Mathematical Induction

- It is a technique for proving a statement $\forall n \in \mathbb{Z}^+ \, P(n)$.
- Can be adapted to prove the correctness of some algorithms.
- As a rule of inference, it is

$$(P(1) \wedge \forall k \, (P(k) \to P(k+1))) \to \forall n \, P(n).$$

  $P(1)$ is called the **basis step**, $P(k) \to P(k+1)$ is called the **inductive step**, and the assumption that the hypothesis $P(k)$ of the inductive step holds is called the **inductive hypothesis**.

Induction is not helpful in discovering new mathematical statements which are true. Once a pattern or truth has been conjectured, however, induction can often establish that it is true.

Examples:

1. $\sum_{j=1}^{n}(2j-1) \; = \; 1+3+5+\cdots+(2n-1) \; = ?.$

   Did Wed.

2. For all positive integers, $23^n - 1$ is divisible by 11.

   Did Wed.

3. For all positive integers, $n < 2^n$.

   Did Wed.

4. For all $n \in \mathbb{N} - \{0,1,2,3\}$, $2^n < n!$

Did Wed.

5. If B is a set with $|B| = n$, then $|\mathcal{P}(B)| = 2^n$, for all $n \in \mathbb{N}$.

$Q(n)$: If set B has cardinality n, then $|\mathcal{P}(B)| = 2^n$.

$Q(0)$: When $|B| = 0$, $|\mathcal{P}(B)| = 2^0 = 1$.

Note: $|B| = 0 \to B = \{\} \to \mathcal{P}(B) = \{\{\}\} \to |\mathcal{P}(B)| = 1$.

Assume now that, for some $k \in \mathbb{N}$, $Q(k)$ holds.

Taking a set B with $|B| = k+1$, notice that $B = \{e_1, e_2, \ldots, e_{k+1}\}$

$$B = \{e_1, e_2, \ldots, e_k\} \cup \{e_{k+1}\}.$$

All the subsets of B are made up from

subset of $\{e_1, \ldots, e_k\}$ either joined with $\{e_{k+1}\}$ or not.

Subsets of B $\to$ subset of $\{e_1, \ldots, e_k\}$ unaltered

$\to$ subset of $\{e_1, \ldots, e_k\} \cup \{e_{k+1}\}$.

$$|\mathcal{P}(B)| = 2 \cdot |\mathcal{P}(\{e_1, \ldots, e_k\})| = 2 \cdot 2^k = 2^{k+1}.$$

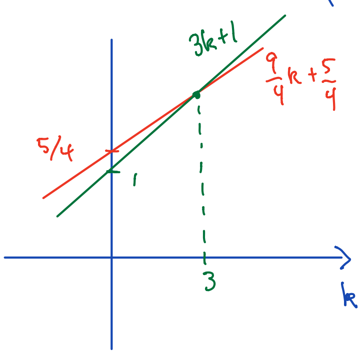
6. Show that $3n^3 + 2n + 7 \leqslant 4n^3$ for $n = 3, 4, 5, \ldots$.

$3k+1 = \frac{9}{4}k + \frac{5}{4} \Rightarrow \frac{3}{4}k = \frac{1}{4} \Rightarrow k = 3$

$P(n)$: $3n^3 + 2n + 7 \leq 4n^3$

Base case: $P(3)$ says $\underbrace{3(3^3) + 2(3) + 7}_{= 94} \leq \underbrace{4(3^3)}_{= 108}$ ✓

Assume $P(k)$ holds for some $k \geq 3$. We must show $P(k+1)$: $\boxed{3(k+1)^3 + 2(k+1) + 7 \leq 4(k+1)^3}$.



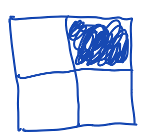
$$
\begin{aligned}
3(k+1)^3 + 2(k+1) + 7 &= 3(k^3 + 3k^2 + 3k + 1) + 2k + 2 + 7 \\
&= 3k^3 + 2k + 7 + 9k^2 + 9k + 5 \\
&\leq 4k^3 + 9k^2 + 9k + 5 \quad \text{(by the induction hypothesis)} \\
&= 4\left(k^3 + \frac{9}{4}k^2 + \frac{9}{4}k + \frac{5}{4}\right) \leq 4\left(k^3 + 3k^2 + \underline{\frac{9}{4}k + \frac{5}{4}}\right) \\
&\leq 4(k^3 + 3k^2 + \underline{3k + 1}) = 4(k+1)^3.
\end{aligned}
$$

↑ for $k \geq 3$

7. One can tile an $2^n \times 2^n$ checkerboard with one space removed using tiles shaped like 

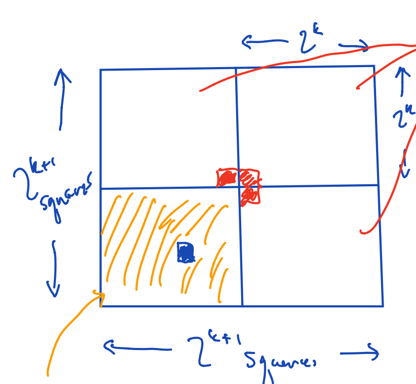
$P(n)$: Given a $2^n \times 2^n$ checkerboard missing one square, we can tile it.

Basis step: $P(1)$



Induction step: Can assume $P(k)$ holds for some $k \in \mathbb{Z}^+$.

Take a $2^{k+1} \times 2^{k+1}$ checkerboard



red-square-omitted sections of these sub-checkerboards can be tiled by induction hyp. Then finish w/ one more tile.

tile-able, by induction hyp.

8. **Induction misused**. Let $P(n)$ be the statement "Any collection of $n \geqslant 2$ distinct lines in the plane, no two of which are parallel, shares a common point.

The following is an attempt to prove $\forall n \in \mathbb{Z}^+, P(n)$:
Base case: $P(2)$ says 2 non-parallel lines in the plane have a common point. This seems true enough without requiring proof.
Inductive step: We assume $P(k)$ is true for some integer $k \geqslant 2$. The case $P(k+1)$ has us considering $(k+1)$ non-parallel lines in the plane: $\{\ell_1, \ell_2, \dots, \ell_k, \ell_{k+1}\}$. Now the collection $\{\ell_1, \ell_2, \dots, \ell_k\}$ has k different non-parallel lines so by the induction hypothesis, this collection has a common point, call it P_1. As well, the induction hypothesis applies to the collection $\{\ell_2, \ell_3, \dots, \ell_k, \ell_{k+1}\}$, so these lines have a common point, call it P_2. But two points in a plane uniquely determine a line, and since no two lines found in both collections can be the same, it must be that points P_1 and P_2 are really the same point. Thus, our original collection $\{\ell_1, \ell_2, \dots, \ell_k, \ell_{k+1}\}$ shares a common point, showing that $P(k+1)$ holds.
Thus, by induction, $P(n)$ holds for all $n = 2, 3, 4, \dots$.

The flaw: The argument in the inductive step does not work for passing from the base case $k=2$ to the case $k+1=3$. This is because, in order to argue that P_1 and P_2 are the same point, we needed the collections

$$\{\ell_1, \ell_2, \ell_3, \dots, \ell_k\} \quad \text{and} \quad \{\ell_2, \ell_3, \dots, \ell_k, \ell_{k+1}\}$$

to have two (or more) lines in common. But in attempting to prove

$$P(2) \rightarrow P(3),$$

you only start with 3 lines $\{\ell_1, \ell_2, \ell_3\}$, and when you pare back to 2 lines to invoke the induction hypothesis, your collections

$$\{\ell_1, \ell_2\} \quad \text{and} \quad \{\ell_2, \ell_3\}$$

do not have two lines in common.

Strong Induction and the Well-Ordering Principle

Mathematical induction can be expressed as the rule of inference

$$(P(a) \wedge (P(k) \to P(k+1))) \to \forall n \geqslant a,\, P(n).$$

Upon reflection, the portion $P(k) \to P(k+1)$, what we call the inductive step, is not the only thing that, coupled with the basis step which leads to the conclusion $\forall n P(n)$. Equally valid would be the conditional statement (containing a stronger hypothesis)

$$(P(i) \text{ is true for integers } a \leqslant i \leqslant k) \to P(k+1).$$

This leads to the following generalization of mathematical induction.

Definition 1 (Principle of Strong Mathematical Induction): Let $P(n)$ be a property that is defined for integers n, and let a, b be fixed integers with $a \leqslant b$. Suppose the following statements are true:

1. $P(a), P(a+1), \ldots, P(b)$ are all true (**basis step**).
2. For any integer $k \geqslant b$, if $P(i)$ is true for all integers i from a through k, then $P(k+1)$ is true (**inductive step**).

Then the statement "for all integers $n \geqslant a$, $P(n)$" is true.

The supposition that $P(i)$ is true for all integers i from a through k in number 2 above is called the **inductive hypothesis**.

To prove this is a valid rule of inference we rely on the **Well-Ordering principle**.

Definition 2 (Well-Ordering Principle): Suppose $A \subseteq \mathbb{N}$. Then A has a *smallest element*. That is, $\exists a \in A$ such that $\forall b \in A$, $(a \leqslant b)$.

Note that the set {positive real numbers} does not have a smallest element, but that this does not violate the well-ordering principle.

Generally speaking, anything provable via one of i) mathematical induction, ii) strong mathematical induction, or iii) the well-ordering principle, is provable with the other two. This is because all three statements are logically equivalent. However, sometimes one approach is easier than another. Some examples of statements and proof methods include:

1. Every integer $n \geqslant 2$ is a prime or can be written as the product of primes (use strong mathematical induction).

2. For any $n \geqslant 8$, n cents can be obtained using 3¢ and 5¢ coins (use strong mathematical induction)..

3. Let $a_0, a_1, a_2, \ldots$ be the sequence defined by the 2^{nd}-order linear recursion relation

$$a_n = 6a_{n-1} - 5a_{n-2}, \quad \text{for } n \geqslant 2, \quad \text{with } a_0 = 0,\ a_1 = 4.$$

Take $P(n)$: $a_n = 5^n - 1$. Then $\forall n \in \mathbb{N}$, $P(n)$ (use strong mathematical induction).

4. Use strong mathematical induction to show the product of n numbers requires $n-1$ multiplications, regardless of grouping.

5. A simple polygon with $n \geqslant 3$ sides can be triangulated into $n-2$ triangles (use strong mathematical induction, and the fact that every simple polygon with at least four sides has an interior diagonal).

6. Given a strictly decreasing sequence of *positive* integers $r_1, r_2, r_3, \ldots$ (so $r_{i+1} < r_i$ for each i), the sequence terminates (use the well-ordering principle).

7. Given any integer n and any positive integer d, there exist integers q and r such that $n = dq + r$ and $0 \leqslant r < d$ (use the well-ordering principle).