Number Theoretic Functions

J. J. P. Veerman*

July 17, 2017

Definition 0.1 A multiplicative function is a function \( f : \mathbb{N} \to \mathbb{C} \) that satisfies \( f(ab) = f(a)f(b) \) if \( \gcd(a, b) = 1 \).

A completely multiplicative function is one where the condition that \( \gcd(a, b) = 1 \) is not needed. Note that completely multiplicative implies multiplicative (but not vice versa).

In the statement of the following lemma, we use the Fundamental Theorem of Arithmetic to characterize the integer \( n \).

Lemma 0.2 Let \( n = \prod_{i=1}^{r} p_i^{\ell_i} \) where the \( p_i \) are primes. Denote \( \vec{a} = (a_1, a_2, \ldots, a_r) \) where \( a_i \) ranges over \( \{0, \ldots, \ell_i\} \). Then

i) the divisors of \( n \) are given by \( d_{\vec{a}} = \prod_{i=1}^{r} p_i^{a_i} \), and
ii) all these divisors are distinct.

Proof: Every \( d_{\vec{a}} = \prod_{i=1}^{r} p_i^{a_i} \) divides \( n \). If there is any other divisor, its factorization either contains a prime not in \( \{p_i\}_{i=1}^{r} \) or one of the \( p_i \) has a power greater than \( \ell_i \). Both are impossible.

The second statement is equivalent to

\[
\prod_{i=1}^{r} p_i^{a_i} = \prod_{i=1}^{r} p_i^{b_i} \iff \forall i : a_i = b_i
\]

This follows by dividing out the factors \( p_i^{m_i} \) where \( m_i = \min(a_i, b_i) \).

Proposition 0.3 Let \( f \) be a multiplicative function on the integers. Then

\[
F(n) = \sum_{d|n} f(d)
\]

is also multiplicative.

*Fariborz Maseeh Dept. of Math. and Stat., Portland State Univ.; e-mail: veerman@pdx.edu
Proof: Let \( n = \prod_{i=1}^{r} p_i^{\ell_i} \). The summation \( \sum_{d|n} f(d) \) can be written out using the previous lemma and the fact the \( f \) is multiplicative:

\[
F(n) = \sum_d f(d) = \sum_{a_1=0}^{\ell_1} \cdots \sum_{a_r=0}^{\ell_r} f(p_1^{a_1}) \cdots f(p_r^{a_r})
\]

\[
= \prod_{i=1}^{r} \left( \sum_{a_i=0}^{\ell_i} f(p_i^{a_i}) \right)
\]

Now let \( a \) and \( b \) two integers such that \( \gcd(a, b) = 1 \) and \( ab = n \). Then by the Unique Factorization Theorem \( a \) and \( b \) can be written as:

\[
a = \prod_{i=1}^{s} p_i^{\ell_i} \quad \text{and} \quad b = \prod_{i=s+1}^{r} p_i^{\ell_i}
\]

Applying the previous computation to \( a \) and \( b \) yields that \( f(a)f(b) = f(n) \).

The best known of these multiplicative are the ones where \( f(n) = n^k \) for some \( k \). Since these functions are special cases of the above construction, they are multiplicative.

Definition 0.4 Let \( k \in \mathbb{R} \). The multiplicative function \( \sigma_k : \mathbb{N} \to \mathbb{R} \) gives the sum of the \( k \)-th power of the positive divisors of \( n \). Equivalently:

\[
\sigma_k(n) = \sum_{d|n} d^k
\]

Special cases are when \( k = 1 \) and \( k = 0 \). In the first case, the function is simply the sum of the positive divisors. The subscript ‘1’ is usually dropped. When \( k = 0 \), the function is usually called \( \tau \), and the function is the number of positive divisors.

Theorem 0.5 Let \( n = \prod_{i=1}^{r} p_i^{\ell_i} \) where the \( p_i \) are primes. Then for \( k \neq 0 \)

\[
\sigma_k(n) = \prod_{i=1}^{r} \left( \frac{p_i^{k(\ell_i+1)} - 1}{p_i^k - 1} \right)
\]

while for \( k = 0 \)

\[
\sigma_0(n) = \tau(n) = \prod_{i=1}^{r} (1 + \ell_i)
\]

Proof: The summation can be written out using the previous lemma:

\[
\sigma_k(n) = \sum_{d|n} d^k = \sum_{a_1=0}^{\ell_1} \cdots \sum_{a_r=0}^{\ell_r} p_1^{a_1} \cdots p_r^{a_r}
\]

\[
= \prod_{i=1}^{r} \left( \sum_{a_i=0}^{\ell_i} p_i^{a_i} \right)
\]
Performing the sum for $k \neq 0$ (a geometric series) gives the first result. When $k = 0$, then $p^{k_{ai}} = 1$ and thus $\sum_{ai=0}^{\ell_i} p_i^{k_{ai}} = 1 + \ell_i$. This gives the second result. ■

However, there are other interesting multiplicative functions beside the powers of the divisors. The Möbius function defined below is one of these, as we will see.

**Definition 0.6** The Möbius function $\mu : \mathbb{N} \to \mathbb{Z}$ is given by: $\mu(1) = 1$ and $\mu(n)$ equals $(-1)^r$ if $n > 1$ is square-free with $r$ prime factors and 0 if $n > 1$ is not square-free. That is:

$$
\mu(n) = \begin{cases} 
1 & \text{if } n = 1 \\
0 & \text{if } \exists p > 1 \text{ with } p^2 | n \\
(-1)^r & \text{if } n = p_1 \cdots p_r \text{ and } p_i \text{ are distinct primes}
\end{cases}
$$

**Lemma 0.7** Define $G(n) \equiv \sum_{d|n} \mu(d)$. Then $G(1) = 1$ and for all $n > 1$, $G(n) = 0$.

**Proof:** It is a straightforward exercise to show that $\mu$ is multiplicative. Therefore $F$ is also multiplicative. It follows that $F(\prod_{i=1}^{r} p_i^{\ell_i})$ can be calculated by evaluating a product of terms like $F(p^\ell)$ where $p$ is prime. The latter is easily seen to be zero unless $\ell = 0$. ■

**Theorem 0.8 (Möbius inversion)** Let $F : \mathbb{N} \to \mathbb{C}$ be any number-theoretic function be given. Then the equation

$$
F(n) = \sum_{d|n} f(d)
$$

determines a unique solution $f : \mathbb{N} \to \mathbb{C}$, given by:

$$
f(d) = \sum_{e|d} \mu(e) F\left(\frac{d}{e}\right)
$$

**Proof of existence:** We show that the given solution satisfies the equation. Define $H$ as

$$
H(n) \equiv \sum_{d|n} f(d) = \sum_{d|n} \sum_{e|d} \mu(e) F\left(\frac{d}{e}\right)
$$

Then we need to prove that $H(n) = F(n)$. This proceeds in three steps. For the first step we write $k = \frac{d}{e}$ and note that if $e$ runs through all divisors of $d$, then so does $k$. Thus we have:

$$
H(n) = \sum_{d|n} \sum_{k|d} \mu\left(\frac{d}{k}\right) F(k)
$$

3
For the second step we fix $k$. The coefficients of $F(k)$ are the set of $\mu(r)$ where

$$r = \frac{d}{k} \quad \text{and} \quad d|n$$

Equivalently,

$$r \mid \left( \frac{n}{k} \right) \quad \text{and} \quad k|n$$

This gives:

$$H(n) = \sum_{d|n} \left( \sum_{r|\left( \frac{n}{k} \right)} \mu(r) \right) F(k)$$

Finally, Lemma 0.7 implies that the term in parentheses equals $G \left( \frac{n}{k} \right)$. It equals 0 except when $k = 1$ when it equals 1. The result follows.

**Proof of uniqueness:** Suppose there are two solutions $f$ and $g$. We have:

$$F(n) = \sum_{d|n} f(d) = \sum_{d|n} g(d)$$

We show by induction on $n$ that $f(n) = g(n)$.

Clearly $F(1) = f(1) = g(1)$. Now suppose that for $i \in \{1, \cdots k\}$, we have $f(i) = g(i)$. Then

$$F(k + 1) = \left( \sum_{d|(k+1), d \leq k} f(d) \right) + f(k + 1) = \left( \sum_{d|(k+1), d \leq k} g(d) \right) + g(k + 1)$$

So that the desired equality for $k + 1$ follows from the induction hypothesis.

**Definition 0.9** Euler’s phi function, also called Euler’s totient function is defined as follows. $\phi(n)$ equals the number of integers in $\{1, \cdots n\}$ that are relative prime to $n$.

**Lemma 0.10 (Gauss)** For $n \in \mathbb{N}$: $n = \sum_{d|n} \phi(d)$.

**Proof:** Define $S(d, n)$ as the set of integers $m$ between 1 and $n$ such that $\gcd(m, n) = d$:

$$S(d, n) = \{m \in \mathbb{N} \mid m \leq n \quad \text{and} \quad \gcd(m, n) = d\}$$

This is equivalent to

$$S(d, n) = \{m \in \mathbb{N} \mid m \leq n \quad \text{and} \quad \gcd\left( \frac{m}{d}, \frac{n}{d} \right) = 1\}$$
From the definition of Euler’s phi function, we see that the cardinality $|S(d, n)|$ of $S(d, n)$ (that is: the number of elements contained in the set) is given by $\phi\left(\frac{n}{d}\right)$. Thus we obtain:

$$n = \sum_{d|n} |S(d, n)| = \sum_{d|n} \phi\left(\frac{n}{d}\right)$$

As $d$ runs through all divisors of $n$ in the last sum, so does $\frac{n}{d}$. Therefore the last sum is equal to $\sum_{d|n} \phi(d)$, which proves the lemma.

**Theorem 0.11** Let $\prod_{i=1}^{r} p_i^{e_i}$ be the prime power factorization of $n$. Then $\phi(n) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right)$.

**Proof:** Apply Möbius inversion to Lemma 0.10:

$$\phi(n) = \sum_{d|n} \mu(d) \frac{n}{d} = n \sum_{d|n} \frac{\mu(d)}{d} \quad (0.1)$$

The functions $\mu$ and $d \rightarrow \frac{1}{d}$ are multiplicative. It is easy to see that the product of two multiplicative functions is also multiplicative. Therefore $d \rightarrow \frac{n(d)}{d}$ is also multiplicative (Proposition 0.3). Thus

$$\phi \left( \prod_{i=1}^{r} p_i^{e_i} \right) = \prod_{i=1}^{r} \phi(p_i^{e_i}) \quad (0.2)$$

So it is sufficient to evaluate the function $\phi$ on prime powers. Noting that the divisors of the prime power $p^\ell$ are $\{1, p, \ldots, p^\ell\}$, we get from Equation 0.1

$$\phi(p^\ell) = p^\ell \sum_{j=0}^{\ell} \frac{\mu(p^j)}{p^j} = p^\ell \left(1 - \frac{1}{p}\right)$$

Substituting this into Equation 0.2 completes the proof.