So, by the principle of induction the statement $P(n)$ is true any natural number $n \geq 4$

So, $n! > 2^n$ for natural numbers $n \geq 4$

2.2.3 Second principle of mathematical induction.

Let $S$ be a subset of $\mathbb{N}$ such that

(i) $1 \in S$ and

(ii) if $\{1, 2, \ldots, k\} \subset S$, then $k+1 \in S$.

Then $S = \mathbb{N}$

Proof: ~~Let S be a subset of N~~ Let $T = \mathbb{N} - S$.

We prove that $T = \phi$. If not, $T$ being a non-empty subset of $\mathbb{N}$ must have a least element, say $m$, by the well ordering property of $\mathbb{N}$.

Since, $1 \in S$, $m \neq 1$. So, $m > 1$. By the choice of $m$, all natural numbers less than $m$ belongs to $S$.

Hence $1, 2, \ldots m-1 \in S$. So, by (ii) $m \in S$, a contradiction.

This proves that $T = \phi$ and therefore $S = \mathbb{N}$.

Worked example (continued)

4. Prove that $(3+\sqrt{7})^n + (3-\sqrt{7})^n$ is an even integer for all $n \in \mathbb{N}$.

Proof: Let $P(n)$ be the statement $(3+\sqrt{7})^n + (3-\sqrt{7})^n$ is an even integer.

The statment $P(1)$ is true, since $(3+\sqrt{7})^1 + (3-\sqrt{7})^1 = 6$ and it is an even integer.

Let us assume that $P(n)$ be true for $n = 1, 2, \ldots, k$

Now, $(3+\sqrt{7})^{k+1} + (3-\sqrt{7})^{k+1} = a^{k+1} + b^{k+1}$, where $a = 3+\sqrt{7}$, $b = 3-\sqrt{7}$

$= (a^k + b^k)(a+b) - (a^{k-1} + b^{k-1})ab$

$= 6(a^k + b^k) - 2(a^{k-1} + b^{k-1})$ (as $a+b = 6$ and $ab = 2$)

So, $a^{k+1} + b^{k+1}$ is an even integer as $a^k + b^k$ and $a^{k-1} + b^{k-1}$ is even (note that $a^{k+1} + b^{k+1}$ is even irrespective of $a^k + b^k$ and $a^{k-1} + b^{k-1}$ be even or odd)

This shows that $P(k+1)$ is true when $P(1), P(2), \ldots, P(k)$ are true. So, by the second principle of Mathematical induction, the statement $P(n)$ is true for all natural numbers $n$. So, $(3+\sqrt{7})^n + (3-\sqrt{7})^n$ is an even integer for all $n \in \mathbb{N}$.

## 2.3 Division algorithm

Given integers $a$ and $b$ with $b > 0$, there exists unique integers $q$ and $r$ such that

$$a = bq + r, \text{ where } 0 \leq r < b.$$

Proof: Let us consider the subset of integers

$$S = \{a - bx \in \mathbb{Z} : x \in \mathbb{Z}, a - bx \geq 0\}$$

First we show that $S$ is non-empty.

Since $b \geq 1$, $|a|b \geq |a|$. So, $a + |a|b \geq a + |a| \geq 0$

This shows that $a + |a|b = a - b(-|a|) \in S$ and so $S$ is non-empty.

Since $S$ is non-empty set of non-negative integers, either

(i) $S$ contains $0$ as its least element or,

(ii) $S$ contains a positive integer as its least element by the well ordering property of the set $\mathbb{N}$.

In either case, we call it $r$. So, there exists $q \in \mathbb{Z}$ such that $a - bq = r$ and $r \geq 0$.

We assert that $r < b$. Because, if $r \geq b$, then

$$a-(q+1)b = (a-qb)-b = r-b \geq 0.$$

This shows that $a-(q+1)b \in S$ and also $a-(q+1)b = r-b < r$.

This leads to a contradiction to the fact that $r$ is the least element in $S$.

Hence $r < b$ and consequently $a = bq + r$ where $0 \leq r < b$.

In order to establish uniqueness of $q$ and $r$, let us suppose that $a$ has two representations: $a = bq_1 + r_1$ and $a = bq_2 + r_2$ where $q_1, q_2 \in \mathbb{Z}$ and $0 \leq r_1 < b$ and $0 \leq r_2 < b$

Then $b(q_1 - q_2) + r_1 - r_2 = 0$ or, $b(q_1 - q_2) = r_2 - r_1$

or, $b|q_1 - q_2| = |r_1 - r_2|$. But $0 \leq r_2 < b$ and $-b < -r_1 \leq 0$

give $-b < r_2 - r_1 < b$, i.e., $|r_2 - r_1| < b$ or, $|r_1 - r_2| < b$

Consequently, $|q_1 - q_2| < 1$

Since $q_1$ and $q_2$ are integers, the only possibility is $q_1 = q_2$.

and so $r_1 = r_2$. This completes the proof.

Definition 2.3.1 $q$ is called the quotient and $r$ is called the remainder in the division of $a$ by $b$.

A more general version of the Division algorithm is obtained by taking $b$ as non-zero integer.

Theorem 2.3.2 Given integers $a$ and $b$, with $b \neq 0$, there exists unique integers $q$ and $r$ such that $a = bq + r$, $0 \leq r < |b|$.

Proof: With the previous theorem already established it is enough to consider the case in which $b$ is negative. Then $|b| > 0$. By the previous theorem, there exist unique integers $q_1$ and $r$ such that

$$a = |b| q_1 + r, \quad 0 \leq r < |b|$$

$$= -b q_1 + r \quad \text{as } |b| = -b \text{ as } b < 0$$

So, $a = bq + r$, $0 \leq r < |b|$ where $q = -q_1$

To illustrate the division algorithm, let us take

$b = 3$, $a = -20, 2, 10$

$-20 = 3.(-7) + 1$ gives $q = -7$, $r = 1$

$2 = 3.0 + 2$ gives $q = 0$, $r = 2$

$10 = 3.3 + 1$ gives $q = 3$, $r = 1$

Let us take $b = -3$, $a = -20, 2, 10$

$-20 = -3.7 + 1$ gives $q = 7$, $r = 1$

$2 = 3.0 + 2$ gives $q = 0$, $r = 2$

$10 = -3.(-3) + 1$ gives $q = -3$, $r = 1$

When the remainder in the division algorithm turns out to be 0, the case is of special interest to us.