§10 Multiplicative functions.

Definition: A function $f: \mathbb{Z}^+ \to \mathbb{Z}$ is called <u>multiplicative</u> if for all $n, m \in \mathbb{Z}^+$ with $\gcd(n,m)=1$

$$f(mn) = f(m) \cdot f(n). \qquad (*)$$

f is called completely multiplicative if $(*)$ holds for all pairs m and n.

Example: $f(n) = n^2$ (more generally $f(n) = n^k$, $k \in \mathbb{N}$) is completely multiplicative.

$((mn)^k = m^k \cdot n^k)$

§10.1 Euler Phi-function.

Recall: $\varphi(n) := \#\{a \in \mathbb{Z} : 0 \le a < n, \gcd(a,n) = 1\}$

(a) $\varphi(p) = p-1$ for prime p

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

(c) $\varphi(pq) = (p-1)(q-1)$ for distinct primes p, q.

Theorem: Euler Phi-function is multiplicative

Proof: Aim: $\varphi(mn) = \varphi(m) \cdot \varphi(n)$ for $\gcd(n,m)=1$

Idea: We construct a bijection (one-to-one correspondence) between two sets:

$$\{x \in \mathbb{Z} : 0 \le x < mn, \gcd(x, mn) = 1\} \xrightarrow{f}$$
$$\{y \in \mathbb{Z} : 0 \le y < m, \gcd(y, m) = 1\} \times \{z \in \mathbb{Z} : 0 \le z < n, \gcd(z, n) = 1\}$$

given by

$$f(x) = (x \pmod{m}, x \pmod{n}).$$

(a) Injection ($f(x) = f(x') \Rightarrow x = x'$)

If $f(x) = f(x')$ then

$$\begin{cases} x \equiv x' \pmod{m} \\ x \equiv x' \pmod{n} \end{cases} \Rightarrow [\text{Principle } 3] \Rightarrow x \equiv x' \pmod{mn}$$

$\Rightarrow x = x'$.

(b) Surjection (Any element (y, z) has at least one preimage).

Consider (y, z) with $\gcd(y, m) = 1$, $\gcd(z, n) = 1$.

Then by CRT the following system

$$\begin{cases} x \equiv y \pmod{m} \\ x \equiv z \pmod{n} \end{cases}$$

has a solution $x \pmod{mn}$. We can take it between 0 and mn.

Notice that $\gcd(x,m)=1$, since $x \equiv y \pmod m$ and $\gcd(y,m)=1$.

By analogy $\gcd(x,n)=1$.

$\Rightarrow \gcd(x,mn)=1$.

Finally $f(x)=(y,z)$.

We have a bijection $f \Rightarrow$ the sizes of the sets coincide:

$\#\{x \in \mathbb{Z} : 0 \le x < mn, \gcd(x,mn)=1\}$

$= \#\{y \in \mathbb{Z} : 0 \le y < m, \gcd(y,m)=1\} \times \{z \in \mathbb{Z} : 0 \le z < n, \gcd(z,n)=1\}$

$\varphi(mn) = \varphi(m) \cdot \varphi(n)$. $\boxtimes$

Examples: (a) $\varphi(100) = \varphi(2^2 \cdot 5^2) \xrightarrow{\text{multiplicity}} \varphi(2^2)\varphi(5^2)$

$= (2^2-2)(5^2-5) = 40$.

(b) $\varphi(2068) = ?$

$2068 = 2 \cdot 1034 = 2^2 \cdot 517$

Try small factors: $\cancel{2}, \cancel{5}, \cancel{7}, 11$.

$2^2 \cdot 517 = 2^2 \cdot 11 \cdot 47$

Now we can compute:

$\varphi(2068) = \varphi(2^2 \cdot 11 \cdot 47) = \varphi(2^2 \cdot 11) \cdot \varphi(47) = \varphi(2^2) \cdot \varphi(11) \cdot \varphi(47)$

$= (2^2-2)\cdot(11-1)(47-1) = 920.$

Proposition. Let $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdot \ldots \cdot p_d^{\alpha_d}$ be a factorization of n as the product of primes. Then

$$\varphi(n) = (p_1^{\alpha_1} - p_1^{\alpha_1 - 1}) \cdot \ldots \cdot (p_d^{\alpha_d} - p_d^{\alpha_d - 1})$$

or $$\varphi(n) = n\cdot\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\ldots\left(1-\frac{1}{p_d}\right) = n\cdot\prod_{i=1}^{d}\left(1-\frac{1}{p_i}\right)$$

Proof: By multiplicity,

$$\varphi(p_1^{\alpha_1}\cdot\ldots\cdot p_d^{\alpha_d}) = \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2})\cdot\ldots\cdot\varphi(p_d^{\alpha_d})$$
$$= (p_1^{\alpha_1} - p_1^{\alpha_1-1})\cdot\ldots\cdot(p_d^{\alpha_d} - p_d^{\alpha_d-1})$$
$$= p_1^{\alpha_1}\left(1-\frac{1}{p_1}\right)\cdot p_2^{\alpha_2}\left(1-\frac{1}{p_2}\right)\cdot\ldots\cdot p_d^{\alpha_d}\left(1-\frac{1}{p_d}\right) = n\cdot\prod_{i=1}^{d}\left(1-\frac{1}{p_i}\right) \boxtimes$$

§10.2. Liouville and Möbius funcions.

Definition: Liouville function is defined as follows: $\lambda(n) := (-1)^{\#\text{ of primes in the factoritation of } n}$

That is $\lambda(p_1^{\alpha_1} p_2^{\alpha_2}\ldots p_d^{\alpha_d}) = (-1)^{\alpha_1+\alpha_2+\ldots+\alpha_d}$

$\lambda(n)$ is completely multiplicative

$$\left(\lambda(mn) = \lambda(p_1^{\alpha_1} \cdots p_d^{\alpha_d} \cdot p_1^{\beta_1} \cdots p_d^{\beta_d}) \right.$$

$$\left. = (-1)^{\alpha_1+\alpha_2+\cdots+\alpha_d+\beta_1+\cdots+\beta_d} = \lambda(m)\lambda(n) \right)$$

Table of $\lambda(n)$ for small values n:

n	1	2	3	4	5	6	7	8	9	10
factorization of n	1	2	3	2^2	5	$2 \cdot 3$	7	2^3	3^2	$2 \cdot 5$
$\lambda(n)$	1	-1	-1	1	-1	1	-1	-1	1	1