Thursday, October 31

Recall: $f : \mathbb{N} \to \mathbb{R}$ is <u>multiplicative</u> if $f(mn) = f(m)f(n)$ whenever $(m,n) = 1$.
f is <u>totally multiplicative</u> if $f(mn) = f(m)f(n)$ for all $m, n \in \mathbb{N}$.

<u>Notation</u>: Let $\omega(n)$ denote the number of distinct prime factors of n, and $\Omega(n)$ the number of prime factors of n counted with multiplicity.

<u>Example</u>: with $n = 720 = 2^4 3^2 5$, $\omega(720) = 3$ while $\Omega(n) = 4+2+1 = 7$.

<u>Exercise</u>: For any $C \in \mathbb{R}$, show that $C^{\omega(n)}$ is multiplicative, and $C^{\Omega(n)}$ is totally multiplicative.

<u>Theorem</u>: Let f be multiplicative, and define $F(n) = \sum_{d \mid n} f(d)$ (the sum is over all divisors of n). Then F is also multiplicative.

<u>Example</u>: take $f(n) = \mathbb{1}(n)$. Then
$$F(n) = \sum_{d \mid n} \mathbb{1}(d) = \sum_{d \mid n} 1 = \tau(n);$$
so this is a third proof that the number-of-divisors function is multiplicative.

<u>Proof</u>: Let $(m,n) = 1$; we need to prove that $F(mn) = F(m)F(n)$. By HW#1 problem 2(b), ✲ the divisors d of mn are in 1-to-1 correspondence with pairs (a,b) where $a \mid m$ and $b \mid n$ (and $ab = d$).

✲ since $(m,n) = 1$.

So

$$F(mn) = \sum_{d \mid mn}{}' f(d) = \sum_{\substack{a \mid m \\ b \mid n}}{}' f(ab).$$

Since $a \mid m$ and $b \mid n$, we have $(a,b) \mid (m,n) = 1$.

Hence since f is multiplicative,

$$F(mn) = \sum_{\substack{a \mid m \\ b \mid n}}{}' f(a)f(b) = \Big(\sum_{a \mid m}{}' f(a)\Big)\Big(\sum_{b \mid n}{}' f(b)\Big)$$

$$= F(m)F(n).$$

We might wonder whether the converse is true. More generally, how can we deduce information about f from info about F? We observe that given F, there's exactly one f such that $F(n) = \sum_{d \mid n}' f(d)$: $f(1) = F(1)$, while for $n \geq 2$, f is defined recursively by

$$f(n) = F(n) - \sum_{\substack{d \mid n \\ d < n}}{}' f(d). \quad (*)$$

<u>Exploration</u>: Let start with $F(n) = \iota(n)$, so that

$$\sum_{d \mid n}{}' f(d) = \iota(n) = \begin{cases} 1, & \text{if } n = 1, \\ 0, & \text{if } n \geq 2. \end{cases}$$

Some values:

- $n = 1$: $f(1) = \iota(1) = 1$.
- $n = 2$: $(*) \Rightarrow f(2) = \iota(2) - \sum_{\substack{d \mid 2 \\ d < 2}}' f(d)$

  $= 0 - f(1) = -1.$

More generally, $f(p) = \iota(p) - f(1) = -1$.

- $n = p^2$: $(*) \Rightarrow f(p^2) = \iota(p^2) - \sum_{\substack{d \mid p^2 \\ d < p^2}}' f(d)$

  $= \iota(p^2) - (f(1) + f(p))$

  $= 0 - (1 - 1) = 0.$

One can prove by induction that $f(p^k) = 0$ for all $k \geq 2$.

- $n = pq$: $(*) \Rightarrow f(pq) = \iota(pq) - (f(1) + f(p) + f(q))$

  $= 0 - (1 - 1 - 1) = 1.$
- $n = p^2 q$: $(*) \Rightarrow f(p^2 q) = \iota(p^2 q) - (f(1) + f(p) + f(p^2) + f(q) + f(pq)) = 0 - (1 - 1 + 0 - 1 + 1) = 0.$

Definition: The Möbius function $\mu(n)$ is the multiplicative function characterized by:
$$\mu(p^r) = \begin{cases} -1, & \text{if } r=1, \\ 0, & \text{if } r \geq 2. \end{cases}$$

In other words,
$$\mu(n) = \begin{cases} (-1)^{\omega(n)}, & \text{if } n \text{ is squarefree}, \\ 0, & \text{if } n \text{ is not squarefree}. \end{cases}$$

Theorem: $$\sum_{d \mid n} \mu(d) = \iota(n) = \begin{cases} 1, & \text{if } n=1, \\ 0, & \text{if } n \geq 2. \end{cases}$$

Note: this property of μ is used way more often than the actual definition.

Proof #1: ($n=1$ ✓) For $n \geq 2$:
$$\sum_{d \mid n} \mu(n) = \sum_{\substack{d \mid n \\ d \text{ squarefree}}} (-1)^{\omega(d)}.$$

If n has k distinct prime factors, then there are $\binom{k}{j}$ squarefree divisors d of n with $\omega(d) = j$. Therefore
$$\sum_{d \mid n} \mu(d) = \sum_{j=0}^{k} \binom{k}{j} (-1)^j$$
$$= (1 + (-1))^k = 0 = \iota(n).$$

Proof #2: Both $\iota(n)$ and $\sum_{d \mid n} \mu(d)$ are multiplicative (by the theorem earlier); so it suffices to show that they're equal on prime powers — but we've already done that in the exploration. //

Exhortation: Whenever we see we're about to do a "Proof 1" type proof — stop and look for a "Proof 2" type proof.

Theorem: (Möbius inversion formula)

Given $f: \mathbb{N} \to \mathbb{R}$, define $F(n) = \sum_{d|n}' f(d)$.

Then $f(n) = \sum_{d|n}' F(d)\mu(n/d)$.

Note: $\sum_{d|n}' F(d)\mu(n/d) = \sum_{\substack{c,d \in \mathbb{N} \\ cd = n}}' F(d)\mu(c)$

$= \sum_{c|n}' \mu(c) F(n/c) = \sum_{d|n}' \mu(d) F(\frac{n}{d})$.

Proof: By the definition of F,

$$\sum_{d|n}' \mu(d) F(n/d) = \sum_{d|n}' \mu(d) \sum_{b|n/d}' f(b)$$

$$= \sum_{\substack{b,d \in \mathbb{N} \\ bd|n}} \mu(d) f(b) = \sum_{b|n}' f(b) \sum_{d|n/b}' \mu(d)$$

$$= \sum_{b|n}' f(b)\, \iota(n/b)$$

$$= f(n)\cdot 1 + \sum_{\substack{b|n \\ b<n}}' f(b)\, 0 = f(n).$$

Exercise: The converse is also true.

Remark: This formula holds regardless of whether f, F are multiplicative.

Example: We've seen that $\sum_{d|n}' \phi(d) = n = id(n)$.

Then Möbius inversion tells us

$$\phi(n) = \sum_{d|n}' \mu(d)\, id(n/d)$$

$$= \sum_{d|n}' \mu(d) \frac{n}{d} \Rightarrow \frac{\phi(n)}{n} = \sum_{d|n}' \frac{\mu(d)}{d}.$$

(We can reconfirm this by checking on prime powers, since both sides are multiplicative: when $n = p^r$, $\frac{\phi(p^r)}{p^r} = 1 - \frac{1}{p}$, while

$$\sum_{d|p^r}' \frac{\mu(d)}{d} = \frac{\mu(1)}{1} + \frac{\mu(p)}{p} + \frac{\mu(p^2)}{p^2} + \cdots + \frac{\mu(p^r)}{p^r}$$

$$= \frac{1}{1} + \frac{-1}{p} + \frac{0}{p^2} + \cdots + \frac{0}{p^r} = 1 - \frac{1}{p}.)$$

Definition: The Dirichlet convolution of two arithmetic functions f and g, written $f*g$, is the arithmetic function defined by

$$(f*g)(n) = \sum_{d\mid n} f(d)\,g(n/d)$$

$$= \sum_{\substack{c,d \\ cd=n}} f(d)\,g(c) = \sum_{c\mid n} f(n/c)\,g(c)$$

$$= \sum_{d\mid n} g(d)\,f(n/d). \quad \cancel{= (g*f)(n).}$$

Notation practice:

- If $g=1$, then $(f*1)(n) = \sum_{d\mid n} f(d)\,1(n/d)$
$$= \sum_{d\mid n} f(d).$$

- We've seen that $\phi * 1 = id$ and $1*1=\tau$.

- Möbius inversion formula:
~~if~~ $F = f*1$, ~~then~~ if and only if $f = F*\mu$.

Theorem: If f and g are both multiplicative, then so is $f*g$.

Proof: Let $(m,n)=1$; we need to show that $(f*g)(mn) = (f*g)(m)\,(f*g)(n)$:

$$(f*g)(mn) = \sum_{d\mid mn} f(d)\,g(mn/d) \qquad [(m,n)=1 \Rightarrow (a,b)=1,\ (\tfrac{m}{a},\tfrac{n}{b})=1]$$

$$= \sum_{\substack{a\mid m\\ b\mid n}} f(ab)\,g(mn/ab)$$

$$= \sum_{\substack{a\mid m\\ b\mid n}} f(a)f(b)\,g\!\left(\frac{m}{a}\right)g\!\left(\frac{n}{b}\right)$$

$$= \left(\sum_{a\mid m} f(a)\,g\!\left(\frac{m}{a}\right)\right)\left(\sum_{b\mid n} f(b)\,g\!\left(\frac{n}{b}\right)\right)$$

$$= (f*g)(m)\cdot(f*g)(n). \quad \checkmark$$

Remark: We saw earlier that if f is multiplicative, then so is $F = f*1 = \sum_{d|n} f(d)$.

Now we can prove the converse: if $F = f*1$ is multiplicative, then by Möbius inversion $f = F*\mu$ is the Dirichlet convolution of two multiplicative functions, which we've just proved is itself multiplicative.

Example: Let $s(n)$ be the indicator function of squares: $s(n) = \begin{cases} 1, & \text{if } n \text{ is a square,} \\ 0, & \text{otherwise.} \end{cases}$

Let's identify $s*(\mu^2)$. (in fact, $\mu^2 = |\mu|$)

Note that s is multiplicative: in fact, $s(p^r) = \begin{cases} 1, & \text{if } r \text{ is even,} \\ 0, & \text{if } r \text{ is odd.} \end{cases}$

μ^2 is also multiplicative. Hence $s*(\mu^2)$ is also multiplicative.

On prime powers,

$$(s*\mu^2)(p^r) = \sum_{d|p^r} s\left(\frac{p^r}{d}\right)\mu^2(d)$$

$$= s(p^r)\mu^2(1) + s(p^{r-1})\mu^2(p) + s(p^{r-2})\mu^2(p^2) + \cdots$$

$$= s(p^r)\cdot 1 + s(p^{r-1})\cdot 1 + 0 + \cdots + 0$$

$$= s(p^r) + s(p^{r-1}) = 1.$$

We conclude that $s*\mu^2 = 1$ (constant).

Interpretation: μ^2 is the indicator function of squarefree numbers; hence

$$(s*\mu^2)(n) = \sum_{cd=n} s(c)\mu^2(d)$$

$$= \#\{cd=n : c \text{ is a square, } d \text{ is squarefree}\}$$

$$= 1.$$

Example: if $n = 2^1 3^2 5^3 7^4$, then $n = cd$ where $c = (3\cdot 5\cdot 7^2)^2$, $d = 2\cdot 5$.