Math 312, Lecture 14, 6/6/2018

Last time: ① Arith. fcn: $f: \mathbb{Z}_{\geq 1} \to \mathbb{R}$ (or $\mathbb{C}$)

Can be added $(f+g)(n) = f(n) + g(n)$

convolved: $(f*g)(n) = \sum_{d|n} f(d)\, g\left(\frac{n}{d}\right) = \sum_{d\cdot e = n} f(d)\, g(e)$

(e.g. $\sum_{d|n} f(d) = (f*I)(n)$ where $I(n) = 1$)

② f is multiplicative if $(m,n)=1 \to f(mn) = f(m)f(n)$
(completely so if $f(mn) = f(m)f(n)$ for all m,n)

③ Thm: (1) f, g mult. $\Rightarrow f*g$ mult.

(2) $f * \delta = f$ where $\delta(n) = \begin{cases} 1 & n=1 \\ 0 & n>1 \end{cases}$

(3) $f = g * I \Rightarrow g = f * \mu$, $\mu(n) = \begin{cases} (-1)^{\omega(n)} & n \text{ sqr free} \\ 0 & \text{else} \end{cases}$

④ Examples: $\tau = I * I$ $\left(\tau(n) = \sum_{d|n} 1\right)$ "divisor function"

$\sigma = I * N$ $\left(\sigma(n) = \sum_{d|n} d\right)$ $(N(n) = n)$

$N = \phi * I$ $\left(\sum_{d|n} \phi(d) = n\right)$

warning: I completely mult but τ is not; $\tau(p^2) = 3 \neq (\tau(p))^2 = 4$

Ex: $((f*g)*h)(n) = (f*(g*h))(n) = \sum_{a\cdot b\cdot c = n} f(a)\, g(b)\, h(c)$

$f*g = g*f$, $f*(g+h) = f*g + f*h$

Applying thm:

τ is mult. $(\tau = I * I,\ I$ is mult$)$

σ " " $(\sigma = N * I,\ N, I$ are mult$)$

ϕ = " " $(\phi = \mu * I,\ \mu, I$ are mult$)$

(last also has combinatorial pf: under CRT bijection

$$\mathbb{Z}/mn\mathbb{Z} \leftrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

invertible residues mod mn correspond to pairs of invertible residues)

Today: ① Proof of thms

② Example: perfect numbers

Thm: Let f, g be mult. Then so is $f * g$

Pf: Let $(m,n)=1$. Then

$$(f*g)(mn) = \sum_{d \cdot e = mn} f(d)\, g(e) \qquad (*)$$

Key point: $\left\{ \begin{array}{c} \text{divisors} \\ \text{of } mn \end{array} \right\} \underset{\text{bijection}}{=} \left\{ d_1 \cdot d_2 : \begin{array}{c} d_1 \mid m \\ d_2 \mid n \end{array} \right\} \overset{1:1}{\longleftrightarrow} \left\{ \begin{array}{c} \text{divisors} \\ \text{of } m \end{array} \right\} \times \left\{ \begin{array}{c} \text{divisors} \\ \text{of } n \end{array} \right\}$

Eg: $60 = 15 \cdot 4$ every divisor of 60 comes from a divisor of 15 + a divisor of 4.

In the sum $(*)$ both d, e are divisors of mn,

so $d = d_1 \cdot d_2$, $e = e_1 \cdot e_2$ where $d_1, e_1 \mid m$, $d_2, e_2 \mid n$

Take-away: studied divisors of m, mn via prime factorization by counting occurences of each prime

---

Möbius inversion

Recall $\delta(n) = \begin{cases} 1 & n=1 \\ 0 & n>1 \end{cases}$ For any f,

$$\cancel{(f*\delta)(n)} = (\delta * f)(n) = \delta(1)\cdot f(n) + \sum_{\substack{d|n \\ d>1}} \delta(d) f(\tfrac{n}{d})$$

$$= 1\cdot f(n) + \sum_{\substack{d|n \\ d>1}} 0 \cdot f(\tfrac{n}{d})$$

$$= f(n)$$

ie $\delta * f = f$

Say "δ is an identity for convolution".

Now say f,g are <u>inverse</u> if $f*g=\delta$

<u>Ex</u>: An arithmetic fcn f is invertible iff $f(1)$ is invertible. (ie. $f(1)\neq 0$) (neccesary since $(f*g)(1) = f(1)g(1)$)

<u>Thm</u>: $\mu * I = \delta$, ie μ and I are inverse to each other

$\Leftrightarrow$ if $f = g*I$ then $g = f*\mu$

<u>Pf</u>: Recall $I(n)=1$ for all n, $\mu(n) = \begin{cases} (-1)^{\omega(n)} & n \text{ squarefree} \\ 0 & p^2|n \end{cases}$

where $\omega(n) = \#$ distinct primes dividing n

<u>claim</u>: μ is multiplicative

<u>Pf</u>: Say m, n are relatively prime.

If $p^2 | mn$ then p^2 divides either m or n (p does not divide both)

Then $\mu(mn) = 0$, $\mu(m) \overset{=0}{} \text{ or } \mu(n) = 0$ and

$$\mu(mn) = \mu(m)\mu(n)$$

Else mn is a pdt of distinct primes. But then m, n are pdts of distinct primes, with no overlap, so

$$\omega(mn) = \omega(m) + \omega(n)$$

$$\mu(mn) = (-1)^{\omega(mn)} = (-1)^{\omega(m)+\omega(n)} = (-1)^{\omega(m)}(-1)^{\omega(n)}$$

$$= \mu(m)\mu(n)$$

Now $mn = d\cdot e = d_1 d_2 e_1 e_2 = (d_1 e_1)\cdot(d_2 \cdot e_2)$

For a prime p dividing m (say k times)

say p occurs α times in d, β times in e. Then $\alpha+\beta=k$

Then p occurs α times in d_1, β times in e_1 (because p does not occur in d_2, e_2) so p occurs $\alpha+\beta=k$ times in $d_1 e_1$. This is true for <u>all</u> primes dividing m, so $m \mid d_1 e_1$

Conversely, primes not occuring in m do not occur in d_1, e_1 so $\boxed{m = d_1 e_1}$; by symmetry $\boxed{n = d_2 e_2}$

Bottom line: bijection:

$$\left\{\begin{matrix}\text{factorizations}\\ mn = d\cdot e\end{matrix}\right\} \longleftrightarrow \left\{\begin{matrix}\text{factorizations}\\ m = d_1 e_1\end{matrix}\right\} \times \left\{\begin{matrix}\text{factorizations}\\ n = d_2 \cdot e_2\end{matrix}\right\}$$

(bijection: $(d,e) \to (d_1, d_2, e_1, e_2)$)

where $d = d_1 d_2$, $e = e_1 e_2$

so $(f*g)(mn) = \sum\limits_{d e = mn} f(d) g(e) = \sum\limits_{\substack{d_1 e_1 = m \\ d_2 \cdot e_2 = n}} f(d_1 d_2)\, g(e_1 e_2)$

$$= \sum_{\substack{d_1 e_1 = m \\ d_2 e_2 = n}} f(d_1) f(d_2) g(e_1) g(e_2)$$

($d_1 | m$, $d_2 | n$ so $(d_1, d_2) | (m,n$ $\Rightarrow$ f, g mult.

$$= \sum_{\substack{d_1 e_1 = m \\ d_2 \cdot e_2 = n}} \big(f(d_1) g(e_1)\big)\big(f(d_2) g(e_2)\big)$$

$$= \Big(\sum_{d_1 e_1 = m} f(d_1) g(e_1)\Big)\Big(\sum_{d_2 e_2 = n} f(d_2) g(e_2)\Big)$$

$= \big((f*g)(m)\big)\cdot\big((f*g)(n)\big)$ ∎