CHAPTER 4 INDUCTION

SECTION 4.1 MATHEMATICAL INDUCTION

Mathematical induction is used to prove statements that asserts that $P(n)$ is true for all $n \in \mathbb{Z}^+$ where $P(n)$ is a propositional function. It is an extremely important proof technique.

> **PRINCIPLE OF MATHEMATICAL INDUCTION**
>
> To prove $\forall n \in \mathbb{Z}^+(P(n))$ where $P(n)$ is a propositional function, we complete two steps:
>
> **BASIS STEP**: Verify that $P(1)$ is true.
>
> **INDUCTIVE STEP**: Show that $\forall k \in \mathbb{Z}^+(P(1) \wedge P(2) \wedge \cdots \wedge P(k) \rightarrow P(k+1))$ is true.

To complete the inductive step, we assume that $P(1), \ldots, P(k)$ are true, (this assumption is known as the **INDUCTION HYPOTHESIS**), and prove that $P(k+1)$ is true. (It may seem circular and thus requires some clarification. We are not asserting that $P(k)$ is true for all k here. What we are saying is that under the hypothesis that $P(1), \ldots, P(k)$ are true, we can prove that $P(k+1)$ is true.)

What we do here is the following.

$$\begin{aligned} P(1) &\quad \text{(basis step)} \\ P(1) \Rightarrow P(2) & \\ P(1) \wedge P(2) \Rightarrow P(3) & \\ P(1) \wedge P(2) \wedge P(3) \Rightarrow P(4) & \\ \cdots & \end{aligned}$$

Eventually, we get $P(5), P(6), \ldots$.

EXAMPLE

- Prove that $\forall n \in \mathbb{Z}^+$, $\displaystyle\sum_{i=1}^{n} i = 1 + 2 + \cdots + n = \frac{n(n+1)}{2}$.

PROOF: Let $P(n)$ be the proposition that $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$.

Basis step: P(1) is true since $\sum_{i=1}^{1} i = 1 = \frac{1(1+1)}{2}$.

Inductive step: Assume that $P(1), \ldots, P(k)$ are true, where $k \geq 1$, i.e.,

$$\sum_{i=1}^{j} i = \frac{j(j+1)}{2} \quad \text{for } j = 1, 2, \ldots, k \quad .$$

Then $P(k+1)$ is true since

$$\begin{aligned}\sum_{i=1}^{k+1} i &= \Big(\sum_{i=1}^{k} i\Big) + (k+1) = \frac{k(k+1)}{2} + (k+1) \quad \text{(we use } P(k) \text{ here)}\\ &= \frac{(k+1)(k+2)}{2} = \frac{(k+1)((k+1)+1)}{2}.\end{aligned}$$

Thus $P(n)$ is true for all $n \in \mathbb{Z}^+$ by mathematical induction.

- Prove that $n < 2^n$ for all $n \in \mathbb{Z}^+$.

PROOF: Let $P(n)$ be the proposition that $n < 2^n$.

Basis step: $P(1)$ is true since $1 < 2^1$.

Inductive step: Assume $P(1), \ldots, P(k)$ are true. From $P(k)$, we have $k < 2^k$. Add 1 to both sides, we have

$$\begin{aligned}k+1 &< 2^k + 1\\ &< 2^k + 2^k = 2^{k+1}\end{aligned}$$

and hence $P(k+1)$ is true.

Therefore by mathematical induction $n < 2^n$ for all $n \in \mathbb{Z}^+$.

- The **HARMONIC NUMBERS** H_j, $j \in \mathbb{Z}^+$, are defined by

$$H_j = \frac{1}{1} + \frac{1}{2} + \cdots + \frac{1}{j}.$$

Prove that $H_{2^n} \geq 1 + \frac{n}{2}$ for all $n \in \mathbb{Z}^*$.

PROOF: Let $P(n)$ be the proposition that $H_{2^n} \geq 1 + \frac{n}{2}$.

Basis step: $P(0)$ is true since $H_{2^0} = \frac{1}{1} \geq 1 + \frac{0}{2}$.

Inductive step: Assume that $P(0), \ldots, P(k)$ are true. Then

$$\begin{aligned}H_{2^{k+1}} &= \Big(\frac{1}{1} + \frac{1}{2} + \cdots + \frac{1}{2^k}\Big) + \Big(\frac{1}{2^k+1} + \frac{1}{2^k+2} + \cdots + \frac{1}{2^{k+1}}\Big)\\ &= H_{2^k} + \Big(\frac{1}{2^k+1} + \frac{1}{2^k+2} + \cdots + \frac{1}{2^{k+1}}\Big)\\ &\geq \Big(1 + \frac{k}{2}\Big) + \Big(\frac{1}{2^k+1} + \frac{1}{2^k+2} + \cdots + \frac{1}{2^{k+1}}\Big) \quad \text{(Use } P(k) \text{ here)}\\ &\geq \Big(1 + \frac{k}{2}\Big) + \Big(\frac{1}{2^{k+1}} + \frac{1}{2^{k+1}} + \cdots + \frac{1}{2^{k+1}}\Big)\\ &= \Big(1 + \frac{k}{2}\Big) + 2^k \cdot \frac{1}{2^{k+1}} = 1 + \frac{k+1}{2}\end{aligned}$$

Thus $P(k+1)$ is true and the result follows by mathematical induction.

THEOREM: NUMBER OF SUBSETS OF A FINITE SET

A set with n elements has 2^n subsets.

PROOF: Let $Q(n)$ be the above proposition.

Basis step: When $n = 0$, the set concerned is $\emptyset$ which has only one subset. Thus $Q(0)$ is true.

Inductive step: Assume that $Q(0), \ldots, Q(k)$ are true.

Let X be any set with $k+1$ elements. Take a particular element $a \in X$. Then $Y = X - \{a\}$ is a set with k elements. By the induction hypothesis,

$$|P(Y)| = 2^k.$$

Subsets of X can be divided into two types:

(i) Those that do not contain a. These are precisely the subsets of Y and there are 2^k subsets of this type.

(ii) Those that contain a. If the element a is deleted, they become subsets of Y. Thus each corresponds to a subset of Y. Therefore there are also 2^k subsets of this type.

Thus

$$|P(X)| = 2^k + 2^k = 2^{k+1}.$$

Hence $Q(k+1)$ is true.

The result then follows by the principle of mathematical induction.

SUM OF GP

For all integers $n \in \mathbb{Z}^*$, and all real numbers $r \neq 1$:

$$\sum_{i=0}^{n} r^i = \frac{r^{n+1} - 1}{r - 1}.$$

PROOF: When $n = 0$, l.h.s $= 1$ and r.h.s $= \frac{r-1}{r-1} = 1$. Thus the formula is true when $n = 0$.

Assume that the formula is true for $n = 0, 1, \ldots, k$. Thus $\sum_{i=0}^{k} r^i = \frac{r^{k+1}-1}{r-1}$. Then

$$\sum_{i=0}^{k+1} r^i = \sum_{i=0}^{k} r^i + r^{k+1} = \frac{r^{k+1} - 1}{r - 1} + r^{k+1} = \frac{r^{k+2} - 1}{r - 1}.$$

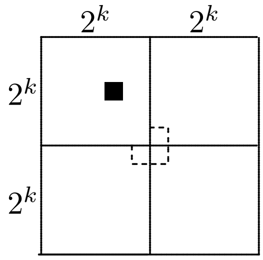
Thus the formula is also true at $k + 1$.

By the principle of mathematical, the formula is true.

• Prove that for any integer $n \geq 1$, if one square is removed from a $2^n \times 2^n$ checkerboard, the remaining squares can be covered by an L-tromino. (An L-tromino is an L-shape formed by 3 squares of the checkerboard.)

SOLN: Let $P(n)$ be the given statement.

Basis step. $P(1)$ is true since the board is itself an L-tromino.



Assume that $P(1), \ldots, P(k)$ are true. Consider a $2^{k+1} \times 2^{k+1}$ checkerboard with one square removed. Divide the checkerboard in 4 equal quadrants so that each quadrant is a $2^k \times 2^k$ board. Without loss of generality, assume that the removed square is from the first quadrant. Now remove a tromino from the centre of the board. (This tromino has one square in each of the last three quadrants.) Now we are left with four $2^k \times 2^k$ checkerboards, each with a square removed. Thus by the induction hypothesis, each can be covered by trominoes. Hence the $2^{k+1} \times 2^{k+1}$ checkerboard with one square removed can be so covered as well. The proof is now complete by mathematical induction.

• **FIBONACCI NUMBERS** $F_0, F_1, \ldots$ are defined by

$$F_0 = 0, F_1 = 1$$
$$F_{n+1} = F_n + F_{n-1} \quad \text{for } n \geq 1$$

$F_0 = 0,\ F_1 = 1,\ F_2 = 1,\ F_3 = 2,\ F_4 = 3,\ F_5 = 5, \ldots$

• Prove that for $n \geq 3$, $F_n > \alpha^{n-2}$, where $\alpha = (1 + \sqrt{5})/2$.

SOLN: Let $P(n)$ be $F_n > \alpha^{n-2}$, $n \geq 3$.

Basis step: Since $F_3 = 2 > \alpha$, and $F_4 = 3 \geq \alpha^2$, $P(3)$ and $P(4)$ are true.

We need both as $P(3)$ on its own will not yield $P(4)$.

Inductive step:

Suppose $P(n)$ is true, i.e., $F_n > \alpha^{n-2}$ for $n = 3, \ldots, k$. First note that

$$\alpha^2 = \frac{(1+\sqrt{5})^2}{4} = \frac{3+\sqrt{5}}{2} = 1 + \alpha.$$

Now $P(k+1)$ is true since

$$F_{k+1} = F_k + F_{k-1} > \alpha^{k-2} + \alpha^{k-3} = \alpha^{k-3}(\alpha + 1) = \alpha^{k-1}$$

LAME'S THEOREM

Let a and b be positive integers with $a \geq b$. Then the number of divisions used by the Euclidean algorithm to find $\gcd(a, b)$ is at most $5 \times$ the number of decimal digits in b.

(For example, to find $\gcd(1034578929341, 2018)$, the number of divisions is $\leq 5 \cdot 4 = 20$.)

PROOF: Let m be the number of digits of b. The algorithm runs as follows: Let $r_1 = a$, $r_2 = b$. Then

$$\begin{aligned} r_1 \,\mathbf{Mod}\, r_2 &= r_3 \\ r_2 \,\mathbf{Mod}\, r_3 &= r_4 \\ &\cdots \\ r_{n-1} \,\mathbf{Mod}\, r_n &= r_{n+1} \\ r_n \,\mathbf{Mod}\, r_{n+1} &= 0 \end{aligned}$$

It stops after n steps with $\gcd(a, b) = r_{n+1}$. We need to prove that $n \leq 5m$. We shall prove that $r_i \geq F_{n+3-i}$ for all $i = 2, \ldots, n + 1$.

We have

$$\begin{aligned} r_{n+1} &\geq 1 = F_2 && (\because \ \gcd = r_{n+1}) \\ r_n &\geq 2 = F_3 && (\because \ r_n \neq \gcd) \\ r_{n-1} &\geq r_n + r_{n+1} && (\because \ r_{n-1} = r_n q + r_{n+1} \ \& \ q \geq 1) \\ &\geq F_3 + F_2 = F_4 \\ &\cdots \\ r_3 &\geq r_4 + r_5 \\ &\geq F_{n-1} + F_{n-2} = F_n \\ b = r_2 &\geq r_3 + r_4 \\ &\geq F_n + F_{n-1} \\ &= F_{n+1} > \alpha^{n-1} \end{aligned}$$

Note that $\log_{10} \alpha > 1/5$ (use your calculator to check). Thus

$$m \geq \log_{10}(b + 1) \geq (n - 1) \log_{10} \alpha > (n - 1)/5.$$

Therefore $n - 1 < 5m$. Since n is an integer, $n \leq 5m$.