Number Theory, Lecture 3

Arithmetical functions, Dirichlet convolution, Multiplicative functions, Möbius inversion

Jan Snellman[1]

[1]Matematiska Institutionen
Linköpings Universitet

TEKNISKA HÖGSKOLAN
LINKÖPINGS UNIVERSITET

Summary

Summary

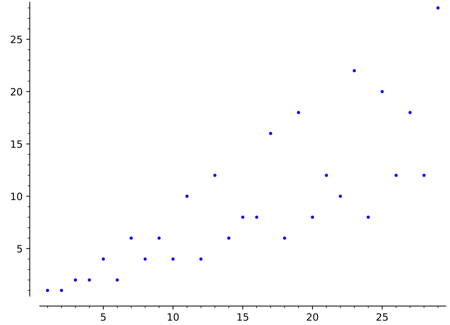
Summary

Definition

An *arithmetical function* is a function $f : \mathbb{P} \to \mathbb{C}$.

We will mostly deal with integer-valued a.f.

Euler ϕ is one:



Arithmetical functions defined by prime factorization

$$n = p_1^{a_1} \cdots p_r^{a_r}, \quad q_i \text{ distinct primes}$$

Liouville function λ, Möbius function μ:

$$\omega(n) = r$$
$$\Omega(n) = a_1 + \cdots + a_r$$
$$\lambda(n) = (-1)^{\Omega(n)}$$
$$\mu(n) = \begin{cases} \lambda(n) & \omega(n) = \Omega(n) \\ 0 & \text{otherwise} \end{cases}$$

Arithmetical functions related to divisors

d number of divisors, σ sum of divisors, and you know Euler ϕ.

$$d(n) = \sum_{k|n} 1$$

$$\sigma(n) = \sum_{k|n} k$$

$$\phi(n) = \sum_{\substack{1 \le k < n \\ \gcd(k,n)=1}} 1$$

Even more Arithmetical functions

p prime. Von Mangoldt function Λ, prime-counting function π, Legendre symbol $\left(\frac{n}{p}\right)$, p-valuation v_p.

$$\Lambda(n) = \begin{cases} \log q & n = q^k,\ q \text{ prime} \\ 0 & \text{otherwise} \end{cases}$$

$$\pi(n) = \sum_{\substack{1 \le k \le n \\ k \text{ prime}}} 1$$

$$\left(\frac{n}{p}\right) = \begin{cases} 0 & n \equiv 0 \mod p \\ +1 & n \not\equiv 0 \mod p \text{ and exists } a \text{ such that } n \equiv a^2 \mod p \\ -1 & n \not\equiv 0 \mod p \text{ and exists no } a \text{ such that } n \equiv a^2 \mod p \end{cases}$$

$$v_p(n) = k,\ p^k | n,\ p^{k+1} \not| n$$

Important arithmetical functions (not standard notation)

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

$$\mathbf{0}(n) = 0$$

$$\mathbf{1}(n) = 1 \qquad \text{often denoted by } \zeta$$

$$\mathbf{I}(n) = n$$

$$\mathbf{e}_i(n) = \begin{cases} 1 & n = i \\ 0 & n \neq i \end{cases}$$

Definition

Let f, g be arithmetical functions. Then their *Dirichlet convolution* is another a.f., defined by

$$(f * g)(n) = \sum_{\substack{1 \le a,b \le n \\ ab=n}} f(a)g(b) = \sum_{\substack{1 \le k \le n \\ k|n}} f(k)g(n/k) = \sum_{\substack{1 \le \ell \le n \\ \ell|n}} f(n/\ell)g(\ell) \qquad \text{(DC)}$$

Example

$$(f * g)(10) = f(1)g(10) + f(2)g(5) + f(5)g(2) + f(10)g(1)$$

The algebra of aritmetical functions

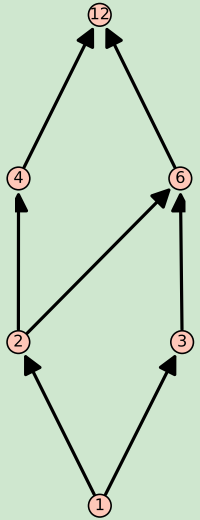
- $f * (g * h) = (f * g) * h$
- $f * g = g * f$
- There is a unit for this multiplication, $\mathbf{e}(1) = 1$, $\mathbf{e}(n) = 0$ for $n > 1$
- Not all a.f. are invertible
- We can add: $(f + g)(n) = f(n) + g(n)$
- We can scale: $(cf)(n) = cf(n)$
- $\mathbf{0}(n) = 0$ is a zero vector
- A $\mathbb{C}$-vector space with multiplication; an *algebra*.

Matrix interpretation

- Let $n \in \mathbb{P}$ and $D(n) = \{ 1 \leq k \leq n | k | n \}$ be its divisors
- We want to understand a.f. restricted to $D(n)$, in particular their multiplication
- Given a.f. f, form matrix A with rows and columns indexed by elems in $D(n)$, and $A_{ij} = f(j/i)$ if $i|j$, 0 otherwise
- Similarly for a.f. g and matrix B
- Then AB is the matrix for $f * g$

Example

- $n = 12$, $D(n)$ as follows



-

- $f = \mathbf{1}$
- $A = \mathbf{??}$
- $A * A = \mathbf{??}$

Summation

- $F(n) = (\mathbf{1} * f)(n) = \sum_{k|n} f(k)$
- The summation of f
- Sometimes F is known and we want to recover f
-

$$
\begin{aligned}
F(1) &= f(1) \\
F(2) &= f(1) + f(2) \\
F(3) &= f(1) + f(3) \\
F(4) &= f(1) + f(2) + f(4) \\
&\vdots
\end{aligned}
$$

Inverses

Theorem

f has inverse $g = f^{-1}$ iff $f(1) \neq 0$

Proof.

Want $f * g = e$, so $(f * g)(m) = 1$ if $m = 1$, 0 otherwise. Gives

$$\begin{aligned}
1 &= (f*g)(1) = f(1)g(1) \\
0 &= (f*g)(2) = f(1)g(2) + f(2)g(1) \\
0 &= (f*g)(3) = f(1)g(3) + f(3)g(1) \\
0 &= (f*g)(4) = f(1)g(4) + f(2)g(2) + f(4)g(1) \\
0 &= (f*g)(5) = f(1)g(5) + f(5)g(1) \\
&\vdots \\
0 &= (f*g)(n) = f(1)g(n) + \sum_{\substack{k|n \\ 1<k\leq n}} f(k)g(n/k)
\end{aligned}$$

so, by induction, we can solve for $g(n)$. □

Normed algebra

Definition

If $f \neq \mathbf{0}$, then the *order* of f is

$$\mathrm{ord}(f) = \min\{\, n | f(n) \neq 0 \,\}$$

and the *norm*

$$\|f\| = 2^{-\mathrm{ord}(f)}$$

Lemma

- *$f = \sum_n f(n) e_n$, i.e., the partial sums of this sum converge to f*
- *if $f(1) = 0$ then $e + f$ is invertible, with inverse given by convergent geometric series:*

$$\frac{e}{e+f} = e - f + f * f - f * f * f + \cdots$$

Definition

- f is *totally multiplicative* if $f(nm) = f(n)f(m)$
- f is *multiplicative* if $f(nm) = f(n)f(m)$ whenever $\gcd(n, m) = 1$

Theorem

Let $n = \prod_j p_j^{a_j}$, prime factorization. Then

- *If f mult then $f(n) = \prod_j f(p^j)$, i.e., f is determined by its values at prime powers*
- *If f tot mult then $f(n) = \prod_j f(p)^j$, i.e., f is determined by its values at primes*

Proof.

Obvious! □

Theorem

The Euler ϕ function is multiplicative.

Proof

Let $\gcd(m,n) = 1$. Want to prove $\phi(mn) = \phi(m)\phi(n)$, in other words,

$$|\mathbb{Z}_{mn}| = |\mathbb{Z}_m|\,|\mathbb{Z}_n| \tag{1}$$

Claim: following bijection:

$$\mathbb{Z}_{mn} \ni [a]_{mn} \mapsto ([a]_m, [a]_n) \in \mathbb{Z}_m \times \mathbb{Z}_n \tag{2}$$

Proof.

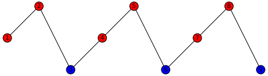
- Well-defined, since $a \equiv a' \mod mn$ implies $a \equiv a' \mod m$ and $a \equiv a' \mod n$.
- Injective, since $a \equiv a' \mod m$ and $a \equiv a' \mod n$ implies $a \equiv a' \mod mn$
- Surjective, by the CRT: take c, d, then exists x with

$$x \equiv c \mod m$$
$$x \equiv d \mod n$$

so $[x]_{mn} \mapsto ([c]_m, [d]_n)$

□

1. Take p prime
2. Then all $1 \leq a < p$ relatively prime to p, so $\phi(p) = p - 1$
3. Now consider prime power p^r
4. For $1 \leq a < p^r$, $\gcd(a, p^r) > 1$ iff $p|n$
5. Example: $p = 3$, $r = 2$:



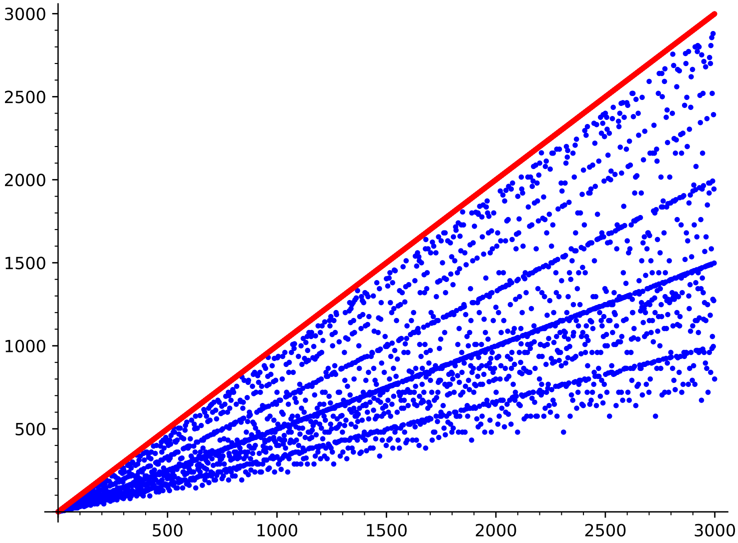
6. So $\phi(p^r) = p^r - \frac{p^r}{p} = p^r \left(1 - \frac{1}{p}\right)$
7. For $n = p_1^{r_1} \cdots p_s^{r_s}$, we have by multiplicativity

$$\begin{aligned} \phi(p_1^{r_1} \cdots p_s^{r_s}) &= \phi(p_1^{r_1}) \cdots \phi(p_s^{r_s}) \\ &= p_1^{r_1} \cdots p_s^{r_s} (1 - 1/p_1) \cdots (1 - 1/p_s) \\ &= n \prod_j (1 - 1/p_j) \end{aligned}$$

Example

- $\phi(15) = \phi(3)\phi(5) = 2 * 4 = 8$
- $\phi(16) = \phi(2^4) = 2^4 - 2^3 = 8$
- $\phi(120) = \phi(2^3 * 3 * 5) = 120(1 - 1/2)(1 - 1/3)(1 - 1/5) = 120 * (4/15) = 32.$

$n = p$ gives $\phi(n) = n - 1$. This is visible in graph of $\phi(n)$.



Theorem

f, g (non-zero) multiplicative arithmetical functions, $h = f * g$

1. $\mathbf{e}$ *is multiplicative*
2. $f(1) = 1$, *so f is invertible*
3. *h is multiplicative*
4. *f^{-1} is multiplicative*

Proof

(i-ii) Trivial. (iii): Suppose $\gcd(m, n) = 1$. Then

$$h(mn) = (f * g)(mn) = \sum_{k|mn} f(k) g(\frac{mn}{k}) = \sum_{\substack{k_1|m \\ k_2|n}} f(k_1 k_2) g(\frac{m}{k_1}\frac{n}{k_2})$$

$$= \sum_{\substack{k_1|m \\ k_2|n}} f(k_1) f(k_2) g(\frac{m}{k_1}) g(\frac{n}{k_2}) = \sum_{k_1|m} f(k_1) g(\frac{m}{k_1}) \sum_{k_2|n} f(k_2) g(\frac{n}{k_2}) = h(m)h(n)$$

Proof.

(iv): The formula for the inverse now becomes

$$f^{-1}(n) = -\sum_{\substack{d|n \\ d<n}} f^{-1}(d) f\left(\frac{nm}{d}\right)$$

so if $\gcd(n, m) = 1$ then

$$f^{-1}(nm) = -\sum_{\substack{d|n \\ d<n}} f^{-1}(d) f\left(\frac{nm}{d}\right) = -\sum_{\substack{d_1|n \\ d_2|m \\ d_1 d_2<n}} f^{-1}(d_1 d_2) f\left(\frac{nm}{d_1 d_2}\right)$$

Assume, by induction that f^{-1} is multiplicative for arguments $< nm$. □

Theorem (Möbius inversion)

1. $\mathbf{1} * \mu = \mathbf{e}$
2. $F(n) = \sum_{k|n} f(k)$ *for all* n *iff* $f(n) = \sum_{k|n} F(k)\mu(n/k)$ *for all* n

Proof.

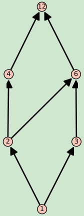
(1): Since the a.f. involved are multiplicative (check!), it suffices to check on prime powers p^r. Then $(\mathbf{1} * \mu)(p^0) = 1$, and for $r > 0$

$$(\mu * \mathbf{1})(p^r) = \sum_{k=0}^{r} \mu(p^k) = 1 - 1 + 0 + \cdots + 0 = 0.$$

(2): If $F = f * \mathbf{1}$ then $f = f * e = f * \mathbf{1} * \mu = F * \mu$. □

Example

- $n = 12$, $D(n)$ as follows



-

- $f = \mathbf{1}$
- $A = \mathbf{??}$
- $g = \mu$
- $C = \mathbf{??}$
- $AC = \mathbf{??}$

Recall

$$d(n) = \sum_{k|n} 1, \qquad \sigma(n) = \sum_{k|n} k$$

We can write this as

$$d = \mathbf{1} * \mathbf{1}, \qquad \sigma = \mathbf{1} * \mathbf{I}$$

from which we conclude that d, σ are multiplicative, and that

$$\mu * d = \mathbf{1}, \qquad \mu * \sigma = \mathbf{I}$$

or in other words

$$\sum_{k|n} \mu(k) d(n/k) = 1, \qquad \sum_{k|n} \mu(k) \sigma(n/k) = n$$

Definition

$\sigma_k(n) = \sum_{d|n} d^k$. In particular, $\sigma_0 = d$, $\sigma_1 = \sigma$.

Lemma

σ_k is multiplicative

Proof.

Suppose $\gcd(m, n) = 1$. Then

$$\sigma_k(mn) = \sum_{d|mn} d^k = \sum_{\substack{d_1|m \\ d_2|n}} (d_1 d_2)^k = \sum_{\substack{d_1|m \\ d_2|n}} d_1^k d_2^k = \sum_{d_1|m} d_1^k \sum_{d_2|n} d_2^k = \sigma_k(m)\sigma_k(n)$$

$\square$

Theorem

1. $\sigma_k(p_1^{a_1} \cdots p_r^{a_r}) = \prod_{j=1}^{r} \frac{1-p_j^{k(a_j+1)}}{1-p_j^k}$
2. $\sum_{d|n} d^k \mu(n/d) = n^k$

Proof.

Try to prove it yourself! ☐

Lemma

$\mathbf{1} * \phi = \mathbf{I}$

Proof.

In other words, want prove

$$\sum_{k|n} \phi(k) = n.$$

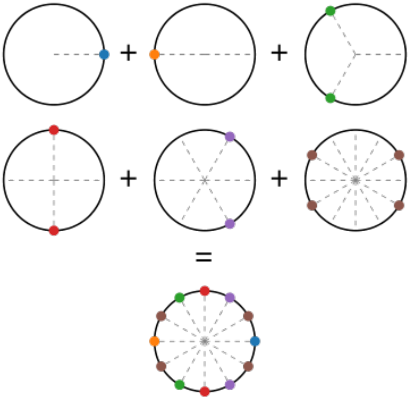
Multiplicative, so put $n = p^r$.

If $r = 0$: $\mathrm{LHS} = 1$, OK.

If $r > 0$: $\mathrm{LHS} = \sum_{j=0}^{r} \phi(p^j) = 1 + \sum_{j=1}^{r}(p^j - p^{j-1}) = p^r$, since sum telescoping. □

Divisors of 12

$$\phi(1) + \phi(2) + \phi(3) + \phi(6) + \phi(12) = 1 + 1 + 2 + 2 + 2 + 4 = 12$$



Theorem

$$\phi(n) = \sum_{k|n} \mu(k)\frac{n}{k} = \sum_{k|n} k\mu(\frac{n}{k})$$

Proof.

Since

$$\mathbf{1} * \phi = \mathbf{I},$$

we have that

$$\phi = \mu * \mathbf{I} = \mathbf{I} * \mu$$

□

Definition

An n'th root of unity is a complex root to $z^n = 1$. A primitive n'th root of unity is not a k'th root of unity for smaller k.

Lemma

Put $\xi_n = \exp(\frac{2\pi}{n} i)$. Then the n'th roots of unity are ξ_n^s, $1 \le s \le n$, and the primitive n'th roots of unity are ξ_n^k, $\gcd(k, n) = 1$.

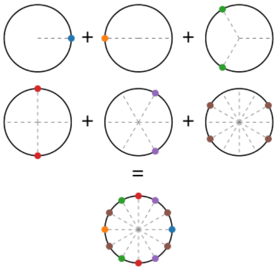
Lemma

If $n > 1$,

$$\sum_{s=1}^{n} \xi_n^s = \frac{\xi_n^n - 1}{\xi_n - 1} = 0.$$

Lemma

$$0 = \sum_{s=1}^{n} \xi_n^s = \sum_{k|n} \sum_{\gcd(\ell,k)=1} \xi_n^\ell$$



Let $f(d)$ denote the sum of the primitive d'th roots of unity. Then $f(1) = 1$, and for $n > 1$, $\sum_{d|n} f(d) = 0$. So $\mathbf{1} * f = e$, hence $f = \mu$. So the Möbius function is the sum of the primitive roots.