$a + b \in \mathbb{N}$
$a \times b \in \mathbb{N}$
$a + b = b + a$
$(a + b) + c = a + (b + c)$
$n \times 1 = n forall n \in \mathbb{N}$
$if m \times z = n \times z for some z \in \mathbb{N} then m = n$
$a \times (b + c) = (a \times b) + (a \times c)$
m is a multiple of n if there is a natural number r such that $m = rn$
If a and b are multiplies of n the, for all $x, y \in \mathbb{N}, xa + yb$ is a a multiple of n
For any natural numbers m and n, the statement $m < n$ means that there is some $x \in \mathbb{N}$ such that $m + x = n$
If $a < b$ and $b < c$ then $a < c$
Given any natural numbers m and n, exactly one of the three statements $m < n, m = n, n < m$ is true.
Suppose that P(n) is a statement with the following properties:
(i) $P(1)$ is true; *induction basis*
(ii) if $P(k)$ is true (*induction hypothesis*) then $P(k + 1)$ (*induction step*) is true for every $k \in \mathbb{N}$.
Then $P(n)$ is true for all $n \in \mathbb{N}$
strong: (ii) assume $P(i) 1 \leq i \leq k$ is true then $P(k + 1)$ is true for every $k \in \mathbb{N}$
Let X be a subset of $\mathbb{N}$. An element $l \in X$ is a **least member** of X if $l \leq x$ for all $x \in X$. An element $g \in X$ is a **greatest member** of X if $g \geq x$ for all $x \in X$. Often l and g are referred to as the **minimum** and **maximum** of X.
Every non-empty subset of X of $\mathbb{N}$ has a least member.
Suppose that X and Y are sets. We say that we have a **function** f **from** X **to** Y if for each x in X we can specify a unque element in Y, which we denote by $f(x)$.
The function f from X to Y is a **surjection** if every y in Y is a value $f(x)$ for at least one x in X. It is an **injection** if every y in Y is a value $f(x)$ for at most one x in X. It is a **bijection** if it is both a surjection and an injection, that is, if every y in Y is a value $f(x)$ for exactly one x in X.
For any set X the function $i : X \to X$ defined by $i(x) = x$ for all $x \in X$ is called the **identity** function on X. If X is a subset of Y, the function $j : X \to Y$ defined by $j(x) = x$ is called the **inclusion** function from X to Y.
If $f : X \to Y$ and $g : Y \to Z$ are injections, then so is the composite $gf : X \to Z$. If f and g are surjections then so is gf. if f and g are bijections then so is gf.
A function $f : X \to Y$ has an **inverse** function $g : Y \to X$ if, for all x in X and y in Y $(gf)(x) = x, (fg)(y) = y$. In other words gf is the identity function on X and fg is the identity function on Y.
A function has an inverse if and only if it is a bijection.
Let m be a natural number. Then the following statement is true for every natural number n: if there is an injection from $\mathbb{N}_n to \mathbb{N}_m$, then $n \leq m$.
If there is a bijective correspondence between S and $\mathbb{N}_m$ then we say that S has size, or cardinality, m and we write $|S| = m$.
If a set S is such that $|S| = s$ and $|S| = t$, then $s = t$.
A set S is **finite** if it is empty of if $|S| = n$ for some $n \in \mathbb{N}$. A set which is not finite is said to be **inifite**.
The set $\mathbb{N}$ is infinite.
If the set S is such that there is a bijection $b : \mathbb{N} \to S$, then S is infinite.
A **relation** R on a set X is a set of ordered pairs of members of X.
reflexive xRx, symmetric xRy, transitive xRy and yRz hence xRz
An **equivalence relation** is a relation that is reflexive, symmetric and transitive.
Let R be an equivalence relation on X. A non-empty set $C \subseteq X$ is an **equivalence class** with respect to R if
(i) any two members of C are R-related; and
(ii) C contains every member of X that is R-related to any member of C.
in symbols, C is such that,
if $x \in C$ then $y \in C \iff xRy$
Given an equivalence relation R on X, every member of X is one and only one equivalence class (with respect to R).
$x + 0 = x$ for every $x \in \mathbb{Z}//$ If $x \times z = y \times z$ and $z \neq 0$ then $x = y$
For any $x \in \mathbb{Z}$ there is an element $-x$ of $\mathbb{Z}$ such that $x + (-x) = 0$.
If $x \leq y$ and $0 leq z$, then $x \times z \leq y \times z$.
The integer b is a **lower bound** for a set $X \subseteq \mathbb{Z}$ if $b \leq x$ for all $x \in X$.
If a non-empty set $S \subseteq \mathbb{Z}$ has a lower bound, then S has a least member.
Given positive integers a and b there exist q and r in $\mathbb{N}_0$ such that $a = bq + r$ and $0 \leq r \leq b$.
If a and b are positive integers (or zero) we say that d is the **greatest common divisor (gcd)** of a and b provided that
(i) $d|a$ and $d|b$; (ii) if $c|a$ and $c|b$, then $c \leq d$.
Let a and b be positive integers, and let $d = gcd(a, b)$. Then there are integers m and n such that $d = ma + nb$.
If $gcd(a, b) = 1$ then we say that a and b are **coprime**. In this case the Theorem asserts that there are integers m and n such that $ma + nb = 1$.
A positive integer p is a **prime** if $p \geq 2$ and the only positive integers which divide p are 1 and p itself.
If p is a prime and $x_1, x_2, \ldots, x_n$ are any integers such that $p|x_1 x_2 \ldots x_n$ then $p|x_i$ for some $x_i (1 \leq i \leq n)$.
(The Fundamental Theorem of Arithmetic) A positive integer $n \geq 2$ has a unique prime factorization, apart from the order of the factors.