Mathematical Induction (Strong Form)

To prove that a formula is true for every integer greater than or equal to M, you have to do the following

1. Prove the formula is true for M.
2. Assume the formula is true for all integers between M and k for some integer k greater than M.
3. Depend on the assumption in the previous part (and may be you need also to depend on other known facts) to prove the formula is true for $k+1$.

If you do all the above, then the principle of mathematical induction (strong form) states your formula is true for every integer greater than or equal to M.

Priciple of Well-ordering

Every nonempty subset of positive integers has a smallest element.

Corollary: Every nonempty subset of nonnegative integers has a smallest element.

Number Theory Definitions and Facts

Definition: Let a and b be integers ($a \neq 0$). We say a divides b (denoted $a|b$) if there exists an integer q such that $b = aq$.

Remark: The following are the same

1. a divides b.
2. a is a factor of b.
3. b is a multiple of a.
4. b is divisble by a.

Facts: Let a and b be integers ($a \neq 0$). Then

1. If a divdes b and b divides a ($b \neq 0$), then $b = \pm a$.
2. If a divdes b, then a divides nb, for every integer n.
3. If a divides b and b divides c ($b \neq 0$), then a divides c.
4. If a divides b and a divides c, then a divides $ma + nb$ for every integers m and n.

Definition: Let p be a positive integer greater than 1. Then p is said to be *prime* if its only positive factors are 1 and itself. If p is not prime, then it is called *composite*.

Division Algorithm

• Let a and b be integers and let $a > 0$. Then there exist unique integers q and r, with $0 \leq r < a$ such that $b = aq + r$.

• Let a and b be integers and let $a \neq 0$. Then there exist unique integers q and r, with $0 \leq r < |a|$ such that $b = aq + r$.

In the above two theorems, q is called the *quotient* and r is called the *remainder* and they are given by

$$q = \begin{cases} \lfloor \frac{b}{a} \rfloor & \text{if } a > 0 \\ \lceil \frac{b}{a} \rceil & \text{if } a < 0 \end{cases}$$

$r = b - aq$.