Proposition. Let $n \in \mathbb{Z}^+$, $d \in \mathbb{Z}^+$, $d \mid n$. Then the cardinality of the following set

$$\{a \in \mathbb{Z} : 0 \le a < n, \gcd(a,n) = d\}$$

is equal to $\varphi(\frac{n}{d})$.

Proof. $\gcd(a,n) = d \Rightarrow \begin{matrix} a = d \cdot b \\ n = d \cdot e \end{matrix}$ for $b, e \in \mathbb{Z}$.

$\gcd(b,e) = 1$ (otherwise $\gcd(b,e) = f > 1$
$f \mid b$, $f \mid e \Rightarrow fd \mid a$, $fd \mid n$
contradiction)

$0 \le a < n \Leftrightarrow 0 \le db < n \Leftrightarrow 0 \le b < \frac{n}{d} = e$.

Therefore b belongs to

$$\{b \in \mathbb{Z} : 0 \le b < e, \gcd(b,e) = 1\} =: B$$

Check that any $b \in B$ gives us $a = d \cdot b$ from the initial set. - Ex.

Therefore the cardinalities of both sets coincide

$$\Rightarrow \#\{a \in \mathbb{Z} : 0 \le a < n, \gcd(a,n) = d\} = \varphi(e) = \varphi(\tfrac{n}{d}).$$

$\boxtimes$

Proof 2 (of $\sum_{d \mid n} \varphi(d) = n$):

Denote by $N_d := \{a \in \mathbb{Z} : 0 \le a < n, \gcd(a,n) = d\}$ where d is taken over all divisors of n, Then $\{0,1,2,\dots,n-1\}$ is a disjoint union of N_d's.

Therefore

$$n=\sum_{d|n}|N_d|=\sum_{d|n}\varphi\left(\frac{n}{d}\right) \quad \text{(by Proposition)}$$

$$=\sum_{e|n}\varphi(e) \qquad \boxtimes$$

§10.6. Möbius Inversion Formula.

Given multiplicative function f we can construct another multiplicative F by

$$F(n)=\sum_{d|n}f(d).$$

Main Q: Given $F(n)$ can we restore $f(n)$?

A: Yes! (with help of Möbius Inversion Formula).

For small n:

$$F(1)=f(1) \Rightarrow f(1)=F(1)$$

$$F(2)=f(1)+f(2) \Rightarrow f(2)=F(2)-F(1)$$

$$F(3)=f(1)+f(3) \Rightarrow f(3)=F(3)-F(1)$$

$$F(4)=f(1)+f(2)+f(4) \Rightarrow f(4)=F(4)-F(1)-(F(2)-F(1))$$

$$=F(4)-F(2).$$

Recall: Möbius function $\mu(n)$ is defined as follows:

$$\mu\cancel{f}(n) = \begin{cases} (-1)^d & \text{if } n = p_1 p_2 \cdots p_d \text{ and all } p_i\text{'s are distinct primes} \\ 0 & \text{otherwise (i.e. } n \text{ is not square-free).} \end{cases}$$

Proposition: $\mu(n)$ is multiplicative
I.e. for any $m, n \in \mathbb{Z}^+$, $\gcd(m,n) = 1$ we have
$$\mu(mn) = \mu(m)\mu(n).$$

Proof. If m is not square-free (i.e. square of some prime p divides m) then neither is mn.

$$\Rightarrow \mu(mn) = 0 = \underbrace{\mu(m)}_{=0}\mu(n)$$

The same is true if n is not square-free.
Consider the case

$$m = p_1 p_2 \cdots p_d$$

$$n = q_1 q_2 \cdots q_r$$

where all $p_1, \dots, p_d, q_1, \dots, q_r$ are distinct primes. (since $\gcd(m,n) = 1$).

$$\mu(mn) = (-1)^{d+r} = (-1)^d \cdot (-1)^r = \mu(m)\mu(n). \qquad \boxtimes$$

Q: if $f(n)=\mu(n)$, what is $F(n) = \sum_{d|n} f(d)$?

Try small n:

$$F(1) = \mu(1) = 1$$

$$F(2) = \mu(1) + \mu(2) = 1 + (-1) = 0$$

$$F(3) = \mu(1) + \mu(3) = 1 + (-1) = 0$$

$$F(4) = \mu(1) + \mu(2) + \mu(4) = 1 + (-1) + 0 = 0$$

Proposition: $F(n) = \sum_{d|n} \mu(d)$ ~~is given by~~ can be computed by the following formula:

$$F(n) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n > 1. \end{cases}$$

Proof: Both sides are multiplicative therefor it is sufficient to check the equality for $n = p^k$, p prime, $k \in \mathbb{N}$.

Then $F(n) = \underbrace{\mu(1)}_{1} + \underbrace{\mu(p)}_{-1} + \underbrace{\mu(p^2)}_{0} + \ldots + \underbrace{\mu(p^k)}_{0} = 0$ $\boxtimes$

Example: $n = 12$. The divisors of n are $1, 2, 3, 4, 6, 12$

$$\underbrace{\mu(1)}_{1} + \underbrace{\mu(2)}_{-1} + \underbrace{\mu(3)}_{-1} + \underbrace{\mu(4)}_{0} + \underbrace{\mu(6)}_{1} + \underbrace{\mu(12)}_{0} = 0.$$