Introduction to Analytic Number Theory

Math 531 Lecture Notes, Fall 2005

A.J. Hildebrand
Department of Mathematics
University of Illinois

http://www.math.uiuc.edu/~hildebr/ant

Version 2013.01.07

Chapter 1

Arithmetic functions I: Elementary theory

1.1 Introduction and basic examples

A simple, but very useful concept in number theory is that of an **arithmetic function**. An arithmetic function is any real- or complex-valued function defined on the set $\mathbb{N}$ of positive integers. (In other words, an arithmetic function is just a *sequence* of real or complex numbers, though this point of view is not particularly useful.)

Examples

(1) **Constant function:** The function defined by $f(n) = c$ for all n, where c is a constant, is denoted by c; in particular, 1 denotes the function that is equal to 1 for all n.

(2) **Unit function:** $e(n)$, defined by $e(1) = 1$ and $e(n) = 0$ for $n \geq 2$.

(3) **Identity function:** $\mathrm{id}(n)$; defined by $\mathrm{id}(n) = n$ for all n.

(4) **Logarithm:** $\log n$, the (natural) logarithm, restricted to $\mathbb{N}$ and regarded as an arithmetic function.

(5) **Moebius function:** $\mu(n)$, defined by $\mu(1) = 1$, $\mu(n) = 0$ if n is not squarefree (i.e., divisible by the square of a prime), and $\mu(n) = (-1)^k$ if n is composed of k *distinct* prime factors (i.e., $n = \prod_i^k p_i$).

(6) **Characteristic function of squarefree integers:** $\mu^2(n)$ or $|\mu(n)|$. From the definition of the Moebius function, it follows that the absolute value (or, equivalently, the square) of μ is the characteristic function of the squarefree integers.

(7) **Liouville function:** $\lambda(n)$, defined by $\lambda(1) = 1$ and $\lambda(n) = (-1)^k$ if n is composed of k *not necessarily distinct* prime factors (i.e., if $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ then $\lambda(n) = \prod_{i=1}^{k}(-1)^{\alpha_i}$).

(8) **Euler phi (totient) function:** $\phi(n)$, the number of positive integers $m \leq n$ that are relatively prime to n; i.e., $\phi(n) = \sum_{m=1,(m,n)=1}^{n} 1$.

(9) **Divisor function:** $d(n)$, the number of positive divisors of n (including the trivial divisors $d = 1$ and $d = n$); i.e., $d(n) = \sum_{d|n} 1$. (Another common notation for this function is $\tau(n)$.)

(10) **Sum-of-divisors function:** $\sigma(n)$, the sum over all positive divisors of n; i.e., $\sigma(n) = \sum_{d|n} d$.

(11) **Generalized sum-of-divisors functions:** $\sigma_\alpha(n)$, defined by $\sigma_\alpha(n) = \sum_{d|n} d^\alpha$. Here α can be any real or complex parameter. This function generalizes the divisor function ($\alpha = 0$) and the sum-of-divisors function ($\alpha = 1$).

(12) **Number of distinct prime factors:** $\omega(n)$, defined by $\omega(1) = 0$ and $\omega(n) = k$ if $n \geq 2$ and $n = \prod_{i=1}^{k} p_i^{\alpha_i}$; i.e., $\omega(n) = \sum_{p|n} 1$.

(13) **Total number of prime divisors:** $\Omega(n)$, defined in the same way as $\omega(n)$, except that prime divisors are counted with multiplicity. Thus, $\Omega(1) = 0$ and $\Omega(n) = \sum_{i=1}^{k} \alpha_i$ if $n \geq 2$ and $n = \prod_{i=1}^{k} p_i^{\alpha_i}$; i.e., $\Omega(n) = \sum_{p^m|n} 1$. For squarefree integers n, the functions $\omega(n)$ and $\Omega(n)$ are equal and are related to the Moebius function by $\mu(n) = (-1)^{\omega(n)}$. For all integers n, $\lambda(n) = (-1)^{\Omega(n)}$.

(14) **Ramanujan sums:** Given a positive integer q, the Ramanujan sum c_q is the arithmetic function defined by $c_q(n) = \sum_{a=1,(a,q)=1}^{q} e^{2\pi i a n/q}$.

(15) **Von Mangoldt function:** $\Lambda(n)$, defined by $\Lambda(n) = 0$ if n is not a prime power, and $\Lambda(p^m) = \log p$ for any prime power p^m.

1.2 Additive and multiplicative functions

Many important arithmetic functions are multiplicative or additive functions, in the sense of the following definition.

Definition. An arithmetic function f is called **multiplicative** if $f \not\equiv 0$ and

$$f(n_1 n_2) = f(n_1) f(n_2) \quad \text{whenever } (n_1, n_2) = 1; \tag{1.1}$$

f is called **additive** if it satisfies

$$f(n_1 n_2) = f(n_1) + f(n_2) \quad \text{whenever } (n_1, n_2) = 1. \tag{1.2}$$

If this condition holds without the restriction $(n_1, n_2) = 1$, then f is called **completely (or totally) multiplicative** resp. **completely (or totally) additive**.

The condition (1.1) can be used to prove the multiplicativity of a given function. (There are also other, indirect, methods for establishing multiplicativity, which we will discuss in the following sections.) However, in order to exploit the multiplicativity of a function known to be multiplicative, the criterion of the following theorem is usually more useful.

Theorem 1.1 (Characterization of multiplicative functions)**.** *An arithmetic function f is multiplicative if and only if $f(1) = 1$ and, for $n \geq 2$,*

$$f(n) = \prod_{p^m || n} f(p^m). \tag{1.3}$$

The function f is completely multiplicative if and only if the above condition is satisfied and, in addition, $f(p^m) = f(p)^m$ for all prime powers p^m.

Remarks. (i) The result shows that a multiplicative function is uniquely determined by its values on prime powers, and a completely multiplicative function is uniquely determined by its values on primes.

(ii) With the convention that an empty product is to be interpreted as 1, the condition $f(1) = 1$ can be regarded as the special case $n = 1$ of (1.3). With this interpretation, f is multiplicative if and only if f satisfies (1.3) for all $n \in \mathbb{N}$.

Proof. Suppose first that f satisfies $f(1) = 1$ and (1.3) for $n \geq 2$. If n_1 and n_2 are positive integers with $(n_1, n_2) = 1$, then the prime factorizations of n_1 and n_2 involve disjoint sets of prime powers, so expressing each of $f(n_1)$,

$f(n_2)$, and $f(n_1 n_2)$ by (1.3) we see that f satisfies (1.1). Moreover, since $f(1) = 1$, f cannot be identically 0. Hence f is multiplicative.

Conversely, suppose that f is multiplicative. Then f is not identically 0, so there exists $n \in \mathbb{N}$ such that $f(n) \neq 0$. Applying (1.3) with $(n_1, n_2) = (n, 1)$, we obtain $f(n) = f(1 \cdot n) = f(1)f(n)$, which yields $f(1) = 1$, upon dividing by $f(n)$.

Next, let $n \geq 2$ be given with prime factorization $n = \prod_{i=1}^{k} p_i^{\alpha_i}$. "Shaving off" prime powers one at a time, and applying (1.3) inductively, we have

$$\begin{aligned} f(n) &= f\left(p_1^{\alpha_1} \cdots p_k^{\alpha_k}\right) = f\left(p_1^{\alpha_1} \cdots p_{k-1}^{\alpha_{k-1}}\right) f\left(p_k^{\alpha_k}\right) \\ &= \cdots = f\left(p_1^{\alpha_1}\right) \cdots f\left(p_k^{\alpha_k}\right), \end{aligned}$$

so (1.3) holds.

If f is completely multiplicative, then for any prime power p^m we have

$$f(p^m) = f(p^{m-1} \cdot p) = f(p^{m-1})f(p) = \cdots = f(p)^m.$$

Conversely, if f is multiplicative and satisfies $f(p^m) = f(p)^m$ for all prime powers p^m, then (1.3) can be written as $f(n) = \prod_{i=1}^{r} f(p_i)$, where now $n = \prod_{i=1}^{r} p_i$ is the factorization of n into single *(not necessarily distinct)* prime factors p_i. Since, for any two positive integers n_1 and n_2, the product of the corresponding factorizations is the factorization of the product, it follows that the multiplicativity property $f(n_1 n_2) = f(n_1)f(n_2)$ holds for any pair (n_1, n_2) of positive integers. Hence f is completely multiplicative. □

Theorem 1.2 (Products and quotients of multiplicative functions)**.** *Assume f and g are multiplicative function. Then:*

(i) The (pointwise) product fg defined by $(fg)(n) = f(n)g(n)$ is multiplicative.

(ii) If g is non-zero, then the quotient f/g (again defined pointwise) is multiplicative.

Proof. The result is immediate from the definition of multiplicativity. □

Analogous properties hold for additive functions: an additive function satisfies $f(1) = 0$ and $f(n) = \sum_{p^m || m} f(p^m)$, and the pointwise sums and differences of additive functions are additive.

Tables 1.1 and 1.2 below list the most important multiplicative and additive arithmetic functions, along with their values at prime powers, and basic properties. (Properties that are not obvious from the definition will be established in the following sections.)

Function	**value at n**	**value at p^m**	**properties**
$e(n)$	1 if $n = 1$, 0 else	0	unit element w.r.t. Dirichlet product, $\boxed{e * f = f * e = f}$
$\mathrm{id}(n)$ (identity function)	n	p^m	
$s(n)$ (char. fct. of squares)	1 if $n = m^2$ with $m \in \mathbb{N}$, 0 else	1 if m is even, 0 if m is odd	
$\mu^2(n)$ (char. fct. of squarefree integers)	1 if n is squarefree, 0 else	1 if $m = 1$, 0 if $m > 1$	
$\mu(n)$ (Moebius function)	1 if $n = 1$, $(-1)^k$ if $n = \prod_{i=1}^k p_i$ (p_i distinct), 0 otherwise	-1 if $m = 1$, 0 if $m > 1$	$\sum_{d\|n} \mu(d) = 0$ if $n \geq 2$ $\boxed{\mu * 1 = e}$
$\lambda(n)$ (Liouville function)	1 if $n = 1$, $(-1)^{\sum_{i=1}^k \alpha_i}$ if $n = \prod_{i=1}^k p_i^{\alpha_i}$	$(-1)^m$	$\sum_{d\|n} \lambda(d) = s(n)$ $\boxed{\lambda * 1 = s}$
$\phi(n)$ (Euler phi function)	$\#\{1 \leq m \leq n : (m, n) = 1\}$	$p^m(1 - 1/p)$	$\sum_{d\|n} \phi(d) = n$ $\boxed{\phi * 1 = \mathrm{id}}$
$d(n)\,(= \tau(n))$ (divisor function)	$\sum_{d\|n} 1$	$m + 1$	$\boxed{d = 1 * 1}$
$\sigma(n)$ (sum of divisor function)	$\sum_{d\|n} d$	$\dfrac{p^{m+1} - 1}{p - 1}$	$\boxed{\sigma = 1 * \mathrm{id}}$

Table 1.1: Some important multiplicative functions

Function	**value at n**	**value at p^m**	**properties**
$\omega(n)$ (number of distinct prime factors)	0 if $n = 1$, k if $n = \prod_{i=1}^{k} p_i^{\alpha_i}$	1	additive
$\Omega(n)$ (total number of prime factors)	0 if $n = 1$, $\sum_{i=1}^{k} \alpha_i$ if $n = \prod_{i=1}^{k} p_i^{\alpha_i}$	m	completely additive
$\log n$ (logarithm)	$\log n$	$\log p^m$	completely additive
$\Lambda(n)$ (von Mangoldt function)	$\log p$ if $n = p^m$, 0 if n is not a prime power	$\log p$	neither additive nor multiplicative $\boxed{\log = \Lambda * 1}$

Table 1.2: Some other important arithmetic functions

1.3 The Moebius function

The fundamental property of the Moebius function is given in the following theorem.

Theorem 1.3 (Moebius identity)**.** *For all $n \in \mathbb{N}$, $\sum_{d|n} \mu(d) = e(n)$; i.e., the sum $\sum_{d|n} \mu(d)$ is zero unless $n = 1$, in which case it is 1.*

Proof. There are many ways to prove this important identity; we give here a combinatorial proof that does not require any special tricks or techniques. We will later give alternate proofs, which are simpler and more elegant, but which depend on some results in the theory of arithmetic functions.

If $n = 1$, then the sum $\sum_{d|n} \mu(d)$ reduces to the single term $\mu(1) = 1$, so the asserted formula holds in this case. Next, suppose $n \geq 2$ and let $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ be the canonical prime factorization of n. Since $\mu(d) = 0$ if d is not squarefree, the sum over d can be restricted to divisors of the form $d = \prod_{i \in I} p_i$, where $I \subset \{1, 2, \ldots, k\}$, and each such divisor contributes a

term $\mu(d) = (-1)^{|I|}$. Hence,

$$\sum_{d|n} \mu(d) = \sum_{I \subset \{1,\ldots,k\}} (-1)^{|I|}.$$

Now note that, for any $r \in \{0, 1, \ldots, k\}$, there are $\binom{k}{r}$ subsets I with $|I| = r$, and for each such subset the summand $(-1)^{|I|}$ is equal to $(-1)^r$. Hence the above sum reduces to

$$\sum_{r=0}^{k} (-1)^r \binom{k}{r} = (1-1)^k = 0,$$

by the binomial theorem. (Note that $k \geq 1$, since we assumed $n \geq 2$.) Hence we have $\sum_{d|n} \mu(d) = 0$ for $n \geq 2$, as claimed. □

Motivation for the Moebius function. The identity given in this theorem is the main reason for the peculiar definition of the Moebius function, which may seem rather artificial. In particular, the definition of $\mu(n)$ as 0 when n is not squarefree appears to be unmotivated. The Liouville function $\lambda(n)$, which is identical to the Moebius function on squarefree integers, but whose definition extends to non-squarefree integers in a natural way, appears to be a much more natural function to work with. However, this function does not satisfy the identity of the theorem, and it is this identity that underlies most of the applications of the Moebius function.

Application: Evaluation of sums involving a coprimality condition. The identity of the theorem states that $\sum_{d|n} \mu(d)$ is the characteristic function of the integer $n = 1$. This fact can be used to extract specific terms from a series. A typical application is the evaluation of sums over integers n that are relatively prime to a given integer k. By the theorem, the characteristic function of integers n with $(n, k) = 1$ is given by $\sum_{d|(n,k)} \mu(d)$. Since the condition $d|(n, k)$ is equivalent to the simultaneous conditions $d|n$ and $d|k$, one can formally rewrite a sum $\sum_{n,(n,k)=1} f(n)$ as follows:

$$\begin{aligned}\sum_{\substack{n \\ (n,k)=1}} f(n) &= \sum_{n} f(n) e((n,k)) = \sum_{n} f(n) \sum_{d|(n,k)} \mu(n) \\ &= \sum_{d|k} \mu(d) \sum_{\substack{n \\ d|n}} f(n) = \sum_{d|k} \mu(d) \sum_{m} f(dm).\end{aligned}$$

The latter sum can usually be evaluated, and doing so yields a formula for the original sum. (Of course, one has to make sure that the series involved converge.) The following examples illustrate the general method.

Evaluation of the Euler phi function. By definition, the Euler phi function is given by $\phi(n) = \sum_{m\le n,(m,n)=1} 1$. Eliminating the coprimality condition $(m,n)=1$, as indicated above, yields the identity

$$\phi(n) = \sum_{m\le n}\sum_{d|(m,n)} \mu(d) = \sum_{d|n}\mu(d)\sum_{m\le n, d|m} 1 = \sum_{d|n}\mu(d)(n/d).$$

(For an alternative proof of this identity see Section 1.7.)

Ramanujan sums. The functions $c_q(n) = \sum_{a=1,(a,q)=1}^{q} \exp(2\pi i a n/q)$, where q is a positive integer, are called Ramanujan sums. By eliminating the condition $(a,q)=1$ using the above method, one can show that $c_q(n) = \sum_{d|(q,n)} d\mu(q/d)$. When $n=1$, this formula reduces to $c_q(1) = \mu(q)$, and we obtain the remarkable identity $\sum_{a=1,(a,q)=1}^{q} \exp(2\pi i a/q) = \mu(q)$, which shows that the sum over all "primitive" k-th roots of unity is equal to $\mu(q)$.

A weighted average of the Moebius function. While the estimation of the partial sums of the Moebius function $\sum_{n\le x}\mu(n)$ is a very deep (and largely unsolved) problem, remarkably enough a weighted version of this sum, namely $\sum_{n\le x}\mu(n)/n$ is easy to bound. In fact, we will prove:

Theorem 1.4. *For any real $x \ge 1$ we have*

$$\left|\sum_{n\le x}\frac{\mu(n)}{n}\right| \le 1. \tag{1.4}$$

Proof. Note first that, without loss of generality, one can assume that $x = N$, where N is a positive integer. We then evaluate the sum $S(N) = \sum_{n\le N} e(n)$ in two different ways. On the one hand, by the definition of $e(n)$, we have $S(N) = 1$; on the other hand, writing $e(n) = \sum_{d|n}\mu(d)$ and interchanging summations, we obtain $S(N) = \sum_{d\le N}\mu(d)[N/d]$, where $[t]$ denotes the greatest integer $\le t$. Now, for $d \le N-1$, $[N/d]$ differs from N/d by an amount that is bounded by 1 in absolute value, while for $d = N$, the

quantities $[N/d]$ and N/d are equal. Replacing $[N/d]$ by N/d and bounding the resulting error, we therefore obtain

$$\left| S(N) - N \sum_{d \le N} \frac{\mu(d)}{d} \right| \le \sum_{d \le N} |\mu(d)| \cdot |[N/d] - (N/d)| \le \sum_{d \le N-1} |\mu(d)| \le N - 1.$$

Hence,

$$\left| N \sum_{d \le N} \frac{\mu(d)}{d} \right| \le (N-1) + |S(N)| = (N-1) + 1 = N,$$

which proves (1.4). □

The Moebius function and the Prime Number Theorem. Part of the interest in studying the Moebius function stems from the fact that the behavior of this function is intimately related to the Prime Number Theorem (PNT), which says that the number $\pi(x)$ of primes below x is asymptotically equal to $x/\log x$ as $x \to \infty$ and which is one of the main results of Analytic Number Theory. We will show later that the PNT is "equivalent" to the fact that $\mu(n)$ has average value ("mean value") zero, i.e., $\lim_{x\to\infty}(1/x)\sum_{n\le x}\mu(n) = 0$. The latter statement has the following probabilistic interpretation: If a squarefree integer is chosen at random, then it is equally likely to have an even and an odd number of prime factors.

Mertens' conjecture. A famous conjecture, attributed to Mertens (though it apparently was first stated by Stieltjes who mistakenly believed that he had proved it) asserts that $|\sum_{n\le x}\mu(n)| \le \sqrt{x}$ for all $x \ge 1$. This conjecture had remained open for more than a century, but was disproved (though only barely!) in 1985 by A. Odlyzko and H. te Riele, who used extensive computer calculations, along with some theoretical arguments, to show that the above sum exceeds $1.06\sqrt{x}$ for infinitely many x. Whether the constant 1.06 can be replaced by any constant c is still an open problem. Heuristic arguments, based on the assumption that the values ± 1 of the Moebius function on squarefree integers are distributed like a random sequence of numbers ± 1, strongly suggest that this is the case, but a proof has remained elusive so far.

1.4 The Euler phi (totient) function

Theorem 1.5. *The Euler phi function satisfies:*

(i) $\sum_{d|n} \phi(d) = n$ *for all* $n \in \mathbb{N}$.

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

(iii) ϕ *is multiplicative.*

(iv) $\phi(n) = \prod_{p^m||n}(p^m - p^{m-1}) = n\prod_{p|n}(1 - 1/p)$ *for all* $n \in \mathbb{N}$.

Proof. (i) Split the set $A = \{1, 2, \ldots, n\}$ into the pairwise disjoint subsets $A_d = \{m \in A : (m, n) = d\}$, $d|n$. Writing an element $m \in A_d$ as $m = dm'$, we see that $A_d = \{dm' : 1 \leq m' \leq n/d, (m', n/d) = 1\}$, and so $|A_d| = \phi(n/d)$. Since $n = |A| = \sum_{d|n} |A_d|$, it follows that $n = \sum_{d|n} \phi(n/d)$. Writing $d' = n/d$ and noting that, as d runs over all positive divisors of n, so does d', we obtain the desired identity.

(ii) This identity was proved in the last section. Alternatively, as we shall show in Section 1.7, one can derive it from the identity (i).

(iii) We defer the proof of the multiplicativity until Section 1.7.

(iv) This follows immediately from the multiplicativity of ϕ and the fact that, at $n = p^m$, $\phi(p^m) = p^m - p^{m-1}$. To see the latter formula, note that an integer is relatively prime to p^m if and only if it is not a multiple of p and that of the p^m positive integers $\leq p^m$ exactly p^{m-1} are multiples of p. □

Formula (iv) of the theorem can be used to quickly compute values of ϕ. For example, the first 7 values are $\phi(1) = 1$, $\phi(2) = (2 - 1) = 1$, $\phi(3) = (3-1) = 2$, $\phi(4) = (2^2-2) = 2$, $\phi(5) = (5-1) = 4$, $\phi(6) = \phi(2\cdot 3) = (2 - 1)(3 - 1) = 2$, $\phi(7) = (7 - 1) = 6$.

Carmichael's conjecture. It is easy to see that not every positive integer occurs as a value of ϕ; for example, $\phi(n)$ is never equal to an odd prime. In other words, the range of ϕ is a proper subset of $\mathbb{N}$. At the beginning of this century, R.D. Carmichael, a professor at the University of Illinois and author of a textbook on number theory, observed that there seems to be no integer that appears exactly once as a value of ϕ; in other words, for each $m \in \mathbb{N}$, the pre-image $\phi^{-1}(m) = \{n \in \mathbb{N} : \phi(n) = m\}$ has either cardinality 0 or has cardinality ≥ 2. In fact, Carmichael claimed to have a proof of this result and included the "proof" as an exercise in his number theory textbook, but his "proof" was incorrect, and he later retracted the claim; he changed the

wording of the exercise, calling the result an "empirical theorem." This "empirical theorem" is still open to this date, and has become a famous conjecture, known as "Carmichael's conjecture," The numerical evidence for the conjecture is overwhelming: the conjecture (that the cardinality of $\phi^{-1}(m)$ is never 1) is true for values m up to $10^{10^{10}}$. While the conjecture is still open, Kevin Ford, a former UIUC graduate student and now a faculty member here, proved a number of related conjectures. In particular, he showed that for every integer $k \geq 2$ there exist infinitely many m such that $\phi^{-1}(m)$ has cardinality k. This was known as "Sierpinski's conjecture", and it complements Carmichael's conjecture which asserts that in the case $k = 1$, the only case not covered by Sierpinski's conjecture, the assertion of Sierpinski's conjecture is not true.

1.5 The von Mangoldt function

The definition of the von Mangoldt function may seem strange at first glance. One motivation for this peculiar definition lies in the following identity.

Theorem 1.6. *We have*

$$\sum_{d|n} \Lambda(d) = \log n \quad (n \in \mathbb{N}).$$

Proof. For $n = 1$, the identity holds since $\Lambda(1) = 0 = \log 1$. For $n \geq 2$ we have, by the definition of Λ,

$$\sum_{d|n} \Lambda(d) = \sum_{p^m|n} \log p = \log n.$$

(For the last step note that, for each prime power $p^\alpha||n$, each of the terms $p^1, p^2, \ldots, p^\alpha$ contributes a term $\log p$ to the sum, so the total contribution arising from powers of p is $\alpha(\log p) = \log p^\alpha$. Adding up those contributions over all prime powers $p^\alpha||n$, gives $\sum_{p^\alpha||n} \log p^\alpha = \log \prod_{p^\alpha||n} p^\alpha = \log n$.) □

The main motivation for introducing the von Mangoldt function is that the partial sums $\sum_{n\leq x} \Lambda(n)$ represent a weighted count of the prime powers $p^m \leq x$, with the weights being $\log p$, the "correct" weights to offset the density of primes. It is not hard to show that higher prime powers (i.e., those with $m \geq 2$) contribute little to the above sum, so the sum is essentially a weighted sum over prime numbers. In fact, studying the asymptotic behavior of the above sum is essentially equivalent to studying the behavior

of the prime counting function $\pi(x)$; for example, the PNT is equivalent to the assertion that $\lim_{x\to\infty}(1/x)\sum_{n\le x}\Lambda(n) = 1$. In fact, most proofs of the PNT proceed by first showing the latter relation, and then deducing from this the original form of the PNT. The reason for doing this is that, because of the identity in the above theorem (and some similar relations), working with $\Lambda(n)$ is technically easier than working directly with the characteristic function of primes.

1.6 The divisor and sum-of-divisors functions

Theorem 1.7. *The divisor function $d(n)$ and the sum-of-divisors function $\sigma(n)$ are multiplicative. Their values at prime powers are given by*

$$d(p^m) = m+1, \quad \sigma(p^m) = \frac{p^{m+1}-1}{p-1}.$$

Proof. To prove the multiplicativity of $d(n)$, let n_1 and n_2 be positive integers with $(n_1, n_2) = 1$. Note that if $d_1|n_1$ and $d_2|n_2$, then $d_1d_2|n_1n_2$. Conversely, by the coprimality condition and the fundamental theorem of arithmetic, any divisor d of n_1n_2 factors *uniquely* into a product $d = d_1d_2$, where $d_1|n_1$ and $d_2|n_2$. Thus, there is a $1-1$ correspondence between the set of divisors of n_1n_2 and the set of pairs (d_1, d_2) with $d_1|n_1$ and $d_2|n_2$. Since there are $d(n_1)d(n_2)$ such pairs and $d(n_1n_2)$ divisors of n_1n_2, we obtain $d(n_1n_2) = d(n_1)d(n_2)$, as required. The multiplicativity of $\sigma(n)$ can be proved in the same way. (Alternate proofs of the multiplicativity of d and σ will be given in the following section.)

The given values for $d(p^m)$ and $\sigma(p^m)$ are obtained on noting that the divisors of p^m are exactly the numbers $p^0, p^1, \ldots, p^m$. Since there are $m+1$ such divisors, we have $d(p^m) = m+1$, and applying the geometric series formula to the sum of these divisors gives the asserted formula for $\sigma(p^m)$. □

Perfect numbers. The sum-of-divisors function is important because of its connection to so-called **perfect numbers**, that is, positive integers n that are equal to the sum of all their *proper* divisors, i.e., all positive divisors except n itself. Since the divisor $d = n$ is counted in the definition of $\sigma(n)$, the sum of proper divisors of n is $\sigma(n) - n$. Thus, *an integer n is perfect if and only if $\sigma(n) = 2n$*. For example, 6 is perfect, since $6 = 1+2+3$. It is an unsolved problem whether there exist infinitely many perfect numbers. However, a result of Euler states:

Theorem (Euler)**.** *An* even *integer n is perfect if and only if n is of the form $n = 2^{p-1}(2^p - 1)$ where p is a prime and $2^p - 1$ is also prime.*

This result is not hard to prove, using the multiplicity of $\sigma(n)$. The problem with this characterization is that it is not known whether there exist infinitely many primes p such that $2^p - 1$ is also prime. (Primes of this form are called Mersenne primes, and whether there exist infinitely many of these is another famous open problem.)

There is no analogous characterization of odd perfect numbers; in fact, no single odd perfect number has been found, and it is an open problem whether odd perfect numbers exist.

1.7 The Dirichlet product of arithmetic functions

The two obvious operations on the set of arithmetic functions are pointwise addition and multiplication. The constant functions $f = 0$ and $f = 1$ are neutral elements with respect to these operations, and the additive and multiplicative inverses of a function f are given by $-f$ and $1/f$, respectively.

While these operations are sometimes useful, by far the most important operation among arithmetic functions is the so-called **Dirichlet product**, an operation that, at first glance, appears mysterious and unmotivated, but which has proved to be an extremely useful tool in the theory of arithmetic functions.

Definition. Given two arithmetic functions f and g, the **Dirichlet product** (or **Dirichlet convolution**) of f and g, denoted by $f * g$, is the arithmetic function defined by

$$(f * g)(n) = \sum_{d|n} f(d)g(n/d).$$

In particular, we have $(f * g)(1) = f(1)g(1)$, $(f * g)(p) = f(1)g(p) + f(p)g(1)$ for any prime p, and $(f * g)(p^m) = \sum_{k=0}^{m} f(p^k)g(p^{m-k})$ for any prime power p^m.

It is sometimes useful to write the Dirichlet product in the symmetric form

$$(f * g)(n) = \sum_{ab=n} f(a)g(b),$$

where the summation runs over all pairs (a, b) of positive integers whose product equals n. The equivalence of the two definitions follows immediately

from the fact that the pairs $(d, n/d)$, where d runs over all divisors of n, are exactly the pairs (a, b) of the above form.

One motivation for introducing this product is the fact that the definitions of many common arithmetic functions have the form of a Dirichlet product, and that many identities among arithmetic functions can be written concisely as identities involving Dirichlet products. Here are some examples:

Examples

(1) $d(n) = \sum_{d|n} 1$, so $d = 1 * 1$.

(2) $\sigma(n) = \sum_{d|n} d$, so $\sigma = \mathrm{id} * 1$.

(3) $\sum_{d|n} \mu(d) = e(n)$ (see Theorem 1.3), so $\mu * 1 = e$.

(4) $\sum_{d|n} \mu(d)(n/d) = \phi(n)$ (one of the applications of the Moebius identity, Theorem 1.3), so $\mu * \mathrm{id} = \phi$.

(5) $\sum_{d|n} \phi(d) = n$ (Theorem 1.5), so $\phi * 1 = \mathrm{id}$.

(6) $\sum_{d|n} \Lambda(d) = \log n$ (Theorem 1.6), so $\Lambda * 1 = \log$.

A second motivation for defining the Dirichlet product in the above manner is that this product has nice algebraic properties.

Theorem 1.8 (Properties of the Dirichlet product)**.**

(i) The function e acts as a unit element for $*$, i.e., $f * e = e * f = f$ for all arithmetic functions f.

(ii) The Dirichlet product is commutative, i.e., $f * g = g * f$ for all f and g.

(iii) The Dirichlet product is associative, i.e., $(f * g) * h = f * (g * h)$ for all f, g, h.

(iv) If $f(1) \neq 0$, then f has a unique Dirichlet inverse, i.e., there is a unique function g such that $f * g = e$.

Proof. (i) follows immediately from the definition of the Dirichlet product. For the proof of (ii) (commutativity) and (iii) (associativity) it is useful to work with the symmetric version of the Dirichlet product, i.e., $(f * g)(n) = \sum_{ab=n} f(a)g(b)$. The commutativity of $*$ is immediate from

this representation. To obtain the associativity, we apply this representation twice to get

$$((f*g)*h)(n) = \sum_{dc=n} (f*g)(d)h(c) = \sum_{dc=n}\sum_{ab=d} f(a)g(b)h(c)$$
$$= \sum_{abc=n} f(a)g(b)h(c),$$

where the last sum runs over all triples (a,b,c) of positive integers whose product is equal to n. Replacing (f,g,h) by (g,h,f) in this formula yields the same final (triple) sum, and we conclude that $(f*g)*h = (g*h)*f = f*(g*h)$, proving that $*$ is associative.

It remains to prove (iv). Let f be an arithmetic function with $f(1) \neq 0$. By definition, a function g is a Dirichlet inverse of f if $(f*g)(1) = e(1) = 1$ and $(f*g)(n) = e(n) = 0$ for all $n \geq 2$. Writing out the Dirichlet product $(f*g)(n)$, we see that this is equivalent to the infinite system of equations

$$(A_1) \qquad f(1)g(1) = 1,$$
$$(A_n) \qquad \sum_{d|n} g(d)f(n/d) = 0 \quad (n \geq 2).$$

We need to show that the system $(A_n)_{n=1}^{\infty}$ has a unique solution g. We do this by inductively constructing the values $g(n)$ and showing that these values are uniquely determined.

For $n = 1$, equation (A_1) gives $g(1) = 1/f(1)$, which is well defined since $f(1) \neq 0$. Hence, $g(1)$ is uniquely defined and (A_1) holds. Let now $n \geq 2$, and suppose we have shown that there exist unique values $g(1), \ldots, g(n-1)$ so that equations (A_1)–(A_{n-1}) hold. Since $f(1) \neq 0$, equation (A_n) is equivalent to

$$g(n) = -\frac{1}{f(1)} \sum_{d|n, d<n} g(d)f(n/d). \tag{1.5}$$

Since the right-hand side involves only values $g(d)$ with $d < n$, this determines $g(n)$ uniquely, and defining $g(n)$ by (1.5) we see that (A_n) (in addition to (A_1)–(A_{n-1})) holds. This completes the induction argument. □

Examples

(1) Since $\mu * 1 = e$, the Moebius function is the Dirichlet inverse of the function 1.

(2) Multiplying the identity $\phi = \mu * \mathrm{id}$ (obtained in the last section) by 1 gives $\phi * 1 = 1 * \phi = 1 * \mu * \mathrm{id} = e * \mathrm{id} = \mathrm{id}$, so we get the identity $\phi * 1 = \mathrm{id}$ stated in Theorem 1.5.

The last example is a special case of an important general principle, which we state as a theorem.

Theorem 1.9 (Moebius inversion formula)**.** *If $g(n) = \sum_{d|n} f(d)$ for all $n \in \mathbb{N}$, then $f(n) = \sum_{d|n} g(d)\mu(n/d)$ for all n.*

Proof. The given relation can be written as $g = f * 1$. Taking the Dirichlet product of each side in this relation with the function μ we obtain $g * \mu = (f * 1) * \mu = f * (1 * \mu) = f * e = f$, which is the asserted relation. □

Finally, a third motivation for the definition of the Dirichlet product is that it preserves the important property of multiplicativity of a function, as shown in the following theorem. This is, again, by no means obvious.

Theorem 1.10 (Dirichlet product and multiplicative functions)**.**

(i) If f and g are multiplicative, then so is $f * g$.

(ii) If f is multiplicative, then so is the Dirichlet inverse f^{-1}.

(iii) If $f * g = h$ and if f and h are multiplicative, then so is g.

(iv) (Distributivity with pointwise multiplication) If h is completely multiplicative, then $h(f * g) = (hf) * (hg)$ for any functions f and g.

Remarks. (i) The product of two *completely* multiplicative functions is multiplicative (by the theorem), but not necessarily completely multiplicative. For example, the divisor function $d(n)$ can be expressed as a product $1 * 1$ in which each factor 1 is completely multiplicative, but the divisor function itself is only multiplicative in the restricted sense (i.e., with the coprimality condition). The same applies to the Dirichlet inverse: if f is completely multiplicative, then f^{-1} is multiplicative, but in general not completely multiplicative.

(ii) By Theorem 1.8, any function f with $f(1) \neq 0$ has a Dirichlet inverse. Since a multiplicative function satisfies $f(1) = 1$, any multiplicative function has a Dirichlet inverse.

(iii) Note that the distributivity asserted in property (iv) only holds when the function h is *completely* multiplicative. (In fact, one can show that this property characterizes completely multiplicative functions: If h is any non-zero function for which the identity in (iv) holds for all functions f and g, then h is necessarily completely multiplicative.)

Proof. (i) Let f and g be multiplicative and let $h = f * g$. Given n_1 and n_2 with $(n_1, n_2) = 1$, we need to show that $h(n_1 n_2) = h(n_1)h(n_2)$. To this end we use the fact (see the proof of Theorem 1.7) that each divisor $d|n_1 n_2$ can be factored uniquely as $d = d_1 d_2$ with $d_1|n_1$ and $d_2|n_2$, and that, conversely, given any pair (d_1, d_2) with $d_1|n_1$ and $d_2|n_2$, the product $d = d_1 d_2$ satisfies $d|n_1 n_2$. Hence

$$h(n_1 n_2) = \sum_{d|n_1 n_2} f(d)g(n_1 n_2/d) = \sum_{d_1|n_1} \sum_{d_2|n_2} f(d_1 d_2)g((n_1 n_2)/(d_1 d_2)).$$

Since $(n_1, n_2) = 1$, any divisors $d_1|n_1$ and $d_2|n_2$ satisfy $(d_1, d_2) = 1$ and $(n_1/d_1, n_2/d_2) = 1$. Hence, in the above double sum we can apply the multiplicativity of f and g to obtain

$$\begin{aligned} h(n_1 n_2) &= \sum_{d_1|n_1} \sum_{d_2|n_2} f(d_1)g(n/d_1)f(d_2)g(n_2/d_2) \\ &= (f * g)(n_1)(f * g)(n_2) = h(n_1)h(n_2), \end{aligned}$$

which is what we had to prove.

(ii) Let f be a multiplicative function and let g be the Dirichlet inverse of f. We prove the multiplicativity property

$$g(n_1 n_2) = g(n_1)g(n_2) \text{ if } (n_1, n_2) = 1 \tag{1.6}$$

by induction on the product $n = n_1 n_2$. If $n_1 n_2 = 1$, then $n_1 = n_2 = 1$, and (1.6) holds trivially. Let $n \geq 2$ be given, and suppose (1.6) holds whenever $n_1 n_2 < n$. Let n_1 and n_2 be given with $n_1 n_2 = n$ and $(n_1, n_2) = 1$. Applying the identity (A_n) above, we obtain, on using the multiplicativity of f and that of g for arguments $< n$,

$$\begin{aligned} 0 &= \sum_{d|n_1 n_2} f(d)g(n_1 n_2/d) \\ &= \sum_{d_1|n_1} \sum_{d_2|n_2} f(d_1)f(d_2)g(n_1/d_1)g(n_2/d_2) + (g(n_1 n_2) - g(n_1)g(n_2)) \\ &= (f * g)(n_1)(f * g)(n_2) + (g(n_1 n_2) - g(n_1)g(n_2)) \\ &= e(n_1)e(n_2) + (g(n_1 n_2) - g(n_1)g(n_2)), \\ &= g(n_1 n_2) - g(n_1)g(n_2), \end{aligned}$$

since, by our assumption $n = n_1 n_2 \geq 2$, at least one of n_1 and n_2 must be ≥ 2, and so $e(n_1)e(n_2) = 0$. Hence we have $g(n_1 n_2) = g(n_1)g(n_2)$. Thus,

(1.6) holds for pairs (n_1, n_2) of relatively prime integers with $n_1 n_2 = n$, and the induction argument is complete.

(iii) The identity $f * g = h$ implies $g = f^{-1} * h$, where f^{-1} is the Dirichlet inverse of f. Since f and h are multiplicative functions, so is f^{-1} (by (ii)) and $f^{-1} * h$ (by (i)). Hence g is multiplicative as well.

(iv) If h is completely multiplicative, then for any divisor $d|n$ we have $h(n) = h(d)h(n/d)$. Hence, for all n,

$$\begin{aligned} h(f*g)(n) &= h(n)\sum_{d|n} f(d)g(n/d) = \sum_{d|n} h(d)f(d)h(n/d)g(n/d) \\ &= ((hf)*(hg))(n), \end{aligned}$$

proving (iv). □

Application I: Proving identities for multiplicative arithmetic functions. The above results can be used to provide simple proofs of identities for arithmetic functions, using the multiplicativity of the functions involved. To prove an identity of the form $f * g = h$ in the case when f, g, and h are known to be multiplicative functions, one simply shows, by direct calculation, that $(*)$ $(f * g)(p^m) = h(p^m)$ holds for every prime power p^m. Since, by the above theorem, the multiplicativity of f and g implies that of $f * g$, and since multiplicative functions are uniquely determined by their values at prime powers, $(*)$ implies that the identity $(f * g)(n) = h(n)$ holds for all $n \in \mathbb{N}$.

Examples

(1) **Alternate proof of the identity $\sum_{d|n} \mu(d) = e(n)$.** The identity can be written as $\mu * 1 = e$, and since all three functions involved are multiplicative, it suffices to verify that the identity holds on prime powers. Since $e(p^m) = 0$ and $(\mu * 1)(p^m) = \sum_{k=0}^{m} \mu(p^k) = 1 - 1 + 0 - 0 \cdots = 0$, this is indeed the case.

(2) **Proof of $\sum_{d|n} \mu^2(d)/\phi(d) = n/\phi(n)$.** This identity is of the form $f * 1 = g$ with $f = \mu^2/\phi$ and $g = \mathrm{id}\,/\phi$. The functions f and g are both quotients of multiplicative functions and therefore are multiplicative. Hence all three functions in the identity $f * 1 = g$ are multiplicative, and it suffices to verify the identity at prime powers. We have $g(p^m) = p^m/\phi(p^m) = p^m/(p^m - p^{m-1}) = (1 - 1/p)^{-1}$, and $(f * 1)(p^m) = \sum_{k=0}^{m}(\mu^2(p^k)/\phi(p^k)) = 1 + 1/(p-1) = (1 - 1/p)^{-1}$, and

so $g(p^m) = (f * 1)(p^m)$ for every prime power p^m. Thus the identity holds at prime powers, and therefore it holds in general.

(3) **The Dirichlet inverse of λ.** Since $\mu * 1 = e$, the function 1 is the Dirichlet inverse of the Moebius function. To find the Dirichlet inverse of λ, i.e., the unique function f such that $\lambda * f = e$, note first that since λ and e are both multiplicative, f must be multiplicative as well, and it therefore suffices to evaluate f at prime powers. Now, for any prime power p^m,

$$0 = e(p^m) = \sum_{k=0}^{m} f(p^k)\lambda(p^{m-k}) = \sum_{k=0}^{m} f(p^k)(-1)^{m-k},$$

so $f(p^m) = -\sum_{k=0}^{m-1} f(p^k)(-1)^k$. This implies $f(p) = 1$, and by induction $f(p^m) = 0$ for $m \geq 2$. Hence f is the characteristic function of the squarefree numbers, i.e., $\lambda^{-1} = \mu^2$.

Application II: Evaluating Dirichlet products of multiplicative functions. Since the Dirichlet product of multiplicative functions is multiplicative, and since a multiplicative function is determined by its values on prime powers, to evaluate a product $f * g$ with both f and g multiplicative, it suffices to compute the values of $f * g$ at prime powers. By comparing these values to those of familiar arithmetic functions, one can often identify $f * g$ in terms of familiar arithmetic functions.

Examples

(1) **The function $\lambda * 1$.** We have $(\lambda * 1)(p^m) = \sum_{k=0}^{m} \lambda(p^k) = \sum_{k=0}^{m} (-1)^k$, which equals 1 if m is even, and 0 otherwise. However, the latter values are exactly the values at prime powers of the characteristic function of the squares, which is easily seen to be multiplicative. Hence $\lambda * 1$ is equal to the characteristic function of the squares.

(2) **The function $f_k(n) = \sum_{d|n,(d,k)=1} \mu(d)$.** Here k is a fixed positive integer, and the summation runs over those divisors of n that are relatively prime to k. We have $f_k = g_k * 1$, where $g_k(n) = \mu(n)$ if $(n, k) = 1$ and $g_k(n) = 0$ otherwise. It is easily seen that g_k is multiplicative, so f_k is also multiplicative. On prime powers p^m, $g_k(p^m) = -1$ if $m = 1$ and $p \nmid k$ and $g_k(p^m) = 0$ otherwise, so

$f_k(p^m) = \sum_{i=0}^{m} g(p^k) = 1 - 1 = 0$ if $p \nmid k$, and $f_k(p^m) = 1$ otherwise. By the multiplicativity of f_k it follows that f_k is the characteristic function of the set $A_k = \{n \in \mathbb{N} : p|n \Rightarrow p|k\}$.

Application III: Proving the multiplicativity of functions, using known identities. This is, in a sense, the previous application in reverse. Suppose we kow that $f * g = h$ and that f and h are multiplicative. Then, by Theorem 1.10, g must be multiplicative as well.

Examples

(1) **Multiplicativity of ϕ.** Since $\phi * 1 = \mathrm{id}$ (see Theorem 1.5) and the functions 1 and id are (obviously) multiplicative, the function ϕ must be multiplicative as well. This is the promised proof of the multiplicativity of the Euler function (part (ii) of Theorem 1.5).

(2) **Multiplicativity of $d(n)$ and $\sigma(n)$.** Since $d = 1 * 1$, and the function 1 is multiplicative, the function d is multiplicative as well. Similarly, since $\sigma = \mathrm{id} * 1$, and 1 and id are multiplicative, σ is multiplicative.

1.8 Exercises

1.1 Evaluate the function $f(n) = \sum_{d^2|n} \mu(d)$ (where the summation runs over all positive integers d such that $d^2|n$), in the sense of expressing it in terms of familiar arithmetic functions.

1.2 The *unitary divisor function* $d^*(n)$ is defined as the number of representations of n as a product of two *coprime* positive integers, i.e.,

$$d^*(n) = \{(a,b) \in \mathbb{N}^2 : ab = n,\ (a,b) = 1\}.$$

Show that d^* is multiplicative, and find its values on prime powers.

1.3 Determine an arithmetic function f such that

$$\frac{1}{\phi(n)} = \sum_{d|n} \frac{1}{d} f\left(\frac{n}{d}\right) \quad (n \in \mathbb{N}).$$

1.4 For each of the following arithmetic functions, "evaluate" the function, or express it in terms of familiar arithmetic functions.

(i) $g_k(n) = \sum_{d|n,(d,k)=1} \mu(d)$, where $k \in \mathbb{N}$ is fixed. (Here the summation runs over all $d \in \mathbb{N}$ that satisfy $d|n$ *and* $(d,k) = 1$.)

(ii) $h_k(n) = \sum_{d|n,k|d} \mu(d)$, where $k \in \mathbb{N}$ is fixed.

1.5 Show that, for every positive integer $n \geq 2$,

$$\sum_{\substack{1 \leq k \leq n-1 \\ (k,n)=1}} k = \frac{n}{2}\phi(n).$$

1.6 Let $f(n) = \sum_{d|n} \mu(d) \log d$. Find a simple expression for $f(n)$ in terms of familiar arithmetic functions.

1.7 Let $f(n) = \#\{(n_1,n_2) \in \mathbb{N}^2 : [n_1,n_2] = n\}$, where $[n_1,n_2]$ is the least common multiple of n_1 and n_2. Show that f is multiplicative and evaluate f at prime powers.

1.8 Let f be a multiplicative function. We know that the Dirichlet inverse f^{-1} is then also multiplicative. Show that f^{-1} is *completely* multiplicative if and only if $f(p^m) = 0$ for all prime powers p^m with $m \geq 2$ (i.e., if and only if f is supported by the squarefree numbers).

1.9 Given an arithmetic function f, a "Dirichlet square root" of f is an arithmetic function g such that $g * g = f$. Prove by elementary techniques that the constant function 1 has two Dirichlet square roots, of the form $\pm g$, where g is a multiplicative function, and find the values of g at prime powers.

1.10 Let $f(n) = \phi(n)/n$, and let $\{n_k\}_{k=1}^{\infty}$ be the sequence of values n at which f attains a "record low"; i.e., $n_1 = 1$ and, for $k \geq 2$, n_k is defined as the smallest integer $> n_{k-1}$ with $f(n_k) < f(n)$ for all $n < n_k$. (For example, since the first few values of the sequence $f(n)$ are $1, 1/2, 2/3, 1/2, 4/5, 1/3, \ldots$, we have $n_1 = 1$, $n_2 = 2$, and $n_3 = 6$, and the corresponding values of f at these arguments are 1, 1/2 and 1/3.) Find (with proof) a general formula for n_k and $f(n_k)$.

1.11 Let f be a multiplicative function satisfying $\lim_{p^m \to \infty} f(p^m) = 0$. Show that $\lim_{n \to \infty} f(n) = 0$.

1.12 An arithmetic function f is called periodic if there exists a positive integer k such that $f(n + k) = f(n)$ for every $n \in \mathbb{N}$; the integer k is called a period for f. Show that if f is completely multiplicative and periodic with period k, then the values of f are either 0 or roots of unity. (An root of unity is a complex number z such that $z^n = 1$ for some $n \in \mathbb{N}$.)