Analytical Number Theory: Lecture 01

5 Feb 2026

1 Arithmetic Functions

Definition 1 (Arithmetic Function). *An arithmetic function is a function $f : \mathbb{N} \to \mathbb{C}$.*

Notation 1. *The set of all arithmetic functions is denoted by $\mathcal{F}$.*

1.1 Examples

The following are well-known arithmetic functions that play an important role in number theory:

1. The Unit Function $u(n)$:
$$u(n) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{otherwise} \end{cases}$$
Note: the unit function can be written as follows:
$$u(n) = \left\lfloor \frac{1}{n} \right\rfloor$$

2. The Constant Function $\mathbb{1}(n)$:
$$\mathbb{1}(n) = 1, \quad \forall n \geq 1$$

3. The Euler Totient Function $\varphi(n)$:
$$\varphi(n) = \#\{1 \leq k \leq n \mid \gcd(k, n) = 1\}, \quad \forall n \geq 1$$

4. The Divisor Function $\sigma_\alpha(n)$: For any $\alpha \in \mathbb{C}$,
$$\sigma_\alpha(n) = \sum_{d|n} d^\alpha$$

5. The Divisor Count Function $\tau(n)$: This is a special case of the divisor function where $\alpha = 0$:
$$\tau(n) = \sigma_0(n) = \sum_{d|n} 1$$
Also denoted simply by $\sigma(n)$ when referring to the sum of divisors ($\alpha = 1$).

6. The Möbius Function $\mu(n)$:

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } p^2 | n \text{ for some prime } p \\ (-1)^k & \text{if } n = p_1 p_2 \dots p_k \text{ (product of distinct primes)} \end{cases}$$

7. The von Mangoldt Function $\Lambda(n)$:

$$\Lambda(n) = \begin{cases} \ln p & \text{if } n = p^k \text{ for some prime } p \text{ and } k \in \mathbb{Z}_{\geq 1} \\ 0 & \text{otherwise} \end{cases}$$

8. The Omega Functions $\omega(n)$ and $\Omega(n)$: Let $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$ be the prime factorization of n.

   - $\omega(n) = k$ (counts the number of *distinct* prime factors).
   - $\Omega(n) = \sum_{i=1}^{k} a_i$ (counts the number of prime factors *with multiplicity*).

9. The Liouville Function $\lambda(n)$:

$$\lambda(n) = (-1)^{\Omega(n)}$$

2 Multiplicative Functions

Definition 2 (Multiplicative Function)**.** *An arithmetic function f is said to be multiplicative if it is not identically zero and:*

$$f(mn) = f(m)f(n) \quad \textit{whenever } \gcd(m, n) = 1$$

Notation 2. *The set of all multiplicative functions is denoted by $\mathcal{M}$.*

Definition 3 (Completely Multiplicative Function)**.** *An arithmetic function f is called completely multiplicative if it is not identically zero and:*

$$f(mn) = f(m)f(n) \quad \textit{for all } m, n \in \mathbb{N}$$

Notation 3. *The set of all completely multiplicative functions is denoted by $\mathcal{CM}$. Clearly, $\mathcal{CM} \subset \mathcal{M} \subset \mathcal{F}$.*

Theorem 1. *If f is multiplicative, then $f(1) = 1$.*

Proof. Since f is not identically zero, there exists some $n \in \mathbb{N}$ such that $f(n) \neq 0$. Since $\gcd(n, 1) = 1$, we have:

$$f(n) = f(n \cdot 1) = f(n)f(1)$$

Hence, $f(n)(1 - f(1)) = 0$, and $f(n) \neq 0$ implying $f(1) = 1$. □

2.1 Examples

1. The Unit Function $u(n)$ is completely multiplicative.

   Proof. By definition, $u(1) = 1$ and $u(n) = 0$ for $n > 1$. Let $m, n \in \mathbb{N}$.

   - If $m = 1$ and $n = 1$, then $mn = 1$. We have $u(1) = 1$ and $u(1)u(1) = 1 \cdot 1 = 1$.
   - If $m > 1$ or $n > 1$, then $mn > 1$, so $u(mn) = 0$. Since at least one of the inputs is greater than 1, either $u(m) = 0$ or $u(n) = 0$, making the product $u(m)u(n) = 0$.

   Thus, $u(mn) = u(m)u(n)$ for all integers m, n. □

2. The Constant Function $\mathbb{1}(n)$ is completely multiplicative.

   Proof. For any $m, n \in \mathbb{N}$:

   $$\mathbb{1}(mn) = 1 \quad \text{and} \quad \mathbb{1}(m)\mathbb{1}(n) = 1 \cdot 1 = 1$$

   The equality $\mathbb{1}(mn) = \mathbb{1}(m)\mathbb{1}(n)$ holds for all integers. □

3. The Euler Totient Function $\varphi(n)$ is multiplicative.

   Proof. We must show $\varphi(mn) = \varphi(m)\varphi(n)$ for $gcd(m, n) = 1$.

   Using elementary number theory. Arrange the integers $1, 2, \ldots, mn$ in a rectangular array with n rows and m columns:

   $$\begin{array}{cccccc} 1 & 2 & \ldots & r & \ldots & m \\ m+1 & m+2 & \ldots & m+r & \ldots & 2m \\ \vdots & \vdots & & \vdots & & \vdots \\ (n-1)m+1 & (n-1)m+2 & \ldots & (n-1)m+r & \ldots & nm \end{array}$$

   We need to count how many entries x in this grid satisfy $gcd(x, mn) = 1$. Since $gcd(m, n) = 1$, the condition $gcd(x, mn) = 1$ is equivalent to satisfying both $gcd(x, m) = 1$ and $gcd(x, n) = 1$.

   In any column, all elements are congruent modulo m. Specifically, the element in the r-th column is of the form $km + r \equiv r \pmod{m}$. Therefore, $gcd(km + r, m) = gcd(r, m)$. An entry is coprime to m if and only if it lies in a column r where $gcd(r, m) = 1$. There are exactly $\varphi(m)$ such columns.

   On the other hand, fix one such valid column r (where $gcd(r, m) = 1$). The entries in this column are:

   $$r, \quad m + r, \quad 2m + r, \quad \ldots, \quad (n-1)m + r$$

   This is an arithmetic progression with step m. Since $gcd(m, n) = 1$, the elements $\{0, m, 2m, \ldots, (n-1)m\}$ form a complete residue system modulo n. Shifting by r implies that the sequence $r, m + r, \ldots, (n-1)m + r$ is also a complete residue system modulo n.

In a complete residue system modulo n, exactly $\varphi(n)$ numbers are coprime to n. Thus, in every valid column, there are exactly $\varphi(n)$ valid entries.

Total valid numbers = (Number of valid columns) $\times$ (Valid entries per column)

$$\varphi(mn) = \varphi(m) \times \varphi(n)$$

$\square$

Proof. Another proof using the Chinese Remainder Theorem

Let R_k denote the ring of integers modulo k, and $R_k^\times$ denote the group of units in that ring. By definition, $\#R_k^\times = \varphi(k)$.

Since $gcd(m, n) = 1$, the Chinese Remainder Theorem states there is a ring isomorphism:

$$\psi : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$$

defined by $\psi(x) = (x \pmod m, x \pmod n)$.

An element $x \in \mathbb{Z}_{mn}$ is a unit (invertible) if and only if its image under ψ is a unit in the product ring. An element $(a, b) \in \mathbb{Z}_m \times \mathbb{Z}_n$ is a unit if and only if a is a unit in $\mathbb{Z}_m$ and b is a unit in $\mathbb{Z}_n$.

Therefore, the group of units of $\mathbb{Z}_{mn}$ is isomorphic to the direct product of the groups of units:

$$\mathbb{Z}_{mn}^\times \cong \mathbb{Z}_m^\times \times \mathbb{Z}_n^\times$$

Taking the order (size) of these groups:

$$\#\mathbb{Z}_{mn}^\times = \#\mathbb{Z}_m^\times \cdot \#\mathbb{Z}_n^\times$$

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

$\square$

To show $\varphi(n)$ is not completely multiplicative, let p be a prime. Then $\varphi(p^2) = p^2 - p$, but $\varphi(p)\varphi(p) = (p-1)^2$. These are not equal.

4. The Divisor Functions $\sigma_\alpha(n) = \sum_{d|n} d^\alpha$ is multiplicative.

Proof. Let $gcd(m, n) = 1$. Since m and n are coprime, every divisor d of the product mn can be written uniquely as $d = ab$, where $a|m$ and $b|n$. Conversely, for any $a|m$ and $b|n$, the product ab divides mn.

$$\sigma_\alpha(mn) = \sum_{d|mn} d^\alpha = \sum_{a|m} \sum_{b|n} (ab)^\alpha$$

Since $(ab)^\alpha = a^\alpha b^\alpha$, we can separate the sums:

$$= \sum_{a|m} \sum_{b|n} a^\alpha b^\alpha = \left(\sum_{a|m} a^\alpha \right) \left(\sum_{b|n} b^\alpha \right) = \sigma_\alpha(m)\sigma_\alpha(n)$$

To show it is not completely multiplicative, take $\alpha = 0$ then we have for any prime p the following $\tau(p^2) = 3 \neq \tau(p)\tau(p) = 4$. $\square$

5. The Möbius Function $\mu(n)$ is multiplicative.

   Proof. Let $gcd(m, n) = 1$.

   - If m or n is not square-free (divisible by some p^2), then mn is also not square-free.
   $$\mu(mn) = 0 \quad \text{and} \quad \mu(m)\mu(n) = 0$$
   - If both m and n are square-free, let $m = p_1 \dots p_k$ and $n = q_1 \dots q_j$. Since $gcd(m, n) = 1$, all primes are distinct. mn is the product of $k + j$ distinct primes.
   $$\mu(mn) = (-1)^{k+j} = (-1)^k(-1)^j = \mu(m)\mu(n)$$

   To show $\mu(n)$ is not complete let p be any prime, then $\mu(p^2) = 0$ while $\mu(p)^2 = (-1)^2 = 1$. □

6. The von Mangoldt Function $\Lambda(n)$ is not multiplicative function.

   Proof. For a function to be multiplicative, it must satisfy $f(1) = 1$.

   By definition, $\Lambda(1) = 0$. Hence, Λ is not multiplicative. □

7. The Omega Functions $\omega(n)$ and $\Omega(n)$ are not multiplicative (Actually they are additive).

   Proof. Both functions count prime factors. For $n = 1$, the count is 0.
   $$\omega(1) = 0 \quad \text{and} \quad \Omega(1) = 0$$
   Since $f(1) \neq 1$, neither function is multiplicative. □

8. The Liouville Function $\lambda(n) = (-1)^{\Omega(n)}$ is completely multiplicative.

   Proof. The function $\Omega(n)$ is completely additive, meaning:
   $$\Omega(mn) = \Omega(m) + \Omega(n) \quad \text{for all } m, n \in \mathbb{N}$$
   Now consider $\lambda(mn)$:
   $$\lambda(mn) = (-1)^{\Omega(mn)} = (-1)^{\Omega(m)+\Omega(n)} = (-1)^{\Omega(m)} \cdot (-1)^{\Omega(n)}$$
   $$\lambda(mn) = \lambda(m)\lambda(n)$$
   Since this relation holds for all integers m, n, the Liouville function is completely multiplicative. □

Theorem 2 (Characterization of Multiplicative Functions)**.** *Let f be an arithmetic function such that $f(1) = 1$. Let $n = p_1^{a_1} \dots p_k^{a_k}$.*

1. *f is multiplicative if and only if:*
$$f(p_1^{a_1} \dots p_k^{a_k}) = f(p_1^{a_1}) \dots f(p_k^{a_k})$$

2. *f is completely multiplicative if and only if:*

$$f(p_1^{a_1} \dots p_k^{a_k}) = f(p_1)^{a_1} \dots f(p_k)^{a_k}$$

Proof. Proof of $\implies$

Assume f is multiplicative. We show that f distributes over the prime factorization. Let $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$. We proceed by induction on k, the number of distinct prime factors.

- Base case ($k = 1$): $f(p_1^{a_1}) = f(p_1^{a_1})$. This is trivial.
- Inductive step: Assume the formula holds for any integer with k distinct prime factors.

  Let n have $k+1$ distinct prime factors. We can write $n = m \cdot p_{k+1}^{a_{k+1}}$, where $m = p_1^{a_1} \dots p_k^{a_k}$. Since p_{k+1} is distinct from primes in m, we have $gcd(m, p_{k+1}^{a_{k+1}}) = 1$. By the definition of multiplicativity:

  $$f(n) = f(m) f(p_{k+1}^{a_{k+1}})$$

  By the induction hypothesis, $f(m) = f(p_1^{a_1}) \dots f(p_k^{a_k})$. Substituting this back:

  $$f(n) = [f(p_1^{a_1}) \dots f(p_k^{a_k})]\, f(p_{k+1}^{a_{k+1}})$$

  Thus, the property holds for $k+1$ factors.

Proof by $\impliedby$

Assume that $f(p_1^{a_1} \dots p_k^{a_k}) = \prod_{i=1}^{k} f(p_i^{a_i})$ for any composite number. We must show that f is multiplicative. Let $m, n \in \mathbb{N}$ such that $gcd(m, n) = 1$.

Let the prime factorizations be:

$$m = p_1^{a_1} \dots p_r^{a_r} \quad \text{and} \quad n = q_1^{b_1} \dots q_s^{b_s}$$

Since $gcd(m, n) = 1$, the sets of primes $\{p_i\}$ and $\{q_j\}$ are disjoint (no prime appears in both sets). The prime factorization of the product mn is simply the concatenation of these factors:

$$mn = p_1^{a_1} \dots p_r^{a_r} q_1^{b_1} \dots q_s^{b_s}$$

By the assumption (that f breaks down into prime powers):

$$f(mn) = f(p_1^{a_1}) \dots f(p_r^{a_r}) f(q_1^{b_1}) \dots f(q_s^{b_s})$$

We can group these terms:

$$f(mn) = \left[\prod_{i=1}^{r} f(p_i^{a_i})\right] \left[\prod_{j=1}^{s} f(q_j^{b_j})\right]$$

Using the assumption again on m and n individually:

$$f(m) = \prod_{i=1}^{r} f(p_i^{a_i}) \quad \text{and} \quad f(n) = \prod_{j=1}^{s} f(q_j^{b_j})$$

Therefore:

$$f(mn) = f(m) f(n)$$

Since this holds for all coprime m, n, f is multiplicative. This concludes the proof of part 1.

Proof of part 2 uses the same resoning. □

Exercise 1. *Let* $f(n) = [\sqrt{n}] - [\sqrt{n-1}]$*. Show that* f *is multiplicative.*

Exercise 2. *Let* $f : \mathbb{N} \to \mathbb{R}$ *be a non-decreasing multiplicative arithmetic function. For integers* $a \geq 3$*, let* $R_t = \sum_{j=0}^{t} a^j$ *and* $S_t = a^t - \sum_{j=0}^{t-1} a^j$*.*

1. *Show that* $f(S_t) \leq (f(a))^t \leq f(R_t)$*.*
2. *Deduce that for all integers* $a, b, n > 2$*, we have:*

$$f(b)^{r-1} \leq f(n) \leq f(a)^{r+2}$$

   where $r = [\log_a n]$ *and similar definitions for bounds involving* b*.*

3. *Show that* $(f(a))^{\frac{1}{\log a}} = (f(b))^{\frac{1}{\log b}}$*.*
4. *Deduce that for all* $n \geq 1$*,* $f(n) = n^k$ *for some constant* k*.*

3 Dirichlet Convolution

Definition 4. *Let* f *and* g *be two arithmetic functions. The Dirichlet convolution of* f *and* g*, denoted* $f * g$*, is the arithmetic function defined by:*

$$(f * g)(n) = \sum_{d|n} f(d)g\left(\frac{n}{d}\right) = \sum_{ab=n} f(a)g(b), \quad \forall n \in \mathbb{N}$$

Theorem 3. *The structure* $(\mathcal{F}, +, *)$ *is a commutative ring with unity and*

$$\mathcal{F}^{\times} = \{f \in \mathcal{F} | f(1) \neq 0\}$$

Proof. We must verify the ring axioms. Let $f, g, h \in \mathcal{F}$.

First, let prove the commutativity of convolution ($f * g = g * f$)

By definition:

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

Let $d' = n/d$. As d runs through the divisors of n, d' also runs through the divisors of n. We can substitute $d = n/d'$:

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

Second, we need to show the associativity of convolution ($(f * g) * h = f * (g * h)$) Consider $((f * g) * h)(n)$:

$$((f * g) * h)(n) = \sum_{d|n} (f * g)(d)h\left(\frac{n}{d}\right) = \sum_{d|n} \left[\sum_{k|d} f(k)g\left(\frac{d}{k}\right)\right] h\left(\frac{n}{d}\right)$$

Let $d = km$. Then $n/d = n/(km)$. The condition $d|n$ and $k|d$ is equivalent to $kmn = n$ for integers k, m, r where $r = n/d$. Effectively, we sum over all triples (a, b, c) such that $abc = n$:

$$= \sum_{abc=n} f(a)g(b)h(c)$$

Similarly, expanding $f * (g * h)$:

$$(f * (g * h))(n) = \sum_{a|n} f(a)(g * h)\left(\frac{n}{a}\right) = \sum_{a|n} f(a) \sum_{bc=n/a} g(b)h(c) = \sum_{abc=n} f(a)g(b)h(c)$$

Since both expressions equal $\sum_{abc=n} f(a)g(b)h(c)$, the operation is associative.

Now we need to show the existence of Unity.
We claim $u(n)$ is the identity.

$$(f * u)(n) = \sum_{d|n} f(d)u\left(\frac{n}{d}\right) = f(n)u(1) + \sum_{\substack{d|n \\ d<n}} f(d)u\left(\frac{n}{d}\right) = f(n)$$

The term $u(n/d)$ is 0 since $n/d > 1$. Thus $f * u = f$ and by commutativity $u * f = f$.

Then we show that the convultion distribute over addition

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

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

Hence $(\mathcal{F}, +, *)$ is a commutative ring with unity.

Now to prove $\mathcal{F}^\times = \{f \in \mathcal{F} | f(1) \neq 0\}$.
Assume f is invertible. Then there exists g such that $(f * g)(n) = u(n)$ for all $n \in \mathbb{N}$. Evaluating the convolution at $n = 1$:

$$(f * g)(1) = \sum_{d|1} f(d)g\left(\frac{1}{d}\right) = f(1)g(1)$$

By the definition of the unit function, $u(1) = 1$. Therefore:

$$f(1)g(1) = 1.$$

Since the product of two complex numbers is non-zero, neither factor can be zero. Hence $f(1) \neq 0$.

On the other hand, assume $f(1) \neq 0$. We wish to construct an arithmetic function g such that $(f * g)(n) = u(n)$ for all n. We define $g(n)$ inductively on n.
Base case ($n = 1$): We require $(f * g)(1) = f(1)g(1) = u(1) = 1$. Since $f(1) \neq 0$, we can uniquely define:

$$g(1) = \frac{1}{f(1)}.$$

Inductive step ($n > 1$): Assume that the values $g(k)$ have been uniquely determined for all $k < n$. We examine the condition for n:

$$(f * g)(n) = \sum_{d|n} f(d)g\left(\frac{n}{d}\right) = u(n) = 0 \quad \text{(since } n > 1\text{)}$$

We isolate the term where $d = 1$ in the sum:

$$f(1)g(n) + \sum_{\substack{d|n \\ d>1}} f(d)g\left(\frac{n}{d}\right) = 0$$

Rearranging the equation to solve for $g(n)$:

$$f(1)g(n) = -\sum_{\substack{d|n \\ d>1}} f(d)g\left(\frac{n}{d}\right)$$

Since $f(1) \neq 0$, we can divide by it:

$$g(n) = \frac{-1}{f(1)} \sum_{\substack{d|n \\ d>1}} f(d)g\left(\frac{n}{d}\right)$$

Notice that for any divisor $d > 1$, the argument $\frac{n}{d}$ is strictly less than n. Thus, the value $g(\frac{n}{d})$ is already known by the induction hypothesis. This formula uniquely determines $g(n)$.

Hence $\mathcal{F}^{\times} = \{f \in \mathcal{F} | f(1) \neq 0\}$. □

Theorem 4. *The set of multiplicative functions $\mathcal{M}$ is a subgroup of the group of units $\mathcal{F}^{\times}$. That is:*

1. *If f and g are multiplicative, then $f * g$ is multiplicative.*
2. *If f is multiplicative, then f^{-1} is multiplicative.*

Proof. Let f and g be multiplicative functions. Let $h = f * g$. We must show that $h(mn) = h(m)h(n)$ whenever $gcd(m, n) = 1$.

Let $m, n \in \mathbb{N}$ such that $gcd(m, n) = 1$.

$$h(mn) = \sum_{d|mn} f(d)g\left(\frac{mn}{d}\right)$$

Since $gcd(m, n) = 1$, every divisor d of mn can be written uniquely as $d = ab$, where $a|m$ and $b|n$. Furthermore, $gcd(a, b) = 1$ and $gcd(\frac{m}{a}, \frac{n}{b}) = 1$. Substituting $d = ab$ into the sum:

$$h(mn) = \sum_{a|m} \sum_{b|n} f(ab)g\left(\frac{mn}{ab}\right)$$

Using the multiplicativity of f and g:

$$f(ab) = f(a)f(b) \quad \text{and} \quad g\left(\frac{m}{a} \cdot \frac{n}{b}\right) = g\left(\frac{m}{a}\right) g\left(\frac{n}{b}\right)$$

Substitute these into the summation:

$$h(mn) = \sum_{a|m} \sum_{b|n} f(a)f(b)g\left(\frac{m}{a}\right) g\left(\frac{n}{b}\right)$$

We can factor the double sum into the product of two single sums:

$$h(mn) = \left(\sum_{a|m} f(a)g\left(\frac{m}{a}\right)\right) \left(\sum_{b|n} f(b)g\left(\frac{n}{b}\right)\right)$$

By definition of convolution, these factors are exactly $(f * g)(m)$ and $(f * g)(n)$.

$$h(mn) = h(m)h(n)$$

Thus, $f * g$ is multiplicative.

Let f be a multiplicative function. Since $f(1) = 1 \neq 0$, f has an inverse $g = f^{-1}$. We must show that g is multiplicative.

We proceed by induction on the product mn. We want to show $g(mn) = g(m)g(n)$ for all $gcd(m, n) = 1$.

Base case ($mn = 1$): Since $m = 1, n = 1$, we have $g(1) = 1/f(1) = 1$. Thus $g(1) = g(1)g(1)$ holds.

For the inductive step, assume $g(ab) = g(a)g(b)$ for all coprime a, b with $ab < mn$. By definition of the inverse, $(f * g)(mn) = u(mn)$. Since $mn > 1$, $u(mn) = 0$.

$$\sum_{d|mn} f(d)g\left(\frac{mn}{d}\right) = 0$$

Since $gcd(m, n) = 1$, every divisor d of mn is uniquely $d = ab$ where $a|m, b|n$.

$$\sum_{a|m} \sum_{b|n} f(ab)g\left(\frac{mn}{ab}\right) = 0$$

Using the multiplicativity of f and separating the term where $a = 1, b = 1$ (so $d = 1$):

$$g(mn) + \sum_{\substack{a|m,b|n \\ ab>1}} f(a)f(b)g\left(\frac{mn}{ab}\right) = 0$$

For $ab > 1$, we have $\frac{mn}{ab} < mn$. Since $gcd(\frac{m}{a}, \frac{n}{b}) = 1$, the induction hypothesis applies:

$$g\left(\frac{mn}{ab}\right) = g\left(\frac{m}{a}\right) g\left(\frac{n}{b}\right)$$

Substitute this back:

$$g(mn) = -\sum_{\substack{a|m,\, b|n \\ ab>1}} f(a)g\left(\frac{m}{a}\right) f(b)g\left(\frac{n}{b}\right)$$

We recognize the sum on the right as the expansion of the product $(f * g)(m) \cdot (f * g)(n)$, excluding the term for $a = 1, b = 1$:

$$(f * g)(m) \cdot (f * g)(n) = \left(\sum_{a|m} f(a)g\left(\frac{m}{a}\right)\right) \left(\sum_{b|n} f(b)g\left(\frac{n}{b}\right)\right)$$

Since $mn > 1$ and $gcd(m, n) = 1$, at least one of $m, n > 1$. Thus, $(f * g)(m)(f * g)(n) = u(m)u(n) = 0$. The full summation over all a, b is 0. The sum restricted to $ab > 1$ is simply the total sum minus the $a = b = 1$ term:

$$\sum_{\substack{a|m,\, b|n \\ ab>1}} f(a)g\left(\frac{m}{a}\right) f(b)g\left(\frac{n}{b}\right) = 0 - [f(1)g(m) \cdot f(1)g(n)] = -g(m)g(n)$$

Then

$$g(mn) = -(-g(m)g(n)) = g(m)g(n)$$

□

Remark 1. *The following results can be concluded:*

1. *The convolution of two completely multiplicative functions is not necessarily completely multiplicative (though it is multiplicative). For example,* $\mathbb{1} * \mathbb{1} = \tau$. *While* $\mathbb{1}$ *is completely multiplicative,* τ *is not.*

2. *If* f *and* g *are arithmetic functions and* $f * g$ *is a multiplicative functions, it does not mean either* f *or* g *is multiplicative.*

3. *To prove a function* f *is multiplicative, sometimes it may be easier to find two multiplicative functions (*g *and* h*) such that* $g * h = f$*, then* f *is multiplicative.*

Exercise 3. *Prove the following identity:*

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

Exercise 4. *Give a simple expression of the following sums:*

1. $\sum_{d|n} \mu(d)\tau(\frac{n}{d})$

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

3. $\sum_{d|n} \mu(d)\tau(d)$