Chapter 6
Group of Arithmetical Functions (Optional)

In this chapter, we show that the set of all arithmetical functions f with $f(1) \neq 0$ forms an abelian group with respect to a special operation. Then, we discuss an important subgroup of this group.

6.1 Arithmetical Functions

In this section we introduce several mathematical functions which play an important role in the study of divisibility properties of integers. We begin with the definition of arithmetical functions.

Definition 6.1 A real or complex-valued function defined on the positive integers is called an *arithmetical function*.

Example 6.2 Euler function φ defined in Definition 4.6 is a arithmetical function.

Theorem 6.3 (Gauss Theorem) *If n is a positive integer, then*

$$\sum_{d|n} \varphi(d) = n.$$

Proof Suppose that $X = \{1,\ 2,\ \ldots, n\}$ and let

$$S(d) = \{k \mid (k, n) = d,\ 1 \leq k \leq n\}.$$

Then, the sets $S(d)$ are disjoint and whose union is equal to X. If $f(d)$ is the number of integers in $S(d)$, then

$$\sum_{d|n} f(d) = n. \tag{6.1}$$

B. Davvaz, *A First Course in Group Theory*,
https://doi.org/10.1007/978-981-16-6365-9_6

Table 6.1 A short table of values $\mu(n)$

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\mu(n)$	1	-1	-1	0	-1	1	-1	0	0	1	-1	0	-1	1	1

Moreover, we have

$$\begin{aligned}(k, n) = d &\Leftrightarrow (k/d, n/d) = 1,\\ 0 < k \le n &\Leftrightarrow 0 < k/d \le n/d.\end{aligned}$$

So, if we take $q = k/d$, then there exists a one to one correspondence between the elements of $S(d)$ and those integers q satisfying $0 < k \le n$ and $(q, n/d) = 1$. The number of such q is equal to $\varphi(n/d)$. Hence, we have $f(d) = \varphi(n/d)$. Now, by (6.1), we conclude that

$$\sum_{d|n} \varphi\left(\frac{n}{d}\right) = n.$$

This completes the proof, because when d runs through all divisors of n so does n/d. ■

A positive integer n is *square-free* if $p^2 \nmid n$, for every prime p.

Definition 6.4 The Möbius function μ is defined as follows:

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

Table 6.1 is a short table of values $\mu(n)$:

Theorem 6.5 *If n is a positive integer, then*

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

Proof Clearly, we have $\mu(1) = 1$. Let $n > 1$ and $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$. We know that $\mu(d)$ is non-zero if $d = 1$ or those divisors of n which are products of distinct primes. Consequently, we can write

$$\begin{aligned}\sum_{d|n} \mu(d) &= \mu(1) + \mu(p_1) + \cdots + \mu(p_k) + \mu(p_1 p_2) + \cdots + \mu(p_{k-1} p_k)\\ &\quad + \cdots + \mu(p_1 p_2 \dots p_k)\\ &= 1 + \binom{k}{1}(-1) + \binom{k}{2}(-1)^2 + \cdots + \binom{k}{k}(-1)^k\\ &= (1 + (-1))^2 = 0.\end{aligned}$$

This completes the proof. ■

The Möbius function is related to the Euler function by the following theorem.

Theorem 6.6 *If n is a positive integer, then*

$$\varphi(n) = \prod_{d|n} \mu(d)\frac{n}{d}.$$

Proof We can write

$$\varphi(n) = \sum_{k=1}^{n} \left[\frac{1}{(n,k)}\right].$$

Then, by Theorem 6.5, we obtain

$$\varphi(n) = \sum_{k=1}^{n} \sum_{d|(n,k)} \mu(d) = \sum_{k=1}^{n} \sum_{\substack{d|n \\ d|k}} \mu(d). \tag{6.2}$$

For a fixed divisor d of n we must sum over all those $1 \leq k \leq n$ which are multiple of d. If $k = qd$, then

$$1 \leq k \leq n \Leftrightarrow 1 \leq q \leq \frac{n}{d}.$$

By using this fact and (6.2), we can write

$$\varphi(n) = \sum_{d|n} \sum_{q=1}^{n/d} \mu(d) = \sum_{d|n} \mu(d) \sum_{q=1}^{n/d} 1 = \sum_{d|n} \mu(d)\frac{n}{d}.$$

This completes our proof. ■

Theorem 6.7 *If n is a positive integer, then*

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

where p is prime.

Proof If $n = 1$, then there are no primes which divide 1. Hence, the product is empty, and so $\varphi(1) = 1$. Suppose that $n > 1$ and let $p_1, p_2, \ldots, p_m$ be the distinct prime divisors of n. The product can be written as

$$\begin{aligned}\prod_{p|n}\left(1-\frac{1}{p}\right)&=\prod_{i=1}^{m}\left(1-\frac{1}{p_i}\right)\\&=\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\ldots\left(1-\frac{1}{p_m}\right)\\&=1-\sum\frac{1}{p_i}+\sum\frac{1}{p_ip_j}-\sum\frac{1}{p_ip_jp_k}+\cdots+\frac{(-1)^m}{p_1p_2\ldots p_m}.\end{aligned}\tag{6.3}$$

On the last line of (6.3), in a term such as $\sum 1/p_ip_jp_k$, it means that we consider all possible products of $p_ip_jp_k$ of distinct prime factors of n taken three at a time. Moreover, each term on the last line of (6.3) is of the form $\pm 1/d$, where d is a divisor of n which is either 1 or a product of distinct primes. The numerator ± 1 is exactly $\mu(d)$. If d is divisible by the square of any prime p_i, then $\mu(d)=0$. So, we observe that (6.3) is exactly the same as

$$\prod_{p|n}\left(1-\frac{1}{p}\right)=\sum_{d|n}\frac{\mu(d)}{d}.$$

Therefore, we conclude that

$$\varphi(n)=\sum_{d|n}\mu(d)\frac{n}{d}=n\sum_{d|n}\frac{\mu(d)}{d}=n\prod_{p|n}\left(1-\frac{1}{p}\right),$$

as desired. ■

Many properties of φ can be easily obtained from Theorem 6.7. Some of these are listed in the next theorem.

Theorem 6.8 *Euler function has the following properties:*

(1) $\varphi(p^\alpha)=p^\alpha-p^{\alpha-1}$, *for each prime number p and $\alpha\geq 1$;*

(2) $\varphi(mn)=\varphi(m)\varphi(n)\left(\dfrac{d}{\varphi(d)}\right)$, *where $d=(m,n)$;*

(3) $\varphi(mn)=\varphi(m)\varphi(n)$, *if $(m,n)=1$;*

(4) *$m|n$ implies $\varphi(m)|\varphi(n)$;*

(5) *$\varphi(n)$ is even, for each $n\geq 3$. In addition, if n has k distinct odd prime factors, then $2^k|\varphi(n)$.*

Proof (1) It is enough if we consider $n=p^\alpha$ in Theorem 6.7.

(2) By Theorem 6.7, for each positive integer n, we can write

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

where p is prime. Each prime divisor of mn is either a prime divisor of m or of n, and those primes which divide both m and n also divide (m, n). Therefore, we have

$$\frac{\varphi(mn)}{mn} = \prod_{p|mn}\left(1-\frac{1}{p}\right) = \frac{\displaystyle\prod_{p|m}\left(1-\frac{1}{p}\right)\prod_{p|n}\left(1-\frac{1}{p}\right)}{\displaystyle\prod_{p|(m,n)}\left(1-\frac{1}{p}\right)} = \frac{\dfrac{\varphi(m)}{m}\dfrac{\varphi(n)}{n}}{\dfrac{\varphi(d)}{d}},$$

and consequently, we obtain (2).

(3) It is a special case of (2). In fact, it is enough to consider $d = 1$ in (2).

(4) Since $m|n$, it follows that there exists an integer $1 \leq c \leq n$ such that $n = cm$. If $c = n$, then $m = 1$ and (4) is obviously satisfied. So, let $c < n$. By using (2), we have

$$\varphi(n) = \varphi(mc) = \varphi(m)\varphi(c)\frac{d}{\varphi(d)} = d\varphi(m)\frac{\varphi(c)}{\varphi(d)}, \tag{6.4}$$

where $d = (m, c)$. Now, we use mathematical induction on n. If $n = 1$, then (4) is true obviously. Assume that (4) is true for each integer less than n. Since $c < n$ and $d|c$, by induction hypothesis, it follows that $\varphi(d)|\varphi(c)$. Therefore, we deduce that the right part of (6.4) is an integer multiple of $\varphi(m)$. This yields that $\varphi(m)|\varphi(n)$.

(5) If $n = 2^\alpha$ and $\alpha \geq 2$, then by part (1) we obtain $\varphi(n) = \varphi(2^\alpha) = 2^{\alpha-1}$. This means that $\varphi(n)$ is even. Now, we assume that n has at least one odd prime factor. Then, we have

$$\begin{aligned}\varphi(n) &= n\prod_{p|n}\left(1-\frac{1}{p}\right) = n\prod_{p|n}\left(\frac{p-1}{p}\right)\\ &= n\,\frac{\displaystyle\prod_{p|n}(p-1)}{\displaystyle\prod_{p|n}p} = \frac{n}{\displaystyle\prod_{p|n}p}\prod_{p|n}(p-1).\end{aligned}$$

Therefore, we conclude that

$$\varphi(n) = c(n)\prod_{p|n}(p-1).$$

where $c(n)$ is an integer. Since the product multiplying $c(n)$ is even, it follows that $\varphi(n)$ is even. In addition, each odd prime p gives a factor 2 to this product. Consequently, if n has k distinct odd prime factors, then $2^k|\varphi(n)$. ■

Exercises

1. Show that if $n-1$ and $n+1$ are both primes, with $n>4$, then
$$\varphi(n)\le\frac{n}{3}.$$
2. Find all n for which $\varphi(n)\equiv 0(\text{mod }4)$.
3. For each of the following statements either give a proof or exhibit a counter example.
   (a) If $(m,n)=1$, then $\big(\varphi(m),\varphi(n)\big)=1$;
   (b) If n is composite, then $\big(n,\varphi(n)\big)>1$;
   (c) If the same primes divide m and n, then $n\varphi(m)=m\varphi(n)$.
4. Prove that $\varphi(n)>n/6$ for all n with at least 8 distinct prime factors.
5. Prove that
$$\sum_{d^2|n}\mu(d)=\mu^2(n).$$

6.2 Dirichlet Product and Its Properties

The Dirichlet product is a binary operation defined on arithmetical functions. It is commutative, associative, and distributive over addition and has other important number-theoretical properties.

Definition 6.9 Let f and g be two arithmetical functions. We define the *Dirichlet product* of f and g by
$$(f*g)(n)=\sum_{d|n}f(d)g\left(\frac{n}{d}\right),$$
for all positive integer n.

Theorem 6.10 *Let AF be the set of arithmetical functions f such that $f(1)\neq 0$. Then, $(AF,*)$ forms an abelian group.*

Proof Since $(f*g)(1)=f(1)g(1)$, it follows that AF is closed under Dirichlet product. The commutative property is evident from noting that
$$\sum_{d|n}f(d)g\left(\frac{n}{d}\right)=\sum_{ab=n}f(a)g(b).$$

In order to prove the associative property, suppose that f, g, and h are any mathematical functions. Let $A=g*h$ and consider $f*A=f*(g*h)$. Then, we obtain

$$\begin{aligned}(f * A)(n) &= \sum_{ad=n} f(a)A(d)\\ &= \sum_{ad=n} f(a) \sum_{bc=d} g(b)h(c)\\ &= \sum_{abc=n} f(a)g(b)h(c).\end{aligned}$$

Similarly, if we assume that $B = f * g$ and consider $B * h = (f * g) * h$, then we have

$$\begin{aligned}(B * h)(n) &= \sum_{ad=n} B(d)h(a)\\ &= \sum_{ad=n} h(a)B(d)\\ &= \sum_{ad=n} h(a) \sum_{bc=d} f(b)g(c)\\ &= \sum_{abc=n} f(b)g(c)h(a).\end{aligned}$$

So, we conclude that $f * (g * h) = (f * g) * h$, i.e., Dirichlet product is associative. Now, let

$$e(n) = \left\lfloor \frac{1}{n} \right\rfloor = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{otherwise} \end{cases}$$

It is clear that $e \in AF$. Moreover, if $f \in AF$, then we have

$$(f * e)(n) = \sum_{d|n} f(d)e\left(\frac{n}{d}\right) = \sum_{d|n} f(d)\left\lfloor \frac{d}{n} \right\rfloor = f(n),$$

for each positive integer n. This means that e is the identity element of AF. Finally, we must show that for given $f \in AF$, there exists $f^{-1} \in AF$ such that $f * f^{-1} = e$.

Let f is given. We construct f^{-1} inductively. First, we need $(f * f^{-1})(1) = e(1)$, which occurs if and only if $f(1)f^{-1}(1) = 1$. Since $f(1) \neq 0$, it follows that $f^{-1}(1)$ is uniquely determined. Now, suppose that $n > 1$ and f^{-1} determined for each $k < n$. Then, we have to solve the equation $(f * f^{-1})(n) = e(n)$, or equivalently

$$\sum_{d|n} f\left(\frac{n}{d}\right) f^{-1}(d) = 0.$$

This can be written as

$$f(1)f^{-1}(n) \sum_{\substack{d|n\\ d<n}} f\left(\frac{n}{d}\right) f^{-1}(d) = 0,$$

and so

$$f^{-1}(n) = \frac{-1}{f(1)} \sum_{\substack{d|n \\ d<n}} f\left(\frac{n}{d}\right) f^{-1}(d).$$

Since the values $f^{-1}(d)$ are known for all divisors $d < n$, it follows that there is a uniquely determined value to $f^{-1}(n)$. Consequently, we may uniquely determine an f^{-1} for each $f \in AF$. ■

Remark 6.11 If we consider the usual product of functions, i.e., $(f \cdot g)(n) = f(n)g(n)$, then the identity element is $I(n) = n$, for all positive integer n, because $I \cdot f = f$, for all function f. In the group AF, however, I is certainly not identity element. But it has the nice property of transferring each function f into its so-called sum-function S_f.

Definition 6.12 We define

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

to be the *sum-function* of $f \in AF$.

Note that $S_f \in AF$ too. Moreover, it is easy to see that $I * f = f * I = S_f$, for all $f \in AF$.

Lemma 6.13 *The Dirichlet inverse of I is the Möbius function μ.*

Proof According to Theorem 6.5, we have

$$\sum_{d|n} \mu(d) = I(n).$$

In the notation of Dirichlet product this becomes $\mu * I = I * \mu = e$. Therefore, I and μ are inverses of each other. ■

Theorem 6.14 *Each arithmetical function f can be expressed in terms of its sum-function S_f as*

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

Proof We have

$$\mu * S_f = \mu * (I * f) = (\mu * I) * f = e * f = f,$$

and this completes the proof. ■

Theorem 6.15 (Möbius Inversion Theorem) *For two arithmetic functions f and g we have the following equivalence:*

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

Proof If $f = g * I$, then we have

$$f * \mu = (g * I) * \mu = g * (I * \mu) = g * e = g.$$

On the other hand, if $f * \mu = g$, then we have

$$g * I = (f * \mu) * I = f * (\mu * I) = f * e = f.$$

This completes the proof. ■

Exercises

1. Solve the following equations:

   (a) $\varphi(2^x 5^y) = 80$;
   (b) $\varphi(n) = 12$;
   (c) $\varphi(n) = 2n/3$;
   (d) $\varphi(n) = n/2$;
   (e) $\varphi(\varphi(n)) = 2^{13}3^3$.

2. If $(p, q) = 1$, prove that

$$\sum_{k=1}^{q-1}\left[\frac{kp}{q}\right] = \sum_{k=1}^{p-1}\left[\frac{kq}{p}\right].$$

   Hint: Use the identity

$$\left[\frac{kp}{q}\right] - \left[\frac{(q-k)p}{q}\right] = p - 1,$$

   for $k = 1, 2, \ldots, q - 1$, and show that both sums equal $(p - 1)(q - 1)/2$.

6.3 Multiplicative Functions

In this section, we study arithmetical functions called multiplicative functions. These functions have the property that their value at the product of two relatively prime integers is equal to the product of the value of the functions at these integers.

Definition 6.16 An arithmetical function f is called *multiplicative* if f is not identically zero and if $f(mn) = f(m)f(n)$, whenever $(m, n) = 1$. A multiplicative function f is called *completely multiplicative* if we also have $f(mn) = f(m)f(n)$, for all positive integers m and n.

Example 6.17 The Euler function φ is multiplicative. This is easily seen from part (3) of Theorem 6.8. But it is not completely multiplicative, since $\varphi(4) = 2$ and $\varphi(2)\varphi(2) = 1$.

Example 6.18 The Möbius function μ is multiplicative. This is easily seen from Definition 6.4. But it is not completely multiplicative, since $\mu(4) = 0$ and $\mu(2)\mu(2) = 1$.

Example 6.19 The identity element e of the group AF is completely multiplicative.

Example 6.20 Let f and g be two arithmetical functions. Then, the ordinary product fg and the quotient product f/g are defined by

$$\begin{aligned}(fg)(n) &= f(n)g(n),\\ \left(\frac{f}{g}\right)(n) &= \frac{f(n)}{g(n)}, \text{ whenever } g(n) \neq 0.\end{aligned}$$

If f and g are multiplicative, so are fg and f/g.

Theorem 6.21 *If f is multiplicative, then $f(1) = 1$.*

Proof Since $(n, 1) = 1$, for all positive integer n, it follows that $f(n) = f(n)f(1)$. Since f is not identically zero, it follows that $f(n) \neq 0$, for some positive integer n. So, we get $f(1) = 1$. ■

The following is a nice characterization of multiplicative functions.

Theorem 6.22 *Let f be an arithmetical function with $f(1) = 1$. Then,*

(1) f is multiplicative if and only if

$$f(p_1^{\alpha_1} \dots p_k^{\alpha_k}) = f(p_1^{\alpha_1}) \dots f(p_k^{\alpha_k}),$$

for all primes p_i and all positive integers α_i;

(2) If f is multiplicative, then f is completely multiplicative if and only if

$$f(p^\alpha) = f(p)^\alpha,$$

for all primes p and all positive integers α.

Proof The proof follows easily from the definition and is left as an exercise for the reader. ■

The following are further examples of well-known arithmetical functions.

Example 6.23 Let n be a positive integer.

(1) The *divisor function* τ is defined to be the number of positive divisors of n, i.e.,

$$\tau(n) = |\{d \in \mathbb{N} \mid d|n\}|;$$

(2) The *sum of divisors function* σ is defined to be the sum of all positive divisors of n, i.e.,

$$\sigma(n) = \sum_{d|n} d.$$

Theorem 6.24 *The divisor function σ and the sum of divisors function σ are multiplicative. Their values at primes powers are given by*

$$\tau(p^\alpha) = \alpha + 1 \text{ and } \sigma(p^\alpha) = \frac{p^{\alpha+1} - 1}{p - 1}.$$

Proof In order to prove τ is multiplicative, assume that n and m are positive integers with $(m, n) = 1$. Note that if $d_1|m$ and $d_2|n$, then $d_1 d_2|mn$. Conversely, if $d|mn$, then $d = d_1 d_2$ such that $d_1|m$ and $d_2|n$. Therefore, there exists a one to one correspondence between the set of divisors of mn and the set

$$A = \{(d_1, d_2) \mid d_1|m \text{ and } d_2|n\}.$$

Since $\tau(mn)$ is the number of divisors of mn and $|A| = \tau(m)\tau(n)$, it follows that $\tau(mn) = \tau(m)\tau(n)$. Similarly, we can prove that σ is multiplicative. Indeed, we have

$$\sigma(mn) = \sum_{d|n} d = \sum_{\substack{d_1|m \\ d_2|n}} d_1 d_2 = \left(\sum_{d_1|m} d_1\right)\left(\sum_{d_2|n} d_2\right) = \sigma(m)\sigma(n).$$

Moreover, since the divisors of p^α are exactly $1, p, \ldots, p^\alpha$, it follows that $\tau(p^\alpha) = \alpha + 1$. Moreover, if we apply the geometric series formula, then we obtain

$$\sigma(p^\alpha) = 1 + p + \cdots + p^\alpha = \frac{p^{\alpha+1} - 1}{p - 1},$$

as desired. ■

Theorem 6.25 *If f and g are multiplicative, so is their Dirichlet product $f * g$.*

Proof Let $h = f * g$ and $(m, n) = 1$. Then, we have

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

Suppose that $d = ab$ such that $a|m$ and $b|n$. Then, we obtain

$$\begin{aligned} h(mn) &= \sum_{\substack{a|m\\ b|n}} f(ab)g\left(\frac{mn}{ab}\right) = \sum_{\substack{a|m\\ b|n}} f(a)f(b)g\left(\frac{m}{a}\right)g\left(\frac{n}{b}\right) \\ &= \sum_{a|m} f(a)g\left(\frac{m}{a}\right)\sum_{b|n} f(b)g\left(\frac{n}{b}\right) = h(m)h(n). \end{aligned}$$

Thus, h is also multiplicative. ■

Theorem 6.26 *If g and $f * g$ are multiplicative, then f is also multiplicative.*

Proof Assume that f is not multiplicative and let $h = f * g$. Then, there exist positive integers m and n with $(m, n) = 1$ such that $f(mn) \neq f(m)f(n)$. By the well-ordering principle, we choose such a pair m and n for which the product mn is as small as possible. We consider the following two cases:

Case 1: If $mn = 1$, then $f(1) \neq f(1)f(1)$, and so $f(1) \neq 1$. Since $h(1) = f(1)g(1) = f(1) \neq 0$, it follows that h is not multiplicative, and this is a contradiction.

Case 2: If $mn > 1$, then $f(ab) = f(a)f(b)$, for all positive integers a and b with $(a, b) = 1$ and $ab < mn$. Therefore, we have

$$\begin{aligned} h(mn) &= \sum_{\substack{a|m\\ b|n}} f(ab)g\left(\frac{mn}{ab}\right) \\ &= \sum_{\substack{a|m\\ b|n\\ ab<mn}} f(ab)g\left(\frac{mn}{ab}\right) + f(mn)g(1) \\ &= \sum_{\substack{a|m\\ b|n\\ ab<mn}} f(a)f(b)g\left(\frac{m}{a}\right)g\left(\frac{n}{b}\right) + f(mn) \\ &= \sum_{a|m} f(a)g\left(\frac{m}{a}\right)\sum_{b|n} f(b)g\left(\frac{n}{b}\right) - f(m)f(n) + f(mn) \\ &= h(m)h(n) - f(m)f(n) + f(mn). \end{aligned}$$

Since $f(mn) \neq f(m)f(n)$, it follows that $h(mn) \neq h(m)h(n)$. This shows that h is not multiplicative, and it is a contradiction. ■

Theorem 6.27 *If f is multiplicative, so is f^{-1}, its Dirichlet inverse.*

Proof The result can be easily obtained from Theorem 6.26. In fact, since both f and $f^{-1} * f = e$ are multiplicative, it follows that f^{-1} is multiplicative. ■

Corollary 6.28 *The set of multiplicative functions is a subgroup of AF.*

Proof It is clear by Theorems 6.25 and 6.27. ■

Theorem 6.29 *Let f be multiplicative. Then, f is completely multiplicative if and only if $f^{-1}(n) = \mu(n)f(n)$, for each positive integer n.*

Proof Let $g(n) = \mu(n)f(n)$. If f is completely implicative, then

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

because $f(1) = 1$ and $e(n) = 0$, for each $n > 1$. Hence, we have $g = f^{-1}$.

Conversely, suppose that $f^{-1}(n) = \mu(n)f(n)$. In order to prove that f is completely multiplicative, it is enough to show that $f(p^\alpha) = f(p)^\alpha$ for prime powers. Since $f * f^{-1} = f * \mu f = e$, it follows that $(f * \mu f)(n) = e(n)$. This yields that

$$\sum_{d|n} \mu(d)f(d)f\left(\frac{n}{d}\right) = 0,$$

for each integer n. Now, we take $n = p^\alpha$, then obtain

$$\mu(1)f(1)f(p^\alpha) + \mu(p)f(p)f(p^{\alpha-1}) = 0.$$

Therefore, we conclude that $f(p^\alpha) = f(p)f(p^{\alpha-1})$. This shows that $f(p^\alpha) = f(p)^\alpha$. ■

Exercises

1. Prove that
$$\frac{\varphi(n)\sigma(n) + 1}{n}$$
is an integer if n is prime, and it is not integer if n is divisible by square of a prime.
2. Prove that f is multiplicative if and only if its sum-function S_f is multiplicative.
3. Let $f(n) = [\sqrt{n}] - [\sqrt{n-1}]$. Prove that f is multiplicative but not completely multiplicative.
4. Solve the equation $\varphi\big(\sigma(2^n)\big) = 2^n$.

6.4 Worked-Out Problems

Problem 6.30 If $\varphi(m)|m - 1$, prove that there does not exist prime number p such that $p^2|m$.

Solution Suppose that there exists prime number p_j such that $p_j^2|m$. Let $m = p_1^{\alpha_1} \dots p_j^{\alpha_j} \dots p_k^{\alpha_k}$, where $\alpha_j \geq 2$. Then, we have

$$p_j \Big| p_j \left(p_j^{\alpha_j-1} - p_j^{\alpha_j-2}\right) = p_j^{\alpha_j} - p_j^{\alpha_j-1} = \varphi(p_j^{\alpha_j}).$$

On the other hand, since $p_j^{\alpha_j}|m$, it follows that $\varphi(p_j^{\alpha_j})|\varphi(m)$. So, we conclude that $p_j|\varphi(m)$. Since $p_j \nmid m-1$, it follows that $\varphi(m) \nmid m-1$. This is a contradiction. ■

Problem 6.31 If m is not prime and $\varphi(m)|m-1$, prove that m has at least three distinct prime factors.

Solution Suppose that m has exactly two distinct prime factors. By Problem 6.30, since $\varphi(m)|m-1$, we conclude that $m = pq$, where p and q are distinct primes. Then, we have

$$\begin{aligned}\frac{m-1}{\varphi(m)} &= \frac{pq-1}{(p-1)(q-1)} \\ &= \frac{pq-p-q+1+p+q-2}{(p-1)(q-1)} \\ &= \frac{(p-1)(q-1)}{(p-1)(q-1)} + \frac{p-1}{(p-1)(q-1)} + \frac{q-1}{(p-1)(q-1)} \\ &= 1 + \frac{1}{q-1} + \frac{1}{p-1}.\end{aligned}$$

Since $\varphi(m)|m-1$, it follows that $(m-1)/\varphi(m)$ is an integer. Moreover, we have

$$1 < 1 + \frac{1}{q-1} + \frac{1}{p-1} \leq 3.$$

So, we must have

$$\frac{1}{q-1} + \frac{1}{p-1} = 1 \text{ or } 2.$$

This implies that $p = q = 2$ or $p = q = 3$. But this contradicts our assumption that p and q are distinct. Consequently, it is impossible for m to have only two distinct prime factors. ■

Problem 6.32 Show that if $m \geq 2$, then the sum of all positive integers which are less than m and relatively prime to m is $(1/2)m\varphi(m)$.

Solution Suppose that $1 \leq k < m$ such that $(k, m) = 1$. If $(m-k, m) = d$, then $d|m$ and $d|m-k$. This implies that $d|k$, and so $d = 1$. Since $k < m$, it follows that $m - k \geq 1$. Also, we have $m - k < m$. Now, assume that

$$\begin{aligned}A &= \{k \mid 1 \leq k \leq m,\ (k, m) = 1\}, \\ B &= \{m-k \mid 1 \leq k \leq m,\ (k, m) = 1\}.\end{aligned}$$

There is a one to one correspondence between A and B given by $f(k) = m - k$. Consequently, we have $|A| = |B| = \varphi(m)$. Therefore, we get

$$\big(k_1 + (m - k_1)\big) + \cdots + \big(k_{\varphi(m)} + (m - k_{\varphi(m)})\big) = 2 \sum_{\substack{0<k<m\\(k,m)=1}} k.$$

This shows that

$$\underbrace{m + \cdots + m}_{\varphi(m)\ \text{times}} = 2S,$$

where S is the required sum. Therefore, we deduce that $S = (1/2)m\varphi(m)$. ■

Problem 6.33 Let $f : \mathbb{N} \to \mathbb{N}$ be multiplicative and strictly increasing. If $f(2) = 2$, prove that $f(n) = n$ for all n.

Solution We have $f(1) = 1$ and $f(2) = 2$. First, we show that $f(3) = 3$. Suppose that $f(3) = k + 3$, where k is a non-negative integer. We can write $f(6) = f(2)f(3) = 2(k + 3) = 2k + 6$. Since f is strictly increasing, it follows that $f(5) \leq 2k + 5$, and so $f(10) = f(2)f(5) \leq 4k + 10$. Hence, we must have $f(9) \leq 4k + 9$, which implies that $f(18) = f(2)f(9) \leq 8k + 18$. This gives

$$f(15) \leq 8k + 15. \tag{6.5}$$

On the other hand, we have

$$f(15) = f(3)f(5) \geq (k + 3)(k + 5) = k^2 + 8k + 15. \tag{6.6}$$

By (6.5) and (6.6) we conclude that $k = 0$. Hence, $f(3) = 3$, as desired. Now, we use mathematical induction. Suppose that

$$f(m) = m, \text{ for all } m = 1, 2, \ldots, 2k - 1,$$

where $k \geq 2$. Then, we have

$$\begin{aligned} f(4k - 2) &= f\big(2(2k - 1)\big) = f(2)f(2k - 1) \\ &= 2f(2k - 1) = 4k - 2. \end{aligned}$$

Since f is strictly increasing, it follows that $f(m) = m$, for all $2k - 1 \leq m \leq 4k - 2$. In particular, we deduce that $f(2k) = 2k$ and $f(2k + 1) = 2k + 1$. This completes the proof.

Problem 6.34 Prove that

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

Solution Since μ and φ are multiplicative and $\varphi(n) \neq 0$, for each positive integer n, it follows that μ^2/φ is multiplicative. So, if $G = S_{\mu^2/\varphi}$, sum-function, then

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

and G is multiplicative, since $(\mu^2/\varphi) * I = G$. Now, if $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$, then

$$\begin{aligned}
G(n) &= G(p_1^{\alpha_1}) \dots G(p_k^{\alpha_k}) \\
&= \left(1 + \frac{1}{\varphi(p_1)}\right) \dots \left(1 + \frac{1}{\varphi(p_k)}\right) \\
&= \frac{p_1}{p_1 - 1} \dots \frac{p_k}{p_k - 1} \\
&= \frac{n}{n\left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_k}\right)} \\
&= \frac{n}{\varphi(n)}.
\end{aligned}$$

This completes the proof. ■

Problem 6.35 Let G be a finite abelian group. We say that $f :: G \to \mathbb{C}$ is a *character* on G if (1) $f(x) \neq 0$, for all $x \in G$, and (2) $f(xy) = f(x)f(y)$, for all $x, y \in G$. Suppose that f is a character on the multiplicative group U_k. We may extend the domain of this character to the entire set of natural numbers in the following manner: First, let $\overline{n} \in U_k$ be the equivalence class modulo k containing n. We extend the domain of f to the entire set of natural numbers as follows:

$$\chi(n) = \begin{cases} f(\overline{n}) & \text{if } (n, k) = 1 \\ 0 & \text{otherwise.} \end{cases}$$

We call χ a *Dirichlet character modulo* k. It is easy to see that χ has the following two important properties:

(1) It is k-periodic, i.e., $\chi(a + k) = \chi(a)$, for all $a \in \mathbb{N}$;
(2) It is completely multiplicative.

Table 6.2 shows the Dirichlet characters modulo 5. It is not difficult to check that no more exist.

If χ is an arithmetical function that is both periodic and completely multiplicative, and it is not zero function, prove that it is a Dirichlet character.

Solution Let k be the minimal period of χ. Since χ is k-periodic, it is constant in each equivalence class modulo k. Moreover, since it is completely multiplicative, its

Table 6.2 Dirichlet characters modulo 5

x (mod 5)	0	1	2	3	4
χ_1	0	1	1	1	1
χ_2	0	1	–1	–1	1
χ_3	0	1	i	$-i$	–1
χ_4	0	1	$-i$	i	–1

values on U_k make it a character. Therefore, we need to show that $\chi(n) = 0$ if and only if $(n, k) \neq 1$. First, assume $(n, k) = 1$. Then we have $n^{\varphi(k)} \equiv 1(\text{mod } k)$. Since χ is completely multiplicative and k-periodic, we have $\chi(n)^{\varphi(k)} = \chi\left(n^{\varphi(k)}\right) = \chi(1)$. Thus, if $\chi(n) = 0$, then $\chi(1) = 0$. However, if $\chi(1) = 0$, then we have $\chi(m) = \chi(1)\chi(m) = 0$, for all m. Hence, if $(n, k) = 1$ and $\chi(n) = 0$, then χ is zero function. On the other hand, we assume that there is n such that $(n, k) > 1$ and $\chi(n) \neq 0$. Then there is at least one prime p such that $p|k$ and $\chi(p) \neq 0$. Consider this p, and let m be any natural number. Because χ is k-periodic and completely multiplicative, we have

$$\chi(m)\chi(p) = \chi(mp) = \chi(mp + k) = \chi(p)\chi\left(m + \frac{k}{p}\right).$$

Since $\chi(p) \neq 0$, we must have $\chi(m) = \chi(m + k/p)$, for all m. But this means that χ is k/p-periodic. This violates the stipulation that k is the minimal period of χ. ■

6.5 Supplementary Exercises

1. Let n be an integer with $n \geq 2$. Show that $\varphi\big(2^n - 1\big)$ is divisible by n.
2. If p is a prime and n is an integer such that $1 < n < p$, prove that

$$\varphi\left(\sum_{k=0}^{p-1} n^k\right) \equiv 0(\text{mod } p).$$

3. Let m and n be positive integers. Prove that, for some positive integer a, each of $\varphi(a), \varphi(a+1), \ldots, \varphi(a+n)$ is a multiple of m.
4. If n is composite, prove that $\varphi(n) \leq n - \sqrt{n}$.
5. Find all solutions of $\varphi(n) = 4$, and prove that there are no more.
6. Find $m, n \in \mathbb{N}$ such that they have no prime divisors other than 2 and 3, $(m, n) = 18$, $\tau(m) = 21$, and $\tau(n) = 10$.
7. Determine an arithmetical function f such that

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

8. An arithmetical function f is called *periodic* if there exists a positive integer k such that $f(n+k) = f(n)$ for each positive integer 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.
9. Let f be a multiplicative function satisfying $\lim\limits_{p^m \to \infty} f(p^m) = 0$. Show that $\lim\limits_{n \to \infty} f(n) = 0$.
10. Prove that the sum-function S_f of a multiplicative function f is given by

$$S_f(n) = \prod_{i=1}^{k} \left(1 + f(p_i) + f(p_i^2) + \cdots + f(p_i^{\alpha_i})\right),$$

whenever $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$.

11. For any real number $x \geq 1$, prove that

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

12. Prove that a finite abelian group G of order n has exactly n distinct characters.
13. For two sequences of complex numbers $\{a_0, a_1, \dots, a_n, \dots\}$ and $\{b_0, b_1, \dots, b_n, \dots\}$ show that the following relations are equivalent:

$$a_n = \sum_{k=0}^{n} b_k \text{ for all } n \Leftrightarrow b_n = \sum_{k=0}^{n} (-1)^{k+n} a_k \text{ for all } n.$$

14. Prove that

$$\sum_{k=1}^{n} \tau(k) = \sum_{k=1}^{n} \left[\frac{n}{k}\right] \text{ and } \sum_{k=1}^{n} \sigma(k) = \sum_{k=1}^{n} k \left[\frac{n}{k}\right].$$