# 8
# Arithmetic Functions

In Chapter 5 we studied Euler's function $\phi$. Two of its most important properties are Theorem 5.6, that if $m$ and $n$ are coprime then $\phi(mn) = \phi(m)\phi(n)$, and Theorem 5.8, that $\sum_{d|n} \phi(d) = n$ for all $n$. In this chapter we will meet other examples of functions with similar properties. Some of these, such as the divisor functions and the Möbius function, have important applications, including the study of perfect numbers and various enumeration problems.

## 8.1 Definition and examples

### Definition

An *arithmetic** *function* is a function $f(n)$ defined for all $n \in \mathbb{N}$; it is usually taken to be complex-valued, so that it is a function $f : \mathbb{N} \to \mathbb{C}$, or equivalently a sequence $(a_n)$ of complex numbers $a_n = f(n)$.

In many of the more important cases, $f(n)$ is an integer, describing some number-theoretic property of $n$; examples include

$$\phi(n) = |U_n|, \quad \text{the number of units mod } (n),$$

* The stress is on the third syllable, to indicate that the word is an adjective, like *algebraic*.

$$\tau(n) = \sum_{d|n} 1, \quad \text{the number of divisors of } n,$$
$$\sigma(n) = \sum_{d|n} d, \quad \text{the sum of the divisors of } n.$$

For instance, the divisors of 12 are $1, 2, 3, 4, 6$ and 12, so $\tau(12) = 6$ and $\sigma(12) = 28$. The functions $\tau$ and $\sigma$ are called *divisor functions*; they are the special cases $k = 0$ and 1 of the function

$$\sigma_k(n) = \sum_{d|n} d^k .$$

In some books, the function $\tau(n)$ is written $d(n)$, but we shall avoid this notation since we often use $d$ to denote a divisor of $n$.

## Definition

An arithmetic function $f$ is *multiplicative* if

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

whenever $\gcd(m, n) = 1$. A simple induction argument shows that if $f$ is multiplicative and $n_1, \ldots, n_k$ are mutually coprime, then

$$f(n_1 \ldots n_k) = f(n_1) \ldots f(n_k);$$

in particular, if $n$ has prime-power factorisation $p_1^{e_1} \ldots p_k^{e_k}$, then

$$f(n) = f(p_1^{e_1}) \ldots f(p_k^{e_k}).$$

In many cases, it is straightforward to evaluate $f(p^e)$ for prime-powers $p^e$, so one can deduce the value of $f(n)$ for all $n$.

For instance, Theorem 5.6 shows that $\phi$ is multiplicative, and we used this property to evaluate $\phi(n)$ in Corollary 5.7. We will prove later that $\tau$ and $\sigma$ are also multiplicative. Theorem 3.11 shows that the number of solutions in $\mathbb{Z}_n$ of a given polynomial congruence is a multiplicative function of $n$; we used this property in Example 3.18 to count solutions of $x^2 \equiv 1 \bmod (n)$ for composite $n$.

### *Exercise 8.1*

Prove that $|Q_n|$, the number of quadratic residues mod $(n)$, is a multiplicative function of $n$.

The following result is very useful for proving that functions are multiplicative:

## Lemma 8.1

If $g$ is a multiplicative function and $f(n) = \sum_{d|n} g(d)$ for all $n$, then $f$ is multiplicative.

## Proof

To show that $f$ is multiplicative, suppose that $m$ and $n$ are coprime. Then the divisors $d$ of $mn$ are the products $d = ab$ where $a \mid m$ and $b \mid n$; each such pair $a$ and $b$ determines a unique divisor $d = ab$, and conversely, since $m$ and $n$ are coprime, each divisor $d$ of $mn$ determines a unique pair $a = \gcd(m, d)$ and $b = \gcd(n, d)$ of divisors of $m$ and $n$. Thus there is a bijection between divisors $d$ of $mn$ and pairs $a, b$ of divisors of $m$ and $n$, so

$$\begin{aligned} f(mn) &= \sum_{d|mn} g(d) \\ &= \sum_{a|m} \sum_{b|n} g(ab)\,. \end{aligned}$$

Now $g$ is multiplicative, and $a$ and $b$ are coprime, so $g(ab) = g(a)g(b)$, giving

$$\begin{aligned} f(mn) &= \sum_{a|m} \sum_{b|n} g(a)g(b) \\ &= \left(\sum_{a|m} g(a)\right) \cdot \left(\sum_{b|n} g(b)\right) \\ &= f(m)f(n)\,, \end{aligned}$$

as required. □

To apply this, we first introduce two more arithmetic functions $u$ and $N$, defined by

$$u(n) = 1 \qquad \text{and} \qquad N(n) = n$$

for all $n$. The function $u$ is sometimes called the *unit function*. Clearly, $u$ and $N$ are both multiplicative. These functions may look rather trivial, but they can be very useful, as the next result shows.

## Theorem 8.2

The divisor functions $\tau$ and $\sigma$ are multiplicative.

### Proof

We have $\tau(n) = \sum_{d|n} 1 = \sum_{d|n} u(d)$ and $\sigma(n) = \sum_{d|n} d = \sum_{d|n} N(d)$. Since $u$ and $N$ are multiplicative, so are $\tau$ and $\sigma$ by Lemma 8.1. □

#### *Exercise 8.2*

Give direct proofs that $\tau$ and $\sigma$ are multiplicative, using the definitions of these functions.

#### *Exercise 8.3*

Show that for each $k$, the function $\sigma_k(n) = \sum_{d|n} d^k$ is multiplicative.

We can use Theorem 8.2 to evaluate the divisor functions, by first evaluating them at the prime-powers $p^e$. Since the divisors of $p^e$ are $d = 1, p, p^2, \ldots, p^e$, we have

$$\tau(p^e) = e + 1 \qquad \text{and} \qquad \sigma(p^e) = 1 + p + p^2 + \cdots + p^e = \frac{p^{e+1} - 1}{p - 1};$$

now $\tau$ and $\sigma$ are multiplicative, so we immediately deduce

### Theorem 8.3

If $n$ has prime-power factorisation $n = p_1^{e_1} \ldots p_k^{e_k}$, then

$$\tau(n) = \prod_{i=1}^{k} (e_i + 1) \qquad \text{and} \qquad \sigma(n) = \prod_{i=1}^{k} \left( \frac{p_i^{e_i+1} - 1}{p_i - 1} \right).$$

#### *Exercise 8.4*

For which integers $n$ is $\tau(n)$ odd?

## 8.2 Perfect numbers

### Definition

A positive integer $n$ is *perfect* if $n$ is the sum of its proper divisors (the positive divisors $d \neq n$). Since $\sigma(n)$ is the sum of all the positive divisors of $n$, this

condition can be written as $n = \sigma(n) - n$, or equivalently

$$\sigma(n) = 2n\,.$$

The perfect numbers were believed by the Ancient Greeks to have particular aesthetic and religious significance. The first two examples are

$$6 = 1 + 2 + 3 \qquad \text{and} \qquad 28 = 1 + 2 + 4 + 7 + 14,$$

and the next is 496.

### *Exercise 8.5*

Verify that 496 is perfect.

Most of what is known about perfect numbers is embodied in the following theorem; the first part is in Euclid's *Elements*, and the second is due to Euler.

### Theorem 8.4

(a) If $n = 2^{p-1}(2^p - 1)$ where $p$ and $2^p - 1$ are both prime (so that $2^p - 1$ is a Mersenne prime $M_p$), then $n$ is perfect.

(b) If $n$ is even and perfect, then $n$ has the form given in (a).

This theorem shows that there is a one-to-one correspondence between even perfect numbers and the Mersenne primes $M_p$ which we met in Chapter 2; for instance the perfect numbers $6, 28$ and $496$ correspond to the Mersenne primes $M_2 = 3, M_3 = 7$ and $M_5 = 31$. No example of an odd perfect number is known, and it is conjectured that they do not exist; if there is one, it must be very large.

### Proof

(a) If $n = 2^{p-1}(2^p - 1)$ as described, then Theorem 8.2 gives $\sigma(n) = \sigma(2^{p-1})\sigma(2^p - 1)$. Now Theorem 8.3 gives $\sigma(2^{p-1}) = (2^p - 1)/(2 - 1) = 2^p - 1$, and since $2^p - 1$ is prime we have $\sigma(2^p - 1) = (2^p - 1) + 1 = 2^p$. Thus $\sigma(n) = (2^p - 1)2^p = 2n$, so $n$ is perfect.

(b) Since $n$ is even, we can write $n = 2^{p-1}q$ for some integer $p \geq 2$, where $q$ is odd. Now $\sigma$ is multiplicative, so $\sigma(n) = \sigma(2^{p-1})\sigma(q) = (2^p - 1)\sigma(q)$. Since $n$ is perfect we also have $\sigma(n) = 2n = 2^p q$, so

$$(2^p - 1)\sigma(q) = 2^p q\,.$$

Thus $2^p - 1$ divides $2^p q$, and hence divides $q$, say $q = (2^p - 1)r$, so substituting for $q$ and then cancelling $2^p - 1$ we get

$$\sigma(q) = 2^p r\,.$$

Now $q$ and $r$ are distinct divisors of $q$, with $q + r = (2^p - 1)r + r = 2^p r = \sigma(q)$, which is the sum of *all* the divisors of $q$; thus $q$ and $r$ must be the *only* divisors of $q$, so $q$ is prime and $r = 1$. Thus $q = 2^p - 1$ and so $n = 2^{p-1}(2^p - 1)$; since $2^p - 1$ is prime, Theorem 2.13 implies that $p$ must be prime. □

### *Exercise 8.6*

Is $2^{10}(2^{11} - 1)$ perfect?

### *Exercise 8.7*

Find two more perfect numbers, other than the examples given above.

### *Exercise 8.8*

Show that $n$ is perfect if and only if $\sigma_{-1}(n) = 2$.

## 8.3 The Möbius Inversion Formula

The multiplicative property can be useful in proving identities between arithmetic functions.

### Lemma 8.5

Let $f$ and $g$ be multiplicative functions, with $f(p^e) = g(p^e)$ for all primes $p$ and integers $e \geq 0$. Then $f = g$.

### Proof

If $n$ has prime-power factorisation $\prod_i p_i^{e_i}$, then

$$f(n) = f\left(\prod_i p_i^{e_i}\right) = \prod_i f(p_i^{e_i}) = \prod_i g(p_i^{e_i}) = g\left(\prod_i p_i^{e_i}\right) = g(n)\,.$$

□

This gives us another proof of Theorem 5.8, that $\sum_{d|n} \phi(d) = n$. Since $\phi$ is multiplicative (by Theorem 5.6), so is the function $f(n) = \sum_{d|n} \phi(d)$, by Lemma 8.1. We have seen that the function $N(n) = n$ is multiplicative, so to prove Theorem 5.8 it is sufficient (by Lemma 8.5) to show that $f$ and $N$ agree on all prime-powers $p^e$. Now the divisors $d$ of $p^e$ are $d = p^i$ $(i = 0, 1, \ldots, e)$, with $\phi(1) = 1$ and $\phi(p^i) = p^i - p^{i-1}$ for $i > 0$, so

$$f(p^e) = 1 + \sum_{i=1}^{e} (p^i - p^{i-1}) = p^e = N(p^e),$$

as required.

We have seen several instances where pairs of arithmetic functions $f$ and $g$ are related by an identity $f(n) = \sum_{d|n} g(d)$: for instance, we can take $f = N$ and $g = \phi$, or $f = \sigma$ and $g = N$. In this situation, it is often useful to be able to invert the roles of $f$ and $g$, that is, to find a similar formula expressing $g$ in terms of $f$. The result which allows us to do this is the Möbius Inversion Formula, but before proving this, we need to study one of its main ingredients, the Möbius function $\mu$. First we define the *identity function* $I$, given by

$$I(n) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{if } n > 1. \end{cases}$$

Clearly $I$ is multiplicative. The name of this function can be a little confusing, since $I$ is *not* the identity function in the set-theoretic sense of sending every $n$ to itself ($N$ does that). We will later introduce an algebraic operation $*$ on arithmetic functions, and show that $f * I = f = I * f$ for all $f$; thus $I$ is the identity with respect to $*$, whereas $N$ is the identity with respect to the operation $\circ$ of composition, since $f \circ N = f = N \circ f$ for all $f$. A useful alternative formula for $I$ is

$$I(n) = \left\lfloor \frac{1}{n} \right\rfloor,$$

the integer part of $1/n$.

We define the *Möbius function* $\mu$ by the formula

$$\sum_{d|n} \mu(d) = I(n) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{if } n > 1. \end{cases}$$

This is an example of an inductive (or recursive) definition: if $n = 1$ (with a unique divisor $d = 1$) then $\mu(1) = 1$, and if $n > 1$ then $\sum_{d|n} \mu(d) = 0$, so

$$\mu(n) = -\sum_{d|n, d<n} \mu(d),$$

which defines $\mu(n)$ in terms of the values of $\mu$ at smaller integers $d$. For instance, if $n$ is prime then its only divisors are $d = 1$ and $d = n$, so $\mu(n) = -\mu(1) = -1$. A little calculation gives the values

$$\mu(n) = 1, -1, -1, 0, -1, 1, -1, 0, 0, 1, -1, 0$$

for $n = 1, 2, \ldots, 12$. In Theorem 8.8 we will give a simple formula for $\mu(n)$ in terms of the prime-power factorisation of $n$, which is more convenient for calculation.

### *Exercise 8.9*

Show that $\mu(n)$ is an integer for each $n \geq 1$.

### *Exercise 8.10*

Show that if $p$ and $q$ are distinct primes, then $\mu(pq) = 1$ and $\mu(p^2) = 0$.

### *Exercise 8.11*

Calculate $\mu(n)$ for all $n \leq 30$, and make a conjecture about the values of $\mu(n)$.

The function $\mu$ derives its importance from the following major result, the *Möbius Inversion Formula*:

### Theorem 8.6

Let $f$ and $g$ be arithmetic functions. If

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

for all $n$, then

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

for all $n$.

This shows that if $f$ is expressed in terms of $g$ as a sum over divisors, then one can invert their roles and define $g$ in terms of $f$ by a similar expression. The relationship between $f$ and $g$ is nearly symmetric, except that the function $\mu$ appears in the expression for $g$.

## Proof

The two expressions for $g(n)$ are easily seen to be equal: if we put $e = n/d$ then the first summation can be written as

$$\sum_{de=n} f(d)\mu(e)\,,$$

where the sum is over all pairs $d, e$ with product $n$; transposing the names of these two dummy variables, we see that this is also equal to

$$\sum_{ed=n} f(e)\mu(d) = \sum_{de=n} \mu(d)f(e)\,,$$

which gives the second summation. It is therefore sufficient to show that the second summation is equal to $g(n)$. Our hypothesis about $f$ implies that

$$f\Big(\frac{n}{d}\Big) = \sum_{e|\frac{n}{d}} g(e)\,,$$

so

$$\sum_{d|n} \mu(d) f\Big(\frac{n}{d}\Big) = \sum_{d|n} \Big(\mu(d) \sum_{e|\frac{n}{d}} g(e)\Big)\,.$$

Now if $e$ divides $n/d$ then it divides $n$; conversely, for each divisor $e$ of $n$, we see that $e$ divides $n/d$ if and only if $d$ divides $n/e$, in which case $d$ also divides $n$. Hence the coefficient of $g(e)$ in this expression is

$$\sum_{d|\frac{n}{e}} \mu(d) = \begin{cases} 1 & \text{if } n/e = 1, \\ 0 & \text{if } n/e > 1. \end{cases}$$

This means that the only term $g(e)$ with a non-zero coefficient is $g(n)$, which has coefficient 1, so the expression is equal to $g(n)$, as required. □

## Corollary 8.7

If $n \geq 1$ then

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

## Proof

By Theorem 5.8 we have $\sum_{d|n} \phi(d) = n = N(n)$, so by applying the Möbius Inversion Formula with $f = N$ and $g = \phi$ we get the required result. □

### Example 8.1

Let $n = 12$, so $\phi(12) = 4$. The divisors of 12 are $d = 1, 2, 3, 4, 6$ and 12, and the values of $\mu$ at the first twelve integers were given on p. 150, so we find that

$$\sum_{d|12} d\mu\left(\frac{12}{d}\right) = 1.0 + 2.1 + 3.0 + 4.(-1) + 6.(-1) + 12.1 = 4$$

and also

$$\sum_{d|12} \mu(d)\frac{12}{d} = 1.\frac{12}{1} - 1.\frac{12}{2} - 1.\frac{12}{3} + 0.\frac{12}{4} + 1.\frac{12}{6} + 0.\frac{12}{12} = 4\,,$$

in agreement with Corollary 8.7.

*Exercise 8.12*

Prove that

$$\sum_{d|n} \tau(d)\mu\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d)\tau\left(\frac{n}{d}\right) = 1$$

and

$$\sum_{d|n} \sigma(d)\mu\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d)\sigma\left(\frac{n}{d}\right) = n$$

for all $n \geq 1$. Verify these equations for $n = 12$.

## 8.4 An application of the Möbius Inversion Formula

In this section we give a totally different application of the Möbius Inversion Formula. A set of $n$ chairs are arranged regularly around a circular table. Each chair may be occupied by a woman ($W$) or by a man ($M$), giving $2^n$ possible patterns of sexes $W$ or $M$ at the table. If the people all rotate one place around the table, a pattern may change, but after $n$ successive rotations it must recur. We say that a pattern has period $d$ if recurs for the first time after $d$ rotations, or equivalently, if rotating the pattern produces exactly $d$ different patterns. Thus a single-sex pattern $WW\ldots W$ or $MM\ldots M$ has period 1, while for even $n$ the two alternating patterns $WMWM\ldots WM$ and $MWMW\ldots MW$ each have period 2. How many different patterns of period $d$ are there, for each $d$?

First note that if a pattern has period $d$, then $d$ must divide $n$: for if $n = qd + r$ with $0 \leq r < d$ then the pattern recurs after both $n$ and $d$ rotations,

and hence also after $r = n - qd$ rotations, so $r = 0$ by the definition of $d$. For each $d$, the number of patterns of period $d$ depends only on $d$, and not on the multiple $n = qd$ of $d$: this is because such a pattern consists of $q$ repetitions of a block of $d$ symbols $W$ or $M$, which is not itself a repetition of smaller blocks, and the number of such blocks of length $d$ depends only on $d$. For instance, a pattern of period $d = 2$ must consist of $q$ repetitions of the block $WM$ or $MW$ (but not $WW$ or $MM$), so there are two such patterns for each even $n$. It follows that if we let $f(d)$ denote the number of patterns of period $d$, then $\sum_{d|n} f(d) = 2^n$, the total number of patterns for $n$ chairs. Putting $g(n) = 2^n$ in Theorem 8.6, we deduce that

$$f(n) = \sum_{d|n} 2^d \mu\Big(\frac{n}{d}\Big),$$

or equivalently (changing notation)

$$f(d) = \sum_{e|d} 2^e \mu\Big(\frac{d}{e}\Big).$$

For instance

$$\begin{aligned} f(12) &= 2^1\mu(12) + 2^2\mu(6) + 2^3\mu(4) + 2^4\mu(3) + 2^6\mu(2) + 2^{12}\mu(1) \\ &= 2^2 - 2^4 - 2^6 + 2^{12} \\ &= 4020. \end{aligned}$$

The expression $2^2 - 2^4 - 2^6 + 2^{12}$ for $f(12)$ can also be obtained from the Inclusion–Exclusion Principle (Exercise 5.10). The term $2^{12}$ counts all the different patterns of length 12, and we need to exclude those which are repetitions of smaller blocks. If a pattern of length 12 is a repetition of smaller blocks, then it consists of either two copies of a block of length 6, or three copies of a block of length 4; any other cases are included in these, for instance four copies of a block $B$ of length 3 can also be regarded as two copies of the block $BB$ of length 6. Now the number of patterns of length 12 consisting of two identical blocks of length 6 is equal to $2^6$, the total number of blocks of this length, so we subtract $2^6$; similarly, we subtract $2^4$ for those consisting of three identical blocks of length 4. In doing this, we have excluded some patterns twice, namely those which consist of two blocks of length 6 and also of three of length 4; these are the patterns $BBBBBB = (BBB)(BBB) = (BB)(BB)(BB)$ consisting of six identical blocks $B$ of length 2; the number of such patterns is $2^2$, so by adding $2^2$ to compensate for this double-counting we obtain the required formula $2^{12} - 2^6 - 2^4 + 2^2$. More generally, the Möbius Inversion Formula can be regarded as an analogue of the Inclusion-Exclusion Principle, in which divisibility of integers has replaced inclusion of sets.

Let us regard two patterns as equivalent if each is a rotation of the other. Thus a pattern of period $d$ lies in a class of $d$ equivalent patterns, so the number of equivalence classes of patterns of period $d$ is

$$\frac{f(d)}{d} = \frac{1}{d}\sum_{e|d} 2^e \mu\left(\frac{d}{e}\right).$$

For instance, there are $4020/12 = 335$ equivalence classes of patterns of period 12.

Although this may not seem a particularly serious application, there are in fact many mathematical situations involving similar types of cyclic symmetry, where this enumeration technique is important. For instance, by using the theory of finite fields one can show that the above formula for $f(d)/d$ also gives the number of irreducible polynomials of degree $d$ with coefficients in $\mathbb{Z}_2$. Indeed a whole branch of mathematics, spanning number theory, combinatorics and algebra, has built itself up around the Möbius Inversion Formula, its generalisations and its applications.

### *Exercise 8.13*

Enumerate and determine all the patterns with periods $d = 2, 3$ and 4, and show how they are divided into equivalence classes.

### *Exercise 8.14*

How would the solution to this problem be affected if there were more than two sexes?

## 8.5 Properties of the Möbius function

Having seen some applications of the Möbius function, we now need a more efficient method of evaluating it than by means of its inductive definition. The evidence for small values of $n$ (Exercise 8.11) may lead one to conjecture the following formula:

### Theorem 8.8

If $n = p_1^{e_1} \dots p_k^{e_k}$, where $p_1, \dots, p_k$ are distinct primes and each $e_i \geq 1$, then

$$\mu(n) = \begin{cases} 0 & \text{if some } e_i > 1, \\ (-1)^k & \text{if each } e_i = 1. \end{cases}$$

(Thus $\mu(n) \neq 0$ if and only if $n$ is square-free. This formula includes the case $\mu(1) = (-1)^0 = 1$, where we regard 1 as the product of the empty set of primes, so that $k = 0$.)

## Proof

Let $\mu'$ be the function defined by the formula in the theorem, so that $\mu'(n) = (-1)^k$ if $n$ is a product of $k$ distinct primes, and $\mu'(n) = 0$ otherwise. We will prove that $\mu(n) = \mu'(n)$ for all $n$ by strong induction on $n$. Clearly $\mu(1) = 1 = \mu'(1)$, so suppose that $n > 1$ and $\mu(d) = \mu'(d)$ for all $d < n$.

We first show that $\sum_{d|n} \mu'(d) = 0$ (so $\mu'$ satisfies the same recurrence relation $\sum_{d|n} \mu'(d) = I(n)$ as $\mu$). If the factorisation of $n$ is as in the theorem (with $k \geq 1$), then by definition of $\mu'$, the non-zero terms in $\sum_{d|n} \mu'(d)$ are those of the form $\mu'(d)$ where $d$ is a product of distinct primes $p_i \in \{p_1, \ldots, p_k\}$. If $d$ is a product of $r$ such primes, where $0 \leq r \leq k$, then $\mu'(d) = (-1)^r$; for each $r$ the number of ways of choosing these $r$ primes is equal to the binomial coefficient $\binom{k}{r}$, so there are $\binom{k}{r}$ such divisors $d$, each contributing $(-1)^r$ to $\sum_{d|n} \mu'(d)$. Summing over all $r$ we therefore have

$$\sum_{d|n} \mu'(d) = \sum_{r=0}^{k} \binom{k}{r} (-1)^r = \Big(1 + (-1)\Big)^k = 0$$

by the Binomial Theorem. (Alternatively, note that $\mu'$ is multiplicative (see Corollary 8.9), and hence by Lemma 8.1 so is the function $f(n) = \sum_{d|n} \mu'(d)$; by Lemma 8.5 it is therefore sufficient to show that $f(p^e) = 0$ for each prime power $p^e > 1$, and this follows immediately from the definition of $\mu'$.) We can write this as

$$\mu'(n) = -\sum_{d|n, d<n} \mu'(d)\,;$$

now the induction hypothesis states that $\mu(d) = \mu'(d)$ for all $d < n$, and the definition of $\mu$ implies that

$$\mu(n) = -\sum_{d|n, d<n} \mu(d)\,,$$

so $\mu(n) = \mu'(n)$ as required. □

## Example 8.2

$15 = 3.5$, so $\mu(15) = (-1)^2 = 1$; $30 = 2.3.5$, so $\mu(30) = (-1)^3 = -1$; $60 = 2^2.3.5$, so $\mu(60) = 0$.

### *Exercise 8.15*

Find a simple formula for $\sum_{d|n} |\mu(d)|$.

We can use Theorem 8.8 to give an alternative proof of Corollary 5.7, that

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

where $p$ ranges over the distinct primes dividing $n$. If we multiply out the factors on the right-hand side, the general term has the form $n(-1)^r/p_1 \dots p_r$ where $p_1, \dots, p_r$ are distinct prime factors of $n$; by Theorem 8.8, this is equal to $n\mu(d)/d$, where $d = p_1 \dots p_r$ is a square-free divisor of $n$. The remaining non-square-free divisors $d$ of $n$ have $\mu(d) = 0$, so the right-hand side can be written as $\sum_{d|n} n\mu(d)/d$. By Corollary 8.7, this is equal to $\phi(n)$. (This argument is not circular: although Corollary 8.7 depends on Theorem 5.8, that $\sum_{d|n} \phi(d) = n$, the proof of this does not use Corollary 5.7.)

## Example 8.3

Taking $n = 12$, we have

$$\phi(12) = 12\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) = \frac{12}{1} - \frac{12}{2} - \frac{12}{3} + \frac{12}{6} = \sum_{d|12} \mu(d)\frac{12}{d}.$$

(The divisors $d = 4$ and 12 have $\mu(d) = 0$, since they are not square-free.)

## Corollary 8.9

The function $\mu$ is multiplicative.

## Proof

We need to prove that $\mu(mn) = \mu(m)\mu(n)$ whenever $m$ and $n$ are coprime. If $m$ and $n$ are not both square-free, then neither is $mn$, so Theorem 8.8 gives $\mu(m)\mu(n) = 0 = \mu(mn)$ as required. We may assume therefore that both $m = p_1 \dots p_k$ and $n = q_1 \dots q_l$ are products of distinct primes. Since they are coprime, no prime $p_i$ dividing $m$ can appear as a prime $q_j$ dividing $n$, so $mn = p_1 \dots p_k q_1 \dots q_l$ is also a product of distinct primes. Thus $\mu(m) = (-1)^k$, $\mu(n) = (-1)^l$ and $\mu(mn) = (-1)^{k+l} = (-1)^k(-1)^l = \mu(m)\mu(n)$. □

## 8.6 The Dirichlet product

Theorems 5.8 and 8.6, Lemma 8.1, Corollary 8.7 and our definition of $\mu$ all involve summation over the divisors $d$ of $n$; these are special cases of a general theory of such sums.

### Definition

If $f$ and $g$ are arithmetic functions, then their *Dirichlet product*, or *convolution*, is the arithmetic function $f * g$ given by

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

equivalently, putting $e = n/d$, we have

$$(f * g)(n) = \sum_{de=n} f(d)g(e)$$

where $\sum_{de=n}$ denotes summation over all pairs $d, e$ such that $de = n$.

### Example 8.4

Theorem 5.8 states that $\sum_{d|n} \phi(d) = n$ for all $n$; using the functions $u(n) = 1$ and $N(n) = n$, we can rewrite this as

$$\sum_{d|n} \phi(d)u\left(\frac{n}{d}\right) = N(n)$$

for all $n$, which becomes, in our new notation, $\phi * u = N$. Similarly, our definition of $\mu$ can be written as $\mu * u = I$, while Corollary 8.7 becomes $\phi = N * \mu = \mu * N$. Lemma 8.1 states that if $g$ is multiplicative, then so is the function $f = g * u$. Theorem 8.6 (the Möbius Inversion Formula) states that if $f = g * u$ then $g = f * \mu = \mu * f$.

#### *Exercise 8.16*

Express the divisor functions $\tau$ and $\sigma$ as Dirichlet products of simpler functions.

The basic algebraic properties of the Dirichlet product are as follows:

### Lemma 8.10

For all arithmetic functions $f, g$ and $h$ we have

(a) $f * g = g * f$,

(b) $(f * g) * h = f * (g * h)$,

(c) $f * I = I * f = f$.

(Thus $*$ is commutative and associative, and has $I$ as an identity.)

## Proof

(a) For all arithmetic functions $f$ and $g$, we have

$$(f * g)(n) = \sum_{de=n} f(d)g(e) = \sum_{ed=n} g(e)f(d) = \sum_{de=n} g(d)f(e) = (g * f)(n).$$

(b) For all arithmetic functions $f, g$ and $h$, we have

$$\begin{aligned} \big((f * g) * h\big)(n) &= \sum_{dc=n} (f * g)(d)h(c) \\ &= \sum_{dc=n} \Big(\sum_{ab=d} f(a)g(b)\Big)h(c) = \sum_{abc=n} f(a)g(b)h(c), \end{aligned}$$

and similarly

$$\begin{aligned} \big(f * (g * h)\big)(n) &= \sum_{ae=n} f(a)(g * h)(e) \\ &= \sum_{ae=n} f(a)\Big(\sum_{bc=e} g(b)h(c)\Big) = \sum_{abc=n} f(n)g(b)h(c). \end{aligned}$$

□

### *Exercise 8.17*

Prove Lemma 8.10(c).

The next result shows that the arithmetic functions $f$ satisfying $f(1) \neq 0$ have inverses with respect to the Dirichlet product:

## Lemma 8.11

If $f$ is an arithmetic function with $f(1) \neq 0$, then there exists an arithmetic function $g$ such that $f * g = I = g * f$; it is given by

$$g(1) = \frac{1}{f(1)} \qquad \text{and} \qquad g(n) = -\frac{1}{f(1)} \sum_{\substack{d|n \\ d<n}} g(d) f\Big(\frac{n}{d}\Big)$$

for all $n > 1$.

(These equations define $g(n)$ for all $n \geq 1$ by induction on $n$.)

## Proof

By the commutativity of $*$ it is sufficient to prove that the given function $g$ satisfies $g * f = I$, that is,

$$\sum_{d|n} g(d) f\left(\frac{n}{d}\right) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{if } n > 1. \end{cases}$$

This is trivial for $n = 1$, since the only divisor is $d = 1$ and we have $g(1)f(1) = 1$ by definition of $g$. If $n > 1$ then

$$\begin{aligned} \sum_{d|n} g(d) f\left(\frac{n}{d}\right) &= g(n)f(1) + \sum_{\substack{d|n \\ d<n}} g(d) f\left(\frac{n}{d}\right) \\ &= -\frac{f(1)}{f(1)} \sum_{\substack{d|n \\ d<n}} g(d) f\left(\frac{n}{d}\right) + \sum_{\substack{d|n \\ d<n}} g(d) f\left(\frac{n}{d}\right) = 0, \end{aligned}$$

as required. □

## Definition

The function $g$ in Lemma 8.11 is called the *Dirichlet inverse* of $f$, denoted by $f^{-1}$ (not to be confused with the inverse function or with the reciprocal of $f$.)

Let $G$ denote the set of all arithmetic functions $f$ for which $f(1) \neq 0$.

## Theorem 8.12

$G$ is an abelian group with respect to the operation $*$, with identity element $I$.

## Proof

To prove closure, let $f, g \in G$, so $f(1), g(1) \neq 0$; then $(f * g)(1) = \sum_{d|1} f(d)g(1/d) = f(1)g(1) \neq 0$, so $f * g \in G$. Associativity, commutativity and the existence of an identity $I$ are proved in Lemma 8.10. Finally, if $f \in G$ then its Dirichlet inverse $g = f^{-1}$ is also in $G$ since $g(1) = 1/f(1) \neq 0$, so every element has an inverse in $G$. □

## Example 8.5

The equation $\mu * u = I$ (which we used to define $\mu$) shows that $\mu$ and $u$ are inverses of each other in $G$, and this helps to explain why the function $\mu$ should

be so important. To illustrate the power of the new notation, we give a one-line proof of the Möbius Inversion Formula (Theorem 8.6), which states that if $f = g*u$ then $g = f*\mu = \mu*f$: if $f = g*u$, then $f*\mu = (g*u)*\mu = g*(u*\mu) = g*I = g$, and so commutativity of $*$ gives $\mu * f = g$. We can also prove the converse of Theorem 8.6: if $g = f*\mu$ then $g*u = (f*\mu)*u = f*(\mu*u) = f*I = f$. These arguments are valid for all arithmetic functions $f$ and $g$, not just those in $G$, so we have proved the following stronger form of the Möbius Inversion Formula:

## Theorem 8.13

Let $f$ and $g$ be arithmetic functions. Then

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

for all $n$ if and only if

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

for all $n$.

## Example 8.6

If we take $f = N$ and $g = \phi$, we see that Theorem 5.8 and Corollary 8.7 are equivalent to each other, that is, $N = \phi * u$ is equivalent to $\phi = N * \mu = \mu * N$.

### *Exercise 8.18*

Which arithmetic functions are represented by $\tau * \mu$ and by $\sigma * \mu$?

We can now prove an extension of Lemma 8.1 (which is the special case $h = u$):

## Theorem 8.14

If $g$ and $h$ are multiplicative functions, and if $f = g*h$, then $f$ is multiplicative.

## Proof

The proof is similar to that of Lemma 8.1. Instead, the first equation now becomes

$$f(mn) = \sum_{d|mn} g(d)h\Big(\frac{mn}{d}\Big),$$

and we carry values of $h$ throughout the calculation. □

### *Exercise 8.19*

Fill in the details of the proof of Theorem 8.14.

### *Exercise 8.20*

Show that if $f$ is multiplicative, and $f$ is not identically zero, then $f \in G$ and the Dirichlet inverse $f^{-1}$ is multiplicative. (Hint: if not, consider the least $mn$ such that $\gcd(m,n) = 1$ and $f^{-1}(mn) \neq f^{-1}(m)f^{-1}(n)$.) Deduce that the set $M$ of non-zero multiplicative functions forms a subgroup of $G$.

We can also prove the converse of Lemma 8.1:

## Corollary 8.15

Suppose that $f(n) = \sum_{d|n} g(d)$. Then $f$ is multiplicative if and only if $g$ is multiplicative.

## Proof

The hypothesis is that $f = g*u$. Now $u$ is multiplicative, so if $g$ is multiplicative then so is $f$, by Theorem 8.14. The converse is similar, using $g = f * \mu$ and Corollary 8.9 (that $\mu$ is multiplicative). □

## Example 8.7

Theorem 5.8 gives $\sum_{d|n} \phi(n) = n = N(n)$. It is obvious that $N$ is multiplicative, so Corollary 8.15 gives an alternative proof that $\phi$ is multiplicative. (This is not a circular argument, since the proof of Theorem 5.8 did not require the multiplicative property of $\phi$.)

## 8.7 Supplementary exercises

### *Exercise 8.21*

(a) Show that $\chi$ is multiplicative, where $\chi(n) = 0, 1$ or $-1$ as $n$ is even or $n \equiv 1$ or $3 \bmod (4)$ respectively.

(b) Let $\tau_1(n)$ and $\tau_3(n)$ denote the number of divisors $d$ of $n$ such that $d \equiv 1$ or $3 \bmod (4)$ respectively; show that the function $g(n) = \tau_1(n) - \tau_3(n)$ is multiplicative, and hence find an expression for $g(n)$ in terms of the prime-power factorisation of $n$. (See Exercise 10.8 for an application of this.)

### *Exercise 8.22*

Show that $\mu(n)$ is the sum of the primitive complex $n$-th roots of 1. (These are the elements $z \in \mathbb{C}$ such that $z^n = 1$ but $z^m \neq 1$ for $1 \leq m < n$.)

### *Exercise 8.23*

Show that if $g$ is multiplicative, then the functions $f(n) = \sum_{d^2|n} g(d^2)$ and $h(n) = \sum_{d^2|n} g(n/d^2)$ are both multiplicative.

### *Exercise 8.24*

The *Mangoldt function* is given by $\Lambda(n) = \ln p$ if $n = p^e$ for some prime $p$ and integer $e > 0$, and $\Lambda(n) = 0$ otherwise. Show that $\sum_{d|n} \Lambda(d) = \ln(n)$ and deduce that $\Lambda(n) = \sum_{d|n} \ln(d)\mu(n/d) = -\sum_{d|n} \ln(d)\mu(d)$.

### *Exercise 8.25*

Show that $(f_1 * \cdots * f_k)(n) = \sum f_1(d_1) \ldots f_k(d_k)$ for all arithmetic functions $f_1, \ldots, f_k$, where the summation is over all $k$-tuples $(d_1, \ldots, d_k)$ with $d_1 \ldots d_k = n$.

### *Exercise 8.26*

Show that the number of subgroups of finite index $n$ in the group $\mathbb{Z}^2$ is equal to $\sigma(n)$. (Hint: you may assume that these subgroups correspond to integer matrices $A = \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)$ where $a, d > 0$, $ad = n$ and $0 \leq b < d$.) How many subgroups of index $n$ are there in the group $\mathbb{Z}^k$?