Mathematical Induction

- **Principle of Mathematical Induction**

  Let $P(n)$ be a property defined on the integers and a be a fixed integer.

  Suppose the following two statements are true:

  1. $P(a)$ is true.
  2. For all integers $n \geq a$, if $P(n)$ is true then $P(n+1)$ is true.

  Then $P(n)$ is true for all integers n with $n \geq a$.

- Mathematical induction is a powerful proof technique. It is called a *principle* because it can not be derived from other facts, but is taken to be an axiom (of the theory of the natural numbers).

Induction Proofs

- A proof by mathematical induction consists of two parts:

  1. **Induction basis**

     Show that $P(a)$ is true.

  2. **Inductive step**

     Show that for all integers $n \geq a$, $P(n+1)$ is true whenever $P(n)$ is true.

- The inductive step requires a proof of

$$\forall n \in \mathbf{Z}, [n \geq a \rightarrow (P(n) \rightarrow P(n+1))].$$

- For this purpose it is sufficient to show that

$$P(k) \rightarrow P(k+1)$$

  is true for an arbitrary but fixed integer k with $k \geq a$.

- The proof of this conditional statement typically proceeds in two steps:
  - Assume that $P(k)$ is true.
  - Show that $P(k+1)$ is true.

- The assumption, that $P(k)$ is true, is called the **inductive hypothesis**.

Example: Sum of Integers

- Let $P(n)$ be the property,

  $$1 + 2 + \cdots + n = \frac{n(n+1)}{2}.$$

  We use mathematical induction to prove that $P(n)$ is true for all integers $n \geq 1$.

- **Basis step**

  If $n = 1$, then both sides of the equation evaluate to 1. Thus $P(1)$ is true.

- **Inductive step**

  Let k be an arbitrary but fixed integer with $k \geq 1$.

  We assume, as inductive hypothesis, that $P(k)$ is true,

  $$1 + 2 + \cdots + k = \frac{k(k+1)}{2}.$$

  We need to show that $P(k+1)$ is true,

  $$1 + 2 + \cdots + k + (k+1) = \frac{(k+1)((k+1)+1)}{2}.$$

We can prove $P(k+1)$ using basic algebra and the inductive hypothesis:

$$\begin{aligned}
&1 + 2 + \cdots + k + (k+1) \\
&\quad = \quad (1 + 2 + \cdots + k) + (k+1) \\
&\quad = \quad k(k+1)/2 + (k+1) \qquad\qquad \text{(by I.H.)} \\
&\quad = \quad k(k+1)/2 + 2(k+1)/2 \\
&\quad = \quad (k+2)(k+1)/2 \\
&\quad = \quad (k+1)((k+1)+1)/2
\end{aligned}$$

Example: Sum of Squares

- Let $P(n)$ be the property that

  $$1 + 4 + \cdots + n^2 = n(n+1)(2n+1)/6.$$

  We use induction to prove that $P(n)$ is true for all integers $n \geq 1$.

- **Basis step**

  If $n = 1$, then both sides of the equation evaluate to 1,

  $$1^2 = 1 = (1 \cdot 2 \cdot 3)/6.$$

  Thus $P(1)$ is true.

- **Inductive step**

  Let k be an arbitrary but fixed integer with $k \geq 1$. We assume, as inductive hypothesis, that $P(k)$ is true,

  $$1 + 4 + \cdots + k^2 = k(k+1)(2k+1)/6,$$

  and need to show that $P(k+1)$ is true,

  $$1 + 4 + \cdots + k^2 + (k+1)^2 = (k+1)(k+2)(2k+3)/6.$$

The key step in the proof is again the application of the inductive hypothesis:

$$
\begin{aligned}
1 + 4 + & \cdots + k^2 + (k+1)^2 \\
&= (1 + 4 + \cdots + k^2) + (k+1)^2 \\
&= k(k+1)(2k+1)/6 + (k+1)^2 && \text{(by I.H.)} \\
&= (k+1)(2k^2+k)/6 + (k+1)6(k+1)/6 \\
&= (k+1)[(2k^2+k) + 6(k+1)]/6 \\
&= (k+1)(2k^2+7k+6)/6 \\
&= (k+1)(k+2)(2k+3)/6
\end{aligned}
$$

Example: An Inequality

- Let $P(n)$ be the property
$$2n + 1 < 2^n.$$
We use mathematical induction to prove that $P(n)$ is true for all $n \geq 3$.

- **Basis step**

If $n = 3$, then
$$2n + 1 = 2 * 3 + 1 = 7 < 8 = 2^3 = 2^n.$$
Thus $P(3)$ is true.

- **Inductive step**

Let k be an arbitrary but fixed integer with $k \geq 3$. We assume, as inductive hypothesis, that $P(k)$ is true,
$$2k + 1 < 2^k,$$
and need to show that $P(k + 1)$ is true,
$$2(k + 1) + 1 < 2^{k+1}.$$

We have
$$\begin{aligned} 2(k+1)+1 &= (2k+2)+1 \\ &= (2k+1)+2 \\ &< 2^k + 2 \qquad \text{(by I.H.)} \\ &< 2 * 2^k \\ &= 2^{k+1} \end{aligned}$$
which completes the proof.

Example: Another Inequality

- Let $P(n)$ be the property
$$2^n > n^3.$$
We use mathematical induction to prove that $P(n)$ is true for all $n \geq 10$.

- **Basis step**

If $n = 10$, then $2^n = 2^{10} = 1024$ and $n^3 = 10^3 = 100$. Thus $P(10)$ is true.

- **Inductive step**

Let k be an arbitrary but fixed integer with $k \geq 10$. We assume, as inductive hypothesis, that $P(k)$ is true,
$$2^k > k^3,$$
and have to show that $P(k+1)$ is true,
$$2^{k+1} > (k+1)^3.$$
We have
$$\begin{array}{rcll} 2^{k+1} & = & 2 * 2^k & \\ & > & 2 * k^3 & \text{(by I.H.)} \\ & = & k^3 + k^3 & \\ & > & k^3 + 7k^2 & \text{(because } k \geq 10\text{)} \\ & > & k^3 + 3k^2 + 3k + 1 & \text{(because } k \geq 10\text{)} \\ & = & (k+1)^3 & \end{array}$$
which completes the proof.

Example: Divisibility

- Let $P(n)$ be the property

  $2^{n+2} + 3^{2n+1}$ is divisible by 7.

  We prove that $P(n)$ is true for all integers $n \geq 0$.

- **Basis step**

  If $n = 0$, then

  $$2^{n+2} + 3^{2n+1} = 2^2 + 3^1 = 4 + 3 = 7,$$

  which indicates that $P(0)$ is true.

- **Inductive step**

  Let k be an arbitrary, but fixed nonnegative integer. We assume, as inductive hypothesis, that $P(k)$ is true. That is, $2^{k+2} + 3^{2k+1}$ is divisible by 7, or equivalently,

  $$2^{k+2} + 3^{2k+1} = 7j,$$

  for some integer j.

  We have to show that $2^{(k+1)+2}+3^{2(k+1)+1}$ is divisible by 7.

In detail:

$$
\begin{aligned}
2^{(k+1)+2} &+ 3^{2(k+1)+1} \\
&= 2^{k+3} + 3^{2k+3} \\
&= 2^{k+3} + 9 * 3^{2k+1} \\
&= (2^{k+3} + 2 * 3^{2k+1}) + 7 * 3^{2k+1} \\
&= 2(2^{k+2} + 3^{2k+1}) + 7 * 3^{2k+1} \\
&= 2(7j) + 7 * 3^{2k+1} \text{ (by I.H.)} \\
&= 7(2j + 3^{2k+1})
\end{aligned}
$$

Another Example

- Let $P(n)$ be the property

  $$a \leq b \rightarrow a^n \leq b^n$$

  where a and b are nonnegative real numbers. We prove that $P(n)$ is true for all integers $n \geq 0$.

- **Basis step**

  Since $a^0 = 1 \leq 1 = b^0$ the property $P(0)$ is trivially true.

- **Inductive step**

  Let k be an arbitrary, but fixed nonnegative integer.

  We assume, as inductive hypothesis, that $P(k)$ is true,

  $$a \leq b \rightarrow a^k \leq b^k,$$

  and have to show that $P(k+1)$ is also true,

  $$a \leq b \rightarrow a^{k+1} \leq b^{k+1}.$$

  To prove the conditional statement $P(k+1)$ we assume

  (1) $a \leq b$

  and then need to show $a^{k+1} \leq b^{k+1}$.

From the inductive hypothesis and (1) we may infer

(2) $a^k \leq b^k$

by Modus Ponens. Since a is nonnegative, we get

(3) $a * a^k \leq a * b^k$

from (2). Since b^k is nonnegative, we also get

(4) $a * b^k \leq b * b^k$

from (1). Putting (3) and (4) together, we obtain the desired conclusion,

$$a^{k+1} = a * a^k \leq b * b^k = b^{k+1}.$$

Strong Mathematical Induction

- **Principle of Strong Mathematical Induction**

  Let $P(n)$ be a property defined on the integers and a be a fixed integer.

  Suppose for all integers $n \geq a$ the following conditional statement is true:

  > If $P(j)$ is true for all integers with $a \leq j < n$, then $P(n)$ is true.

  Then $P(n)$ is true for all natural numbers n with $n \geq a$.

- Strong mathematical induction requires a proof of the following formula:

$$\begin{aligned} &\forall n \in \mathbf{Z}, [n \geq a \rightarrow \\ &\quad (\forall j \in \mathbf{Z}, (a \leq j < n \rightarrow P(j)) \rightarrow P(n))] \end{aligned}$$

- For this purpose it is sufficient to show that, for an arbitrary but fixed integer k with $k \geq a$, if

$$\forall j \in \mathbf{Z}, (a \leq j < k \rightarrow P(j))$$

  is true, then $P(k)$ is also true.

- The formula

$$\forall j \in \mathbf{Z}, (a \leq j < k \rightarrow P(j))$$

  is called the *inductive hypothesis*.

Divisibility by a Prime

- Let $P(n)$ be the property that

  n is divisible by a prime number.

  We use strong mathematical induction to prove that $P(n)$ is true for all integers n with $n \geq 2$.

- Let k be an arbitrary, but fixed nonnegative integer with $k \geq 2$. We have to prove

  $$\forall j \in \mathbf{Z}, (2 \leq j < k \rightarrow P(j)) \rightarrow P(k).$$

  We assume, as inductive hypothesis, that

  $$\forall j \in \mathbf{Z}, (2 \leq j < k \rightarrow P(j))$$

  is true and have to show that $P(k)$ is true.

  We distinguish two cases.

  - If k is a prime number, then $P(k)$ is obviously true because every number divides itself.
  - If k is not a prime number, then it is a product $k = s * t$ of two integers s and t, such that $1 < s < k$ and $1 < t < k$.

    By the inductive hypothesis, t is divisible by a prime number. By the transitivity of divisibility, k is also divisible by a prime.

  We have shown that in either case k is divisible by a prime number, which completes the proof.

Fibonacci Numbers

- The *Fibonacci numbers* are defined recursively by:

$$F_n = \begin{cases} 1 & \text{if } n = 0 \\ 1 & \text{if } n = 1 \\ F_{n-1} + F_{n-2} & \text{if } n > 1 \end{cases}$$

- Let ϕ be the number $(1+\sqrt{5})/2$ and $P(n)$ be the property that

$$F_n \leq \phi^n.$$

  We use strong mathematical induction to prove that $P(n)$ is true for all nonnegative integers n.

- The proof will be in three parts.
  - If $n = 0$, then $F_n = F_0 = 1 = \phi^0 = \phi^n$. Thus $P(0)$ is true.
  - If $n = 1$, then $F_n = F_1 = 1 < 3/2 < (1+\sqrt{5})/2 = \phi = \phi^n$. Thus $P(1)$ is true.
  - Let k be an arbitrary but fixed integer with $k \geq 2$. We assume, as inductive hypothsis, that $P(j)$ is true for all j with $0 \leq j < k$, and have to show that $P(k)$ is true.

In detail,

$$\begin{aligned}
F_k &= F_{k-1} + F_{k-2} && \text{(by def. of } F_k\text{)} \\
&\leq \phi^{k-1} + \phi^{k-2} && \text{(from I.H.)} \\
&= \phi^{k-2}(\phi + 1) && \\
&= \phi^{k-2}\phi^2 && \text{(see below)} \\
&= \phi^k &&
\end{aligned}$$

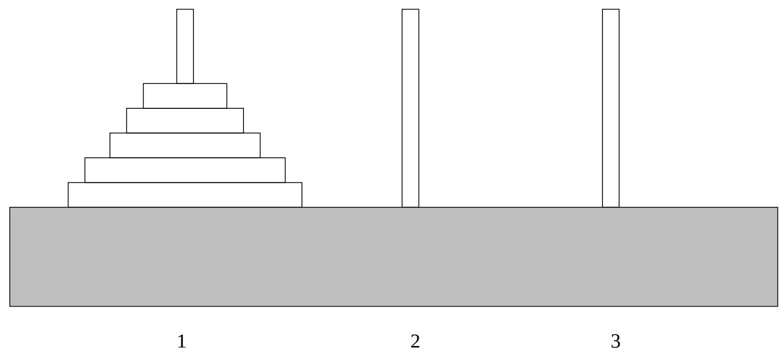
Note that

$$\begin{aligned}
\phi^2 &= (6 + 2\sqrt{5})/4 &&= (3 + \sqrt{5})/2 \\
&= 1 + (1 + \sqrt{5})/2 &&= 1 + \phi.
\end{aligned}$$

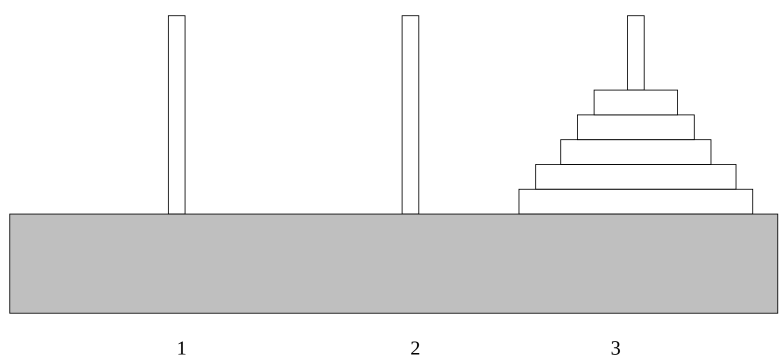
This completes the proof.

The Tower of Hanoi

- The **tower of Hanoi** consists of a fixed number of **disks** stacked on a pole in decreasing size, that is, with the smallest disk at the top.



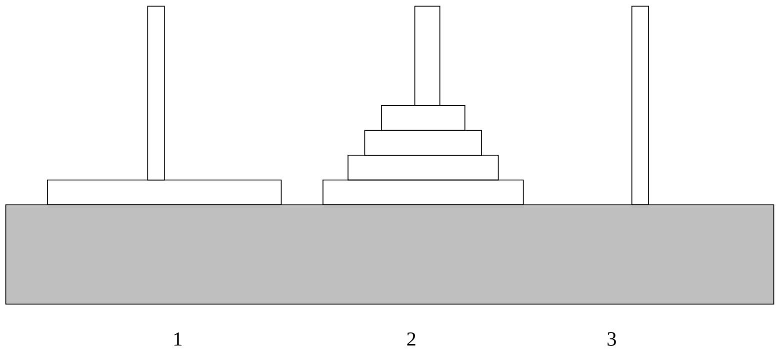
- There are two other **poles** and the task is to transfer all disks from the first to the third pole, one at a time without ever placing a larger disk on top of a smaller one.



- There is an elegant solution to this problem by recursion.

Solution: Tower of Hanoi

- First observe that the largest disk can only be moved if all smaller disks are stacked on a single pole:



- This suggests the following solution for moving a tower of n disks from any pole a to any other pole b (with c being the third pole):
  - First transfer the stack of $n-1$ smaller disks from a to c.
  - Then move the largest disks from a to b.
  - Finally transfer the stack of $n-1$ smaller disks from c to b.

- The minimum number of moves required to transfer n disks from one pole to another pole can thus be defined recursively as follows:

$$\begin{aligned} M(1) &= 1 \text{ and} \\ M(n) &= 2M(n-1)+1 \text{ if } n>1 \end{aligned}$$

Number of Moves

- Let $P(n)$ be the property that

  $$M(n) = 2^n - 1.$$

  We use mathematical induction to prove that $P(n)$ is true for all $n \geq 1$.

- Since $M(1) = 1 = 2^1 - 1$ we know that $P(0)$ is true.

- Let k be an arbitrary but fixed integer with $k > 1$. We assume, as inductive hypothsis, that $P(j)$ is true for all j with $1 \leq j < k$, and show that $P(k)$ is true.

  In detail,

  $$\begin{array}{rcll} M(k) & = & 2 * M(k-1) + 1 & \text{(by def. of } M(k)\text{)} \\ & = & 2 * (2^{k-1} - 1) + 1 & \text{(by I.H.)} \\ & = & (2^k - 2) + 1 & \\ & = & 2^k - 1 & \end{array}$$