Tuesday, October 29

Definition: An *arithmetic function* is a function $f: \mathbb{N} \to \mathbb{R}$.

Recall a property of the Euler phi-function: if $(m,n)=1$ then $\phi(mn) = \phi(m)\phi(n)$. From this we deduced

$$\phi(p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}) = \phi(p_1^{r_1})\phi(p_2^{r_2}) \cdots \phi(p_k^{r_k})$$
$$= p_1^{r_1-1}(p_1-1)\,p_2^{r_2-1}(p_2-1) \cdots p_k^{r_k-1}(p_k-1).$$

Notation: We say p^r *exactly divides* n, and we write $p^r \| n$, if $p^r \mid n$ and $p^{r+1} \nmid n$.

In this notation, $\phi(n) = \prod_{p^r \| n} \phi(p^r)$

$= \prod_{p^r \| n} p^{r-1}(p-1)$. [Side note: $\frac{\phi(n)}{n} = \prod_{p \mid n} \left(1 - \frac{1}{p}\right)$.]

Definition: An arithmetic function f, not identically 0, is *multiplicative* if $f(mn) = f(m)f(n)$ whenever $(m,n)=1$.

Equivalently, f is multiplicative if and only if $f(n) = \prod_{p^r \| n} f(p^r)$.

We say f is *totally multiplicative* if $f(mn) = f(m)f(n)$ for all $m, n \in \mathbb{N}$.

Example: Let $\tau(n)$ denote the number of (positive) divisors of n. Then $\tau(n)$ is multiplicative:

Proof 1: If $n = p_1^{r_1} \cdots p_k^{r_k}$, then all divisors of n are $p_1^{s_1} \cdots p_k^{s_k}$ where each $0 \le s_j \le r_j$; hence $\tau(n) = \prod_{p^r \| n} (r+1) = \prod_{p^r \| n} \tau(p^r)$.

Proof 2: HW #1 problem 2(a): $\{\text{divisors of } mn\} \overset{1-1}{\longleftrightarrow} \{(a,b) : a \mid m, b \mid n\}$ when $(m,n)=1$.

Example: Let $g(X) \in \mathbb{Z}[X]$, and let $\sigma_g(n)$ be the number of solutions to $g(X) \equiv 0 \pmod{n}$. We've seen that the Chinese remainder theorem implies σ_g is multiplicative.

Fact: If f is multiplicative, then f is determined by its values on prime powers. Conversely, we can set $f(p^r)$ to be anything we want for each p^r, and then extend f to a multiplicative function $f(n) = \prod_{p^r \| n} f(p^r)$.

Fact: If f is multiplicative, then $f(1) = 1$: choose $n \in \mathbb{N}$ with $f(n) \neq 0$; then $f(n) = f(1 \cdot n) \underset{\substack{\uparrow \\ \text{since } (1,n)=1.}}{=} f(1)f(n) \Rightarrow 1 = f(1)$.

More examples:

- For $\alpha \in \mathbb{R}$, define $e_\alpha(n) = n^\alpha$.

Then e_α is totally multiplicative.

Special cases:

- $1(n) = e_0(n) = n^0 = 1$.
- $id(n) = e_1(n) = n^1 = n$.
- $(\alpha \to -\infty)$ the iota function
$$\iota(n) = \begin{cases} 1, & \text{if } n=1, \\ 0, & \text{if } n \geq 2. \end{cases}$$

Example:

- $f(n) = (-1)^n$ is not multiplicative.
  - $f(1) = -1 \neq 1$
  - $-1 = (-1)^{15} = f(15)$ but $f(3)f(5) = (-1)^3(-1)^5 = +1$.
- $f(n) = (-1)^{n-1}$ is multiplicative (!).

Indeed $f(n) = \prod_{p^r \| n} f(p^r)$ with $f(p^r) = \begin{cases} -1, & \text{if } p=2, \\ 1, & \text{otherwise.} \end{cases}$