Möbius inversion and applications

Def. Let n be a positive integer.

We let $\mu(n) = \begin{cases} 1, & n \text{ is squarefree w/ an even number of prime factors} \\ -1, & \text{" " " " odd " " " "} \\ 0, & n \text{ is not squarefree} \end{cases}$

μ is the Möbius function

e.g. $\mu(1) = 1$

$\mu(p) = -1$

$\mu(4) = 0$

$\mu(10) = 1$

$\mu(30) = -1$

Thm (Möbius inversion). Let A be an additive group and $f, g : \mathbb{Z}^{\geq 1} \longrightarrow A$ be functions.

Suppose $g(n) = \sum_{d \mid n} f(d)$

Then $f(n) = \sum_{d \mid n} \mu(d) g\left(\frac{n}{d}\right)$.

Lemma 1. $\sum_{d|n} \mu(d) = \begin{cases} 1 & n=1 \\ 0 & n \neq 1 \end{cases}$

Pf. $\sum_{d|1} \mu(d) = \mu(1) = 1.$

Now suppose $n > 1$.

Let S be the set of all distinct prime factors of n.

Then $\{d | n : \mu(d) \neq 0\} \xleftrightarrow{\sim} P(S)$, the power set

$$\prod_{t \in T} t \longleftarrow T$$

$$d \longmapsto \{p \text{ prime} : p | d\}$$

Let $T \in P(S)$. $d = \prod t$ $\mu(d) = \begin{cases} 1 & |T| \text{ even} \\ -1 & |T| \text{ odd} \end{cases}$

So to get our cancellation, we prove the following:

Lemma 2. Let $S \neq \emptyset$ be finite. Then $P(S)$ contains the same number of even and odd cardinality elements.

Pf. Induct on $|S|$.

$|S| = 1$. $P(S) = \{\emptyset, S\}$.

$|S| > 1$. Fix $x \in S$. We know the result for $S - \{x\}$ by induction

$$P(S) = \{T \subseteq S \mid x \in T\} \amalg \underbrace{\{T \subseteq S \mid x \notin T\}}_{\parallel \; P(S - \{x\})}$$

$T \cup \{x\} \sim$ $T \mapsto T$, $P(S - \{x\})$

and we know the result for $P(S - \{x\})$

$T \longmapsto T$ preserves parity

$T \longmapsto T \cup \{x\}$ swaps parity

so by induction, lemma 2 holds. $\square$

Now, $$\sum_{d \mid n} \mu(d) = \sum_{\substack{T \subseteq S \\ |T| \text{ even}}} 1 + \sum_{\substack{T \subseteq S \\ |T| \text{ odd}}} -1$$

$$= 0 \qquad \square$$

Now we prove Möbius inversion.

Pf. $$\sum_{d \mid n} \mu(d)\, g\left(\frac{n}{d}\right) = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) g(d)$$

$$= \sum_{d \mid n} \mu\left(\frac{n}{d}\right) \sum_{e \mid d} f(e)$$

Let $d, e \mid n$. Then $e \mid d \iff \frac{n}{d} \,\Big|\, \frac{n}{e}$. Let $k = \frac{n}{d}$.

$$= \sum_{e \mid n} f(e) \underbrace{\sum_{k \mid \frac{n}{e}} \mu(k)}_{\substack{1 \quad n/e = 1 \\ 0 \quad \text{o/w}}} \text{ by lemma 1.}$$

$$= f(n) \qquad \square$$

Applications

i) Let F be a finite field.

Let $\varphi(k) = \left|\{1 \le a \le k \mid (a,k)=1\}\right|$, the Euler totient.

Let $\psi(k) = \left|\{x \in F^\times \mid \operatorname{ord}(x) = k\}\right|$

Let $n = |F^\times|$. For $d \mid n$, $\{x \in F^\times \mid x^d = 1\}$ is a subgroup of $F^\times$.

Furthermore, as F is a field and $(d, \operatorname{char}(F)) = 1$, $x^d - 1$ has exactly d solutions.

So $\sum_{e \mid d} \psi(e) = d$. Möbius inversion shows then that

$$\psi(d) = \sum_{e \mid d} \mu(e) \frac{d}{e}$$

OTOH, $\varphi(k) = \#$ generators of a cyclic group of k elements.

If $d \mid n$, $\frac{d}{e} \mathbb{Z}/d\mathbb{Z}$ is the unique cyclic subgroup of order e in $\mathbb{Z}/d\mathbb{Z}$,

so $\varphi(e) = \#$ elements of $\mathbb{Z}/d\mathbb{Z}$ of order e

Thus, $\sum_{e \mid d} \varphi(e) = d$, so $\varphi(d) = \sum_{e \mid d} \mu(e) \frac{d}{e}$

So $\psi(d) = \varphi(d)$ $\forall d \mid n$. Hence, $\psi(n) = \varphi(n) \neq 0$ so there is an element of order n in $F^\times$. So $F^\times$ is cyclic.

ii) Let $\Phi_d(t) = \prod_{k \in (\mathbb{Z}/n\mathbb{Z})^\times} (t - \zeta_n^k)$ for ζ_n a primitive n^{th} root of unity / $\mathbb{Q}$, e.g. $e^{2\pi i/n}$.

By HW28, $\Phi_d(t) \in \mathbb{Z}[t]$ (and is in fact irreducible).

We call it the d^{th} cyclotomic polynomial.

Then $\prod_{d|n} \Phi_d(t) = t^n - 1$

By Möbius inversion,

$$\Phi_n(t) = \prod_{d|n} (x^d - 1)^{\mu(n/d)}$$

iii) Using HW10, we can show that $t^{p^n} - t$ is the product of all irreducible monic polynomials in $\mathbb{F}_p[t]$ of degree dividing n.

Let $\psi(n) = |\{f \in \mathbb{F}_p[t] \text{ deg } n \text{ irreducible}\}|$.

Then $p^n = \sum_{d|n} d\,\psi(d)$

So by Möbius inversion, $n\psi(n) = \sum_{d|n} \mu(d) p^{n/d}$

So $\psi(n) = \frac{1}{n} \sum_{d|n} \mu(d) p^{n/d}$.

Dirichlet Series

Let $f: \mathbb{Z}^{\geq 1} \longrightarrow \mathbb{C}$.

We define its associated Dirichlet Series to be

$$\hat{f}(s) = \sum_{n \geq 1} \frac{f(n)}{n^s}$$

e.g. let $\mathbb{1}(n) = 1$. Then its associated Dirichlet Series is

$$\zeta(s) = \sum_{n \geq 1} \frac{1}{n^s}$$

the Riemann zeta function.

Def. Let $f, g: \mathbb{Z}^{\geq 1} \longrightarrow A$.

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

This is called Dirichlet convolution.

Fact. Let $f, g: \mathbb{Z}^{\geq 1} \longrightarrow \mathbb{C}$. Then

$$\widehat{f * g} = \hat{f}\, \hat{g}$$

i.e. $$\sum_{n \geq 1} \frac{\sum_{d \mid n} f(d)\, g(n/d)}{n^s} = \left(\sum_{n \geq 1} \frac{f(n)}{n^s} \right) \left(\sum_{n \geq 1} \frac{g(n)}{n^s} \right)$$

Lemma 1 says $\mathbb{1} * \mu = \delta$, where $\delta(n) = \begin{cases} 1 & n=1 \\ 0 & o/w \end{cases}$

Hence, $$\frac{1}{\zeta(s)} = \sum_{n \geq 1} \frac{\mu(n)}{n^s}.$$

Rmk. $\{f : \mathbb{Z}^{\geq 1} \longrightarrow \mathbb{C}\}$ is an additive group under pointwise addition.

$*$ makes it into a commutative ring w/ identity δ.

Möbius inversion says that if $g = f * \mu$ then $f = g * \mathbb{1}$.

Indeed, this follows from $\mathbb{1} * \mu = \delta$ and that δ is the multiplication identity.

Now, consider $$\frac{d}{ds}\hat{f}(s) = \frac{d}{ds} \sum_{n \geq 1} \frac{f(n)}{n^s}$$
$$= \sum_{n \geq 1} \frac{d}{ds} \frac{f(n)}{n^s}$$
$$\frac{d}{ds}\left(\frac{1}{n}\right)^s = \log\left(\frac{1}{n}\right)\left(\frac{1}{n}\right)^s$$
$$= \sum_{n \geq 1} \frac{-\log(n) f(n)}{n^s}$$

So $$\frac{d}{ds}\hat{f} = \widehat{(-\log(n) f(n))}$$

Hence, $\zeta'(s) = \sum_{n \geq 1} \frac{-\log(n)}{n^s}$

$\frac{1}{\zeta}(s) = \sum_{n \geq 1} \frac{\mu(n)}{n^s}$

Thus $\frac{\zeta'}{\zeta}(s) = \sum_{n \geq 1} \frac{-(\mu * \log)(n)}{n^s}$

Let $\Lambda(n) = \begin{cases} \log(p) & n = p^k \\ 0 & o/w \end{cases}$, p prime, $k \geq 1$

Then FTA $\iff \log(n) = \sum_{d \mid n} \Lambda(d)$

$\therefore \Lambda = -(\mu * \log)$

So $\frac{\zeta'}{\zeta}(s) = \sum_{n \geq 1} \frac{\Lambda(n)}{n^s}$

Λ is the von Mangoldt function.

Fact. $\sum_{n \leq x} \Lambda(n) = x + O_\varepsilon(x^{1/2+\varepsilon})$ $\forall \varepsilon > 0$

is equivalent to the Riemann hypothesis!