Integers:

$\mathbb{Z}$ or $I = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$

Properties of Integers:

Well Ordering Principle:

Every nonempty set of positive integers contains a smallest number.

Division Algorithm:

Let a and b be any integers with $b > 0$. Then there exist unique integers q and r with the property that

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

Revise GCD, relatively prime integers:

GCD is a linear Combination:

For any nonzero integers a and b, there exist integers s and t such that $\gcd(a, b) = as + bt$. Moreover, $\gcd(a, b)$ is the smallest positive integer of the form $as + bt$.

Euclid's Lemma:

$p \mid ab \Rightarrow p \mid a$ or $p \mid b$

If p is a prime that divides ab, then p divides a or p divides b.

Fundamental Theorem of Arithmetic:

Every integer greater than 1 is a prime or a product of primes. This product is unique, except for order in which the factors appear.

for any number $n > 1$,

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$

where p_i's are primes and e_i's are natural numbers.

Revise LCM

Revise modular Arithmetic

$a \equiv b \pmod n \Rightarrow n \mid (a-b)$

Revise Mathematical Induction

~~Revise Set.~~

Set :

The set is a collection of well defined objects.

Relation :

$R \subseteq A \times B$

Relation is a subset of cartesian product of two sets.

Equivalence relation :

An equivalence relation on a set A is a set R of ordered pairs of elements of A such that

① $(a,a) \in R \quad \forall a \in A$

② $(a,b) \in R \Rightarrow (b,a) \in R \quad \forall a,b \in A$

③ $(a,b) \in R$ and $(b,c) \in R \Rightarrow (a,c) \in R$

$\forall a,b,c \in A.$

Revise equivalance class.

Function (mapping):

A function (or mapping) f from a set A to a set B is a rule that assigns ~~to~~ each element a of A to exactly one element b of B.

$$f : A \to B$$

Domain   Codomain.

$$Im(f) = \{f(x) \mid x \in A\}.$$

Revise one-one, onto functions

Revise composition of functions.