

In this section, we study the arithmetic functions.

Definition: An arithmetic function is a function defined over integers, i.e. $f: \mathbb{N} \rightarrow \mathbb{C}$.

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

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

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

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

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

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

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

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

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

An arithmetic function $f: \mathbb{N} \rightarrow \mathbb{C}$ is

completely multiplicative if $f(mn) = f(m)f(n)$ for all m, n .

Remark: f completely multiplicative \Rightarrow multiplicative.

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

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

but not completely multiplicative.

(counter) example: $\phi(4)=2$ $\phi(2)=1$

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

13) $d(m)$ is multiplicative

but not completely multiplicative.

(counter) example: $d(4)=3$ $d(2)=2$

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

14) $\mu(m)$ is multiplicative

but not completely multiplicative.

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

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

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

Notations:

sum notation: \sum

product notation: \prod

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

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

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

$$\begin{aligned} \prod_{p|6} (1 - \frac{1}{p}) &= (1 - \frac{1}{2})(1 - \frac{1}{3}) \\ &= \frac{1}{2} \cdot \frac{2}{3} = \frac{1}{3}. \end{aligned}$$

Question: why the multiplicative functions are important.

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

Let f be multiplicative.

$$\text{Then } f(m) = f(p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r})$$

$$= f(p_1^{\alpha_1}) f(p_2^{\alpha_2}) \dots f(p_r^{\alpha_r})$$

$$= \prod_{p^\alpha \parallel m} f(p^\alpha)$$

f is totally determined by its values at prime powers.

Moreover, if f is completely multiplicative.

$$f(m) = f(p_1)^{\alpha_1} f(p_2)^{\alpha_2} \dots f(p_r)^{\alpha_r}$$

$$= \prod_{p^\alpha \parallel m} f(p)^\alpha$$

f is totally determined by its values at primes.

First example: Euler's Phi function.

Theorem (11.1 Euler's Phi function 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 $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$

$$\begin{aligned}\phi(m) &= p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right) \\ &= m \cdot \prod_{p|m} \left(1 - \frac{1}{p}\right)\end{aligned}$$

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

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

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

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

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

□.

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

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

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

We can show:

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

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

This implies:

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

□.

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

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

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

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

$$\left(\begin{array}{l} \text{We need to show: } \phi(mn) = \phi(m)\phi(n) \text{ i.e.} \\ \#A = \#B \cdot \#C \end{array} \right)$$

We look at the following set:

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

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

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

Strategy: we construct an one-to-one map from A to M .

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

- f is injective if $f(b_1) = f(b_2) \Rightarrow b_1 = b_2$

- f is surjective if for any $b \in B$, we can find $a \in A$ such that $f(a) = b$.

- f is a bijection if f is both injective and surjective.

Let A, B be finite sets. If there is a bijective map $f: A \rightarrow B$, then $\#A = \#B$.

We construct the following map:

$$f: A \longrightarrow M$$

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

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

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: $a_1 = a_2$)

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

$$\Rightarrow a_1 \equiv a_2 \pmod{m}$$

$$a_1 \equiv a_2 \pmod{n}.$$

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

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

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

We look at the linear congruence 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
$$x = my_1 + b.$$

$$x \equiv b \pmod m$$

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

Take a between 1 and mn such that

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

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

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

□.

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

$$A = \left\{ a: 1 \leq a \leq mn, \gcd(a, mn) = 1 \right\}$$

and

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

is one to one.

Therefore $\# A = \# M$

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

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

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

□

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

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

has exactly one solution with $0 \leq x < mn$.