Tuesday, November 5

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

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

Recall!

(Abstract algebra comments:

Let $A = \{\text{all } f: \mathbb{N} \to \mathbb{R}\}$. Then Dirichlet convolution $*$ is a commutative binary operation on A; and $\iota(n) = \begin{cases} 1, & \text{if } n=1, \\ 0, & \text{if } n \geq 2 \end{cases}$ is the identity element for $*$. A is a "monoid".

Let $A^\times = \{f \in A : f(1) \neq 0\}$. Then $A^\times$ is an abelian group under $*$: Inverses exist in $A^\times$ (HW #8 problem). In particular, μ is the inverse of 1 ($\mu * 1 = \iota$), which justifies Möbius inversion $F = f*1 \Leftrightarrow f = F*\mu$.

Technical note: $*$ is associative — we can show

$$((f*g)*h)(n) = \cdots = \sum_{bcd=n} f(b)g(c)h(d)$$
$$= \cdots = (f*(g*h))(n).$$

Bonus fact: $\{\text{all multiplicative functions}\}$ is a subgroup of $A^\times$.)

Let's practice some Dirichlet convolutions.

Recall $\sigma(n) = \sum_{d|n} d$ is the sum-of-divisors function.

<u>Example</u>: Prove that $\sigma(n) = \sum_{d|n} \phi(d)\tau(n/d)$.

($\tau(n) =$ # of divisors of n)

<u>Proof 1</u>: Both sides are multiplicative, so it suffices to check $\sigma(p^r) = \sum_{d|p^r} \phi(d)\tau(n/d)$.

r	0	1	2	3
$\sigma(p^r)$	1	$p+1$	p^2+p+1	p^3+p^2+p+1
$\phi(p^r)$	1	$p-1$	$p(p-1)$	$p^2(p-1)$
$\tau(p^r)$	1	2	3	4
$(\phi*\tau)(p^r)$	1	$(p-1)1 + 1\cdot 2$	$p(p-1) + 2(p-1) + 3$	$p^2(p-1)+2p(p-1)+3(p-1)+4$

(Computes $(f*g)(p^r)$ without knowing the answer ahead of time.)

Formally, we'd need to show

$$\sum_{j=0}^{r} p^j = \sigma(p^r) = \sum_{j=0}^{r} \phi(p^j)\tau(p^{r-j})$$

$$= 1(r+1) + \sum_{j=1}^{r} p^{j-1}(p-1)(r-j+1).$$

<u>Proof 2</u>:
$$\phi*\tau = \phi*(1*1)$$
$$= (\phi*1)*1$$
$$= id*1 = \sigma. \quad //$$

Observation: Dirichlet convolutions on prime powers looks like convolutions of sequences — the way we calculate coefficients of products of polynomials or of power series. In other words, if $h = f * g$ then we have the (formal) power series identity

$$\sum_{j=0}^{\infty} h(p^j)x^j = \left(\sum_{j=0}^{\infty} f(p^j)x^j\right)\left(\sum_{j=0}^{\infty} g(p^j)x^j\right).$$

Example: Recall that

$$s(n) = \begin{cases} 1, & \text{if } n \text{ is a square,} \\ 0, & \text{otherwise.} \end{cases}$$

Let's reprove that $s * (\mu^2) = 1$.

Solution: (all functions are multiplicative)

$$\sum_{j=0}^{\infty} s(p^j)x^j = 1 + 0x + 1x^2 + 0x^3 + 1x^4 + \cdots$$
$$= \frac{1}{1-x^2}.$$

$$\sum_{j=0}^{\infty} \mu^2(p^j)x^j = 1 + 1x + 0x^2 + 0x^3 + \cdots$$
$$= 1 + x.$$

And

$$\frac{1}{1-x^2}(1+x) = \frac{1}{1-x} = \sum_{j=0}^{\infty} 1x^j = \sum_{j=0}^{\infty} 1(p^j)x^j.$$

//