CHAPTER 6

NUMBER-THEORETIC FUNCTIONS

Mathematicians are like Frenchmen: whatever you say to them they translate into their own language and forthwith it is something entirely different.

GOETHE

6.1 THE SUM AND NUMBER OF DIVISORS

Certain functions are found to be of special importance in connection with the study of the divisors of an integer. Any function whose domain of definition is the set of positive integers is said to be a *number-theoretic* (or *arithmetic*) *function*. Although the value of a number-theoretic function is not required to be a positive integer or, for that matter, even an integer, most of the number-theoretic functions that we shall encounter are integer-valued. Among the easiest to handle, and the most natural, are the functions τ and σ.

Definition 6.1. Given a positive integer n, let $\tau(n)$ denote the number of positive divisors of n and $\sigma(n)$ denote the sum of these divisors.

For an example of these notions, consider $n = 12$. Because 12 has the positive divisors 1, 2, 3, 4, 6, 12, we find that

$$\tau(12) = 6 \qquad \text{and} \qquad \sigma(12) = 1 + 2 + 3 + 4 + 6 + 12 = 28$$

For the first few integers,

$$\tau(1) = 1 \quad \tau(2) = 2 \quad \tau(3) = 2 \quad \tau(4) = 3 \quad \tau(5) = 2 \quad \tau(6) = 4, \ldots$$

and

$$\sigma(1) = 1, \sigma(2) = 3, \sigma(3) = 4, \sigma(4) = 7, \sigma(5) = 6, \sigma(6) = 12, \ldots$$

It is not difficult to see that $\tau(n) = 2$ if and only if n is a prime number; also, $\sigma(n) = n + 1$ if and only if n is a prime.

Before studying the functions τ and σ in more detail, we wish to introduce notation that will clarify a number of situations later. It is customary to interpret the symbol

$$\sum_{d \mid n} f(d)$$

to mean, "Sum the values $f(d)$ as d runs over all the positive divisors of the positive integer n." For instance, we have

$$\sum_{d \mid 20} f(d) = f(1) + f(2) + f(4) + f(5) + f(10) + f(20)$$

With this understanding, τ and σ may be expressed in the form

$$\tau(n) = \sum_{d \mid n} 1 \qquad \sigma(n) = \sum_{d \mid n} d$$

The notation $\sum_{d \mid n} 1$, in particular, says that we are to add together as many 1's as there are positive divisors of n. To illustrate: the integer 10 has the four positive divisors 1, 2, 5, 10, whence

$$\tau(10) = \sum_{d \mid 10} 1 = 1 + 1 + 1 + 1 = 4$$

and

$$\sigma(10) = \sum_{d \mid 10} d = 1 + 2 + 5 + 10 = 18$$

Our first theorem makes it easy to obtain the positive divisors of a positive integer n once its prime factorization is known.

Theorem 6.1. If $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ is the prime factorization of $n > 1$, then the positive divisors of n are precisely those integers d of the form

$$d = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$$

where $0 \le a_i \le k_i$ $(i = 1, 2, \ldots, r)$.

Proof. Note that the divisor $d = 1$ is obtained when $a_1 = a_2 = \cdots = a_r = 0$, and n itself occurs when $a_1 = k_1, a_2 = k_2, \ldots, a_r = k_r$. Suppose that d divides n nontrivially; say, $n = dd'$, where $d > 1$, $d' > 1$. Express both d and d' as products of (not necessarily distinct) primes:

$$d = q_1 q_2 \cdots q_s \qquad d' = t_1 t_2 \cdots t_u$$

with q_i, t_j prime. Then

$$p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r} = q_1 \cdots q_s t_1 \cdots t_u$$

are two prime factorizations of the positive integer n. By the uniqueness of the prime factorization, each prime q_i must be one of the p_j. Collecting the equal primes into a single integral power, we get

$$d = q_1 q_2 \cdots q_s = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$$

where the possibility that $a_i = 0$ is allowed.

Conversely, every number $d = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ $(0 \leq a_i \leq k_i)$ turns out to be a divisor of n. For we can write

$$\begin{aligned} n &= p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r} \\ &= \left(p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}\right)\left(p_1^{k_1-a_1} p_2^{k_2-a_2} \cdots p_r^{k_r-a_r}\right) \\ &= dd' \end{aligned}$$

with $d' = p_1^{k_1-a_1} p_2^{k_2-a_2} \cdots p_r^{k_r-a_r}$ and $k_i - a_i \geq 0$ for each i. Then $d' > 0$ and $d \mid n$.

We put this theorem to work at once.

Theorem 6.2. If $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ is the prime factorization of $n > 1$, then

(a) $\tau(n) = (k_1 + 1)(k_2 + 1) \cdots (k_r + 1)$, and

(b) $\sigma(n) = \dfrac{p_1^{k_1+1} - 1}{p_1 - 1} \dfrac{p_2^{k_2+1} - 1}{p_2 - 1} \cdots \dfrac{p_r^{k_r+1} - 1}{p_r - 1}$.

Proof. According to Theorem 6.1, the positive divisors of n are precisely those integers

$$d = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$$

where $0 \leq a_i \leq k_i$. There are $k_1 + 1$ choices for the exponent a_1; $k_2 + 1$ choices for $a_2, \ldots$; and $k_r + 1$ choices for a_r. Hence, there are

$$(k_1 + 1)(k_2 + 1) \cdots (k_r + 1)$$

possible divisors of n.

To evaluate $\sigma(n)$, consider the product

$$\left(1 + p_1 + p_1^2 + \cdots + p_1^{k_1}\right)\left(1 + p_2 + p_2^2 + \cdots + p_2^{k_2}\right) \cdots \left(1 + p_r + p_r^2 + \cdots + p_r^{k_r}\right)$$

Each positive divisor of n appears once and only once as a term in the expansion of this product, so that

$$\sigma(n) = \left(1 + p_1 + p_1^2 + \cdots + p_1^{k_1}\right) \cdots \left(1 + p_r + p_r^2 + \cdots + p_r^{k_r}\right)$$

Applying the formula for the sum of a finite geometric series to the ith factor on the right-hand side, we get

$$1 + p_i + p_i^2 + \cdots + p_i^{k_i} = \frac{p_i^{k_i+1} - 1}{p_i - 1}$$

It follows that

$$\sigma(n) = \frac{p_1^{k_1+1} - 1}{p_1 - 1} \frac{p_2^{k_2+1} - 1}{p_2 - 1} \cdots \frac{p_r^{k_r+1} - 1}{p_r - 1}$$

Corresponding to the $\sum$ notation for sums, the notation for products may be defined using $\prod$, the Greek capital letter pi. The restriction delimiting the numbers over which the product is to be made is usually put under the $\prod$ sign. Examples are

$$\prod_{1 \le d \le 5} f(d) = f(1)f(2)f(3)f(4)f(5)$$

$$\prod_{d \mid 9} f(d) = f(1)f(3)f(9)$$

$$\prod_{\substack{p \mid 30 \\ p \text{ prime}}} f(p) = f(2)f(3)f(5)$$

With this convention, the conclusion to Theorem 6.2 takes the compact form: if $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ is the prime factorization of $n > 1$, then

$$\tau(n) = \prod_{1 \le i \le r} (k_i + 1)$$

and

$$\sigma(n) = \prod_{1 \le i \le r} \frac{p_i^{k_i+1} - 1}{p_i - 1}$$

Example 6.1. The number $180 = 2^2 \cdot 3^2 \cdot 5$ has

$$\tau(180) = (2+1)(2+1)(1+1) = 18$$

positive divisors. These are integers of the form

$$2^{a_1} \cdot 3^{a_2} \cdot 5^{a_3}$$

where $a_1 = 0, 1, 2$; $a_2 = 0, 1, 2$; and $a_3 = 0, 1$. Specifically, we obtain

$$1, 2, 3, 4, 5, 6, 9, 10, 12, 15, 18, 20, 30, 36, 45, 60, 90, 180$$

The sum of these integers is

$$\sigma(180) = \frac{2^3 - 1}{2 - 1} \frac{3^3 - 1}{3 - 1} \frac{5^2 - 1}{5 - 1} = \frac{7}{1} \frac{26}{2} \frac{24}{4} = 7 \cdot 13 \cdot 6 = 546$$

One of the more interesting properties of the divisor function τ is that the product of the positive divisors of an integer $n > 1$ is equal to $n^{\tau(n)/2}$. It is not difficult to get at this fact: Let d denote an arbitrary positive divisor of n, so that $n = dd'$ for some d'. As d ranges over all $\tau(n)$ positive divisors of n, $\tau(n)$ such equations occur. Multiplying these together, we get

$$n^{\tau(n)} = \prod_{d \mid n} d \cdot \prod_{d' \mid n} d'$$

But as d runs through the divisors of n, so does d'; hence, $\prod_{d \mid n} d = \prod_{d' \mid n} d'$. The situation is now this:

$$n^{\tau(n)} = \left(\prod_{d \mid n} d\right)^2$$

or equivalently

$$n^{\tau(n)/2} = \prod_{d \mid n} d$$

The reader might (or, at any rate, should) have one lingering doubt concerning this equation. For it is by no means obvious that the left-hand side is always an integer. If $\tau(n)$ is even, there is certainly no problem. When $\tau(n)$ is odd, n turns out to be a perfect square (Problem 7, Section 6.1), say, $n = m^2$; thus $n^{\tau(n)/2} = m^{\tau(n)}$, settling all suspicions.

For a numerical example, the product of the five divisors of 16 (namely, 1, 2, 4, 8, 16) is

$$\prod_{d \mid 16} d = 16^{\tau(16)/2} = 16^{5/2} = 4^5 = 1024$$

Multiplicative functions arise naturally in the study of the prime factorization of an integer. Before presenting the definition, we observe that

$$\tau(2 \cdot 10) = \tau(20) = 6 \neq 2 \cdot 4 = \tau(2) \cdot \tau(10)$$

At the same time,

$$\sigma(2 \cdot 10) = \sigma(20) = 42 \neq 3 \cdot 18 = \sigma(2) \cdot \sigma(10)$$

These calculations bring out the nasty fact that, in general, it need not be true that

$$\tau(mn) = \tau(m)\tau(n) \qquad \text{and} \qquad \sigma(mn) = \sigma(m)\sigma(n)$$

On the positive side of the ledger, equality always holds provided we stick to relatively prime m and n. This circumstance is what prompts Definition 6.2.

Definition 6.2. A number-theoretic function f is said to be *multiplicative* if

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

whenever $\gcd(m, n) = 1$.

For simple illustrations of multiplicative functions, we need only consider the functions given by $f(n) = 1$ and $g(n) = n$ for all $n \geq 1$. It follows by induction that if f is multiplicative and $n_1, n_2, \ldots, n_r$ are positive integers that are pairwise relatively prime, then

$$f(n_1 n_2 \cdots n_r) = f(n_1)f(n_2) \cdots f(n_r)$$

Multiplicative functions have one big advantage for us: they are completely determined once their values at prime powers are known. Indeed, if $n > 1$ is a given positive integer, then we can write $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ in canonical form; because the

$p_i^{k_i}$ are relatively prime in pairs, the multiplicative property ensures that

$$f(n) = f\left(p_1^{k_1}\right) f\left(p_2^{k_2}\right) \cdots f\left(p_r^{k_r}\right)$$

If f is a multiplicative function that does not vanish identically, then there exists an integer n such that $f(n) \neq 0$. But

$$f(n) = f(n \cdot 1) = f(n) f(1)$$

Being nonzero, $f(n)$ may be canceled from both sides of this equation to give $f(1) = 1$. The point to which we wish to call attention is that $f(1) = 1$ for any multiplicative function not identically zero.

We now establish that τ and σ have the multiplicative property.

Theorem 6.3. The functions τ and σ are both multiplicative functions.

Proof. Let m and n be relatively prime integers. Because the result is trivially true if either m or n is equal to 1, we may assume that $m > 1$ and $n > 1$. If

$$m = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r} \qquad \text{and} \qquad n = q_1^{j_1} q_2^{j_2} \cdots q_s^{j_s}$$

are the prime factorizations of m and n, then because $\gcd(m, n) = 1$, no p_i can occur among the q_j. It follows that the prime factorization of the product mn is given by

$$mn = p_1^{k_1} \cdots p_r^{k_r} q_1^{j_1} \cdots q_s^{j_s}$$

Appealing to Theorem 6.2, we obtain

$$\begin{aligned} \tau(mn) &= [(k_1 + 1) \cdots (k_r + 1)][(j_1 + 1) \cdots (j_s + 1)] \\ &= \tau(m)\tau(n) \end{aligned}$$

In a similar fashion, Theorem 6.2 gives

$$\begin{aligned} \sigma(mn) &= \left[\frac{p_1^{k_1+1} - 1}{p_1 - 1} \cdots \frac{p_r^{k_r+1} - 1}{p_r - 1}\right]\left[\frac{q_1^{j_1+1} - 1}{q_1 - 1} \cdots \frac{q_s^{j_s+1} - 1}{q_s - 1}\right] \\ &= \sigma(m)\sigma(n) \end{aligned}$$

Thus, τ and σ are multiplicative functions.

We continue our program by proving a general result on multiplicative functions. This requires a preparatory lemma.

Lemma. If $\gcd(m, n) = 1$, then the set of positive divisors of mn consists of all products $d_1 d_2$, where $d_1 \mid m$, $d_2 \mid n$ and $\gcd(d_1, d_2) = 1$; furthermore, these products are all distinct.

Proof. It is harmless to assume that $m > 1$ and $n > 1$; let $m = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ and $n = q_1^{j_1} q_2^{j_2} \cdots q_s^{j_s}$ be their respective prime factorizations. Inasmuch as the primes $p_1, \ldots, p_r, q_1, \ldots, q_s$ are all distinct, the prime factorization of mn is

$$mn = p_1^{k_1} \cdots p_r^{k_r} q_1^{j_1} \cdots q_s^{j_s}$$

Hence, any positive divisor d of mn will be uniquely representable in the form

$$d = p_1^{a_1} \cdots p_r^{a_r} q_1^{b_1} \cdots q_s^{b_s} \qquad 0 \le a_i \le k_i, 0 \le b_i \le j_i$$

This allows us to write d as $d = d_1 d_2$, where $d_1 = p_1^{a_1} \cdots p_r^{a_r}$ divides m and $d_2 = q_1^{b_1} \cdots q_s^{b_s}$ divides n. Because no p_i is equal to any q_j, we surely must have $\gcd(d_1, d_2) = 1$.

A keystone in much of our subsequent work is Theorem 6.4.

Theorem 6.4. If f is a multiplicative function and F is defined by

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

then F is also multiplicative.

Proof. Let m and n be relatively prime positive integers. Then

$$\begin{aligned} F(mn) &= \sum_{d \mid mn} f(d) \\ &= \sum_{\substack{d_1 \mid m \\ d_2 \mid n}} f(d_1 d_2) \end{aligned}$$

because every divisor d of mn can be uniquely written as a product of a divisor d_1 of m and a divisor d_2 of n, where $\gcd(d_1, d_2) = 1$. By the definition of a multiplicative function,

$$f(d_1 d_2) = f(d_1) f(d_2)$$

It follows that

$$\begin{aligned} F(mn) &= \sum_{\substack{d_1 \mid m \\ d_2 \mid n}} f(d_1) f(d_2) \\ &= \left(\sum_{d_1 \mid m} f(d_1)\right)\left(\sum_{d_2 \mid n} f(d_2)\right) \\ &= F(m)F(n) \end{aligned}$$

It might be helpful to take time out and run through the proof of Theorem 6.4 in a concrete case. Letting $m = 8$ and $n = 3$, we have

$$\begin{aligned} F(8 \cdot 3) &= \sum_{d \mid 24} f(d) \\ &= f(1) + f(2) + f(3) + f(4) + f(6) + f(8) + f(12) + f(24) \\ &= f(1 \cdot 1) + f(2 \cdot 1) + f(1 \cdot 3) + f(4 \cdot 1) + f(2 \cdot 3) \\ &\quad + f(8 \cdot 1) + f(4 \cdot 3) + f(8 \cdot 3) \\ &= f(1)f(1) + f(2)f(1) + f(1)f(3) + f(4)f(1) + f(2)f(3) \\ &\quad + f(8)f(1) + f(4)f(3) + f(8)f(3) \\ &= [f(1) + f(2) + f(4) + f(8)][f(1) + f(3)] \\ &= \sum_{d \mid 8} f(d) \cdot \sum_{d \mid 3} f(d) = F(8)F(3) \end{aligned}$$

Theorem 6.4 provides a deceptively short way of drawing the conclusion that τ and σ are multiplicative.

Corollary. The functions τ and σ are multiplicative functions.

Proof. We have mentioned that the constant function $f(n) = 1$ is multiplicative, as is the identity function $f(n) = n$. Because τ and σ may be represented in the form

$$\tau(n) = \sum_{d \mid n} 1 \qquad \text{and} \qquad \sigma(n) = \sum_{d \mid n} d$$

the stated result follows immediately from Theorem 6.4.

PROBLEMS 6.1

1. Let m and n be positive integers and $p_1, p_2, \ldots, p_r$ be the distinct primes that divide at least one of m or n. Then m and n may be written in the form

$$m = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r} \qquad \text{with } k_i \geq 0 \text{ for } i = 1, 2, \ldots, r$$

$$n = p_1^{j_1} p_2^{j_2} \cdots p_r^{j_r} \qquad \text{with } j_i \geq 0 \text{ for } i = 1, 2, \ldots, r$$

Prove that

$$\gcd(m, n) = p_1^{u_1} p_2^{u_2} \cdots p_r^{u_r} \qquad \operatorname{lcm}(m, n) = p_1^{v_1} p_2^{v_2} \cdots p_r^{v_r}$$

where $u_i = \min\{k_i, j_i\}$, the smaller of k_i and j_i; and $v_i = \max\{k_i, j_i\}$, the larger of k_i and j_i.

2. Use the result of Problem 1 to calculate gcd(12378, 3054) and lcm(12378, 3054).

3. Deduce from Problem 1 that $\gcd(m, n)\operatorname{lcm}(m, n) = mn$ for positive integers m and n.

4. In the notation of Problem 1, show that $\gcd(m, n) = 1$ if and only if $k_i j_i = 0$ for $i = 1, 2, \ldots, r$.

5. (a) Verify that $\tau(n) = \tau(n+1) = \tau(n+2) = \tau(n+3)$ holds for $n = 3655$ and 4503.
(b) When $n = 14, 206$, and 957, show that $\sigma(n) = \sigma(n+1)$.

6. For any integer $n \geq 1$, establish the inequality $\tau(n) \leq 2\sqrt{n}$.
[*Hint:* If $d \mid n$, then one of d or n/d is less than or equal to $\sqrt{n}$.]

7. Prove the following.
(a) $\tau(n)$ is an odd integer if and only if n is a perfect square.
(b) $\sigma(n)$ is an odd integer if and only if n is a perfect square or twice a perfect square.
[*Hint:* If p is an odd prime, then $1 + p + p^2 + \cdots + p^k$ is odd only when k is even.]

8. Show that $\sum_{d \mid n} 1/d = \sigma(n)/n$ for every positive integer n.

9. If n is a square-free integer, prove that $\tau(n) = 2^r$, where r is the number of prime divisors of n.

10. Establish the assertions below:
(a) If $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ is the prime factorization of $n > 1$, then

$$1 > \frac{n}{\sigma(n)} > \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right)$$

(b) For any positive integer n,

$$\frac{\sigma(n!)}{n!} \geq 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}$$

[*Hint:* See Problem 8.]
(c) If $n > 1$ is a composite number, then $\sigma(n) > n + \sqrt{n}$.
[*Hint:* Let $d \mid n$, where $1 < d < n$, so $1 < n/d < n$. If $d \leq \sqrt{n}$, then $n/d \geq \sqrt{n}$.]

11. Given a positive integer $k > 1$, show that there are infinitely many integers n for which $\tau(n) = k$, but at most finitely many n with $\sigma(n) = k$.
[*Hint:* Use Problem 10(a).]

12. (a) Find the form of all positive integers n satisfying $\tau(n) = 10$. What is the smallest positive integer for which this is true?
(b) Show that there are no positive integers n satisfying $\sigma(n) = 10$.
[*Hint:* Note that for $n > 1$, $\sigma(n) > n$.]

13. Prove that there are infinitely many pairs of integers m and n with $\sigma(m^2) = \sigma(n^2)$.
[*Hint:* Choose k such that $\gcd(k, 10) = 1$ and consider the integers $m = 5k$, $n = 4k$.]

14. For $k \geq 2$, show each of the following:
(a) $n = 2^{k-1}$ satisfies the equation $\sigma(n) = 2n - 1$.
(b) If $2^k - 1$ is prime, then $n = 2^{k-1}(2^k - 1)$ satisfies the equation $\sigma(n) = 2n$.
(c) If $2^k - 3$ is prime, then $n = 2^{k-1}(2^k - 3)$ satisfies $\sigma(n) = 2n + 2$.
It is not known if there are any positive integers n for which $\sigma(n) = 2n + 1$.

15. If n and $n + 2$ are a pair of twin primes, establish that $\sigma(n + 2) = \sigma(n) + 2$; this also holds for $n = 434$ and 8575.

16. (a) For any integer $n > 1$, prove that there exist integers n_1 and n_2 for which $\tau(n_1) + \tau(n_2) = n$.
(b) Prove that the Goldbach conjecture implies that for each even integer $2n$ there exist integers n_1 and n_2 with $\sigma(n_1) + \sigma(n_2) = 2n$.

17. For a fixed integer k, show that the function f defined by $f(n) = n^k$ is multiplicative.

18. Let f and g be multiplicative functions that are not identically zero and have the property that $f(p^k) = g(p^k)$ for each prime p and $k \geq 1$. Prove that $f = g$.

19. Prove that if f and g are multiplicative functions, then so is their product fg and quotient f/g (whenever the latter function is defined).

20. Let $\omega(n)$ denote the number of distinct prime divisors of $n > 1$, with $\omega(1) = 0$. For instance, $\omega(360) = \omega(2^3 \cdot 3^2 \cdot 5) = 3$.
(a) Show that $2^{\omega(n)}$ is a multiplicative function.
(b) For a positive integer n, establish the formula

$$\tau(n^2) = \sum_{d \mid n} 2^{\omega(d)}$$

21. For any positive integer n, prove that $\sum_{d \mid n} \tau(d)^3 = (\sum_{d \mid n} \tau(d))^2$.
[*Hint:* Both sides of the equation in question are multiplicative functions of n, so that it suffices to consider the case $n = p^k$, where p is a prime.]

22. Given $n \geq 1$, let $\sigma_s(n)$ denote the sum of the sth powers of the positive divisors of n; that is,

$$\sigma_s(n) = \sum_{d \mid n} d^s$$

Verify the following:
(a) $\sigma_0 = \tau$ and $\sigma_1 = \sigma$.
(b) σ_s is a multiplicative function.
[*Hint:* The function f, defined by $f(n) = n^s$, is multiplicative.]
(c) If $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ is the prime factorization of n, then

$$\sigma_s(n) = \left(\frac{p_1^{s(k_1+1)} - 1}{p_1^s - 1}\right)\left(\frac{p_2^{s(k_2+1)} - 1}{p_2^s - 1}\right) \cdots \left(\frac{p_r^{s(k_r+1)} - 1}{p_r^s - 1}\right)$$

23. For any positive integer n, show the following:

(a) $\sum_{d\,|\,n} \sigma(d) = \sum_{d\,|\,n} (n/d)\tau(d)$.

(b) $\sum_{d\,|\,n} (n/d)\sigma(d) = \sum_{d\,|\,n} d\tau(d)$.

[*Hint:* Because the functions

$$F(n) = \sum_{d\,|\,n} \sigma(d) \qquad \text{and} \qquad G(n) = \sum_{d\,|\,n} \frac{n}{d}\tau(d)$$

are both multiplicative, it suffices to prove that $F(p^k) = G(p^k)$ for any prime p.]

6.2 THE MÖBIUS INVERSION FORMULA

We introduce another naturally defined function on the positive integers, the Möbius μ-function.

Definition 6.3. For a positive integer n, define μ by the rules

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } p^2 \mid n \text{ for some prime } p \\ (-1)^r & \text{if } n = p_1 p_2 \cdots p_r, \text{ where } p_i \text{ are distinct primes} \end{cases}$$

Put somewhat differently, Definition 6.3 states that $\mu(n) = 0$ if n is not a square-free integer, whereas $\mu(n) = (-1)^r$ if n is square-free with r prime factors. For example: $\mu(30) = \mu(2 \cdot 3 \cdot 5) = (-1)^3 = -1$. The first few values of μ are

$$\mu(1) = 1 \quad \mu(2) = -1 \quad \mu(3) = -1 \quad \mu(4) = 0 \quad \mu(5) = -1 \quad \mu(6) = 1, \ldots$$

If p is a prime number, it is clear that $\mu(p) = -1$; in addition, $\mu(p^k) = 0$ for $k \geq 2$.

As the reader may have guessed already, the Möbius μ-function is multiplicative. This is the content of Theorem 6.5.

Theorem 6.5. The function μ is a multiplicative function.

Proof. We want to show that $\mu(mn) = \mu(m)\mu(n)$, whenever m and n are relatively prime. If either $p^2 \mid m$ or $p^2 \mid n$, p a prime, then $p^2 \mid mn$; hence, $\mu(mn) = 0 = \mu(m)\mu(n)$, and the formula holds trivially. We therefore may assume that both m and n are square-free integers. Say, $m = p_1 p_2 \cdots p_r$, $n = q_1 q_2 \cdots q_s$, with all the primes p_i and q_j being distinct. Then

$$\begin{aligned} \mu(mn) = \mu(p_1 \cdots p_r q_1 \cdots q_s) &= (-1)^{r+s} \\ &= (-1)^r(-1)^s = \mu(m)\mu(n) \end{aligned}$$

which completes the proof.

Let us see what happens if $\mu(d)$ is evaluated for all the positive divisors d of an integer n and the results are added. In the case where $n = 1$, the answer is easy; here,

$$\sum_{d\,|\,1} \mu(d) = \mu(1) = 1$$

Suppose that $n > 1$ and put

$$F(n) = \sum_{d \mid n} \mu(d)$$

To prepare the ground, we first calculate $F(n)$ for the power of a prime, say, $n = p^k$. The positive divisors of p^k are just the $k + 1$ integers $1, p, p^2, \ldots, p^k$, so that

$$\begin{aligned} F(p^k) &= \sum_{d \mid p^k} \mu(d) = \mu(1) + \mu(p) + \mu(p^2) + \cdots + \mu(p^k) \\ &= \mu(1) + \mu(p) = 1 + (-1) = 0 \end{aligned}$$

Because μ is known to be a multiplicative function, an appeal to Theorem 6.4 is legitimate; this result guarantees that F also is multiplicative. Thus, if the canonical factorization of n is $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$, then $F(n)$ is the product of the values assigned to F for the prime powers in this representation:

$$F(n) = F\left(p_1^{k_1}\right) F\left(p_2^{k_2}\right) \cdots F\left(p_r^{k_r}\right) = 0$$

We record this result as Theorem 6.6.

Theorem 6.6. For each positive integer $n \geq 1$,

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

where d runs through the positive divisors of n.

For an illustration of this last theorem, consider $n = 10$. The positive divisors of 10 are 1, 2, 5, 10 and the desired sum is

$$\begin{aligned} \sum_{d \mid 10} \mu(d) &= \mu(1) + \mu(2) + \mu(5) + \mu(10) \\ &= 1 + (-1) + (-1) + 1 = 0 \end{aligned}$$

The full significance of the Möbius μ-function should become apparent with the next theorem.

Theorem 6.7 Möbius inversion formula. Let F and f be two number-theoretic functions related by the formula

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

Then

$$f(n) = \sum_{d \mid n} \mu(d) F\left(\frac{n}{d}\right) = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) F(d)$$

Proof. The two sums mentioned in the conclusion of the theorem are seen to be the same upon replacing the dummy index d by $d' = n/d$; as d ranges over all positive divisors of n, so does d'.

Carrying out the required computation, we get

$$\begin{aligned}\sum_{d\mid n}\mu(d)F\left(\frac{n}{d}\right) &= \sum_{d\mid n}\left(\mu(d)\sum_{c\mid(n/d)}f(c)\right)\\ &= \sum_{d\mid n}\left(\sum_{c\mid(n/d)}\mu(d)f(c)\right)\end{aligned} \tag{1}$$

It is easily verified that $d \mid n$ and $c \mid (n/d)$ if and only if $c \mid n$ and $d \mid (n/c)$. Because of this, the last expression in Eq. (1) becomes

$$\begin{aligned}\sum_{d\mid n}\left(\sum_{c\mid(n/d)}\mu(d)f(c)\right) &= \sum_{c\mid n}\left(\sum_{d\mid(n/c)}f(c)\mu(d)\right)\\ &= \sum_{c\mid n}\left(f(c)\sum_{d\mid(n/c)}\mu(d)\right)\end{aligned} \tag{2}$$

In compliance with Theorem 6.6, the sum $\sum_{d\mid(n/c)}\mu(d)$ must vanish except when $n/c = 1$ (that is, when $n = c$), in which case it is equal to 1; the upshot is that the right-hand side of Eq. (2) simplifies to

$$\begin{aligned}\sum_{c\mid n}\left(f(c)\sum_{d\mid(n/c)}\mu(d)\right) &= \sum_{c=n}f(c)\cdot 1\\ &= f(n)\end{aligned}$$

giving us the stated result.

Let us use $n = 10$ again to illustrate how the double sum in Eq. (2) is turned around. In this instance, we find that

$$\begin{aligned}\sum_{d\mid 10}\left(\sum_{c\mid(10/d)}\mu(d)f(c)\right) &= \mu(1)[f(1)+f(2)+f(5)+f(10)]\\ &\quad + \mu(2)[f(1)+f(5)] + \mu(5)[f(1)+f(2)]\\ &\quad + \mu(10)f(1)\\ &= f(1)[\mu(1)+\mu(2)+\mu(5)+\mu(10)]\\ &\quad + f(2)[\mu(1)+\mu(5)] + f(5)[\mu(1)+\mu(2)]\\ &\quad + f(10)\mu(1)\\ &= \sum_{c\mid 10}\left(\sum_{d\mid(10/c)}f(c)\mu(d)\right)\end{aligned}$$

To see how the Möbius inversion formula works in a particular case, we remind the reader that the functions τ and σ may both be described as "sum functions":

$$\tau(n) = \sum_{d\mid n}1 \qquad \text{and} \qquad \sigma(n) = \sum_{d\mid n}d$$

Theorem 6.7 tells us that these formulas may be inverted to give

$$1 = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) \tau(d) \qquad \text{and} \qquad n = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) \sigma(d)$$

which are valid for all $n \geq 1$.

Theorem 6.4 ensures that if f is a multiplicative function, then so is $F(n) = \sum_{d \mid n} f(d)$. Turning the situation around, one might ask whether the multiplicative nature of F forces that of f. Surprisingly enough, this is exactly what happens.

Theorem 6.8. If F is a multiplicative function and

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

then f is also multiplicative.

Proof. Let m and n be relatively prime positive integers. We recall that any divisor d of mn can be uniquely written as $d = d_1 d_2$, where $d_1 \mid m$, $d_2 \mid n$, and $\gcd(d_1, d_2) = 1$. Thus, using the inversion formula,

$$\begin{aligned} f(mn) &= \sum_{d \mid mn} \mu(d) F\left(\frac{mn}{d}\right) \\ &= \sum_{\substack{d_1 \mid m \\ d_2 \mid n}} \mu(d_1 d_2) F\left(\frac{mn}{d_1 d_2}\right) \\ &= \sum_{\substack{d_1 \mid m \\ d_2 \mid n}} \mu(d_1) \mu(d_2) F\left(\frac{m}{d_1}\right) F\left(\frac{n}{d_2}\right) \\ &= \sum_{d_1 \mid m} \mu(d_1) F\left(\frac{m}{d_1}\right) \sum_{d_2 \mid n} \mu(d_2) F\left(\frac{n}{d_2}\right) \\ &= f(m) f(n) \end{aligned}$$

which is the assertion of the theorem. Needless to say, the multiplicative character of μ and of F is crucial to the previous calculation.

For $n \geq 1$, we define the sum

$$M(n) = \sum_{k=1}^{n} \mu(k)$$

Then $M(n)$ is the difference between the number of square-free positive integers $k \leq n$ with an even number of prime factors and those with an odd number of prime factors. For example, $M(9) = 2 - 4 = -2$. In 1897, Franz Mertens (1840–1927) published a paper with a 50-page table of values of $M(n)$ for $n = 1, 2, \ldots, 10000$. On the basis of the tabular evidence, Mertens concluded that the inequality

$$|M(n)| < \sqrt{n} \qquad n > 1$$

is "very probable." (In the previous example, $|M(9)| = 2 < \sqrt{9}$.) This conclusion later became known as the Mertens conjecture. A computer search carried out in

1963 verified the conjecture for all n up to 10 billion. But in 1984, Andrew Odlyzko and Herman te Riele showed that the Mertens conjecture is false. Their proof, which involved the use of a computer, was indirect and produced no specific value of n for which $|M(n)| \geq \sqrt{n}$; all it demonstrated was that such a number n must exist somewhere. Subsequently, it has been shown that there is a counterexample to the Mertens conjecture for at least one $n \leq (3.21)10^{64}$.

PROBLEMS 6.2

1. (a) For each positive integer n, show that

$$\mu(n)\mu(n+1)\mu(n+2)\mu(n+3) = 0$$

(b) For any integer $n \geq 3$, show that $\sum_{k=1}^{n} \mu(k!) = 1$.

2. The *Mangoldt function* Λ is defined by

$$\Lambda(n) = \begin{cases} \log p & \text{if } n = p^k, \text{ where } p \text{ is a prime and } k \geq 1 \\ 0 & \text{otherwise} \end{cases}$$

Prove that $\Lambda(n) = \sum_{d \mid n} \mu(n/d) \log d = -\sum_{d \mid n} \mu(d) \log d$.
[*Hint:* First show that $\sum_{d \mid n} \Lambda(d) = \log n$ and then apply the Möbius inversion formula.]

3. Let $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ be the prime factorization of the integer $n > 1$. If f is a multiplicative function that is not identically zero, prove that

$$\sum_{d \mid n} \mu(d) f(d) = (1 - f(p_1))(1 - f(p_2)) \cdots (1 - f(p_r))$$

[*Hint:* By Theorem 6.4, the function F defined by $F(n) = \sum_{d \mid n} \mu(d) f(d)$ is multiplicative; hence, $F(n)$ is the product of the values $F(p_i^{k_i})$.]

4. If the integer $n > 1$ has the prime factorization $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$, use Problem 3 to establish the following:
(a) $\sum_{d \mid n} \mu(d)\tau(d) = (-1)^r$.
(b) $\sum_{d \mid n} \mu(d)\sigma(d) = (-1)^r p_1 p_2 \cdots p_r$.
(c) $\sum_{d \mid n} \mu(d)/d = (1 - 1/p_1)(1 - 1/p_2) \cdots (1 - 1/p_r)$.
(d) $\sum_{d \mid n} d\mu(d) = (1 - p_1)(1 - p_2) \cdots (1 - p_r)$.

5. Let $S(n)$ denote the number of square-free divisors of n. Establish that

$$S(n) = \sum_{d \mid n} |\mu(d)| = 2^{\omega(n)}$$

where $\omega(n)$ is the number of distinct prime divisors of n.
[*Hint:* S is a multiplicative function.]

6. Find formulas for $\sum_{d \mid n} \mu^2(d)/\tau(d)$ and $\sum_{d \mid n} \mu^2(d)/\sigma(d)$ in terms of the prime factorization of n.

7. The *Liouville λ-function* is defined by $\lambda(1) = 1$ and $\lambda(n) = (-1)^{k_1 + k_2 + \cdots + k_r}$, if the prime factorization of $n > 1$ is $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$. For instance,

$$\lambda(360) = \lambda(2^3 \cdot 3^2 \cdot 5) = (-1)^{3+2+1} = (-1)^6 = 1$$

(a) Prove that λ is a multiplicative function.

(b) Given a positive integer n, verify that

$$\sum_{d \mid n} \lambda(d) = \begin{cases} 1 & \text{if } n = m^2 \text{ for some integer } m \\ 0 & \text{otherwise} \end{cases}$$

8. For an integer $n \geq 1$, verify the formulas below:
(a) $\sum_{d \mid n} \mu(d)\lambda(d) = 2^{\omega(n)}$.
(b) $\sum_{d \mid n} \lambda(n/d)2^{\omega(d)} = 1$.

6.3 THE GREATEST INTEGER FUNCTION

The greatest integer or "bracket" function [ ] is especially suitable for treating divisibility problems. Although not strictly a number-theoretic function, its study has a natural place in this chapter.

Definition 6.4. For an arbitrary real number x, we denote by $[x]$ the largest integer less than or equal to x; that is, $[x]$ is the unique integer satisfying $x - 1 < [x] \leq x$.

By way of illustration, [ ] assumes the particular values

$$[-3/2] = -2 \quad [\sqrt{2}] = 1 \quad [1/3] = 0 \quad [\pi] = 3 \quad [-\pi] = -4$$

The important observation to be made here is that the equality $[x] = x$ holds if and only if x is an integer. Definition 6.4 also makes plain that any real number x can be written as

$$x = [x] + \theta$$

for a suitable choice of θ, with $0 \leq \theta < 1$.

We now plan to investigate the question of how many times a particular prime p appears in $n!$. For instance, if $p = 3$ and $n = 9$, then

$$\begin{aligned} 9! &= 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \\ &= 2^7 \cdot 3^4 \cdot 5 \cdot 7 \end{aligned}$$

so that the exact power of 3 that divides $9!$ is 4. It is desirable to have a formula that will give this count, without the necessity of always writing $n!$ in canonical form. This is accomplished by Theorem 6.9.

Theorem 6.9. If n is a positive integer and p a prime, then the exponent of the highest power of p that divides $n!$ is

$$\sum_{k=1}^{\infty} \left[\frac{n}{p^k} \right]$$

where the series is finite, because $[n/p^k] = 0$ for $p^k > n$.

Proof. Among the first n positive integers, those divisible by p are $p, 2p, \ldots, tp$, where t is the largest integer such that $tp \leq n$; in other words, t is the largest integer less than or equal to n/p (which is to say $t = [n/p]$). Thus, there are exactly $[n/p]$ multiples of p occurring in the product that defines $n!$, namely,

$$p, 2p, \ldots, \left[\frac{n}{p}\right]p \tag{1}$$

The exponent of p in the prime factorization of $n!$ is obtained by adding to the number of integers in Eq. (1), the number of integers among 1, 2, ..., n divisible by p^2, and then the number divisible by p^3, and so on. Reasoning as in the first paragraph, the integers between 1 and n that are divisible by p^2 are

$$p^2, 2p^2, \ldots, \left[\frac{n}{p^2}\right]p^2 \tag{2}$$

which are $[n/p^2]$ in number. Of these, $[n/p^3]$ are again divisible by p:

$$p^3, 2p^3, \ldots, \left[\frac{n}{p^3}\right]p^3 \tag{3}$$

After a finite number of repetitions of this process, we are led to conclude that the total number of times p divides $n!$ is

$$\sum_{k=1}^{\infty}\left[\frac{n}{p^k}\right]$$

This result can be cast as the following equation, which usually appears under the name of the Legendre formula:

$$n! = \prod_{p \leq n} p^{\sum_{k=1}^{\infty}[n/p^k]}$$

Example 6.2. We would like to find the number of zeros with which the decimal representation of 50! terminates. In determining the number of times 10 enters into the product 50!, it is enough to find the exponents of 2 and 5 in the prime factorization of 50!, and then to select the smaller figure.

By direct calculation we see that

$$\begin{aligned}[50/2] + [50/2^2] + [50/2^3] + [50/2^4] + [50/2^5]\\ = 25 + 12 + 6 + 3 + 1\\ = 47\end{aligned}$$

Theorem 6.9 tells us that 2^{47} divides 50!, but 2^{48} does not. Similarly,

$$[50/5] + [50/5^2] = 10 + 2 = 12$$

and so the highest power of 5 dividing 50! is 12. This means that 50! ends with 12 zeros.

We cannot resist using Theorem 6.9 to prove the following fact.

Theorem 6.10. If n and r are positive integers with $1 \leq r < n$, then the binomial coefficient

$$\binom{n}{r} = \frac{n!}{r!(n-r)!}$$

is also an integer.

Proof. The argument rests on the observation that if a and b are arbitrary real numbers, then $[a+b] \geq [a] + [b]$. In particular, for each prime factor p of $r!(n-r)!$,

$$\left[\frac{n}{p^k}\right] \geq \left[\frac{r}{p^k}\right] + \left[\frac{(n-r)}{p^k}\right] \qquad k = 1, 2, \ldots$$

Adding these inequalities, we obtain

$$\sum_{k \geq 1} \left[\frac{n}{p^k}\right] \geq \sum_{k \geq 1} \left[\frac{r}{p^k}\right] + \sum_{k \geq 1} \left[\frac{(n-r)}{p^k}\right] \tag{1}$$

The left-hand side of Eq. (1) gives the exponent of the highest power of the prime p that divides $n!$, whereas the right-hand side equals the highest power of this prime contained in $r!(n-r)!$. Hence, p appears in the numerator of $n!/r!(n-r)!$ at least as many times as it occurs in the denominator. Because this holds true for every prime divisor of the denominator, $r!(n-r)!$ must divide $n!$, making $n!/r!(n-r)!$ an integer.

Corollary. For a positive integer r, the product of any r consecutive positive integers is divisible by $r!$.

Proof. The product of r consecutive positive integers, the largest of which is n, is

$$n(n-1)(n-2)\cdots(n-r+1)$$

Now we have

$$n(n-1)\cdots(n-r+1) = \left(\frac{n!}{r!(n-r)!}\right)r!$$

Because $n!/r!(n-r)!$ is an integer by the theorem, it follows that $r!$ must divide the product $n(n-1)\cdots(n-r+1)$, as asserted.

We pick up a few loose threads. Having introduced the greatest integer function, let us see what it has to do with the study of number-theoretic functions. Their relationship is brought out by Theorem 6.11.

Theorem 6.11. Let f and F be number-theoretic functions such that

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

Then, for any positive integer N,

$$\sum_{n=1}^{N} F(n) = \sum_{k=1}^{N} f(k) \left[\frac{N}{k}\right]$$

Proof. We begin by noting that

$$\sum_{n=1}^{N} F(n) = \sum_{n=1}^{N} \sum_{d \mid n} f(d) \tag{1}$$

The strategy is to collect terms with equal values of $f(d)$ in this double sum. For a fixed positive integer $k \leq N$, the term $f(k)$ appears in $\sum_{d \mid n} f(d)$ if and only if k is a divisor of n. (Because each integer has itself as a divisor, the right-hand side of Eq. (1) includes $f(k)$, at least once.) Now, to calculate the number of sums $\sum_{d \mid n} f(d)$ in which $f(k)$ occurs as a term, it is sufficient to find the number of integers among 1, 2, . . . , N, which are divisible by k. There are exactly $[N/k]$ of them:

$$k, 2k, 3k, \ldots, \left[\frac{N}{k}\right] k$$

Thus, for each k such that $1 \leq k \leq N$, $f(k)$ is a term of the sum $\sum_{d \mid n} f(d)$ for $[N/k]$ different positive integers less than or equal to N. Knowing this, we may rewrite the double sum in Eq. (1) as

$$\sum_{n=1}^{N} \sum_{d \mid n} f(d) = \sum_{k=1}^{N} f(k) \left[\frac{N}{k}\right]$$

and our task is complete.

As an immediate application of Theorem 6.11, we deduce Corollary 1.

Corollary 1. If N is a positive integer, then

$$\sum_{n=1}^{N} \tau(n) = \sum_{n=1}^{N} \left[\frac{N}{n}\right]$$

Proof. Noting that $\tau(n) = \sum_{d \mid n} 1$, we may write τ for F and take f to be the constant function $f(n) = 1$ for all n.

In the same way, the relation $\sigma(n) = \sum_{d \mid n} d$ yields Corollary 2.

Corollary 2. If N is a positive integer, then

$$\sum_{n=1}^{N} \sigma(n) = \sum_{n=1}^{N} n \left[\frac{N}{n}\right]$$

These last two corollaries, can perhaps, be clarified with an example.

Example 6.3. Consider the case $N = 6$. The definition of τ tells us that

$$\sum_{n=1}^{6} \tau(n) = 14$$

From Corollary 1,

$$\begin{aligned}\sum_{n=1}^{6}\left[\frac{6}{n}\right] &= [6]+[3]+[2]+[3/2]+[6/5]+[1]\\ &= 6+3+2+1+1+1\\ &= 14\end{aligned}$$

as it should. In the present case, we also have

$$\sum_{n=1}^{6}\sigma(n) = 33$$

and a simple calculation leads to

$$\begin{aligned}\sum_{n=1}^{6} n\left[\frac{6}{n}\right] &= 1[6]+2[3]+3[2]+4[3/2]+5[6/5]+6[1]\\ &= 1\cdot 6+2\cdot 3+3\cdot 2+4\cdot 1+5\cdot 1+6\cdot 1\\ &= 33\end{aligned}$$

PROBLEMS 6.3

1. Given integers a and $b > 0$, show that there exists a unique integer r with $0 \leq r < b$ satisfying $a = [a/b]b + r$.

2. Let x and y be real numbers. Prove that the greatest integer function satisfies the following properties:

(a) $[x+n] = [x] + n$ for any integer n.

(b) $[x] + [-x] = 0$ or -1, according as x is an integer or not.
[*Hint:* Write $x = [x] + \theta$, with $0 \leq \theta < 1$, so that $-x = -[x] - 1 + (1 - \theta)$.]

(c) $[x] + [y] \leq [x+y]$ and, when x and y are positive, $[x][y] \leq [xy]$.

(d) $[x/n] = [[x]/n]$ for any positive integer n.
[*Hint:* Let $x/n = [x/n] + \theta$, where $0 \leq \theta < 1$; then $[x] = n[x/n] + [n\theta]$.]

(e) $[nm/k] \geq n[m/k]$ for positive integers, n, m, k.

(f) $[x] + [y] + [x+y] \leq [2x] + [2y]$.
[*Hint:* Let $x = [x] + \theta, 0 \leq \theta < 1$, and $y = [y] + \theta', 0 \leq \theta' < 1$. Consider cases in which neither, one, or both of θ and θ' are greater than or equal to $\frac{1}{2}$.]

3. Find the highest power of 5 dividing 1000! and the highest power of 7 dividing 2000!.

4. For an integer $n \geq 0$, show that $[n/2] - [-n/2] = n$.

5. (a) Verify that 1000! terminates in 249 zeros.

(b) For what values of n does $n!$ terminate in 37 zeros?

6. If $n \geq 1$ and p is a prime, prove that

(a) $(2n)!/(n!)^2$ is an even integer.
[*Hint:* Use Theorem 6.10.]

(b) The exponent of the highest power of p that divides $(2n)!/(n!)^2$ is

$$\sum_{k=1}^{\infty}\left(\left[\frac{2n}{p^k}\right] - 2\left[\frac{n}{p^k}\right]\right)$$

(c) In the prime factorization of $(2n)!/(n!)^2$ the exponent of any prime p such that $n < p < 2n$ is equal to 1.

7. Let the positive integer n be written in terms of powers of the prime p so that we have $n = a_k p^k + \cdots + a_2 p^2 + a_1 p + a_0$, where $0 \leq a_i < p$. Show that the exponent of the highest power of p appearing in the prime factorization of $n!$ is

$$\frac{n - (a_k + \cdots + a_2 + a_1 + a_0)}{p - 1}$$

8. (a) Using Problem 7, show that the exponent of highest power of p dividing $(p^k - 1)!$ is $[p^k - (p-1)k - 1]/(p-1)$.
[*Hint:* Recall the identity $p^k - 1 = (p-1)(p^{k-1} + \cdots + p^2 + p + 1)$.]

(b) Determine the highest power of 3 dividing 80! and the highest power of 7 dividing 2400!.
[*Hint:* $2400 = 7^4 - 1$.]

9. Find an integer $n \geq 1$ such that the highest power of 5 contained in $n!$ is 100.
[*Hint:* Because the sum of coefficients of the powers of 5 needed to express n in the base 5 is at least 1, begin by considering the equation $(n-1)/4 = 100$.]

10. Given a positive integer N, show the following:

(a) $\sum_{n=1}^{N} \mu(n)[N/n] = 1$.

(b) $|\sum_{n=1}^{N} \mu(n)/n| \leq 1$.

11. Illustrate Problem 10 in the case where $N = 6$.

12. Verify that the formula

$$\sum_{n=1}^{N} \lambda(n)\left[\frac{N}{n}\right] = [\sqrt{N}]$$

holds for any positive integer N.
[*Hint:* Apply Theorem 6.11 to the multiplicative function $F(n) = \sum_{d \mid n} \lambda(d)$, noting that there are $[\sqrt{n}]$ perfect squares not exceeding n.]

13. If N is a positive integer, establish the following:

(a) $N = \sum_{n=1}^{2N} \tau(n) - \sum_{n=1}^{N} [2N/n]$.

(b) $\tau(N) = \sum_{n=1}^{N} ([N/n] - [(N-1)/n])$.

6.4 AN APPLICATION TO THE CALENDAR

Our familiar calendar, the Gregorian calendar, goes back as far as the second half of the 16th century. The earlier Julian calendar, introduced by Julius Caesar, was based on a year of $365\frac{1}{4}$ days, with a leap year every fourth year. This was not a precise enough measure, because the length of a solar year—the time required for the earth to complete an orbit about the sun—is apparently 365.2422 days. The small error meant that the Julian calendar receded a day from its astronomical norm every 128 years.

By the 16th century, the accumulating inaccuracy caused the vernal equinox (the first day of Spring) to fall on March 11 instead of its proper day, March 21. The calendar's inaccuracy naturally persisted throughout the year, but at this season it meant that the Easter festival was celebrated at the wrong astronomical time. Pope Gregory XIII rectified the discrepancy in a new calendar, imposed on the predominantly Catholic countries of Europe. He decreed that 10 days were to be omitted from the year 1582, by having October 15 of that year immediately follow

October 4. At the same time, the Jesuit mathematician Christopher Clavius amended the scheme for leap years: these would be years divisible by 4, except for those marking centuries. Century years would be leap years only if they were divisible by 400. (For example, the century years 1600 and 2000 are leap years, but 1700, 1800, 1900, and 2100 are not.)

Because the edict came from Rome, Protestant England and her possessions—including the American colonies—resisted. They did not officially adopt the Gregorian calendar until 1752. By then it was necessary to drop 11 days in September from the Old Style, or Julian, calendar. So it happened that George Washington, who was born on February 11, 1732, celebrated his birthday as an adult on February 22. Other nations gradually adopted the reformed calendar: Russia in 1918, and China as late as 1949.

Our goal in the present section is to determine the day of the week for a given date after the year 1600 in the Gregorian calendar. Because the leap year day is added at the end of February, let us adopt the convenient fiction that each year ends at the end of February. According to this plan, in the Gregorian year Y March and April are counted as the first and second months. January and February of the Gregorian year $Y + 1$ are, for convenience, counted as the eleventh and twelfth months of the year Y.

Another convenience is to designate the days of the week, Sunday through Saturday, by the numbers $0, 1, \ldots, 6$:

Sun	Mon	Tue	Wed	Thu	Fri	Sat
0	1	2	3	4	5	6

The number of days in a common year is $365 \equiv 1 \pmod 7$, whereas in leap years there are $366 \equiv 2 \pmod 7$ days. Because February 28 is the 365th day of the year, and $365 \equiv 1 \pmod 7$, February 28 always falls on the same weekday as the previous March 1. Thus if a particular March 1 immediately follows February 28, its weekday number will be one more, modulo 7, than the weekday number of the previous March 1. But if it follows a leap year day, February 29, its weekday number will be increased by two.

For instance, if D_{1600} is the weekday number for March 1, 1600, then March 1 in the years 1601, 1602, and 1603 has numbers congruent modulo 7 to $D_{1600} + 1$, $D_{1600} + 2$, and $D_{1600} + 3$, respectively; but the number corresponding to March 1, 1604 is $D_{1600} + 5 \pmod 7$.

We can summarize this: the weekday number D_Y for March 1 of any year $Y > 1600$ will satisfy the congruence

$$D_Y \equiv D_{1600} + (Y - 1600) + L \pmod 7 \qquad (1)$$

where L is the number of leap year days between March 1, 1600, and March 1 of the year Y.

Let us first find L, the number of leap year days between 1600 and the year Y. To do this, we count the number of these years that are divisible by 4, deduct the number of century years, and then add back the number of century years divisible by 400. According to Problem 2(a) of Section 6.3, $[x - a] = [x] - a$ whenever a is an integer. Hence the number of years n in the interval $1600 < n \leq Y$ that are divisible by 4 is given by

$$\left[\frac{Y-1600}{4}\right] = \left[\frac{Y}{4} - 400\right] = \left[\frac{Y}{4}\right] - 400$$

Likewise, the number of elapsed century years is

$$\left[\frac{Y-1600}{100}\right] = \left[\frac{Y}{100} - 16\right] = \left[\frac{Y}{100}\right] - 16$$

whereas among those there are

$$\left[\frac{Y-1600}{400}\right] = \left[\frac{Y}{400} - 4\right] = \left[\frac{Y}{400}\right] - 4$$

century years that are divisible by 400. Taken together, these statements yield

$$\begin{aligned} L &= \left(\left[\frac{Y}{4}\right] - 400\right) - \left(\left[\frac{Y}{100}\right] - 16\right) + \left(\left[\frac{Y}{400}\right] - 4\right) \\ &= \left[\frac{Y}{4}\right] - \left[\frac{Y}{100}\right] + \left[\frac{Y}{400}\right] - 388 \end{aligned}$$

Let us obtain, for a typical example, the number of leap years between 1600 and 1995. We compute:

$$\begin{aligned} L &= [1995/4] - [1995/100] + [1995/400] - 388 \\ &= 498 - 19 + 4 - 388 = 95 \end{aligned}$$

Together with congruence (1), this allows us to find a value for D_{1600}. Days and dates of recent years can still be recalled; we can easily look up the weekday (Wednesday) for March 1, 1995. That is, $D_{1995} = 3$. Then from (1),

$$3 \equiv D_{1600} + (1995 - 1600) + 95 \equiv D_{1600} \pmod{7}$$

and so March 1, 1600, also occurred on a Wednesday. The congruence giving the day of the week for March 1 in any year Y may now be reformulated as

$$D_Y \equiv 3 + (Y - 1600) + L \pmod{7} \qquad (2)$$

An alternate formula for L comes from writing the year Y as

$$Y = 100c + y \qquad 0 \leq y < 100$$

where c denotes the number of centuries and y the year number within the century. Upon substitution, the previous expression for L becomes

$$\begin{aligned} L &= \left[25c + \frac{y}{4}\right] - \left[c + \frac{y}{100}\right] + \left[\frac{c}{4} + \frac{y}{400}\right] - 388 \\ &= 24c + \left[\frac{y}{4}\right] + \left[\frac{c}{4}\right] - 388 \end{aligned}$$

(Notice that $[y/100] = 0$ and $y/400 < \frac{1}{4}$.) Then the congruence for D_Y appears as

$$D_Y \equiv 3 + (100c + y - 1600) + 24c + \left[\frac{y}{4}\right] + \left[\frac{c}{4}\right] - 388 \pmod 7$$

which reduces to

$$D_Y \equiv 3 - 2c + y + \left[\frac{c}{4}\right] + \left[\frac{y}{4}\right] \pmod 7 \qquad (3)$$

Example 6.4 We can use the latest congruence to calculate the day of the week on which March 1, 1990, fell. For this year, $c = 19$ and $y = 90$ so that (3) gives

$$\begin{aligned} D_{1990} &\equiv 3 - 38 + 90 + [19/4] + [90/4] \\ &\equiv 55 + 4 + 22 \equiv 4 \pmod 7 \end{aligned}$$

March 1 was on a Thursday in 1990.

We move on to determining the day of the week on which the first of each month of the year would fall. Because $30 \equiv 2 \pmod 7$, a 30-day month advances by two the weekday on which the next month begins. A 31-day month increases it by 3. So, for example, the number of June 1 will always be $3 + 2 + 3 \equiv 1 \pmod 7$ greater than that of the preceding March 1 because March, April, and May are months of 31, 30, and 31 days, respectively. The table below gives the value that must be added to the day-number of March 1 to arrive at the number of the first day of each month in any year Y.

March	0	September	2
April	3	October	4
May	5	November	0
June	1	December	2
July	3	January	5
August	6	February	1

For $m = 1, 2, \ldots, 12$, the expression

$$[(2.6)m - 0.2] - 2 \pmod 7$$

produces the same monthly increases as indicated by the table. Thus the number of the first day of the mth month of the year Y is given by

$$D_Y + [(2.6)m - 0.2] - 2 \pmod 7$$

Taking December 1, 1990, as an example, we have

$$D_{1990} + [(2.6)10 - 0.2] - 2 \equiv 4 + 25 - 2 \equiv 6 \pmod 7$$

that is, the first of December in 1990 fell on a Saturday.

Finally, the number w of day d, month m, year $Y = 100c + y$ is determined from congruence

$$w \equiv (d - 1) + D_Y + [(2.6)m - 0.2] - 2 \pmod 7$$

We can use Eq. (3) to recast this:

$$w \equiv d + [(2.6)m - 0.2] - 2c + y + \left[\frac{c}{4}\right] + \left[\frac{y}{4}\right] \pmod 7 \qquad (4)$$

We summarize the results of this section in the following theorem.

Theorem 6.12. The date with month m, day d, year $Y = 100c + y$ where $c \geq 16$ and $0 \leq y < 100$, has weekday number

$$w \equiv d + [(2.6)m - 0.2] - 2c + y + \left[\frac{c}{4}\right] + \left[\frac{y}{4}\right] \pmod 7$$

provided that March is taken as the first month of the year and January and February are assumed to be the eleventh and twelfth months of the previous year.

Let us give an example using the calendar formula.

Example 6.5. On what day of the week will January 14, 2020, occur?

In our convention, January of 2020 is treated as the eleventh month of the year 2019. The weekday number corresponding to its fourteenth day is computed as

$$\begin{aligned} w &\equiv 14 + [(2.6)11 - 0.2] - 40 + 19 + [20/4] + [19/4] \\ &\equiv 14 + 28 - 40 + 19 + 5 + 4 \equiv 2 \pmod 7 \end{aligned}$$

We conclude that January 14, 2020, will take place on a Tuesday.

An interesting question to ask about the calendar is whether every year contains a Friday the thirteenth. Phrased differently, does the congruence

$$5 \equiv 13 + [(2.6)m - 0.2] - 2c + y + \left[\frac{c}{4}\right] + \left[\frac{y}{4}\right] \pmod 7$$

hold for each year $Y = 100c + y$? Notice that the expression $[(2.6)m - 0.2]$ assumes, modulo 7, each of the values $0, 1, \ldots, 6$ as m varies from 3 to 9—values corresponding to the months May through November. Hence there will always be a month for which the indicated congruence is satisfied: in fact, there will always be a Friday the thirteenth during these seven months of any year. For the year 2022, as an example, the Friday the thirteenth congruence reduces to

$$0 \equiv [(2.6)m - 0.2] \pmod 7$$

which holds when $m = 3$. In 2022, there is a Friday the thirteenth in May.

PROBLEMS 6.4

1. Find the number n of leap years such that $1600 < n < Y$, when
(a) $Y = 1825$.
(b) $Y = 1950$.
(c) $Y = 2075$.

2. Determine the day of the week on which you were born.

3. Find the day of the week for the important dates below:
(a) November 19, 1863 (Lincoln's Gettysburg Address).
(b) April 18, 1906 (San Francisco earthquake).
(c) November 11, 1918 (Great War ends).
(d) October 24, 1929 (Black Day on the New York stock market).

(e) June 6, 1944 (Allies land in Normandy).

(f) February 15, 1898 (Battleship *Maine* blown up).

4. Show that days with the identical calendar date in the years 1999 and 1915 fell on the same day of the week.

[*Hint:* If W_1 and W_2 are the weekday numbers for the same date in 1999 and 1915, respectively, verify that $W_1 - W_2 \equiv 0 \pmod 7$.]

5. For the year 2010, determine the following:

(a) the calendar dates on which Mondays will occur in March.

(b) the months in which the thirteenth will fall on a Friday.

6. Find the years in the decade 2000 to 2009 when November 29 is on a Sunday.