In this section, we study the arithmetic functions.

Definition: An <u>arithmetic function</u> is a function defined over integers, i.e. $f: \mathbb{N} \to \mathbb{C}$.

Example: (1) The trivial function $\mathbb{1}: \mathbb{N} \to \mathbb{C}$.

$$\mathbb{1}(n) = 1 \quad \text{for all } n \in \mathbb{N}.$$

(2) The Euler's Phi function: $\phi: \mathbb{N} \to \mathbb{C}$

$$\phi(m) := \#\{a : 1 \le a \le m, \gcd(a,m) = 1\}$$

(3) The divisor function : $d: \mathbb{N} \to \mathbb{C}$

$$d(m) := \#\{a : a \mid m\}.$$

(4) The Möbius function: $\mu: \mathbb{N} \to \mathbb{C}$.

$$\mu(m) = \begin{cases} (-1)^r & \text{if } m = p_1 p_2 \cdots p_r \text{ with } p_i \text{ distinct.} \\ 0 & \text{otherwise.} \end{cases}$$

Definition: An arithmetic function: $f: \mathbb{N} \to \mathbb{C}$ is <u>multiplicative</u> if $f(mn) = f(m)f(n)$ when $\gcd(m,n) = 1$.

An arithmetic function $f: \mathbb{N} \to \mathbb{C}$ is <u>completely multiplicative</u> if $f(mn) = f(m)f(n)$ for all m, n.

Remark: f completely multiplicative $\Rightarrow$ multiplicative.

In fact: (1) $\mathbb{1}(m)$ is completely multiplicative.

(2) $\phi(m)$ is multiplicative $\rightsquigarrow$ will show later.

but not completely multiplicative.

(outer) example: $\phi(4)=2$ $\quad \phi(2)=1$

$$\phi(4)=\phi(2\cdot 2) \neq \phi(2)\cdot\phi(2)$$

(3) $d(m)$ is multiplicative

but not completely multiplicative.

(outer) example: $d(4)=3$ $\quad d(2)=2$

$$d(4)=d(2\cdot 2)\neq d(2)\cdot d(2)$$

(4). $\mu(m)$ is compliative

but not completely multiplicative.

(outer) example: $4=2\cdot 2=2^2$

$$\mu(4)=0 \qquad \mu(2)=-1.$$

$$\mu(4)=\mu(2\cdot 2)\neq \mu(2)\cdot\mu(2).$$

Notations:

sum notation: $\sum$

product notation: $\prod$

example: $\sum_{p|n} p$ means: find all primes divides n and sum them.

$$\sum_{p|10} = 2+5 = 7$$

$\prod_{p|n}\left(1-\frac{1}{p}\right)$ means: multiply all $\left(1-\frac{1}{p}\right)$ where $p|n$.

$$\prod_{p|6}\left(1-\frac{1}{p}\right) = \left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)$$

$$= \frac{1}{2}\cdot\frac{2}{3} = \frac{1}{3}.$$

Question: why the multiplicative functions are important.

Ans: Let $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ with p_i distinct.

Let f be multiplicative.

Then
$$f(m) = f(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r})$$
$$= f(p_1^{\alpha_1}) f(p_2^{\alpha_2}) \cdots f(p_r^{\alpha_r})$$
$$= \prod_{p^\alpha \| m} f(p^\alpha)$$

f is totally determined by its values at prime powers.

Moreover, if f is completely multiplicative.

$$f(m) = f(p_1)^{\alpha_1} f(p_2)^{\alpha_2} \cdots f(p_r)^{\alpha_r}$$
$$= \prod_{p^\alpha \| m} f(p)^\alpha$$

f is totally determined by its values at primes.

First example: Euler's Phi funtion.

Theorem (11.1 Euler's Phi funtion formula)

(a) If p is a prime and $k \geq 1$, then

$$\phi(p^k) = p^k - p^{k-1} = p^k\left(1 - \frac{1}{p}\right)$$

(b) If $\gcd(m,n) = 1$, then

$$\phi(mn) = \phi(m)\phi(n).$$

(c) For $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$

$$\phi(m) = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right)$$

$$= m \cdot \prod_{p \mid m} \left(1 - \frac{1}{p}\right)$$

Proof of (c): By (a), (b)

$$\phi(m) = \phi(p_1^{\alpha_1})\,\phi(p_2^{\alpha_2}) \cdots \phi(p_r^{\alpha_r})$$

$$= (p_1^{\alpha_1} - p_1^{\alpha_1 - 1})(p_2^{\alpha_2} - p_2^{\alpha_2 - 1}) \cdots (p_r^{\alpha_r} - p_r^{\alpha_r - 1})$$

$$= p_1^{\alpha_1}\left(1 - \frac{1}{p_1}\right) p_2^{\alpha_2}\left(1 - \frac{1}{p_2}\right) \cdots p_r^{\alpha_r}\left(1 - \frac{1}{p_r}\right)$$

$$= m \cdot \prod_{p \mid m} \left(1 - \frac{1}{p}\right)$$ $\square$.

Proof of (a). Let p be a prime and $k \geq 1$.

$$\phi(p^k) = \#\{a : 1 \leq a \leq p^k,\ \gcd(a, p^k) = 1\}$$

$$= p^k - \#\{a : 1 \leq a \leq p^k,\ p \mid a\}$$

We can show:

$$\{a : 1 \leq a \leq p^k,\ p \mid a\} = \{p, 2p, 3p, 4p, \cdots (p^{k-1} - 1)p, p^k\}$$

$$\Rightarrow \#\{a : 1 \leq a \leq p^k,\ p \mid a\} = p^{k-1}$$

This implies:

$$\phi(p^k) = p^k - p^{k-1}$$ $\square$.

Let $\gcd(m, n) = 1$.

$$A = \{a : 1 \leq a \leq mn,\ \gcd(a, mn) = 1\} \qquad \phi(mn) = \#A.$$

$$B = \{b : 1 \leq b \leq m,\ \gcd(b, m) = 1\} \qquad \phi(m) = \#B.$$

$C = \{c : 1 \leq c \leq n, \gcd(c, n) = 1\}$ $\phi(n) = \# C$.

(We need to show: $\phi(mn) = \phi(m)\phi(n)$ i.e.

$\# A = \# B \cdot \# C$)

We look at the following set:

$$M = \left\{ (b, c) : \begin{array}{l} 1 \leq b \leq m, \gcd(b, m) = 1 \\ 1 \leq c \leq n, \gcd(c, n) = 1 \end{array} \right\}$$

We can show: $\# B \cdot \# C = \# M$

Therefore, it suffices to show: $\# A = \# M$.

Strategy: we construct an <u>one-to-one</u> map from A to M.

Definition: Let $f : A \to B$ be a map.

- f is <u>injective</u> if $f(b_1) = f(b_2) \Rightarrow b_1 = b_2$
- f is <u>surjective</u> if for any $b \in B$, we can find $a \in A$ such that $f(a) = b$.
- f is a <u>bijection</u> if f is both injective and surjective.
  one-to one map

Let A, B be finite sets. If there is an <u>one-to-one</u> map $f: A \to B$, then $\# A = \# B$.

We construct the following map:

$$f: A \longrightarrow M$$

$$\left\{ a : \begin{array}{l} 1 \le a \le mn \\ \gcd(a, mn) = 1 \end{array} \right\} \longrightarrow \left\{ (b, c) : \begin{array}{l} 1 \le b \le m \quad \gcd(b, m) = 1 \\ 1 \le c \le n \quad \gcd(c, n) = 1 \end{array} \right\}$$

$$a \longmapsto (a \pmod m, \ a \pmod n).$$

We need to show f is both injective and surjective.

- injective: Let $a_1, a_2 \in A$ with $f(a_1) = f(a_2)$

  (we need to show: $a_1 = a_2$)

$$(a_1 \pmod m, \ a_1 \pmod n) = (a_2 \pmod m, \ a_2 \pmod n)$$

$$\Rightarrow \quad \begin{array}{l} a_1 \equiv a_2 \pmod m \\ a_1 \equiv a_2 \pmod n. \end{array}$$

$$\gcd(m, n) = 1 \Rightarrow a_1 \equiv a_2 \pmod{mn}$$

$1 \leqslant a_1 \leqslant mn \quad 1 \leqslant a_2 \leqslant mn \Rightarrow a_1 = a_2.$

- surjective: $\left(\text{Let } (b,c) \in M, \text{ then we can find } a \in A \text{ such that } (a \pmod m, a \pmod n) = (b,c) \right)$.

We look at the linear congruent equation:

$$my \equiv (c-b) \pmod n$$

$\gcd(m,n) = 1 \Rightarrow$ we can find y_1 such that

$$my_1 \equiv (c-b) \pmod n.$$

Set $\quad X = my_1 + b.$

$$X \equiv b \pmod m$$

$$X = my_1 + b \equiv (c-b+b) \pmod n \equiv c \pmod n.$$

Take a between 1 and mn such that

$$a \equiv x \pmod{mn}.$$

$$a \equiv x \pmod m \equiv b \pmod m$$

$$a \equiv x \pmod n \equiv c \pmod n$$

$\square$.

Proof of (c): We showed: the map between

$$A = \{ a : 1 \le a \le mn, \ \gcd(a, mn) = 1 \}$$

and

$$M = \left\{ (b,c) : \begin{array}{ll} 1 \le b \le m & \gcd(b,m) = 1 \\ 1 \le c \le n & \gcd(c,n) = 1 \end{array} \right\}$$

is one to one.

Therefore $\# A = \# M$

$$\# A = \phi(mn)$$

$$\# M = \# B \cdot \# C = \phi(m) \cdot \phi(n).$$

$$\Rightarrow \phi(mn) = \phi(m)\,\phi(n). \qquad \square$$

The "surjective" part can be generalized to the following theorem:

Theorem (11.2 Chinese Remainder Theorem) Let m, n be integers with $\gcd(m,n) = 1$. Let b, c be integers. Then the simultaneous congruences

$$x \equiv b \pmod{m} \qquad x \equiv c \pmod{n}$$

has exactly one solution with $0 \le x \le mn$.