Math 312, lecture 13, 5/6/2018

(0) Admin

Today: (1) Review

(2) Arithmetical functions

So far

① Integers: Well-ordering, division thm, gcd, unique factorization, divisibility, Diophantine equations

② Congruences: modular arithmetic, modular inverse, equations in congruence, CRT

③ The multiplicative group: multiplication, exponentiation, multiplicative order, Fermat's little thm, Euler's thm.

Def: $\phi(m) = \#U(m) = \#\{0 \le a < m \mid (a,m)=1\}$ = number of invertible residues mod m

Euler: $(a,m)=1 \Rightarrow a^{\phi(m)} \equiv 1 \ (m)$

Now: ④ Arithmetical functions

⑤ Cryptography and RSA

Arithmetic functions

Def: An arithmetic function is a function $f: \mathbb{Z}_{\geq 1} \to \mathbb{R}$ (or $\mathbb{C}$)

Example: (any sequence)

(1) $I(n) = 1$ for all n, $N(n) = n$ for all n

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

(2) $\tau(n)$ = divisor fcn $= \#\{d \geq 1 \mid d|n\}$

$\tau(1)=1,\ \tau(p)=2,\ \tau(4)=3,\ \tau(6)=4,\ \ldots$

(3) $\sigma(n)$ = sum of divisors $= \sum_{d|n} d$

(4) $P(n) = \begin{cases} 1 & n \text{ prime} \\ 0 & n \text{ composite} \end{cases}$ (indicator function of the primes)

($\Rightarrow$ prime counting fcns $\pi(x) = \sum_{n \leq x} P(n)$ not arithmetic: defined for $x \in \mathbb{R}$)

von-Mangoldt fcn: $\Lambda(n) = \begin{cases} \log p & n = p^e \text{ prime power} \\ 0 & n \text{ not prime power} \end{cases}$

$\Lambda(2) = \Lambda(4) = \Lambda(8) = \log 2$

$\Lambda(6) = 0$

Ex: $\sum_{d|n} \Lambda(d) = \log n$ ($\Leftrightarrow$ unique factorization)

($\Rightarrow$ prime-counting Ψ-fcn $\Psi(x) = \sum_{n \leq x} \Lambda(n)$)

(5) $\omega(n) = \#\{p \text{ prime} \mid p|n\}$: $\omega(2) = \omega(4) = \omega(8) = 1$

$\omega(6) = \omega(12) = 2$

If $n = \prod_p p^{e_p}$ set $\Omega(n) = \sum_p e_p$ = total # of prime divisors

$\Omega(2)=1, \Omega(4)=2, \Omega(8)=3$

$\Omega(6)=2, \Omega(12)=3$

$\Omega(1)=0, \Omega(4)=2, \Omega(8)=3$

$\Omega(8)=3, \Omega(12)=3$

From this: Möbius fcn $\mu(n) = \begin{cases} (-1)^{\omega(n)} & \text{if } n \text{ is squarefree} \\ 0 & \text{else} \end{cases}$ ($p^2 \nmid n$)

$\mu(p) = -1$, $\mu(pq) = 1$ ($p \neq q$ primes)

$\mu(pq^2) = 0$ $\quad \mu(2) = \mu(3) = -1$

$\mu(6) = 1$ $\quad \mu(12) = 0$

Liouville fcn: $\lambda(n) = (-1)^{\Omega(n)}$ $\quad \lambda(p^2) = 1$

but $\mu(p^2) = 0$

Intuition: $\mu(n)$, $\lambda(n)$ "sequence of random coin tosses".

Fact: $\frac{1}{x} \sum_{n \le x} \mu(n) \to 0 \iff$ PNT: $\pi(x) \sim \frac{x}{\log x}$

Conj: $\left| \sum_{n \le x} \mu(n) \right| \le \sqrt{x}$ ("Riemann hypothesis")

(6) $\phi(n) = \#\{a \bmod m \mid (a,m) = 1\}$ ("Euler's totient function")

Two phenomena (1) Often see sums $\sum_{d \mid n} f(n)$

(2) Often can compute $f(n)$ from prime factorization, each p^{ep} contributes separately.

Multiplicative functions

Def: Call f **multiplicative** if $f(mn) = f(m)f(n)$ **whenever** $(m,n)=1$

(**completely multiplicative** if $f(mn)=f(m)f(n)$ for all $m,n \geq 1$)

Remark: Often has to do with CRT

Examples: - $I(n)=1$, $N(n)=n$, $\delta(n)=\begin{cases}1 & n=1\\ 0 & n>1\end{cases}$ completely mult.

- $\lambda(n)$ ($\Omega(mn)=\Omega(m)+\Omega(n)$)

total # of prime divisors of mn = sum of totals for m,n

- $\chi_4(n)=\begin{cases}1 & n\equiv 1 \pmod 4\\ -1 & n\equiv -1 \pmod 4\\ 0 & n\equiv 0 \pmod 2\end{cases}$ same

---

- $\tau(n)$, $\sigma(n)$, $\phi(n)$ all multiplicative. (pf later)

Lemma: f multiplicative. Either $f(n)=0$ and $f(n)=0$ for all n or $f(1)=1$

Pf: $1=1\cdot 1$ and $(1,1)=1$ so $f(1)=f(1\cdot 1)=f(1)f(1)$

only real numbers to satisfy $x=x^2$ are $x=0, 1$

If $f(1)=0$ then $f(n)=f(n\cdot 1)=f(n)f(1)=f(n)\cdot 0=0$ ($(n,1)=1$)

Prop: Let f be multiplicative, $n = \prod_p p^{e_p}$. Then

$$f(n) = \prod_p f(p^{e_p}) = \prod_{p \mid n} f(p^{e_p})$$

Pf: By induction on # primes dividing n

$$f(60) = f(2^2 \cdot 3 \cdot 5) = f((2^2 \cdot 3) \cdot 5) = f(2^2 \cdot 3) \cdot f(5) = f(2^2) \cdot f(3) \cdot f(5)$$

Example: $\phi(p^e) = \#\{a \bmod p^e \mid (a, p^e) = 1\}$

$e \geq 1$ $= \#\{1 \leq a \leq p^e \mid p \nmid a\} = p^e - \#\{a \mid p \mid a\}$

or $0 \leq a \leq p^e - 1$ $= p^e - p^{e-1} = p^e\left(1 - \frac{1}{p}\right)$

(roughly $\frac{1}{p}$ of integers are divisible by p, $1 - \frac{1}{p}$ are not)

So $\phi(n) = \phi\left(\prod_p p^{e_p}\right) = \prod_{p \mid n} \left(p^{e_p} \cdot \left(1 - \frac{1}{p}\right)\right) = \left(\prod_{p \mid n} p^{e_p}\right) \cdot \prod_{p \mid n} \left(1 - \frac{1}{p}\right)$

need $e_p \geq 1$ $= n \cdot \prod_{p \mid n} \left(1 - \frac{1}{p}\right)$

$\phi(12) = 12 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{3}\right) = 12 \cdot \frac{1}{2} \cdot \frac{2}{3} = 4$ (at home: enumerate the residues)

Def: the multiplicative (or Dirichlet) convolution of f, g is the function

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

Example: $\tau(n) = \sum_{d|n} 1 = \sum_{d|n} I(d)\cdot I\left(\frac{n}{d}\right) = (I*I)(n)$

(τ: divisor fcn; $I(n) \equiv 1$)

Example: $f = (\phi * I)$:

$f(1) = \phi(1)\cdot I(1) = 1\cdot 1 = 1$

$f(p) = \phi(1)\cdot I(p) + \phi(p) I(1) = 1\cdot 1 + (p-1)\cdot 1$

$= p$

($p = 1\cdot p = p\cdot 1$)

$f(p^2) = \phi(1)\cdot I(p^2) + \phi(p)\cdot I(p) + \phi(p^2)\cdot I(1) =$

$= 1\cdot 1 + (p-1)\cdot 1 + (p^2-p)\cdot 1$

$= (p^2-p) + (p-1) + 1 = p^2$

($p^2 = 1\cdot p^2 = p\cdot p = p^2\cdot 1$)

$f(pq) = \phi(1)\cdot I(pq) + \phi(p) I(q) + \phi(q) I(p) + \phi(pq)\cdot I(1)$

$= 1\cdot 1 + (p-1) + (q-1) + (pq - q - p + 1)$

(pq: all classes mod pq; q: classes $\equiv 0 (p)$; p: classes $\equiv 0 (q)$; 1: class 0, counted twice)

$= pq - q - p + p + q + 1 + 1 - 1 - 1 = pq$

Thm: $\phi * I = N$, i.e. $\sum_{d|n} \phi(d) = n$

Pf: Consider $\$ * \phi$, i.e. $\sum_{d|n} \phi\left(\frac{n}{d}\right)$

Let A be the set of residue classes mod n
(also know $\#A = n$) For $d|n$ let $A_d = \{a \bmod n \mid (a,n) = d\}$

(Euclid: (a,n) depends only on class of a mod n)

(or: $A = \{1, 2, 3, \ldots, n\}$, $A_d = \{1 \le a \le n \mid (a,n) = d\}$)

each element of A belongs to exactly one A_d, so

$$n = \#A = \sum_{d|n} \#A_d$$

What is $\#A_d$? $A_d = \{a \bmod n \mid (a,n) = d\}$

but if $a \in A_d$ $\left(\frac{a}{d}, \frac{n}{d}\right) = 1$

conversely, if $(a', \frac{n}{d}) = 1$ then $(d \cdot a', n) = d$

So $\#A_d$ = #residues prime to $\frac{n}{d}$ $= \phi\left(\frac{n}{d}\right)$

In other words, $n = \sum_{d|n} \phi\left(\frac{n}{d}\right) = \sum_{d|n} \phi(d)$.

Thm: If f, g multiplicative, so is $f * g$.

Thm: (Möbius inversion) (1) $\delta * f = f$

(2) $\mu * I = \delta$

Cor: $\tau(n), \sigma(n)$ mult: $\tau = I * I$, $\sigma = I * N$ (I, N completely mult)

Cor: $\phi(n)$ mult:

$$\phi * I = N$$

$$\Downarrow$$

$$\phi * I * \mu = N * \mu$$

$I * \mu = \delta$, $\delta * \phi = \phi$

$$\phi = \phi * \delta \overset{(1)}{=} N * \mu$$

both N, μ mult.