinct real roots

$$\lambda_1 = \frac{-1 + \sqrt{5}}{2} \qquad \text{and} \qquad \lambda_2 = \frac{-1 - \sqrt{5}}{2}.$$

Since each term in the sequence satisfies $0 < \gamma_n < 1$, then the limit is the positive root

$$u = \lim_{n\to\infty} \gamma_n = \frac{\sqrt{5} - 1}{2}.$$

It follows from this that

$$\lim_{n\to\infty} \frac{F_{n+1}}{F_n} = \frac{1 + \sqrt{5}}{2}$$

the *Golden Ratio.*

Example 10. For any $m \geq 1$ and $n \geq 1$, we have

$$(m+1)^n > mn.$$

SOLUTION: The proof is by double induction. For each $m \geq 1$ and $n \geq 1$, let $P(m, n)$ be the statement that $(m+1)^n > mn$.

For $m = 1$ and $n = 1$, the statement $P(1, 1)$ is just the inequality

$$(1+1)^1 > 1 \cdot 1,$$

that is $2 > 1$, which is true.

Now suppose that $m \geq 1$, and $P(m, 1)$ is true, then

$$\big((m+1) + 1\big)^1 = m + 2 > m + 1 = (m+1) \cdot 1,$$

so that $P(m+1, 1)$ is true also.

Finally, let $n \geq 1$, and suppose that $P(m,n)$ is true for all $m \geq 1$, then

$$(m+1)^{n+1} = (m+1)(m+1)^n > (m+1)(mn) \geq mn + m = m(n+1),$$

since $m \geq 1$ and $n \geq 1$ imply that $m^2n + mn \geq mn + m$. Therefore, $P(m, n+1)$ is true for all $m \geq 1$.

Thus, we have shown that

(i) $P(1,1)$ is true,

(ii) For all $m \geq 1$, if $P(m,1)$ is true, then $P(m+1,1)$ is true,

(iii) For all $n \geq 1$, if $P(m,n)$ is true for all $m \geq 1$, then $P(m,n+1)$ is true for all $m \geq 1$,

and by the principle of double induction, $P(m,n)$ is true for all $m \geq 1$ and $n \geq 1$.

Inductive and Recursive Definitions

Definition. A function $f : \mathbb{Z}^+ \to \mathbb{R}$ is said to be defined **inductively** if and only if

(i) $f(1)$ is given,

(ii) $f(n+1)$ is given in terms of $f(n)$, or even in terms of all $f(k)$, for $k = 1, 2, \ldots, n$.

Examples of functions that are defined inductively are given below.

Example 11. The **factorial function**

$$f(n) = n!$$

for $n \geq 1$, is defined inductively by

$$f(1) = 1$$
$$f(n+1) = (n+1) \cdot f(n), \quad n \geq 1.$$

Example 12. The **power function**

$$f(n) = 2^n$$

for $n \geq 0$, is defined inductively by

$$f(0) = 1,$$
$$f(n+1) = 2 \cdot f(n), \quad n \geq 0.$$

Definition. A function $f :\to \mathbb{R}$ is said to be defined **recursively** if and only if each value $f(n)$ is either

(i) given explicitly, or

(ii) given in terms of previously defined values of f.

Examples of recursively defined functions are given below.

Example 13. The **Fibonacci sequence** $\{f_n\}_{n\geq 0}$ given by

f_0	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	f_9	f_{10}	f_{11}	f_{12}	$\cdots$
0	1	1	2	3	5	8	13	21	34	55	89	144	$\cdots$

is defined recursively by

$$f_0 = 0$$

$$f_1 = 1$$

$$f_{n+2} = f_{n+1} + f_n, \quad n \geq 0.$$

We can give an explicit formula for the terms in the Fibonacci sequence:

$$f_n = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right]$$

for $n \geq 0$, namely, *Binet's formula*.

We will prove this using strong induction (earlier we gave a proof by solving a discrete initial value problem). Let

$$\alpha = \frac{1+\sqrt{5}}{2} \qquad \text{and} \qquad \beta = \frac{1-\sqrt{5}}{2},$$

then $\alpha^2 = \alpha + 1$ and $\beta^2 = \beta + 1$. We will show that

$$f_n = \frac{1}{\sqrt{5}}\left[\alpha^n - \beta^n\right] \tag{$*$}$$

for all integers $n \geq 0$.

Base Case: $n = 0$:

$$\frac{1}{\sqrt{5}}\left[\alpha^0 - \beta^0\right] = \frac{1}{\sqrt{5}}\left[1 - 1\right] = 0,$$

and $f_0 = 0$, so that $(*)$ holds for $n = 0$.

Inductive Step: Assume that $(*)$ is true for all integers k with $0 \leq k \leq n+1$, we will show that this implies that $(*)$ is true for $n+2$. Let

$$a_m = \frac{1}{\sqrt{5}}\left[\alpha^m - \beta^m\right]$$

for $m \geq 0$, then we have

$$\begin{aligned}
a_{n+2} &= \frac{1}{\sqrt{5}}\left[\alpha^{n+2} - \beta^{n+2}\right] \\
&= \frac{1}{\sqrt{5}}\left[\alpha^n\alpha^2 - \beta^n\beta^2\right] \\
&= \frac{1}{\sqrt{5}}\left[(\alpha+1)\alpha^n - (\beta+1)\beta^n\right] \\
&= \frac{1}{\sqrt{5}}\left[\alpha^{n+1} - \beta^{n+1}\right] + \frac{1}{\sqrt{5}}\left[\alpha^n - \beta^n\right] \\
&= f_{n+1} + f_n
\end{aligned}$$

from the inductive hypothesis. Thus,

$$\frac{1}{\sqrt{5}}\left[\alpha^{n+2} - \beta^{n+2}\right] = f_{n+1} + f_n = f_{n+2},$$

and $(*)$ is true for $n+2$. By the principle of mathematical induction, $(*)$ is true for all integers $n \geq 0$.

Example 14. The **binomial coefficients** $\binom{n}{k}$ given by

$$\binom{n}{k} = \begin{cases} \dfrac{n!}{k!(n-k)!} & \text{for } 0 \le k \le n, \\ 0 & \text{otherwise} \end{cases}$$

for $n \geq 0$, are defined recursively by

$$\binom{n}{0} = 1, \quad n \geq 0,$$

$$\binom{0}{k} = 0, \quad k \geq 1,$$

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}, \quad 1 \le k \le n.$$

Note: Recursive definitions are more general than inductive definitions in that the value of $f(n)$ may be defined using previous values of $f(k)$ with $k > n$.

Inductive definitions have the important advantage that it is easy to verify that they really are definitions. Recursive definitions often require special arguments to verify that $f(n)$ is indeed defined for all positive integers n.

Example 15. A recursive definition that is **not** an inductive definition.

For $n \geq 1$, define

$$f(n) = \begin{cases} 1 & \text{if } n \text{ is a multiple of 3,} \\ 1 + f(n+1) & \text{if } n \text{ is not a multiple of 3.} \end{cases}$$

Note that from the first part of the recursive definition, we have

$$f(3) = f(6) = f(9) = f(12) = f(15) = \cdots = 1.$$

Now we compute

$$f(1) = 1 + f(2)$$

and

$$f(2) = 1 + f(3) = 1 + 1 = 2,$$

so that

$$f(1) = 1 + 2 = 3.$$

Continuing,

$$f(4) = 1 + f(5) = 1 + 1 + f(6) = 1 + 1 + 1 = 3,$$

$$f(7) = 1 + f(8) = 1 + 1 + f(9) = 1 + 1 + 1 = 3,$$

$$f(8) = 1 + f(9) = 1 + 1 = 2,$$

$$\vdots$$

and it is easy to see, since for any three consecutive integers, one of them has to be a multiple of 3, that the computation of $f(n)$ always terminates after using at most two other values of n. Thus, the function f is in fact defined for all $n \geq 1$.

In fact, we can define f nonrecursively as

$$f(n) = \begin{cases} 1 & \text{for } n \equiv 0 \pmod 3 \\ 3 & \text{for } n \equiv 1 \pmod 3 \\ 2 & \text{for } n \equiv 2 \pmod 3 \end{cases}$$

for $n \geq 1$.