Arithmetic Functions

Any real-valued function on the integers \( f: \mathbb{N} \to \mathbb{R} \) (or complex-valued function \( f: \mathbb{N} \to \mathbb{C} \)) is called an arithmetic function.

*Examples:* \( \tau(n) = \) number of divisors of \( n \); \( \varphi(n) = \) number of invertible congruence classes mod \( n \).

The most important arithmetic functions in number theory are the multiplicative functions, those which satisfy \( (m, n) = 1 \Rightarrow f(mn) = f(m)f(n) \).

Indeed, there are some very simple multiplicative functions.

*Examples:* The functions \( i(n) = n \) and \( u(n) = 1 \) are multiplicative, as is the indicator function, defined as

\[
I(n) = \begin{cases} 
1 & \text{if } n = 1 \\
0 & \text{if } n > 1
\end{cases}
\]

These functions are also totally multiplicative: they satisfy \( f(mn) = f(m)f(n) \) for all \( m \) and \( n \).

Multiplicative functions have some nice properties. Chief among them is the following
**Theorem**  If \( f(n) \) is multiplicative, then so is its summation function \( F(n) = \sum_{d|n} f(d) \).

**Proof**  If \((m,n) = 1\), every divisor of \(mn\) has the form \(ab\) where \(a|m\) and \(b|n\), and necessarily, \((a,b) = 1\). Conversely, if \(a|m\) and \(b|n\), then \(ab|mn\) (and necessarily, \((a,b) = 1\)). Therefore, if \(f\) is multiplicative,

\[
F(n) = \sum_{d|mn} f(d) \\
= \sum_{a|m} \sum_{b|n} f(ab) \\
= \sum_{a|m} f(a) \sum_{b|n} f(b) \\
= F(m)F(n)
\]

so \( F \) is multiplicative as well. //

**Corollary**  \( \tau \) is multiplicative.

**Proof**  \( \tau(n) \) is the summation function \( \sum_{d|n} u(d) \). //

**Corollary**  \( \sigma(n) = (\text{sum of the divisors of } n) \) is multiplicative.

**Proof**  \( \sigma(n) \) is the summation function \( \sum_{d|n} i(d) \). //
A consequence of the fact that $\tau$ and $\sigma$ are multiplicative functions is that we can provide product formulas for them based on prime factorizations:

**Theorem** Suppose $n = \prod_{i=1}^{r} p_i^{e_i}$ is the prime factorization of $n$. Then

$$
\tau(n) = \prod_{i=1}^{r} (e_i + 1) \quad \text{and} \quad \sigma(n) = \prod_{i=1}^{r} \frac{p_i^{e_i+1} - 1}{p_i - 1}.
$$

**Proof** If $p$ is prime, then the factors of $p^e$ are the numbers $1, p, p^2, \ldots, p^e$. Thus, $\tau(p^e) = e + 1$ and

$$
\sigma(p^e) = 1 + p + p^2 + \cdots + p^e = \frac{p^{e+1} - 1}{p - 1}.
$$

The theorem now follows from the multiplicativity of the functions. //

Not only is the summation function of a multiplicative function also multiplicative, but the converse of this is also true. This fact was proved by August Möbius, a protegé of Gauss, in the 1830s.
In the process Möbius defined a new arithmetic function that played an important role in the proof, the Möbius function

\[
\mu(n) = \begin{cases} 
1 & \text{if } n = 1 \\
0 & \text{if } n \text{ is not square-free} \\
(-1)^k & \text{if } n \text{ is the product of } k \text{ distinct primes}
\end{cases}
\]

**Proposition** \( \mu \) is multiplicative.  //

**Proposition** The summation function of the Möbius function is the indicator function:

\[
\sum_{d \mid n} \mu(d) = I(n)
\]

**Proof** The case \( n = 1 \) is clear. Suppose then that \( n \) is a prime power: \( n = p^e \). Then

\[
\sum_{d \mid n} \mu(d) = \mu(1) + \mu(p) + \mu(p^2) + \cdots + \mu(p^e)
\]

\[
= 1 - 1 + 0 + \cdots + 0
\]

\[
= 0
\]

Since \( \mu \) is multiplicative, so is its summation function, and the result follows.  //
Johann Peter Gustav Lejeune Dirichlet, a contemporary of Möbius, devised an “arithmetic of functions” that preserved the property of being multiplicative. If \( f \) and \( g \) are arithmetic functions, their **Dirichlet product** (also called their **convolution**) is defined as

\[
(f \ast g)(n) = \sum_{d \mid n} f(d)g\left(\frac{n}{d}\right).
\]

**Proposition** If \( f \) and \( g \) are arithmetic functions,

1. \( f \ast g = g \ast f \) [Dirichlet product is commutative];
2. \( (f \ast g) \ast h = f \ast (g \ast h) \) [and associative];
3. \( f \ast I = f \) [with \( I \) as identity object]; and
4. \( F = f \ast u \) is the summation function of \( f \).

**Proof** Easy. //

**Theorem** If \( f \) and \( g \) are multiplicative functions, then so is \( h = f \ast g \).

**Proof** Suppose \((m,n) = 1\). Then

\[
h(mn) = \sum_{d \mid mn} f(d)g\left(\frac{mn}{d}\right).
\]
Since \((m,n) = 1\), every divisor \(d\) of \(mn\) can be represented uniquely as a product \(ab\) where \(a \mid m\) and \(b \mid n\). In fact, \((a,b) = 1\) because \((m,n) = 1\). So

\[
h(mn) = \sum_{a \mid m, b \mid n} f(ab)g\left(\frac{mn}{ab}\right)
\]

\[
= \sum_{a \mid m} \sum_{b \mid n} f(ab)g\left(\frac{mn}{ab}\right)
\]

\[
= \sum_{a \mid m} \sum_{b \mid n} f(a)f(b)g\left(\frac{m}{a}\right)g\left(\frac{n}{b}\right)
\]

where we are using the fact that \(f\) and \(g\) are multiplicative. Since the inner sum depends only the choice of \(b\), we may write

\[
h(mn) = \sum_{a \mid m} f(a)g\left(\frac{m}{a}\right)\left(\sum_{b \mid n} f(b)g\left(\frac{n}{b}\right)\right)
\]

\[
= \sum_{a \mid m} f(a)g\left(\frac{m}{a}\right)h(n)
\]

\[
= h(n) \cdot \sum_{a \mid m} f(a)g\left(\frac{m}{a}\right)
\]

\[
= h(n) \cdot h(m)
\]

and the proof is complete.  //

The converse of this theorem is also true:
**Theorem**  If \( h = f \ast g \), and \( g \) and \( h \) are nonzero multiplicative functions, then \( f \) must also be multiplicative.

**Proof**  If \( f \) were not multiplicative, then there would have to be some pair of relatively prime integers \( m \) and \( n \) so that \( f(mn) \neq f(m)f(n) \). Since \( g \) and \( h \) are nonzero multiplicative functions, then \( g(1) = h(1) = 1 \). But since \( h(1) = f(1)g(1) \), it follows that \( f(1) = 1 \). In particular, then, \( mn > 1 \). As in the proof of the previous theorem, we can represent each divisor \( d \) of \( mn \) as a product \( ab \) of a factor \( a \) of \( m \) with a factor \( b \) of \( n \), noting that \( a \) and \( b \) are relatively prime since \( m \) and \( n \) are. Thus,

\[
\begin{align*}
  h(mn) &= \sum_{d \mid mn} g(mn)f\left( \frac{mn}{d} \right) \\
  &= g(1)f(mn) + \sum_{d \mid mn, d > 1} g(mn)f\left( \frac{mn}{d} \right) \\
  &= f(mn) + \sum_{a \mid m, b \mid n \atop a, b > 1} g(a)g(b)\left( \frac{m}{a} \right)f\left( \frac{n}{b} \right) \\
  &= f(mn) - f(m)f(n) + \sum_{a \mid m, b \mid n} g(a)g(b)\left( \frac{m}{a} \right)f\left( \frac{n}{b} \right) \\
  &= f(mn) - f(m)f(n) + \sum_{a \mid m} g(a)\left( \frac{m}{a} \right) \cdot \sum_{b \mid n} g(b)f\left( \frac{n}{b} \right) \\
  &= f(mn) - f(m)f(n) + h(m)h(n).
\end{align*}
\]
It follows from this that since \( f(mn) \neq f(m)f(n) \), we must have \( h(mn) \neq h(m)h(n) \) as well, contradicting the fact that \( h \) is multiplicative. //

**Corollary** If \( f \) is an arithmetic function whose summation function \( F(n) = \sum_{d|n} f(d) \) is multiplicative, then \( f \) must be multiplicative also.

**Proof** \( F = f \ast u \), so if \( F \) is multiplicative, then \( f \) must be as well, for we know that \( u \) is. //

The properties of the Dirichlet product appear to suggest that it is a group operation on multiplicative functions. This is in fact the case.

**Proposition** Any arithmetic function \( f \) for which \( f(1) \neq 0 \) has a unique **Dirichlet inverse** \( f^{-1} \). In other words, there exists another arithmetic function \( g = f^{-1} \) so that \( f \ast g = I \).

**Proof** Define \( g \) so that \( g(1) = 1/f(1) \) and for \( n > 1 \),

\[
g(n) = -\frac{1}{f(1)} \cdot \sum_{d|n, d>1} f(d)g\left(\frac{n}{d}\right).
\]

Then \( (f \ast g)(1) = f(1)g(1) = 1 \), and if \( n > 1 \),
\[(f * g)(n) = f(1)g(n) + \sum_{d|n, d>1} f(d)g\left(\frac{n}{d}\right) = f(1)g(n) - f(1)g(n) = 0\]

so \(f * g = I\). The proof of the uniqueness is left as an exercise. //

Since any nonzero multiplicative function \(f\) must satisfy \(f(1) = 1 \neq 0\), all nonzero multiplicative functions have Dirichlet inverses.

**Proposition** The Dirichlet inverse of a nonzero multiplicative function is itself a nonzero multiplicative function.

**Proof** \(f * f^{-1} = I\), and \(f\) and \(I\) are multiplicative, so \(f^{-1}\) must be as multiplicative well. Further, if \(f^{-1}\) were the zero function, \(I(1) = (f * f^{-1})(1) = f(1)f^{-1}(1) = 1 \cdot 0 = 0\), which is impossible, so \(f^{-1}\) must be nonzero. //

The Möbius function plays an important role in the structure of these functions, by relating arithmetic functions with their associated summation functions.
The Möbius Inversion Formula  Let \( f \) be any arithmetic function and let \( F(n) = \sum_{d|n} f(d) = (f * u)(n) \) be its summation function. Then
\[
f(n) = (\mu * F)(n) = \sum_{d|n} \mu(d) \cdot F\left(\frac{n}{d}\right) = \sum_{d|n} \mu\left(\frac{n}{d}\right) \cdot F(d).
\]

Proof  We proved above that \( \sum_{d|n} \mu(d) = I(n) \). This is equivalent to stating that \( \mu * u = I \). Therefore,
\[
F = f * u \Rightarrow \\
\mu * F = \mu * (f * u) = (f * u) * \mu = f * (u * \mu) = f * I = f.
\]
The final equality of the two summations is immediate, for as \( d \) runs through the set of divisors of \( n \), so does \( n/d \).

Since summation has the characteristic properties of integration, we may view “convolution with \( \mu \)” as an analogue of differentiation!