Arithmetic Functions.

complex numbers

Definition: a function $f: \mathbb{Z}_+ \to \mathbb{C}$ is an arithmetic function.

Goal: to study the algebra of arithmetic functions under (usual) addition and "Dirichlet multiplication" (a.k.a. convolution).

Notes:

(i) ALWAYS: for $n \in \mathbb{Z}_+$, $\sum_{d|n} f(d)$ denotes the sum over positive divisors d of n.

(ii) For today: given $n > 1$, write $n = \prod_{i=1}^{r} p_i^{a_i}$, where a_i is a positive integer for $1 \le i \le r$ (so p_i is not necessarily the i^{th} largest prime).

Example 1. The Möbius function μ is defined by

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{if } a_i > 1 \text{ for some } i \in \{1, 2, \dots, r\}, \\ (-1)^r & \text{if } a_i = 1 \text{ for } 1 \le i \le r. \end{cases}$$

Note that $\mu(n) \neq 0$, for $n > 1$, iff n is squarefree (i.e. indivisible by any perfect square > 1).

Now let $[x]$ denote the greatest integer $\le x$.

Thm 2.1

$$\sum_{d|n} \mu(d) = \left[\frac{1}{n}\right] = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{if } n > 1. \end{cases}$$

Proof

The case $n=1$ is clear.

Now suppose $n>1$.

Note that $d|n$, $d>1$, and $\mu(d)\neq 0$

$\Longleftrightarrow$

d is a product of j distinct primes $p_1, p_2, \ldots, p_r$, each to the first power, for some $1\leq j\leq r$. There are $\binom{r}{j}$ such products. So

$$\sum_{d|n}\mu(d) = 1+\binom{r}{1}\cdot(-1)+\binom{r}{2}(-1)^2+\binom{r}{3}(-1)^3$$

$$+\ldots+\binom{r}{r}(-1)^r = (1-1)^r = 0. \qquad \square$$

by the binomial theorem

Example 2: Euler's "totient" or "phi" function.

Definition: $\varphi(n)$ = # of positive integers k with $k\leq n$ and $(n,k)=1$. That is,

$$\varphi(n) = \sum_{\substack{k=1\\(k,n)=1}}^{n} 1.$$

We have

Thm. 2.2: $\displaystyle\sum_{d|n}\varphi(d)=n.$

Proof. Let

$$S = \left\{\frac{1}{n}, \frac{2}{n}, \frac{3}{n}, \ldots, \frac{n}{n}\right\}.$$

Note that $\exists\, m/n \in S$ with reduced form k/d iff:

(a) d is a positive divisor of n; and

(b) $1 \le k \le d$ and $(k,d) = 1$.

Also, this association $m/n \leftrightarrow k/d$ is one-to-one.

[Example:

$$\left\{ \tfrac{1}{12}, \tfrac{2}{12}, \tfrac{3}{12}, \tfrac{4}{12}, \tfrac{5}{12}, \tfrac{6}{12}, \tfrac{7}{12}, \tfrac{8}{12}, \tfrac{9}{12}, \tfrac{10}{12}, \tfrac{11}{12}, \tfrac{12}{12} \right\}$$

$$= \left\{ \tfrac{1}{12}, \tfrac{1}{6}, \tfrac{1}{4}, \tfrac{1}{3}, \tfrac{5}{12}, \tfrac{1}{2}, \tfrac{7}{12}, \tfrac{2}{3}, \tfrac{3}{4}, \tfrac{5}{6}, \tfrac{11}{12}, \tfrac{1}{1} \right\}.$$

There are:

$4 = \varphi(12)$ terms with denom. $= 12$;
$2 = \varphi(6)$ terms with denom. $= 6$;
$2 = \varphi(4)$ terms with denom. $= 4$;
$2 = \varphi(3)$ terms with denom. $= 3$;
$1 = \varphi(2)$ terms with denom. $= 2$;
$1 = \varphi(1)$ terms with denom. $= 1$.

$$12 = \sum_{d \mid 12} \varphi(d) \quad !! \;]$$

So

$$n = |S| = \left| \bigcup_{\substack{d \mid n \\ d \ge 1}} \left\{ k/d : 1 \le k \le d \text{ and } (k,d) = 1 \right\} \right|$$

$$= \sum_{d \mid n} \left| \left\{ k/d : 1 \le k \le d \text{ and } (k,d) = 1 \right\} \right|$$

$$= \sum_{d \mid n} \varphi(d),$$

since the union is disjoint. $\square$

Next: μ and φ are related by:

Thm. 2.3.

$$\varphi(n) = \sum_{d|n} \mu(d)\, n/d.$$

Proof.

We rewrite the definition

$$\varphi(n) = \sum_{\substack{k|n \\ (k,n)=1}} 1$$

in the form

$$\varphi(n) = \sum_{k=1}^{n} \left[\frac{1}{(n,k)} \right].$$

By Thm. 2.1, then,

$$\varphi(n) = \sum_{k=1}^{n} \sum_{d|(n,k)} \mu(d) = \sum_{k=1}^{n} \sum_{\substack{d|n \\ d|k}} \mu(d). \qquad (*)$$

Each summand on the right side of $(*)$, of course, equals $\mu(d)$ for some positive divisor d of n.

Question:

given such a d, how many times does $\mu(d)$ appear there?

Answer: $\mu(d)$ appears exactly when $\exists\, k \in \mathbb{Z}_+$ with $1 \le k \le n$ and $d|k$. This will happen exactly when $\exists\, q \in \mathbb{Z}_+$ with $dq = k$ for some $1 \le k \le n$. This will happen exactly when $dq \le n$, meaning $q \le n/d$. There are n/d such q.

So, by $(*)$,

$$\varphi(n) = \sum_{d|n} \mu(d) \cdot n/d. \qquad \square$$