

---

---

# CHAPTER 1

---

## PRELIMINARIES

### 1 Sets, functions and all that

#### Definition 1.1: Preliminary definitions

1. (Cartesian Product): if  $A$  and  $B$  are non empty sets, the *Cartesian Product*  $A \times B$  is defined as the set of ordered pairs  $a, b$  wherein  $a \in A, b \in B$ . i.e,  $A \times B := \{(a, b) : a \in A, b \in B\}$
2. (Function): A function from  $A$  to  $B$  is a set  $f \subseteq A \times B$  such that,  $a, b \in f$  and  $a, c \in f \implies b = c$ .  $A$  is called the **Domain of  $f$** .  $Range(f) := f(A)$  (see next definition)
3. (Direct Image): Direct image  $f(A) := \{y \in B : \exists x \in A \text{ such that } f(x) = y\}$
4. (Inverse Image):  $f^{-1}(S \subseteq B) := \{x \in A : f(x) \in S\}$
5. (Relation): Any subset  $R \subseteq A \times B$  is a relation from  $A$  to  $B$ .  
We say  $x \in X$  is "related to"  $y \in Y$  under the relation  $R$ , or simply  $xRy$  or  $R(x) = y$  if  $(x, y) \in R \subseteq X \times Y$ .
6. (Injection):  $f : A \rightarrow B$  is injective if  $\forall x_1, x_2 \in A, (x_1, b) \in f \text{ and } (x_2, b) \in f \iff x_1 = x_2$
7. (Surjection):  $f : A \rightarrow B$  is surjective if  $\forall b \in B, \exists a \in A \text{ such that } f(a) = b$
8. (Bijection):  $f : A \rightarrow B$  is bijective if its both surjective and injective.
9. (Identity function on a set):  $I_A : A \rightarrow A$  defined by  $\forall x \in A, I_A(x) = x$
10. (Permutation): Simply a bijection from  $A$  to itself is called a permutation.

**Definition 1.2: (Left Inverse)**

We say  $f : A \rightarrow B$  has a left inverse if there is a function  $g : B \rightarrow A$  such that  $g \circ f = I_A$

**Theorem 1.3**

$f : A \rightarrow B$  has a left inverse if and only if it is injective.

*Proof for Theorem.*

$\Rightarrow$ ) If  $f$  has a left inverse  $g$ , Consider  $x, y \in A$  such that  $f(x) = f(y) = p$ .  
We have  $g \circ f(x) = g(p) = x = g \circ f(y) = y$ . Hence,  $x = y$ , Injective.  
 $\Leftarrow$ ) Given that  $f : A \rightarrow B$  is injective, define  $g : B \rightarrow A$  as:

$$g(z \in B) = \begin{cases} a, & \text{where } f(a) = z, \text{ if } z \in f(A) \\ \text{whatever,} & \text{if } z \notin f(A) \end{cases}$$

consider  $g \circ f(x \in A) = g \circ (f(x))$ .

Obviously,  $f(x) \in f(A)$ , therefore,  $g(f(x)) =$  that  $a$  such that  $f(a) = f(x)$ .

That  $a$  is  $x$ . Hence,  $g(f(x)) = x$  ■

**Definition 1.4: (Right Inverse)**

$f : A \rightarrow B$  is said to have a right inverse if there is a function  $g : B \rightarrow A$  such that  $f \circ g = I_B$

**Theorem 1.5**

$f : A \rightarrow B$  has a right inverse if and only if  $f$  is Surjective.

*Proof for Theorem.*

$\Rightarrow$ ) If  $f$  has a right inverse  $g$ , such that  $f \circ g = I_B : B \rightarrow B$ , then it is evident that the range of  $f$  is  $B$ , for if not, range of  $f \circ g$  wouldn't be  $B$  either.

$\Leftarrow$ ) If  $f$  is surjective, then for all  $b \in B$ , there exists atleast one  $a \in A$  such that  $f(a) = b$  define  $g$  as:

$$g(x \in B) = \text{one of those } a \in A \text{ such that } f(a) = b$$

Consider  $f \circ g(x \in B) = f(\text{one of the } a \text{ such that } f(a) = b) = b, \forall b \in B$

Hence,  $f \circ g = I_B$  ■

**Theorem 1.6**

If  $f$  has left inverse  $g_1$  and right inverse  $g_2$ , then  $g_1 = g_2$ . *(True for anything that is Associative, and function composition is associative.)*

*Proof for Theorem.*

$$\begin{aligned}
 g_1 \circ f &= I_A \text{ and } f \circ g_2 = I_B \\
 g_1 \circ (f \circ g_2) &= g_1 \circ I_B = g \\
 &= (g_1 \circ f) \circ g_2 = I_A \circ g_2 = g_2 \\
 \text{Hence } g_1 &= g_2
 \end{aligned}$$

### Corollary 1.7

$f$  is invertible (i.e, both left and right inverse exist) if and only if it is bijective.

*Proof for Corollary.*

Obvious

## 1.1 Operations on Relations

If  $R$  and  $S$  are binary relations over  $X \times Y$ :

1.  $R \cup S := \{(x, y) | xRy \text{ or } xSy\}$
2.  $R \cap S := \{(x, y) | xRy \text{ and } xSy\}$
3. Given  $S : Y \rightarrow Z$  and  $R : X \rightarrow Y$ ,  $S \circ R := \{(x, z) | \exists y \text{ such that } ySz \text{ \& } xRy\}$
4. If  $R$  is binary over  $X \times Y$ ,  $\bar{R} := \{(x, y) | \neg(xRy)\}$

## 1.2 Homogeneous Relations

If  $R$  is a binary relation over  $X \times X$ , it is Homogeneous.

### Definition 1.8: Definitions Regarding Relations

1. (Reflexive):  $\forall x \in X, xRx$
2. (Symmetric):  $\forall x, y \in X, xRy \implies yRx$
3. (Transitive):  $\forall x, y, z \in X, \text{ if } xRy \ \& \ yRz \implies xRz$
4. (Dense):  $\forall x, y \in X, \text{ if } xRy, \text{ then there is some } z \in X \text{ such that } xRz \ \& \ zRy$
5. (**Equivalence Relation**):  $R$  is an equivalence relation if it is Reflexive, Symmetric and Transitive.
6. (Equivalence class of  $a \in A$  (where there is an equivalence relation defined)): Set of all  $b \in A$  such that  $bRa$ .
7. (Partition of  $A$ ): Any collection of sets  $\{A_i : i \in I\}$  (where  $I$  is some indexing set) such that:

$$A = \bigcup_{i \in I} A_i$$

$$A_i \cap A_j = \phi \text{ if } \forall i, j \in I, i \neq j$$

### Theorem 1.9

Let  $A$  be a non-empty set. If  $R$  defines an equivalence Relation on  $A$ , then the set of all equivalence classes of  $R$  form a partition of  $A$

#### *Proof for Theorem.*

Define our collection  $\{A_\alpha\}$  as the set of all equivalence classes of  $A$ . Clearly,  $\bigcup_{\alpha \in I} A_\alpha = A$ . If  $A$  only has one element, obviously, that singleton set makes up the partition. Let  $A_\alpha$  and  $A_{\alpha'}$  be equivalence classes of two elements  $a$  and  $a'$  in  $A$ . If  $aRa'$ , then  $A_\alpha = A_{\alpha'}$  since every element in the equivalence class of  $a$  will, from the transitive property, be in the equivalence class of  $a'$ . Suppose  $\neg(aRa')$ . If, then,  $\exists x \in A_\alpha$  such that  $x \in A_{\alpha'}$ , this means that  $xR\alpha$  and  $xR\alpha'$ , but from transitive property, this means  $\alpha R\alpha'$ , which is a contradiction. Therefore, the pairwise intersection is disjoint. ■

### Theorem 1.10

If  $\{A_i : i \in I\}$  is a partition of  $A$ , then there exists an equivalence relation  $R$  on  $A$  whose equivalence classes are  $\{A_i : i \in I\}$ .

#### *Proof for Theorem.*

Define  $R(x, y)$  if and only if  $\exists$  unique  $m \in I$  such that  $x \in A_m$  and  $y \in A_m$ .  
 $R(x, x)$  is obvious if non empty, hence  $R$  is reflexive.

Suppose  $R(x, y)$  and  $R(y, z)$ . Then, there exists a unique  $m \in I$  such that  $x, y$  are in  $A_m$ . Similarly, there exists a unique  $n \in I$  such that  $y, z$  are in  $A_n$ . Obviously, if  $n \neq m$ , intersection of  $A_n$  and  $A_m$  would be non empty, hence,  $n = m$ . Hence,  $R$  is transitive.

Consider  $R(x, y)$ , which means  $\exists$  unique  $n \in I$  such that  $x, y \in A_n \implies R(y, x)$ . Hence,  $R$  is an equivalence relation. ■

## 2 Induction, Naturals, Rationals and the Axiom of Choice

### Axiom 2.1: Peano Axioms, characterisation of $\mathbb{N}$

1.  $1 \in \mathbb{N}$
2. every  $n \in \mathbb{N}$  has a predecessor  $n - 1 \in \mathbb{N}$  except 1
3. if  $n \in \mathbb{N} \implies n + 1 \in \mathbb{N}$

### Definition 2.2: (Sequence of something)

A sequence of some object is simply a collection of objects  $\{O_l : l \in \mathbb{N}\}$  which can be counted.

### Axiom 2.3: Well Ordering Property of $\mathbb{N}$

Every non empty subset of  $\mathbb{N}$  has a least element.

### Axiom 2.4: Weak Induction

For all subsets  $S \subseteq \mathbb{N}$ ,  $((1 \in S) \& ((\forall k \in \mathbb{N})(k \in S \implies k + 1 \in S))) \iff S = \mathbb{N}$

**Weak Induction's Negation:**(One direction)

There exists subset  $S_0 \subseteq \mathbb{N}$ ,  $((1 \in S_0) \& ((\forall k \in \mathbb{N})(k \in S_0 \implies k + 1 \in S_0)))$  but  $S_0 \neq \mathbb{N}$

### Axiom 2.5: Strong Induction

For all subsets  $S \subseteq \mathbb{N}$ ,  $((1 \in S) \& ((\forall k \in \mathbb{N})(1, 2, \dots, k \in S' \implies k + 1 \in S'))) \iff S = \mathbb{N}$

**Strong Induction's Negation:**(One direction)

There exists subset  $S' \subseteq \mathbb{N}$ ,  $((1 \in S') \& ((\forall k \in \mathbb{N})(1, 2, \dots, k \in S' \implies k + 1 \in S'))) but  $S' \neq \mathbb{N}$$

**Theorem 2.6**

Weak Induction  $\iff$  Strong Induction.

**Proof for Theorem.**

$\implies$ ) Suppose Weak induction is true, but not strong induction. Take our set to be that  $S'$  in the negation of the Strong Induction Statement.  $S' \neq \mathbb{N}$  implies that, either  $1 \notin S'$  or  $\exists k \in \mathbb{N}$  such that  $k \in S'$  but  $k + 1 \notin S'$ . We know that  $1 \in S'$ , so it must be that  $\exists k \in \mathbb{N}$  such that  $k \in S'$  but  $k + 1 \notin S'$ .  $\{1\} \in S' \implies \{1, 2\} \in S'$ . Assume that for  $n$ ,  $\{1, 2, \dots, n\} \in S'$ . This means that  $\{1, 2, \dots, n + 1\} \in S'$ . This means that for every  $n \in \mathbb{N}$ ,  $\{1, 2, \dots, n\} \in S' \implies n \in S'$ . Contradiction.

$\impliedby$ ) Suppose Strong Induction is true, but not weak induction. Take the set  $S_0$  from the negation of Weak Induction.  $S_0 \neq \mathbb{N}$ . This means, from strong induction, either  $1 \notin S_0$  or  $\exists k \in \mathbb{N}$  such that  $1, 2, \dots, k \in S_0$  but  $k + 1 \notin S_0$ .  $1 \in S_0$ , hence,  $2 \in S_0$  and  $\{1, 2\} \in S_0$ . assume that  $\{1, 2, \dots, n\} \in S_0$ . This means,  $n \in S_0 \implies n + 1 \in S_0$ , which means that  $\forall k \in \mathbb{N}, \{1, 2, \dots, k\} \in S_0 \implies k + 1 \in S_0$ . Therefore,  $S_0$  is  $\mathbb{N}$ . ■

**Theorem 2.7**

Weak Induction  $\iff$  Strong Induction  $\iff$  Well ordering.

**Proof for Theorem.**

$\implies$ ) Suppose that, on the contrary,  $S_0$  is a non empty subset of  $\mathbb{N}$ , with no least element. Does 1 exist in  $S_0$ ? No, for that will be the least element. Likewise, then, 2 does not belong in  $S_0$ . Assume that  $\{1, 2, \dots, n\} \notin S_0$ . Does  $n + 1$  exist in  $S_0$ ? No, for that will become the least element then. From Strong Induction,  $\mathbb{N} - S_0 = \mathbb{N} \implies S_0 = \emptyset$ . Contradiction.

$\impliedby$ ) Suppose  $\exists S_0 \subseteq \mathbb{N}$  such that  $1 \in S_0$  and  $\forall k \in \mathbb{N}, k \in S_0 \implies k + 1 \in S_0$ . Suppose on the contrary,  $S_0$  is not  $\mathbb{N}$ .  $\mathbb{N} - S_0$  is then, non-empty. From Well Ordering, there is a least element  $q \in \mathbb{N} - S_0$ .  $\implies, q - 1 \in S_0$ . But this would imply  $q - 1 + 1 \in S_0$ . Contradiction.  $\mathbb{N} - S_0$  is empty. ■

**Definition 2.8: (Finite Sets)**

A set  $X$  is said to be finite, with  $n$  elements in it, if  $\exists n \in \mathbb{N}$  such that there exists a bijection  $f : \{1, 2, \dots, n\} \rightarrow X$ . Set  $X$  is *infinite* if it is non-finite.

**Theorem 2.9**

If  $A$  and  $B$  are finite sets with  $m$  and  $n$  elements respectively, and  $A \cap B = \emptyset$ , then  $A \cup B$  is finite, with  $m + n$  elements.

**Proof for Theorem.**

$f : \mathbb{N}_m \rightarrow A$  and  $g : \mathbb{N}_n \rightarrow B$ .

Define  $h : \mathbb{N}_{m+n} \rightarrow A \cup B$  given by:

$$h(i) = \begin{cases} f(i) & \text{if } i = 1, 2, \dots, m \\ g(i - m) & \text{if } i = m + 1, m + 2, \dots, m + n \end{cases}$$

If  $i = 1, 2, \dots, m$ ,  $h(i)$  covers all the elements in  $A$  through  $f$ . If  $i = m + 1, \dots, m + n$ ,  $h(i)$  covers all the elements in  $B$  through  $g$ .

Moreover,  $h(i) \neq h(j)$ ;  $i \in [1, m]$ ,  $j \in [m + 1, m + n]$  since  $A \cap B = \emptyset$  ■

### Theorem 2.10

If  $C$  is infinite, and  $B$  is finite, then  $C - B$  is infinite.

#### *Proof for Theorem.*

Suppose  $C - B$  is finite. We have  $B \cap (C - B) = \emptyset$  and  $B \cup (C - B) = C \cup B$

$n(C \cup B) = n(B \cup (C - B)) = n(B) + n(C - B)$  This implies  $C \cup B$  is finite. Contradiction. ■

### Theorem 2.11

**Theorem:** Suppose  $T$  and  $S$  are sets such that  $T \subseteq S$ . Then:

- a) If  $S$  is finite,  $T$  is finite.
- b) If  $T$  is infinite,  $S$  is infinite.

#### *Proof for Theorem.*

Given that  $S$  is finite, there is a function  $f : \mathbb{N}_m \rightarrow S$ . Suppose that  $S$  has 1 element. Then either  $T$  is empty, or  $S$  itself, which means  $T$  is finite. Suppose that, upto  $n$ , it is true that, if  $S$  is finite with  $n$  elements, all its subsets are finite. Consider  $S$  with  $n + 1$  elements.

$f : \mathbb{N}_{n+1} \rightarrow S$ .

If  $f(n + 1) \in T$ , consider  $T_1 := T - \{f(n + 1)\}$ . We have  $T_1 \subseteq S - \{f(n + 1)\}$ , and since  $S - \{f(n + 1)\}$  is a finite set with  $n$  elements, from induction hypothesis,  $T_1$  is finite.

Moreover, since  $T = T_1 \cup \{f(n + 1)\}$ ,  $T$  is also finite with one more element than  $T_1$ .

If  $f(n + 1) \notin T$ , then  $T \subseteq S - \{f(n + 1)\}$ , we are done.

(b) is simply the contrapositive of (a). ■

### Definition 2.12: (Countable Sets)

A set  $S$  is said to be *countable*, or *denumerable* if, either  $S$  is finite, or  $\exists f : \mathbb{N} \rightarrow S$  which is a bijection. If  $S$  is *not countable*,  $S$  is said to be *uncountable*

**Theorem 2.13**

The set  $\mathbb{N} \times \mathbb{N}$  is countable.

***Proof for Theorem.***

The number of points on diagonals  $1, 2, \dots, l$  are:  $\psi(k) = 1 + 2 + \dots + k = \frac{k(k+1)}{2}$

The point  $(m, n)$  occurs on the  $(m + n - 1)$  th diagonal, on which the number  $m + n$  is an invariant. The  $(m, n)$  point occurs  $m$  points down the diagonal. So, to characterise a point, it is enough to specify the diagonal it falls in, and its ordinate (the "rank" of that point on that diagonal). Count the elements till the  $m + n - 2$ nd diagonal, then add  $m$ , and this would be the position of the point  $(m, n)$ .

Define  $r : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$  given by  $r(m, n) = \psi(m + n - 2) + m$ . That this is a bijection is pretty clear because we are counting the position of the point  $(m, n)$ . For a given point  $(m, m)$ , there can only be one unique diagonal on which it exists, and on the diagonal, its rank is unique. Moreover, for every  $q \in \mathbb{N}$ , there corresponds an  $(m, n)$  such that  $r(m, n) = q$ , for, we simply count along each diagonal in the "zig-zag" manner until we reach that  $(m, n)$  for which the position is given by  $q$ . Therefore,  $r$  is a bijection. (There are other explicit bijections too) ■

**Theorem 2.14**

The following are equivalent:

1.  $S$  is countable
2.  $\exists$  a surjective function from  $\mathbb{N} \rightarrow S$
3.  $\exists$  an injective function from  $S \rightarrow \mathbb{N}$

***Proof for Theorem.***

(1  $\implies$  2) is obvious

(2  $\implies$  3)  $f : \mathbb{N} \rightarrow S$ , every element of  $S$  has atleast one preimage in  $\mathbb{N}$ . Define a function from  $S \rightarrow \mathbb{N}$  by taking for each  $s \in S$  the least such  $n \in \mathbb{N}$  such that  $f(n) = s$ . This defines an injection.

(3  $\implies$  1) If there is an injection from  $S \rightarrow \mathbb{N}$ , then there is a bijection from  $S \rightarrow$  a subset of  $\mathbb{N}$ , which implies  $S$  is countable. ■

**Corollary 2.15**

The set of Rational Numbers  $\mathbb{Q}$  is countable.

***Proof for Corollary.***

We know that a surjection from  $\mathbb{N} \times \mathbb{N}$  to  $\mathbb{Q}$  exists (where  $f(0, 0) = 0$ , and  $f(m, n) = \frac{m}{n}$ ). We know that  $\mathbb{N} \times \mathbb{N}$  is bijective to  $\mathbb{N}$ . This means  $\mathbb{N}$  is surjective to  $\mathbb{Q}$ . We are Done. ■



**Theorem 2.16**

Every infinite subset of a countable set is countable.

**Proof for Theorem.**

Consider  $N_s \subseteq \mathbb{N}$  which is infinite.

Define  $g(1) = \text{least number in } N_s$

Having defined  $g(n)$ , define  $g(n+1) = \text{least number in } N_s \text{ which is larger than } g(n)$ .

That it is an injection is obvious, for  $g(m) > g(n)$  if  $m > n$ .

Suppose it is not a surjection, i.e,  $g(\mathbb{N}) \neq N_s \implies g(\mathbb{N}) \subset N_s \implies N_s - g(\mathbb{N}) \neq \emptyset$ . Therefore,  $N_s - g(\mathbb{N})$  has a least element,  $k$ . This means that  $k-1$  is in  $g(\mathbb{N})$ . Therefore, there exists  $q$  in  $\mathbb{N}$  such that  $g(q) = k-1$ . But then,  $g(q+1) = \text{least number in } N_s \text{ such that it is bigger than } g(q)$ . This would, ofcourse be,  $k$ , which means  $k = g(q+1)$ , which puts  $k$  in  $g(\mathbb{N})$ . Contradiction. Hence,  $g(\mathbb{N}) = N_s$ , therefore,  $g$  is a bijection from  $\mathbb{N} \rightarrow N_s$ . Since every countable set is bijective to  $\mathbb{N}$ , and every infinite subset of a countable set is bijective to an infinite subset of  $\mathbb{N}$ , the theorem holds generally for countable sets. ■

**Theorem 2.17**

$\mathbb{N} \times \mathbb{N} \cdots \mathbb{N}$  is bijective to  $\mathbb{N}$

**Proof for Theorem.**

$\mathbb{N} \times \mathbb{N}$  is bijective to  $\mathbb{N}$  obviously. Assume that  $f : \mathbb{N} \rightarrow \mathbb{N} \cdots \mathbb{N} (n \text{ times})$  is bijective.

Consider  $g : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N} \cdots \mathbb{N} (n+1 \text{ times})$  given by  $g(m, n) = (f(m), n)$ . Clearly, this is bijective. ■

**2.1 Axiom of Choice****Axiom 2.18: Axiom of Choice (AC)**

For any collection of non empty sets  $C = \{A_l : l \in L\}$ , there exists a function  $f$  called the "counting function" which maps each set  $A_l$  to an element in  $A_l$ .

Formally:  $f : C \rightarrow \bigcup_l A_l$  such that  $\forall l \in L, f(A_l) \in A_l$

**Theorem 2.19**

Countable union of Countable sets is countable *(This theorem is an example of a theorem that requires Axiom of Choice)*

**Proof for Theorem.**

Suppose we are given a sequence of countable sets  $\{S_n : n \in \mathbb{N}\}$ . Since each  $S_j$  is countable, we have for each  $j$ , at least one bijective map  $f_j : \mathbb{N} \rightarrow S_j$ . Define  $k : \mathbb{N} \times \mathbb{N} \rightarrow \bigcup_j S_j$  given by:  $k(m, n) = f_m(n)$ . Suppose  $x \in \bigcup_j S_j$ , i.e.  $x \in S_j$  for some  $j$ . This means that,  $f(n) = x$  for some  $n$ . Therefore,  $k(j, n) = x$ . Hence,  $k$  is surjective. From theorem 2.14, we are done.

**(Remark:** Keep in mind, for each  $S_j$ , there are a myriad of functions  $(f_j)_k : \mathbb{N} \rightarrow S_j$ . For each  $S_j$ , which is countably infinite, we have to choose one of the many functions that biject  $\mathbb{N}$  to  $S_j$ . So we have a countable collection of sets  $C = \{E_j : j \in \mathbb{N}\}$ , where  $E_j$  denotes the set of all functions that biject  $\mathbb{N}$  into  $S_j$ . So for every element in  $C$ , we need to choose one element in each element of  $C$ . This is where the Axiom of Choice comes into play.) ■

### Theorem 2.20

If  $f : A \rightarrow B$  is a surjection, then  $B$  is bijective to a subset of  $A$

#### *Proof for Theorem.*

We are told that  $f(A) = B$ , i.e. for every  $b \in B$ ,  $\exists x_b$  (many such  $x_b$ -s are possible) such that  $f(x_b) = b$ . Define a function  $g : B \rightarrow A$  as:  $g(b) =$  one of those  $x_b$  such that  $f(x_b) = b$ .  $g$  is bijective to the set of all the chosen  $x_b$  for every  $b$  ■

#### **Remark.**

We make use of the Axiom of Choice in the previous theorem when we choose an  $x_b$  from a set of all possible  $x_b$ -s for  $b$ . Let  $A_b$  be the set of all possible  $x_b$ -s. Then the collection  $\{A_b : b \in B\}$  is a collection of non-empty sets. And we are to select "one" element from each  $A_b$ . This requires AC.

### Definition 2.21: (Power Set of a set)

Power set of  $A$ , denoted by  $P(A)$  is the set of all subsets of  $A$ .

### Theorem 2.22: Cantor's Theorem

For any set  $A$ , there *does not exist* any surjection from  $A$  onto  $P(A)$

#### *Proof for Theorem.*

Suppose, on the contrary, a surjection  $\psi : A \rightarrow P(A)$  exists. For every subset  $A_s$  of  $A$ , there exists an element  $x$  of  $A$  such that  $\psi(x) = A_s$ . Either this  $x$  exists in  $A_s$ , or it doesn't. Consider  $D := \{x \in A : x \notin \psi(x)\}$ .  $D$  is a subset of  $A$ , so there must be some element  $y \in A$  such that  $\psi(y) = D$ . Does  $y$  belong in  $D$ ? If so,  $y \notin \psi(y) = D$ . Which means  $y \notin D$ . If, though,  $y \notin D$ , that implies  $y \in \psi(y) \implies y \in D$ . Contradictions left and right. ■

### 3 Elementary Results regarding Integers

#### Definition 3.1

1. (Divides) We say  $a \in \mathbb{Z} \setminus \{0\}$  divides  $b \in \mathbb{Z}$  if there exists an integer  $\delta$  such that  $a\delta = b$ . We denote it by  $a|b$ .
2. (GCD) We call a number  $d$  the "Greatest Common Divisor" of two integers  $a$  and  $b$  if  $d|a$  and  $d|b$ , and  $d$  is the largest such number that divides both  $a$  and  $b$  (that the largest such number exists is clear, since divisors are finite).
3. (LCM) We call a number  $l$  the "Least Common Multiple" of two integers  $a$  and  $b$  if  $a|l$  and  $b|l$  and  $l$  is the smallest such integer.

#### Definition 3.2: Prime Number

A number  $p$  in  $\mathbb{N}$  is *prime* if it has only itself and 1 as divisors. Non-primes are called composite.

#### Theorem 3.3

1. The GCD  $d$  of  $a, b \in \mathbb{Z}$  is unique, and has the property that, if any other integer  $q$  is a divisor of  $a$  and  $b$ , then  $q$  divides  $d$ .
2. The LCM  $l$  of  $a, b \in \mathbb{Z}$  is unique, and has the property that, if another integer  $p$  is a multiple of  $a$  and  $b$ , then  $l$  divides  $p$ .
3. If LCM of  $a, b$  and GCD of  $a, b$  are  $l$  and  $d$  respectively, then  $dl = ab$ .

#### *Proof for Theorem.*

(1) This will be proved below with the division algorithm. For now note that, if every divisor divides  $d$ , then  $d$  is the GCD.

(2) This is also proved using the division algorithm. For now note that if every multiple of  $a, b$  is divisible by a multiple  $l$ , then it is the least common multiple.

(3) Suppose  $d$  is the unique GCD of  $a, b$  and  $l$  is the unique LCM of  $a, b$ .

Note that  $d|ab$  which means  $dc_0 = ab$  for some  $c_0$ .  $c_0 = a(\frac{b}{d})$  and  $c_0 = b(\frac{a}{d})$ . This means  $c_0$  is a multiple of  $a$  and  $b$  which means  $l|c_0$ . We have  $lq_0 = c_0$  for some  $q_0$ . This means  $dlq_0 = dc_0 = ab$ .  $(dq_0)(\frac{l}{a}) = b$  and  $(dq_0)(\frac{l}{b}) = a$  which makes  $dq_0$  a divisor. This would necessarily mean  $q_0 = 1$ , whence, we are done. ■

### 3.1 Euclid's Divison Algorithm

#### Lemma 3.4: The Lemma

Given integers  $a, b \in \mathbb{Z}$  with  $b \neq 0$ , we get a unique  $q \in \mathbb{Z}$  and  $r \in \mathbb{Z}$  such that:

$$a = bq + r$$

with  $0 \leq r < |b|$ .

#### *Proof for Lemma*

We Prove for the case that  $a, b \in \mathbb{N}$ . Assume that for  $a_0 \in \mathbb{N}$ , the divison lemma works, i.e,  $\exists q_0$  and  $r_0$  so that

$$a_0 = bq_0 + r_0$$

with  $0 \leq r_0 < |b|$ . Look at  $a_0 + 1 = bq_0 + r_0 + 1$ . We have that, either  $r_0 + 1 = b$ , or  $r_0 + 1 < b$ . If its the former, then we see that  $a_0 + 1 = bq_0 + b = b(q_0 + 1) + 0$  whence we see that the new quotient is  $q_0 + 1$  and the new remainder is 0. Hence, by induction, the lemma is proved.

For the cases where  $a < 0$  or  $b < 0$ , we can simply multiply by  $-1$  to get the result. ■

#### The Algorithm:

We start with  $a, b \in \mathbb{Z} \setminus \{0\}$ , and without loss of generality, we assume that  $a \geq b$ . We then have:

$$a = bq_0 + r_0 \text{ with } 0 \leq r_0 < |b|$$

$$b = r_0q_1 + r_1 \text{ with } 0 \leq r_1 < r_0 < |b|$$

$$r_0 = r_1q_2 + r_2 \text{ with } 0 \leq r_2 < r_1 < r_0 < |b|$$

$$r_1 = r_2q_3 + r_3 \text{ with } 0 \leq r_3 < r_2 < r_1 < r_0 < |b|$$

$$\vdots$$

$$r_{n_0-1} = r_{n_0}q_{n_0+1} + r_{n_0+1} \text{ with } 0 \leq r_{n_0+1} < r_{n_0} \cdots b$$

$$r_{n_0} = r_{n_0+1}q_{n_0+2} + r_{n_0+2} \text{ with } 0 \leq r_{n_0+2} < r_{n_0+1} \cdots < b$$

Since we cannot have a sequence of strictly decreasing positive integers, we note that at some point,  $r_n = 0 (= r_{n_0+2}$  for our sake).

We would then have (in the last step),

$$r_{n_0} = r_{n_0+1}q_{n_0+2} + 0$$

and back substituting,

$$r_{n_0-1} = r_{n_0+1}(q_{n_0+2}q_{n_0+1} + 1)$$

$$r_{n_0-2} = (r_{n_0+1}(q_{n_0+2}q_{n_0+1} + 1))q_{n_0} + r_{n_0+1}q_{n_0+2}$$

And finally we would end up with

$$a = r_{n_0+1}(\text{something}_1)$$

and

$$b = r_{n_0+1}(\text{something}_2)$$

with the added fact that  $r_{n_0+1}$  divides every remainder  $r_n$  in the division algorithm performed with  $a$  and  $b$ .

**Proof that any divisor divides the GCD:** Suppose that  $z$  is a divisor of  $a$  and  $b$ . From  $a = bq_0 + r_0$ , and

$$\frac{a}{z} = \frac{b}{z}q_0 + \frac{r_0}{z}$$

we see that  $z$  divides  $r_0$ . From  $b = r_0q_1 + r_1$  and

$$\frac{b}{z} = \frac{r_0}{z}q_1 + \frac{r_1}{z}$$

we see that  $z$  divides  $r_1$  too. Suppose  $z$  divides all remainders till  $r_{n_0}$ .  $r_{n_0-1} = r_{n_0}q_{n_0+1} + r_{n_0+1}$  gives us  $\frac{r_{n_0-1}}{z} = \frac{r_{n_0}}{z}q_{n_0+1} + \frac{r_{n_0+1}}{z}$  whence we see that  $r_{n_0+1}$  is divisible by  $z$ . Therefore,  $r_{n_0+1}$  is the GCD.

**Proof that any multiple is divisible by LCM:** Suppose that  $l$  and  $m$  are multiples of  $a, b$  and  $l$  is the least such multiple. Then  $l \leq m$  with equality case being trivial. Suppose  $l < m$ . From Euclid's division lemma, we have  $m = lq_0 + r_0$  with  $0 < r_0 < l < m$ . Both  $a$  and  $b$  divide  $m$  and  $l$ , which means

$$\frac{m}{a} = \frac{l}{a}q_0 + \frac{r_0}{a}$$

and

$$\frac{m}{b} = \frac{l}{b}q_0 + \frac{r_0}{b}$$

Which makes  $r_0$  a multiple of  $a$  and  $b$ , which is absurd.

### Theorem 3.5: Bezout's Theorem

If  $a, b \in \mathbb{Z} \setminus \{0\}$ , then there exists  $x, y \in \mathbb{Z}$  so that  $\gcd(a, b) = xa + yb$

**Proof for Theorem.**

From the first equation we see

$$a = bq_0 + r_0 \implies r_0 = a - bq_0$$

putting  $r_0$  in the 2nd equation we see:

$$b = (a - bq_0)q_1 + r_1 \implies r_1 = b - (a - bq_0)q_1$$

Putting  $r_1$  and  $r_0$  into the 3rd equation, we get, likewise,  $r_2$  in terms of  $a$  and  $b$  (a linear combination of  $a$  and  $b$ ) As such, we can keep doing this to express  $r_{n_0+1}$  as a linear combination of  $a$  and  $b$ , like,  $xa + yb$ . ■

### Theorem 3.6: Fundamental Theorem of Arithmetic

Given an integer  $a > 1$ , we can decompose  $a$  as a product of primes uniquely (upto ordering)

#### *Proof for Theorem.*

If  $a = 2$ , obviously we can. Suppose we can decompose every positive integer  $q$   $1 < q < n_0$  as a product of primes. Consider  $n_0 + 1 = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n} + 1$ . Either  $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n} + 1$  is a prime or is composite. If it is prime, we are done. If it is a composite number, then  $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n} + 1 = xy$  where  $x$  and  $y$  are numbers smaller than  $n_0 + 1$ . But since  $x$  and  $y$  can be expressed as a product of primes, we see that  $n_0 + 1$  can also be represented as a product of primes.

Suppose  $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$ , but also  $a = p_1^{\alpha'_1} p_2^{\alpha'_2} \cdots p_m^{\alpha'_m}$ .

We have ( $m \geq n$ ):

$$1 = p_1^{\alpha_1 - \alpha'_1} p_2^{\alpha_2 - \alpha'_2} \cdots p_n^{\alpha_n - \alpha'_n} p_{n+1}^{-\alpha'_{n+1}} \cdots p_m^{-\alpha'_m}$$

$$1 = p_1^{\alpha'_1 - \alpha_1} p_2^{\alpha'_2 - \alpha_2} \cdots p_n^{\alpha'_n - \alpha_n} p_{n+1}^{\alpha'_{n+1}} \cdots p_m^{\alpha'_m}$$

Obviously, not all  $\alpha_j - \alpha'_j$  are positive, in the same way they all aren't negative. Suppose some of these powers are positive, while some negative. Consider some  $p_j^{\delta_j}$  for which the power is negative, which moves it to the denominator. We have:

$$1 = \frac{\text{some primes raised to negative} \cdot \text{some primes raised to positive}}{p_j^{\delta_j}}$$

If we multiply the negative powers out to both sides, we get to a stage where we see that  $p_j$  divides a product of primes (raised to positive powers). But,  $p_j$  is different from all the primes, and hence does not divide any of them individually, which means, from the lemma(s) below, that  $p_j$  actually does not divide the whole product. A contradiction. Hence, the only case remaining is that of product of primes raised to 0 powers, which makes it unique.

#### Requisite Lemmas:

Lemma: Suppose  $m$  is such that  $\gcd(a, m) = 1$ , and  $|ab|$ . Then, we have that  $m|b$ .

To see this, we use Bezout's Theorem: there exists  $x$  and  $y$  integers such that  $ax + my = 1$ .

This means  $abx + mby = b \implies \frac{ab}{m}x + by = \frac{b}{m}$  whence it becomes clear.

Lemma: If a prime  $p$  divides  $z^n$  for some integer  $z$  and some natural  $n$ , then  $p$  divides  $z$ .

To see this, Suppose that  $p$  does not divide  $z$ . Which means, from the lemma above, that  $p$  divides  $z^{n-1}$ , which likewise means it divides  $z^{n-2}$  and finally reaching to a contradiction that it finally divides  $z$ . ■

If we arrange the primes  $p_1, p_2, \dots, p_n$  in ascending order, we find that this representation becomes the only one (no order permutations).

### AN ALTERNATE LOOK AT GCD AND LCM:

Suppose that  $a = p_1^{q_1} p_2^{q_2} \dots p_n^{q_n}$  and  $b = p_1^{r_1} p_2^{r_2} \dots p_n^{r_n} \dots p_m^{r_m}$ . Since all numbers whatsoever are product of primes, we have that every divisor is of the form (for a number  $z = p_1^{l_1} p_2^{l_2} \dots p_k^{l_k}$ )  $p_1^{j_1} p_2^{j_2} \dots p_k^{j_k}$  with  $j_1 \leq l_1, j_2 \leq l_2 \dots j_k \leq l_k$ . The number of divisors for a given  $z = p_1^{l_1} p_2^{l_2} \dots p_k^{l_k}$  would therefore be:  $\binom{l_1+1}{1} \binom{l_2+1}{1} \dots \binom{l_k+1}{1}$ .

We note that, given  $a = p_1^{x_1} p_2^{x_2} \dots p_m^{x_m}$  and  $b = p_1^{y_1} p_2^{y_2} \dots p_m^{y_m}$  with  $x_j, y_j \geq 0$ ,

$$\gcd(a, b) = p_1^{\min(x_1, y_1)} p_2^{\min(x_2, y_2)} \dots p_m^{\min(x_m, y_m)}$$

and

$$\text{lcm}(a, b) = p_1^{\max(x_1, y_1)} p_2^{\max(x_2, y_2)} \dots p_m^{\max(x_m, y_m)}$$

### Euler Totient Function ( $\phi$ ):

The Euler Totient function  $\phi$  is defined as follows:

$$\phi(n) = \text{number of positive integers } z \text{ less than or equal to } n \text{ such that } \gcd(n, z) = 1$$

For primes  $p$ , every number smaller than  $p$  is coprime to  $p$ , hence  $\phi(p) = p - 1$ . More generally we have for primes  $p$  and natural  $q$ ,  $\phi(p^q) = p^q - p^{q-1}$ .

**Proof.** Consider  $\phi(p^k) = ||\text{all such numbers } x \text{ such that } x \leq p^k \text{ and } \gcd(x, p^k) = 1||$ . Note that apart from the multiples of  $p, p^2, p^3 \dots$ , all else are coprimes with  $p^k$ . The numbers that are not coprimes with  $p^k$  can be counted as:  $1p, 2p, \dots, p(p), \dots, (p^2)p \dots p^{k-1}p$ . Hence, the number of multiples of  $p$  in this list are  $p^{k-1}$ . Total number of "numbers" smaller or equal to  $p^k$  are obviously,  $p^k$ . From here, the answer is obvious. □

*Just accept the following fact*

#### Fact 3.7

If  $(m, n) = 1$ , then  $\phi(mn) = \phi(m)\phi(n)$

**Proof.**

□

### 3.2 Modular Arithmetic:

Given  $n \in \mathbb{N}$  and the set of all integers  $\mathbb{Z}$ , we define the following equivalence class:

$$aRb \iff n|(b-a)$$

We have  $aRa$  obviously. If  $aRb$ , obviously  $bRa$ . If  $aRb$  and  $bRc$ , then  $n|(b-a)$  and  $n|(c-b)$  which means  $n|(b-a) + (c-b) \implies n|c-a$ . Hence,  $R$  is an equivalence relation. Consider arbitrary  $a \in \mathbb{Z}$ . A number  $x$  is in the equivalence class of  $a$  under the relation defined above if and only if  $n|(x-a)$  which means  $\exists z \in \mathbb{Z}$  so that  $nz = x-a \implies x = a+nz$ . A number  $x$  is in the equivalence class of  $a$  under  $R$  (also called as *congruence class of  $a \bmod n$* ) if and only if  $x$  is  $a$  plus an integral multiple of  $n$ .

It is also fruitful to view this from the following perspective:

**Conjecture:**  $zRa$  (i.e.,  $n|z-a$ ) if and only if  $z$ , when divided by  $n$ , gives the same remainder as  $a$  when divided by  $n$ .

**Proof.** ( $\implies$ ) Consider  $n|z-a$  which means  $\exists p$  so that  $z = a + pn$ . If  $a < n$ , we have the remainder when  $a$  is divided by  $n$ , as  $a$  itself, whence we see that the remainder when  $z$  is divided by  $x$  is  $a$  as well. If  $a > n$ , then  $a = qn + r_0$  with  $0 \leq r_0 < n$ . We then have  $z = pn + a = pn + qn + r_0 = z_0n + r_0$  where  $r_0 < n$ . Therefore, same remainder.

( $\impliedby$ ) Suppose  $z$  and  $a$  give the same remainder when divided by  $n$ . This means  $z = q_zn + r$  and  $a = q_an + r$  which means  $z - a = (q_z - q_a)n$  which means  $n|z - a$ .  $\square$

**Notation:** We say  $zRb$  in the above context if either  $n|z-b$  or  $z$  and  $b$  share the same remainders when divided by  $n$ . The equivalence class of  $a$  in this context is sometimes also called as *congruence class of  $a \bmod n$* . A symbolic way to say  $zRa$  in this context is

$$z \equiv a \bmod(n)$$

We also denote the congruence class (or residue class) of an integer  $a$  by  $\bar{a}$ .

#### Theorem 3.8

If  $z$  is a given integer, and  $n$  is a given natural number, then the congruence class that  $z$  falls in would be one of the congruence classes formed by the  $n-1$  numbers before  $n$ . Therefore, the entire partition created by  $R$  can be listed out as the congruence classes of the  $n-1$  numbers before  $n$

#### Proof for Theorem.

Suppose  $z < n$ . then obviously there is an integer  $q$  less than  $n$  (which is  $z$  itself) so that  $q \equiv z \bmod(n)$ . If  $z > n$ , then  $z = qn + r$  where  $0 \leq r < n$ , which also means that, when  $r$  is divided by  $n$ , the remainder is  $r$ , just like  $z$ . This means  $z \equiv r \bmod(n)$ . From here it is clear that every number in  $\mathbb{Z}$  would be in the equivalence class of some integer less than  $n$ . It is also obvious that for any two integers less than  $n$ , they each form unique residue classes.  $\blacksquare$



From the previous lemma, it is clear to see that all the residue classes, or "partitions" of  $\mathbb{Z}$  under the congruence mod  $(n)$  relation, can be succinctly listed out as

$$\overline{0}, \overline{1}, \overline{2} \dots \overline{n-1}$$

### Definition 3.9: $\mathbb{Z}/n\mathbb{Z}$

The set of all equivalence classes (or residue classes) under the relation defined by  $n$  on  $\mathbb{Z}$  is denoted by

$$\mathbb{Z}/n\mathbb{Z}$$

which is basically  $\overline{0}, \overline{1}, \overline{2} \dots \overline{n-1}$

### Theorem 3.10

If  $a_1 \equiv b_1 \pmod{n}$  and  $a_2 \equiv b_2 \pmod{n}$ , then  $a_1 + a_2 \in \overline{b_1 + b_2}$  and  $a_1 a_2 \in \overline{b_1 b_2}$

*Proof for Theorem.*

(1) We have  $a_1 = b_1 + kn$  and  $a_2 = b_2 + ln$  which gives  $a_1 + a_2 = (k+l)n + b_1 + b_2$  where we see that  $a_1 + a_2$  is integer multiple of  $n + b_1 + b_2$ . Therefore,  $a_1 + a_2 \in \overline{b_1 + b_2}$ .

Consider  $a_1 a_2 = (kn + b_1)(ln + b_2) = (kln^2 + b_2kn + b_1ln) + b_1b_2$ . Obvious from here. ■

### Definition 3.11: Modular Arithmetic

Treating the residue classes that form  $\mathbb{Z}/n\mathbb{Z}$  as elements with which arithmetic can be done, we define addition and multiplication as follows:

$$\overline{a} + \overline{b} = \overline{a + b}$$

i.e, the sum of two residue classes is the residue class of the sum of an element from the class of  $a$  and the class of  $b$ . (This sum is well defined from the previous theorem.)

$$\overline{a} \overline{b} = \overline{ab}$$

i.e, the product of residue class of  $a$  and  $b$  is the residue class of the product of an element in the class of  $a$  and an element from the class of  $b$ . (Yet again, well defined)

### Definition 3.12: $(\mathbb{Z}/n\mathbb{Z})^*$

$$(\mathbb{Z}/n\mathbb{Z})^* := \{\overline{a} \in \mathbb{Z}/n\mathbb{Z} : \exists \overline{c} \in \mathbb{Z}/n\mathbb{Z} \text{ such that } \overline{c} \cdot \overline{a} = \overline{1}\}$$

**Lemma 3.13**

If  $\gcd(a, n) = 1$ , i.e,  $a$  and  $n$  are coprimes, then every element in the residue class of  $a \bmod(n)$  is coprimes with  $n$

**Proof for Lemma**

Consider  $z = a + kn$  for some  $k$  to be "non coprimes with  $n$ ". i.e,  $\gcd(z, n) = j \neq 1$ . We have  $j|a + kn$  and  $j|n$ . But this means directly that  $j|a$  whence we see that  $j \neq 1$  is a divisor of  $a$  and  $n$ . Absurd. ■

**Lemma 3.14**

If  $a \in \bar{a} \in \mathbb{Z}/n\mathbb{Z}$ ,  $a \leq n$  and if  $\gcd(a, n) = j$ , then for any  $z \in \bar{a}$ ,  $\gcd(z, n) = j$ .

**Proof for Lemma**

$\gcd(a, n) = k$ . Consider  $\gcd(a + gn, n)$ . We apply the division algorithm:

$$(a + gn) = g_0(n) + a$$

$$n = g_1a + r_1$$

$$\vdots$$

Notice that after step (1), the procedure is exactly the same as the procedure to find  $\gcd(a, n)$ . The last living remainder is the GCD, and from here we can clearly see that the gcd are the same. ■

**Lemma 3.15**

If  $1 \leq a \leq n$ , with  $n \geq 2$ , and  $(a, n) = j \neq 1 (\geq 2)$ , then there exists a number  $1 \leq b < n$  so that  $\bar{a} \cdot \bar{b} = \bar{0}$ . A corollary of this is that there exists *no*  $c \in \mathbb{Z}$  so that  $\bar{a} \cdot \bar{c} = \bar{1}$

**Proof for Lemma**

We know  $\gcd(a, n) = j \neq 1 (\geq 2)$ . This means  $j\alpha = a$ ,  $j\mu = n$  where  $\alpha < a$  and  $\mu < n$ . We can see that  $a\mu = j\mu\alpha = n\alpha$ . So the  $b$  in the lemma is the  $\mu$  here. Therefore,  $\bar{a} \cdot \bar{b} = \bar{0}$ . Suppose  $ac \equiv 1 \bmod(n)$ . This means from the multiplicative property of  $\bmod(n)$ , we have  $ac(b) \equiv b \bmod(n)$ , but if you commute the multiplication, we see

$$c(ab) = \bar{c} \cdot \overline{ab} = \bar{c} \cdot \bar{0} \equiv 0 \bmod(n)$$

But this would imply  $b \equiv 0 \bmod(n)$  which is not true. Hence, there can be no  $c$  so that  $ac \equiv 1 \bmod(n)$ . ■

**Proposition 3.16**

$\mathbb{Z}/n\mathbb{Z}^*$  is the same as  $\{\bar{a} \in \mathbb{Z}/n\mathbb{Z} : (a, n) = 1\}$

**Proof.** Let

$$A = \{\bar{a} \in \mathbb{Z}/n\mathbb{Z} : \exists \bar{z} \in \mathbb{Z}/n\mathbb{Z} \text{ such that } \bar{z} \cdot \bar{a} = \bar{1}\}$$

and

$$B = \{\bar{b} \in \mathbb{Z}/n\mathbb{Z} : (b, n) = 1\}$$

Consider an arbitrary  $\bar{a}$  in  $B$  such that  $\forall z \in \bar{a}$  we have  $\gcd(z, n) = 1$ . We know that  $z = a + k_z n$ . From Bezout Identity, we have  $x_z$  and  $y_z$  so that  $x_z(a + k_z n) + y_z(n) = 1$  which gives us  $x_z a = (-y_z - k_z x_z)(n) + 1$ . We see That  $x_z a \in \bar{1}$ . Consider arbitrary  $t \in \bar{x}_z$ . We have  $t = x_z + jn$  or  $x_z = t - jn$ . Plugging this back we have  $x_z a = (t - jn)a = (-y_z - k_z(t - jn))n + 1$  whence we can easily see that  $ta \in \bar{1}$ . Therefore,  $\bar{a} \cdot \bar{x} = \bar{1}$ . Therefore, if  $\bar{b}$  is such that  $(b, n) = 1$ , then an inverse exists for it. Hence,  $B \subseteq A$ .

We showed that if  $x$  is in  $B$ , it must be in  $A$ . Consider  $x$  not in  $B$ . i.e, it is not co-primes with  $n$ . From the previous proposition, we see that there would exist no  $c$  so that  $\bar{x} \cdot \bar{c} = \bar{1}$ , i.e, no inverse element for any  $x$  not in  $B$ . Inexistence in  $B$  therefore implies inexistence in  $A$ , which gives us  $A \subseteq B$ . We can conclude that  $A = B$  or in pithy words:

"The set of all congruence classes  $b$  so that  $\gcd(b, n) = 1$  is the same as the set of all congruence classes  $b$  so that there exists another congruence class  $c$  so that  $\bar{b} \cdot \bar{c} = \bar{1}$  "

Symbolically:

$$\{\bar{b} \in \mathbb{Z}/n\mathbb{Z} : \gcd(b, n) = 1\} = \{\bar{b} \in \mathbb{Z}/n\mathbb{Z} : \exists \bar{c} \in \mathbb{Z}/n\mathbb{Z} : \bar{b} \cdot \bar{c} = \bar{1}\} = (\mathbb{Z}/n\mathbb{Z})^*$$

□

**Theorem 3.17: Generalised Bezout's Identity**

Suppose  $j_1, j_2 \dots j_n$  are given integers such that  $\gcd(j_1, j_2 \dots j_n) = d$ , then there exists integers  $x_1, x_2 \dots x_n$  so that  $x_1 j_1 + x_2 j_2 \dots x_n j_n = d$

**Proof for Theorem.**

We prime decompose each of  $j_1, j_2 \dots j_n$ . For  $j_k$ , we have

$$j_k = p_1^{q_1^k} p_2^{q_2^k} \dots p_{n_k}^{q_{n_k}^k}$$

We note that the gcd of all these numbers are the minimum of each index for each prime multiplied throughout. An important bit of information will be crucial here:

$$\min\{w_1, w_2 \dots w_k, w_{k+1} \dots w_n\} = \min\{\min\{w_1, w_2 \dots w_k\}, \min\{w_{k+1}, w_{k+2} \dots w_n\}\}$$

So we split  $\gcd(j_1, j_2, \dots j_n)$  into  $\gcd(\gcd(j_1, j_2), \gcd(j_3 \dots j_n)) = \text{some linear combination of } j_1, j_2 \text{ and } \gcd(j_3, \dots j_n)$ . Do the same split to  $\gcd(j_3, \dots j_n)$ , to keep getting linear combinations, until finally you find  $\gcd(j_1, j_2 \dots j_n) = x_1 j_1 + x_2 j_2 \dots x_n j_n$  ■