Math 342 Tutorial

June 18, 2025

Recall an algebraic monoid is a set G together with a binary operation $G \times G \to G$ satisfying the following:

M1 Associativity: $a(bc) = (ab)c$ for all $a,\ b,\ c \in G$.

M2 Identity: There is an element $e \in G$ for which $ea = ae = a$ for all $a \in G$.

An example of a monoid is the set of all $n \times n$ matrices with entries over $\mathbf{C}$.
An algebraic group is a monoid G satisfying the additional axiom:

G1 Inverse: For every $a \in G$, there is a $b \in G$ for which $ab = ba = e$.

An example of a group is the set of all $n \times n$ matrices over $\mathbf{C}$ which are invertible.
The reader is also reminded of the following definition used previously. If $f,\ g$ are two arithmetic functions, then their Dirchlet product $f * g$ is defined as

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

Question 1. For this question, you will need to use results we have proven in previous tutorials. Do the following. **(a)** Prove the set $\mathscr{F}$ of all arithmetic functions is a monoid. What is the identity element of $\mathscr{F}$? **(b)** What is the largest subset $\mathscr{G}$ of $\mathscr{F}$ such that $\mathscr{G}$ is a group? **(c)** Name a second subset $\mathscr{M} \neq \mathscr{G}$ of $\mathscr{F}$ for which $\mathscr{M}$ is also a group.

(a) In a previous tutorial, we proved that $(f * g) * h = f * (g * h)$, and that there is an identity with respect to the Dirichlet product, namely, $\iota(n) = \lfloor \frac{1}{n} \rfloor$. This shows that the set of arithmetic functions forms a monoid. Also, since $f * g = g * f$, this monoid is commutative.

(b) The largest subset of $\mathscr{F}$ which is a group is simply the subset of elements which have an inverse. Again, from a previous tutorial, these are those arithmetic functions f for which $f(1) \neq 0$.

(c) A smaller subset inside $\mathscr{G}$ which is also a group, i.e., a subgroup, consists of the multiplicative arithmetic functions. Indeed, previously, we showed that if $f,\ g$ are multiplicative, then $f * g$ is multiplicative. Further, if f is multiplicative, then $f(1) = 1$ as follows. We have that $f(n) = f(1)f(n)$ since $(n,\ 1) = 1$. But as f is not identically 0, there is some n for which $f(n) \neq 0$, hence $f(1) = 1$. Thus, the subset of multiplicative arithmetic functions forms subgroup of $\mathscr{G}$.

Question 2. Do the following. **(a)** Prove the Möbius inversion formula: Given $f(n) = \sum_{d|n} g(d)$, one has $g(n) = \sum_{d|n} f(d)\mu(\frac{n}{d})$. **(b)** We previously established that $\phi(n) = \sum_{d|n} d\mu(\frac{n}{d})$. Use part **(a)** to show that $n = \sum_{d|n} \phi(d)$.

(a) Let u be the arithmetic function defined as $u(n) = 1$ for all $n \geqq 1$. Previously, we have shown that $\sum_{d|n} \mu(d) = \lfloor \frac{1}{n} \rfloor$, i.e., we have shown that $u * \mu = \iota$ so that $u \equiv \mu^{-1}$. Therefore, $f = g * u$ if and only if $f * \mu = (g * u) * \mu = g * (\mu * u) = g * \iota = g$, which is the enunciation of part (a).

(b) Let id be the function defined by $\mathrm{id}(n) = n$ for all $n \geqq 1$. Then $\mathrm{id} = u * \phi$ if and only if $\phi = \mathrm{id} * \mu$, as required.

Question 3. The Mangolt function $\Lambda(n)$ is defined as

$$\Lambda(n) = \begin{cases} \log p & \text{if } n = p^a \text{ for some prime } p, \\ 0 & \text{otherwise.} \end{cases}$$

Show the following. **(a)** If $n \geqq 1$, then $\log n = \sum_{d|n} \Lambda(d)$. **(b)** Use part **(a)** to show that $\Lambda(n) = \sum_{d|n} \mu(d) \log \frac{n}{d} = -\sum_{d|n} \mu(d) \log d$.

(a) Certainly, $\log 1 = \Lambda(1) = 0$. So assume that $n > 1$, and write $n = p_1^{e_1} \cdots p_k^{e_k}$. Then

$$\log n = \sum_{j=1}^{k} e_j \log p_j = \sum_{j=1}^{k} \sum_{i=1}^{e_j} \log p_j = \sum_{j=1}^{k} \sum_{i=1}^{e_j} \Lambda(p_j^i) = \sum_{d|n} \Lambda(d)$$

since $\Lambda(d) = 0$ whenever d is not of the form p_j^i for some $1 \leqq j \leqq k$ and $1 \leqq i \leqq e_j$.

(b) Let u be the arithmetic function defined by $u(n) = 1$ for all $n \geqq 1$. Then part (a) asserts that $\log n = (u * \Lambda)(n)$. Möbius inversion shows that

$$\begin{aligned}\Lambda(n) = (\mu * \log)(n) &= \sum_{d|n} \mu(d) \log \frac{n}{d} = \log n \sum_{d|n} \mu(d) - \sum_{d|n} \mu(d) \log d \\ &= \log n\iota(n) - \sum_{d|n} \mu(d) \log d = -\sum_{d|n} \mu(d) \log d\end{aligned}$$

since $\log n \cdot \iota(n) = 0$ for all $n \geqq 0$.

An arithmetic function f is completely multiplicative if $f(mn) = f(m)f(n)$ for all $m, n \in \mathbf{Z}$ (we drop the condition that $(m, n) = 1$).

Question 4. Let f be an arithmetic function. Show the following. **(a)** let f be multiplicative. Then f is completely multiplicative if and only if $f^{-1} = \mu f$, where f^{-1} is the Dirichlet inverse of f. **(b)** If f is multiplicative, then $\sum_{d|n} \mu(d)f(d) = \prod_{p|n}(1 - f(p))$.

(a) Let $g = \mu f$. If f is completely multiplicative, then

$$(f * g) = \sum_{d|n} \mu(d)f(d)f\left(\frac{n}{d}\right) = f(n) \sum_{d|n} \mu(d) = f(n)\iota(n) = \iota(n)$$

since $f(1) = 1$ and $\iota(n) = 0$ if $n > 1$. Hence, $g \equiv f^{-1}$.
Conversely, assume that $f^{-1} = \mu f$. To show that f is completely multiplicative, it suffices to show that $f(p^e) = f(p)^e$. Taking the Dirichlet product of both sides of $f^{-1} = \mu f$ with f implies that

$$0 = \sum_{d|n} \mu(d)f(d)f\left(\frac{n}{d}\right).$$

Taking $n = p^e$, we have that

$$0 = \mu(1)f(1)f(p^e) + \mu(p)f(p)f(p^{e-1}) = f(p^e) - f(p)f(p^{e-1}),$$

hence $f(p^e) = f(p)f(p^{e-1})$. An obvious induction implies $f(p^e) = f(p)^e$, as required. This shows that f is completely multiplicative.

(b) Let $g(n) = \sum_{d|n} \mu(d)f(d)$; then g is multiplicative. Observe,

$$g(p^e) = \sum_{d\ midp^e} \mu(d)f(d) = \mu(1)f(1) + \mu(p)f(p) = 1 - f(p).$$

Since g is multiplicative, we have that

$$g(n) = \prod_{p^e \| n} g(p^e) = \prod_{p|n} (1 - f(p)).$$

Question 5. If $n = p_1^{e_1} \cdots p_k^{e_k}$, then Liouville's function λ is defined as

$$\lambda(n) = (-1)^{e_1+\cdots+e_k}.$$

Show the following. **(a)** λ is completely multiplicative. **(b)** $\sum_{d|n} \lambda(d) = 1$ if n is a square and 0 otherwise. Also, $\lambda^{-1} = |\mu|$.

(a) Let $n = p_1^{e_1} \cdots p_k^{e_k}$ and $m = p_1^{f_1} \cdots p_k^{f_k}$. Then
$\lambda(nm) = \lambda(p_1^{e_1+f_1} \cdots p_k^{e_k+f_k}) = (-1)^{(e_1+f_1)+\cdots+(e_k+f_k)} = (-1)^{e_1+\cdots+e_k}(-1)^{f_1+\cdots+f_k} = \lambda(n)\lambda(m).$

(b) Let $g(n) = \sum_{d|n} \lambda(d)$. Then g is multiplicative. Observe,

$$g(p^e) = \sum_{d|p^e} \lambda(d) = 1 + (-1) + 1 + \cdots + (-1)^e = \begin{cases} 0 & \text{if } e \text{ is odd,} \\ 1 & \text{if } e \text{ is even.} \end{cases}$$

Hence, since g is multiplicative, $g(n)$ is 1 or 0 according as n is a square or not.

Question 6. Show the following identities.

(a)

$$\frac{n}{\phi(n)} = \sum_{d|n} \frac{\mu^2(d)}{\phi(d)}.$$

[Hint: Show first that $\frac{\mu(n)}{\phi(n)}$ is multiplicative. Then use question 4.]

(b) Show for each $k \geqq 1$ that

$$\sum_{\substack{d|n \\ d^k|n}} \mu(d) = \begin{cases} 0 & \text{if } m^k \mid n \text{ for some } m > 1, \\ 1 & \text{otherwise.} \end{cases}$$

(a) We know that μ is multiplicative. Since ϕ is multiplicative, $1/\phi$ is also multiplicative, hence a fortiori μ/ϕ is multiplicative. From question 4, we have that

$$\sum_{d|n} \mu(d)\frac{\mu(d)}{\phi(d)} = \prod_{p|n}\left(1 - \frac{\mu(p)}{\phi(p)}\right) = \prod_{p|n}\left(1 + \frac{1}{p-1}\right) = \prod_{p|n} \frac{1}{1-1/p}.$$

But

$$\phi(n) = n\prod_{p|n}\left(1 - \frac{1}{p}\right),$$

hence

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

(b) First note that 1 always satisfies $1 \mid n$ and $1^k \mid n$. Therefore, if there is no $m > 1$ for which $m^k \mid n$, then the sum is simply $\mu(1) = 1$. Assume there is some $m > 1$ for which $m^k \mid n$. Suppose, in fact, there are ℓ prime power factors of n with exponent greater than k, and which are square free. Then

$$\sum_{\substack{d|n \\ d^k|n}} \mu(d) = \binom{\ell}{0} + \binom{\ell}{1}(-1) + \cdots + \binom{\ell}{\ell}(-1)^\ell = (1-1)^\ell = 0.$$