Chapter 27

Functions of Number Theory

T. M. Apostol[1]

[1]California Institute of Technology, Pasadena, California.

Acknowledgments: The author thanks Basil Gordon for comments on an earlier draft, and David Bressoud for providing §§27.12, 27.18, 27.19, and 27.22.

Notation

27.1 Special Notation

(For other notation see pp. xiv and 873.)

d, k, m, n	positive integers (unless otherwise indicated).
$d \mid n$	d divides n.
(m, n)	greatest common divisor of m, n. If $(m, n) = 1$, m and n are called relatively prime, or coprime.
$(d_1, \ldots, d_n)$	greatest common divisor of $d_1, \ldots, d_n$.
$\sum_{d\mid n}$, $\prod_{d\mid n}$	sum, product taken over divisors of n.
$\sum_{(m,n)=1}$	sum taken over m, $1 \le m \le n$ and m relatively prime to n.
$p, p_1, p_2, \ldots$	prime numbers (or primes): integers (> 1) with only two positive integer divisors, 1 and the number itself.
$\sum_p$, $\prod_p$	sum, product extended over all primes.
x, y	real numbers.
$\sum_{n\le x}$	$\sum_{n=1}^{\lfloor x\rfloor}$.
$\log x$	natural logarithm of x, written as $\ln x$ in other chapters.
$\zeta(s)$	Riemann zeta function; see §25.2(i).
$(n\|P)$	Jacobi symbol; see §27.9.
$(n\|p)$	Legendre symbol; see §27.9.

Multiplicative Number Theory

27.2 Functions

27.2(i) Definitions

Functions in this section derive their properties from the *fundamental theorem of arithmetic*, which states that every integer $n > 1$ can be represented uniquely as a product of prime powers,

$$n = \prod_{r=1}^{\nu(n)} p_r^{a_r}, \tag{27.2.1}$$

where $p_1, p_2, \ldots, p_{\nu(n)}$ are the distinct prime factors of n, each exponent a_r is positive, and $\nu(n)$ is the number of distinct primes dividing n. ($\nu(1)$ is defined to be 0.) Euclid's Elements (Euclid (1908, Book IX, Proposition 20)) gives an elegant proof that there are infinitely many primes. Tables of primes (§27.21) reveal great irregularity in their distribution. They tend to thin out among the large integers, but this thinning out is not completely regular. There is great interest in the function $\pi(x)$ that counts the number of primes not exceeding x. It can be expressed as a sum over all primes $p \le x$:

$$\pi(x) = \sum_{p\le x} 1. \tag{27.2.2}$$

Gauss and Legendre conjectured that $\pi(x)$ is asymptotic to $x/\log x$ as $x \to \infty$:

$$\pi(x) \sim \frac{x}{\log x}. \tag{27.2.3}$$

(See Gauss (1863, Band II, pp. 437–477) and Legendre (1808, p. 394).)

This result, first proved in Hadamard (1896) and de la Vallée Poussin (1896a,b), is known as the *prime number theorem*. An equivalent form states that the nth prime p_n (when the primes are listed in increasing order) is asymptotic to $n \log n$ as $n \to \infty$:

$$p_n \sim n \log n. \tag{27.2.4}$$

(See also §27.12.) Other examples of number-theoretic functions treated in this chapter are as follows.

$$\left\lfloor \frac{1}{n} \right\rfloor = \begin{cases} 1, & n = 1, \\ 0, & n > 1. \end{cases} \tag{27.2.5}$$

$$\phi_k(n) = \sum_{(m,n)=1} m^k, \tag{27.2.6}$$

the sum of the kth powers of the positive integers $m \le n$ that are relatively prime to n.

$$\phi(n) = \phi_0(n). \tag{27.2.7}$$

This is the number of positive integers $\le n$ that are relatively prime to n; $\phi(n)$ is *Euler's totient*.

If $(a, n) = 1$, then the *Euler–Fermat theorem* states that

$$a^{\phi(n)} \equiv 1 \pmod{n}, \tag{27.2.8}$$

and if $\phi(n)$ is the smallest positive integer f such that $a^f \equiv 1 \pmod{n}$, then a is a *primitive root* mod n. The $\phi(n)$ numbers $a, a^2, \ldots, a^{\phi(n)}$ are relatively prime to n and distinct (mod n). Such a set is a *reduced residue system* modulo n.

$$d(n) = \sum_{d\mid n} 1 \tag{27.2.9}$$

is the number of divisors of n and is the *divisor function*. It is the special case $k = 2$ of the function $d_k(n)$ that counts the number of ways of expressing n as the product of k factors, with the order of factors taken into account.

$$\sigma_\alpha(n) = \sum_{d\mid n} d^\alpha, \tag{27.2.10}$$

is the sum of the αth powers of the divisors of n, where the exponent α can be real or complex. Note that $\sigma_0(n) = d(n)$.

$$J_k(n) = \sum_{((d_1,\ldots,d_k),n)=1} 1, \tag{27.2.11}$$

is the number of k-tuples of integers $\leq n$ whose greatest common divisor is relatively prime to n. This is *Jordan's function*. Note that $J_1(n) = \phi(n)$.

In the following examples, $a_1, \ldots, a_{\nu(n)}$ are the exponents in the factorization of n in (27.2.1).

27.2.12 $$\mu(n) = \begin{cases} 1, & n = 1, \\ (-1)^{\nu(n)}, & a_1 = a_2 = \cdots = a_{\nu(n)} = 1, \\ 0, & \text{otherwise.} \end{cases}$$

This is the *Möbius function*.

27.2.13 $$\lambda(n) = \begin{cases} 1, & n = 1, \\ (-1)^{a_1 + \cdots + a_{\nu(n)}}, & n > 1. \end{cases}$$

This is *Liouville's function*.

27.2.14 $$\Lambda(n) = \log p, \qquad n = p^a,$$

where p^a is a prime power with $a \geq 1$; otherwise $\Lambda(n) = 0$. This is *Mangoldt's function*.

27.2(ii) Tables

Table 27.2.1 lists the first 100 prime numbers p_n. Table 27.2.2 tabulates the Euler totient function $\phi(n)$, the divisor function $d(n)$ $(= \sigma_0(n))$, and the sum of the divisors $\sigma(n)$ $(= \sigma_1(n))$, for $n = 1(1)52$.

Table 27.2.1: Primes.

n	p_n	p_{n+10}	p_{n+20}	p_{n+30}	p_{n+40}	p_{n+50}	p_{n+60}	p_{n+70}	p_{n+80}	p_{n+90}
1	2	31	73	127	179	233	283	353	419	467
2	3	37	79	131	181	239	293	359	421	479
3	5	41	83	137	191	241	307	367	431	487
4	7	43	89	139	193	251	311	373	433	491
5	11	47	97	149	197	257	313	379	439	499
6	13	53	101	151	199	263	317	383	443	503
7	17	59	103	157	211	269	331	389	449	509
8	19	61	107	163	223	271	337	397	457	521
9	23	67	109	167	227	277	347	401	461	523
10	29	71	113	173	229	281	349	409	463	541

Table 27.2.2: Functions related to division.

n	$\phi(n)$	$d(n)$	$\sigma(n)$	n	$\phi(n)$	$d(n)$	$\sigma(n)$	n	$\phi(n)$	$d(n)$	$\sigma(n)$	n	$\phi(n)$	$d(n)$	$\sigma(n)$
1	1	1	1	14	6	4	24	27	18	4	40	40	16	8	90
2	1	2	3	15	8	4	24	28	12	6	56	41	40	2	42
3	2	2	4	16	8	5	31	29	28	2	30	42	12	8	96
4	2	3	7	17	16	2	18	30	8	8	72	43	42	2	44
5	4	2	6	18	6	6	39	31	30	2	32	44	20	6	84
6	2	4	12	19	18	2	20	32	16	6	63	45	24	6	78
7	6	2	8	20	8	6	42	33	20	4	48	46	22	4	72
8	4	4	15	21	12	4	32	34	16	4	54	47	46	2	48
9	6	3	13	22	10	4	36	35	24	4	48	48	16	10	124
10	4	4	18	23	22	2	24	36	12	9	91	49	42	3	57
11	10	2	12	24	8	8	60	37	36	2	38	50	20	6	93
12	4	6	28	25	20	3	31	38	18	4	60	51	32	4	72
13	12	2	14	26	12	4	42	39	24	4	56	52	24	6	98

27.3 Multiplicative Properties

Except for $\nu(n)$, $\Lambda(n)$, p_n, and $\pi(x)$, the functions in §27.2 are *multiplicative*, which means $f(1) = 1$ and

27.3.1 $$f(mn) = f(m)f(n), \qquad (m,n) = 1.$$

If f is multiplicative, then the values $f(n)$ for $n > 1$ are determined by the values at the prime powers. Specifically, if n is factored as in (27.2.1), then

27.3.2 $$f(n) = \prod_{r=1}^{\nu(n)} f(p_r^{a_r}).$$

In particular,

27.3.3 $$\phi(n) = n\prod_{p|n}(1-p^{-1}),$$

27.3.4 $$J_k(n) = n^k\prod_{p|n}(1-p^{-k}),$$

27.3.5 $$d(n) = \prod_{r=1}^{\nu(n)}(1+a_r),$$

27.3.6 $$\sigma_\alpha(n) = \prod_{r=1}^{\nu(n)}\frac{p_r^{\alpha(1+a_r)}-1}{p_r^\alpha-1}, \qquad \alpha \neq 0.$$

Related multiplicative properties are

27.3.7 $$\sigma_\alpha(m)\,\sigma_\alpha(n) = \sum_{d|(m,n)} d^\alpha\,\sigma_\alpha\left(\frac{mn}{d^2}\right),$$

27.3.8 $$\phi(m)\,\phi(n) = \phi(mn)\,\phi((m,n))/\,(m,n)\,.$$

A function f is *completely multiplicative* if $f(1) = 1$ and

27.3.9 $$f(mn) = f(m)f(n), \quad m,n = 1,2,\ldots.$$

Examples are $\lfloor 1/n \rfloor$ and $\lambda(n)$, and the Dirichlet characters, defined in §27.8.

If f is completely multiplicative, then (27.3.2) becomes

27.3.10 $$f(n) = \prod_{r=1}^{\nu(n)} (f(p_r))^{a_r}\,.$$

27.4 Euler Products and Dirichlet Series

The fundamental theorem of arithmetic is linked to analysis through the concept of the Euler product. Every multiplicative f satisfies the identity

27.4.1 $$\sum_{n=1}^{\infty} f(n) = \prod_p \left(1 + \sum_{r=1}^{\infty} f(p^r)\right),$$

if the series on the left is absolutely convergent. In this case the infinite product on the right (extended over all primes p) is also absolutely convergent and is called the *Euler product* of the series. If $f(n)$ is completely multiplicative, then each factor in the product is a geometric series and the Euler product becomes

27.4.2 $$\sum_{n=1}^{\infty} f(n) = \prod_p (1-f(p))^{-1}.$$

Euler products are used to find series that generate many functions of multiplicative number theory. The completely multiplicative function $f(n) = n^{-s}$ gives the Euler product representation of the *Riemann zeta function* $\zeta(s)$ (§25.2(i)):

27.4.3 $$\zeta(s) = \sum_{n=1}^{\infty} n^{-s} = \prod_p (1-p^{-s})^{-1}, \qquad \Re s > 1.$$

The Riemann zeta function is the prototype of series of the form

27.4.4 $$F(s) = \sum_{n=1}^{\infty} f(n)n^{-s},$$

called *Dirichlet series* with coefficients $f(n)$. The function $F(s)$ is a *generating function*, or more precisely, a *Dirichlet generating function*, for the coefficients. The following examples have generating functions related to the zeta function:

27.4.5 $$\sum_{n=1}^{\infty} \mu(n)n^{-s} = \frac{1}{\zeta(s)}, \qquad \Re s > 1,$$

27.4.6 $$\sum_{n=1}^{\infty} \phi(n)n^{-s} = \frac{\zeta(s-1)}{\zeta(s)}, \qquad \Re s > 2,$$

27.4.7 $$\sum_{n=1}^{\infty} \lambda(n)n^{-s} = \frac{\zeta(2s)}{\zeta(s)}, \qquad \Re s > 1,$$

27.4.8 $$\sum_{n=1}^{\infty} |\,\mu(n)|n^{-s} = \frac{\zeta(s)}{\zeta(2s)}, \qquad \Re s > 1,$$

27.4.9 $$\sum_{n=1}^{\infty} 2^{\nu(n)}n^{-s} = \frac{(\zeta(s))^2}{\zeta(2s)}, \qquad \Re s > 1,$$

27.4.10 $$\sum_{n=1}^{\infty} d_k(n)n^{-s} = (\zeta(s))^k, \qquad \Re s > 1,$$

27.4.11 $$\sum_{n=1}^{\infty} \sigma_\alpha(n)n^{-s} = \zeta(s)\,\zeta(s-\alpha), \quad \Re s > \max(1, 1+\Re\alpha),$$

27.4.12 $$\sum_{n=1}^{\infty} \Lambda(n)n^{-s} = -\frac{\zeta'(s)}{\zeta(s)}, \qquad \Re s > 1,$$

27.4.13 $$\sum_{n=2}^{\infty} (\log\, n)n^{-s} = -\,\zeta'(s), \qquad \Re s > 1.$$

In (27.4.12) and (27.4.13) $\zeta'(s)$ is the derivative of $\zeta(s)$.

27.5 Inversion Formulas

If a Dirichlet series $F(s)$ generates $f(n)$, and $G(s)$ generates $g(n)$, then the product $F(s)G(s)$ generates

27.5.1 $$h(n) = \sum_{d|n} f(d) g\left(\frac{n}{d}\right),$$

called the *Dirichlet product* (or *convolution*) of f and g. The set of all number-theoretic functions f with $f(1) \neq 0$ forms an abelian group under Dirichlet multiplication, with the function $\lfloor 1/n \rfloor$ in (27.2.5) as identity element; see Apostol (1976, p. 129). The multiplicative functions are a subgroup of this group. Generating functions yield many relations connecting number-theoretic functions. For example, the equation $\zeta(s)\cdot(1/\zeta(s)) = 1$ is equivalent to the identity

27.5.2 $$\sum_{d|n} \mu(d) = \left\lfloor \frac{1}{n} \right\rfloor,$$

which, in turn, is the basis for the *Möbius inversion formula* relating sums over divisors:

27.5.3 $$g(n) = \sum_{d|n} f(d) \iff f(n) = \sum_{d|n} g(d)\,\mu\Big(\frac{n}{d}\Big).$$

Special cases of Möbius inversion pairs are:

27.5.4 $$n = \sum_{d|n} \phi(d) \iff \phi(n) = \sum_{d|n} d\,\mu\Big(\frac{n}{d}\Big),$$

27.5.5 $$\log n = \sum_{d|n} \Lambda(d) \iff \Lambda(n) = \sum_{d|n} (\log d)\,\mu\Big(\frac{n}{d}\Big).$$

Other types of Möbius inversion formulas include:

27.5.6 $$G(x) = \sum_{n\le x} F\left(\frac{x}{n}\right) \iff F(x) = \sum_{n\le x} \mu(n) G\left(\frac{x}{n}\right),$$

27.5.7
$$G(x) = \sum_{m=1}^{\infty} \frac{F(mx)}{m^s} \iff F(x) = \sum_{m=1}^{\infty} \mu(m) \frac{G(mx)}{m^s},$$

27.5.8 $$g(n) = \prod_{d|n} f(d) \iff f(n) = \prod_{d|n} \left(g\left(\frac{n}{d}\right)\right)^{\mu(d)}.$$

For a general theory of Möbius inversion with applications to combinatorial theory see Rota (1964).

27.6 Divisor Sums

Sums of number-theoretic functions extended over divisors are of special interest. For example,

27.6.1 $$\sum_{d|n} \lambda(d) = \begin{cases} 1, & n \text{ is a square,} \\ 0, & \text{otherwise.} \end{cases}$$

If f is multiplicative, then

27.6.2 $$\sum_{d|n} \mu(d) f(d) = \prod_{p|n} (1 - f(p)), \qquad n > 1.$$

Generating functions, Euler products, and Möbius inversion are used to evaluate many sums extended over divisors. Examples include:

27.6.3 $$\sum_{d|n} |\,\mu(d)| = 2^{\nu(n)},$$

27.6.4 $$\sum_{d^2|n} \mu(d) = |\,\mu(n)|,$$

27.6.5 $$\sum_{d|n} \frac{|\,\mu(d)|}{\phi(d)} = \frac{n}{\phi(n)},$$

27.6.6 $$\sum_{d|n} \phi_k(d) \left(\frac{n}{d}\right)^k = 1^k + 2^k + \cdots + n^k,$$

27.6.7 $$\sum_{d|n} \mu(d) \left(\frac{n}{d}\right)^k = J_k(n),$$

27.6.8 $$\sum_{d|n} J_k(d) = n^k.$$

27.7 Lambert Series as Generating Functions

Lambert series have the form

27.7.1 $$\sum_{n=1}^{\infty} f(n) \frac{x^n}{1 - x^n}.$$

If $|x| < 1$, then the quotient $x^n/(1 - x^n)$ is the sum of a geometric series, and when the series (27.7.1) converges absolutely it can be rearranged as a power series:

27.7.2 $$\sum_{n=1}^{\infty} f(n) \frac{x^n}{1 - x^n} = \sum_{n=1}^{\infty} \sum_{d|n} f(d) x^n.$$

Again with $|x| < 1$, special cases of (27.7.2) include:

27.7.3 $$\sum_{n=1}^{\infty} \mu(n) \frac{x^n}{1 - x^n} = x,$$

27.7.4 $$\sum_{n=1}^{\infty} \phi(n) \frac{x^n}{1 - x^n} = \frac{x}{(1 - x)^2},$$

27.7.5 $$\sum_{n=1}^{\infty} n^{\alpha} \frac{x^n}{1 - x^n} = \sum_{n=1}^{\infty} \sigma_{\alpha}(n) x^n,$$

27.7.6 $$\sum_{n=1}^{\infty} \lambda(n) \frac{x^n}{1 - x^n} = \sum_{n=1}^{\infty} x^{n^2}.$$

27.8 Dirichlet Characters

If k (>1) is a given integer, then a function $\chi(n)$ is called a *Dirichlet character* (mod k) if it is completely multiplicative, periodic with period k, and vanishes when $(n,k)>1$. In other words, Dirichlet characters (mod k) satisfy the four conditions:

27.8.1 $$\chi(1)=1,$$

27.8.2 $$\chi(mn)=\chi(m)\,\chi(n), \qquad m,n=1,2,\dots,$$

27.8.3 $$\chi(n+k)=\chi(n), \qquad n=1,2,\dots,$$

27.8.4 $$\chi(n)=0, \qquad (n,k)>1.$$

An example is the *principal character* (mod k):

27.8.5 $$\chi_1(n)=\begin{cases}1, & (n,k)=1,\\ 0, & (n,k)>1.\end{cases}$$

For any character χ (mod k), $\chi(n)\neq 0$ if and only if $(n,k)=1$, in which case the Euler–Fermat theorem (27.2.8) implies $(\chi(n))^{\phi(k)}=1$. There are exactly $\phi(k)$ different characters (mod k), which can be labeled as $\chi_1,\dots,\chi_{\phi(k)}$. If χ is a character (mod k), so is its complex conjugate $\overline{\chi}$. If $(n,k)=1$, then the characters satisfy the *orthogonality relation*

27.8.6 $$\sum_{r=1}^{\phi(k)}\chi_r(m)\overline{\chi}_r(n)=\begin{cases}\phi(k), & m\equiv n \pmod k,\\ 0, & \text{otherwise.}\end{cases}$$

A Dirichlet character χ (mod k) is called *primitive* (mod k) if for every proper divisor d of k (that is, a divisor $d<k$), there exists an integer $a\equiv 1 \pmod d$, with $(a,k)=1$ and $\chi(a)\neq 1$. If k is prime, then every nonprincipal character χ (mod k) is primitive. A divisor d of k is called an *induced modulus* for χ if

27.8.7 $$\chi(a)=1 \text{ for all } a\equiv 1 \pmod d, \quad (a,k)=1.$$

Every Dirichlet character χ (mod k) is a product

27.8.8 $$\chi(n)=\chi_0(n)\,\chi_1(n),$$

where χ_0 is a character (mod d) for some induced modulus d for χ, and χ_1 is the principal character (mod k). A character is *real* if all its values are real. If k is odd, then the real characters (mod k) are the principal character and the quadratic characters described in the next section.

27.9 Quadratic Characters

For an odd prime p, the *Legendre symbol* $(n|p)$ is defined as follows. If p divides n, then the value of $(n|p)$ is 0. If p does not divide n, then $(n|p)$ has the value 1 when the quadratic congruence $x^2\equiv n \pmod p$ has a solution, and the value -1 when this congruence has no solution. The Legendre symbol $(n|p)$, as a function of n, is a Dirichlet character (mod p). It is sometimes written as $\left(\frac{n}{p}\right)$. Special values include:

27.9.1 $$(-1|p)=(-1)^{(p-1)/2},$$

27.9.2 $$(2|p)=(-1)^{(p^2-1)/8}.$$

If p,q are distinct odd primes, then the *quadratic reciprocity law* states that

27.9.3 $$(p|q)\,(q|p)=(-1)^{(p-1)(q-1)/4}.$$

If an odd integer P has prime factorization $P=\prod_{r=1}^{\nu(n)}p_r^{a_r}$, then the *Jacobi symbol* $(n|P)$ is defined by $(n|P)=\prod_{r=1}^{\nu(n)}(n|p_r)^{a_r}$, with $(n|1)=1$. The Jacobi symbol $(n|P)$ is a Dirichlet character (mod P). Both (27.9.1) and (27.9.2) are valid with p replaced by P; the reciprocity law (27.9.3) holds if p,q are replaced by any two relatively prime odd integers P,Q.

27.10 Periodic Number-Theoretic Functions

If k is a fixed positive integer, then a number-theoretic function f is *periodic* (mod k) if

27.10.1 $$f(n+k)=f(n), \qquad n=1,2,\dots.$$

Examples are the Dirichlet characters (mod k) and the greatest common divisor (n,k) regarded as a function of n.

Every function periodic (mod k) can be expressed as a *finite Fourier series* of the form

27.10.2 $$f(n)=\sum_{m=1}^{k}g(m)e^{2\pi imn/k},$$

where $g(m)$ is also periodic (mod k), and is given by

27.10.3 $$g(m)=\frac{1}{k}\sum_{n=1}^{k}f(n)e^{-2\pi imn/k}.$$

An example is *Ramanujan's sum*:

27.10.4 $$c_k(n)=\sum_{m=1}^{k}\chi_1(m)e^{2\pi imn/k},$$

where χ_1 is the principal character (mod k). This is the sum of the nth powers of the primitive kth roots of unity. It can also be expressed in terms of the Möbius function as a divisor sum:

27.10.5 $$c_k(n)=\sum_{d|(n,k)}d\,\mu\left(\frac{k}{d}\right).$$

More generally, if f and g are arbitrary, then the sum

27.10.6 $$s_k(n)=\sum_{d|(n,k)}f(d)g\left(\frac{k}{d}\right)$$

is a periodic function of $n \pmod k$ and has the finite Fourier-series expansion

$$s_k(n) = \sum_{m=1}^{k} a_k(m) e^{2\pi i m n/k}, \tag{27.10.7}$$

where

$$a_k(m) = \sum_{d|(m,k)} g(d) f\left(\frac{k}{d}\right) \frac{d}{k}. \tag{27.10.8}$$

Another generalization of Ramanujan's sum is the *Gauss sum* $G(n,\chi)$ associated with a Dirichlet character $\chi \pmod k$. It is defined by the relation

$$G(n,\chi) = \sum_{m=1}^{k} \chi(m) e^{2\pi i m n/k}. \tag{27.10.9}$$

In particular, $G(n,\chi_1) = c_k(n)$.

$G(n,\chi)$ is *separable* for some n if

$$G(n,\chi) = \overline{\chi}(n)\, G(1,\chi). \tag{27.10.10}$$

For any Dirichlet character $\chi \pmod k$, $G(n,\chi)$ is separable for n if $(n,k) = 1$, and is separable for every n if and only if $G(n,\chi) = 0$ whenever $(n,k) > 1$. For a primitive character $\chi \pmod k$, $G(n,\chi)$ is separable for every n, and

$$|G(1,\chi)|^2 = k. \tag{27.10.11}$$

Conversely, if $G(n,\chi)$ is separable for every n, then χ is primitive $\pmod k$.

The finite Fourier expansion of a primitive Dirichlet character $\chi \pmod k$ has the form

$$\chi(n) = \frac{G(1,\chi)}{k} \sum_{m=1}^{k} \overline{\chi}(m) e^{-2\pi i m n/k}. \tag{27.10.12}$$

27.11 Asymptotic Formulas: Partial Sums

The behavior of a number-theoretic function $f(n)$ for large n is often difficult to determine because the function values can fluctuate considerably as n increases. It is more fruitful to study partial sums and seek asymptotic formulas of the form

$$\sum_{n\le x} f(n) = F(x) + O(g(x)), \tag{27.11.1}$$

where $F(x)$ is a known function of x, and $O(g(x))$ represents the error, a function of smaller order than $F(x)$ for all x in some prescribed range. For example, Dirichlet (1849) proves that for all $x \ge 1$,

$$\sum_{n\le x} d(n) = x\log x + (2\gamma - 1)x + O\big(\sqrt{x}\big), \tag{27.11.2}$$

where γ is Euler's constant (§5.2(ii)). *Dirichlet's divisor problem* (unsolved in 2009) is to determine the least number θ_0 such that the error term in (27.11.2) is $O\big(x^{\theta}\big)$ for all $\theta > \theta_0$. Kolesnik (1969) proves that $\theta_0 \le \frac{12}{37}$.

Equations (27.11.3)–(27.11.11) list further asymptotic formulas related to some of the functions listed in §27.2. They are valid for all $x \ge 2$. The error terms given here are not necessarily the best known.

$$\sum_{n\le x} \frac{d(n)}{n} = \frac{1}{2}(\log x)^2 + 2\gamma \log x + O(1), \tag{27.11.3}$$

where γ again is Euler's constant.

$$\sum_{n\le x} \sigma_1(n) = \frac{\pi^2}{12} x^2 + O(x\log x). \tag{27.11.4}$$

$$\sum_{n\le x} \sigma_\alpha(n) = \frac{\zeta(\alpha+1)}{\alpha+1} x^{\alpha+1} + O\big(x^{\beta}\big), \tag{27.11.5}$$

$$\alpha > 0,\ \alpha \ne 1,\ \beta = \max(1,\alpha).$$

$$\sum_{n\le x} \phi(n) = \frac{3}{\pi^2} x^2 + O(x\log x). \tag{27.11.6}$$

$$\sum_{n\le x} \frac{\phi(n)}{n} = \frac{6}{\pi^2} x + O(\log x). \tag{27.11.7}$$

$$\sum_{p\le x} \frac{1}{p} = \log\log x + A + O\left(\frac{1}{\log x}\right), \tag{27.11.8}$$

where A is a constant.

$$\sum_{\substack{p\le x \\ p\equiv h \,(\mathrm{mod}\ k)}} \frac{1}{p} = \frac{1}{\phi(k)} \log\log x + B + O\left(\frac{1}{\log x}\right), \tag{27.11.9}$$

where $(h,k) = 1$, $k > 0$, and B is a constant depending on h and k.

$$\sum_{p\le x} \frac{\log p}{p} = \log x + O(1). \tag{27.11.10}$$

$$\sum_{\substack{p\le x \\ p\equiv h \,(\mathrm{mod}\ k)}} \frac{\log p}{p} = \frac{1}{\phi(k)} \log x + O(1), \tag{27.11.11}$$

where $(h,k) = 1$, $k > 0$.

Letting $x \to \infty$ in (27.11.9) or in (27.11.11) we see that there are infinitely many primes $p \equiv h \pmod k$ if h, k are coprime; this is *Dirichlet's theorem on primes in arithmetic progressions*.

$$\sum_{n\le x} \mu(n) = O\left(x e^{-C\sqrt{\log x}}\right), \qquad x \to \infty, \tag{27.11.12}$$

for some positive constant C,

$$\lim_{x\to\infty} \frac{1}{x} \sum_{n\le x} \mu(n) = 0, \tag{27.11.13}$$

$$\lim_{x\to\infty} \sum_{n\le x} \frac{\mu(n)}{n} = 0, \tag{27.11.14}$$

$$\lim_{x\to\infty} \sum_{n\le x} \frac{\mu(n)\log n}{n} = -1. \tag{27.11.15}$$

Each of (27.11.13)–(27.11.15) is equivalent to the prime number theorem (27.2.3). *The prime number theorem for arithmetic progressions*—an extension of (27.2.3) and first proved in de la Vallée Poussin (1896a,b)—states that if $(h,k)=1$, then the number of primes $p\le x$ with $p\equiv h \pmod k$ is asymptotic to $x/(\phi(k)\log x)$ as $x\to\infty$.

27.12 Asymptotic Formulas: Primes

p_n is the nth prime, beginning with $p_1=2$. $\pi(x)$ is the number of primes less than or equal to x.

27.12.1
$$\lim_{n\to\infty}\frac{p_n}{n\log n}=1,$$

27.12.2
$$p_n>n\log n, \qquad n=1,2,\dots.$$

27.12.3
$$\pi(x)=\lfloor x\rfloor-1-\sum_{p_j\le\sqrt{x}}\left\lfloor\frac{x}{p_j}\right\rfloor+\sum_{r\ge2}(-1)^r\sum_{p_{j_1}<p_{j_2}<\cdots<p_{j_r}\le\sqrt{x}}\left\lfloor\frac{x}{p_{j_1}p_{j_2}\cdots p_{j_r}}\right\rfloor, \qquad x\ge1,$$

where the series terminates when the product of the first r primes exceeds x.

As $x\to\infty$

27.12.4
$$\pi(x)\sim\sum_{k=1}^{\infty}\frac{(k-1)!\,x}{(\log x)^k}.$$

Prime Number Theorem

There exists a positive constant c such that

27.12.5
$$|\pi(x)-\operatorname{li}(x)|=O\left(x\exp\left(-c\sqrt{\log x}\right)\right),\quad x\to\infty.$$

For the logarithmic integral $\operatorname{li}(x)$ see (6.2.8). The best available asymptotic error estimate (2009) appears in Korobov (1958) and Vinogradov (1958): there exists a positive constant d such that

27.12.6
$$|\pi(x)-\operatorname{li}(x)|=O\left(x\exp\left(-d(\log x)^{3/5}(\log\log x)^{-1/5}\right)\right).$$

$\pi(x)-\operatorname{li}(x)$ changes sign infinitely often as $x\to\infty$; see Littlewood (1914), Bays and Hudson (2000).

The *Riemann hypothesis* (§25.10(i)) is equivalent to the statement that for every $x\ge2657$,

27.12.7
$$|\pi(x)-\operatorname{li}(x)|<\frac{1}{8\pi}\sqrt{x}\log x.$$

If a is relatively prime to the modulus m, then there are infinitely many primes congruent to $a \pmod m$.

The number of such primes not exceeding x is

27.12.8
$$\frac{x}{\phi(m)}+O\left(x\exp\left(-\lambda(\alpha)(\log x)^{1/2}\right)\right), \qquad m\le(\log x)^{\alpha},\ \alpha>0,$$

where $\lambda(\alpha)$ depends only on α, and $\phi(m)$ is the Euler totient function (§27.2).

A *Mersenne prime* is a prime of the form 2^p-1. The largest known prime (2009) is the Mersenne prime $2^{43,112,609}-1$. For current records online, see http://dlmf.nist.gov/27.12.

A *pseudoprime test* is a test that correctly identifies most composite numbers. For example, if $2^n\not\equiv2 \pmod n$, then n is composite. Descriptions and comparisons of pseudoprime tests are given in Bressoud and Wagon (2000, §§2.4, 4.2, and 8.2) and Crandall and Pomerance (2005, §§3.4–3.6).

A *Carmichael number* is a composite number n for which $b^n\equiv b \pmod n$ for all $b\in\mathbb{N}$. There are infinitely many Carmichael numbers.

Additive Number Theory

27.13 Functions

27.13(i) Introduction

Whereas multiplicative number theory is concerned with functions arising from prime factorization, additive number theory treats functions related to addition of integers. The basic problem is that of expressing a given positive integer n as a sum of integers from some prescribed set S whose members are primes, squares, cubes, or other special integers. Each representation of n as a sum of elements of S is called a *partition* of n, and the number $S(n)$ of such partitions is often of great interest. The subsections that follow describe problems from additive number theory. See also Apostol (1976, Chapter 14) and Apostol and Niven (1994, pp. 33–34).

27.13(ii) Goldbach Conjecture

Every even integer $n>4$ is the sum of two odd primes. In this case, $S(n)$ is the number of solutions of the equation $n=p+q$, where p and q are odd primes. Goldbach's assertion is that $S(n)\ge1$ for all even $n>4$. This conjecture dates back to 1742 and was undecided in 2009, although it has been confirmed numerically up to very large numbers. Vinogradov (1937) proves that every sufficiently large odd integer is the sum of three odd primes, and Chen (1966) shows that every sufficiently large even integer is the sum of a prime and a number with no more than two prime factors.

For an online account of the current status of Goldbach's conjecture see http://dlmf.nist.gov/27.13.ii.

27.13(iii) Waring's Problem

This problem is named after Edward Waring who, in 1770, stated without proof and with limited numerical evidence, that every positive integer n is the sum of four squares, of nine cubes, of nineteen fourth powers, and so on. Waring's problem is to find, for each positive integer k, whether there is an integer m (depending only on k) such that the equation

27.13.1 $$n = x_1^k + x_2^k + \cdots + x_m^k$$

has nonnegative integer solutions for all $n \geq 1$. The smallest m that exists for a given k is denoted by $g(k)$. Similarly, $G(k)$ denotes the smallest m for which (27.13.1) has nonnegative integer solutions for all sufficiently large n.

Lagrange (1770) proves that $g(2) = 4$, and during the next 139 years the existence of $g(k)$ was shown for $k = 3, 4, 5, 6, 7, 8, 10$. Hilbert (1909) proves the existence of $g(k)$ for every k but does not determine its corresponding numerical value. The exact value of $g(k)$ is now known for every $k \leq 200,000$. For example, $g(3) = 9$, $g(4) = 19$, $g(5) = 37$, $g(6) = 73$, $g(7) = 143$, and $g(8) = 279$. A general formula states that

27.13.2 $$g(k) \geq 2^k + \left\lfloor \frac{3^k}{2^k} \right\rfloor - 2,$$

for all $k \geq 2$, with equality if $4 \leq k \leq 200,000$. If $3^k = q2^k + r$ with $0 < r < 2^k$, then equality holds in (27.13.2) provided $r + q \leq 2^k$, a condition that is satisfied with at most a finite number of exceptions.

The existence of $G(k)$ follows from that of $g(k)$ because $G(k) \leq g(k)$, but only the values $G(2) = 4$ and $G(4) = 16$ are known exactly. Some upper bounds smaller than $g(k)$ are known. For example, $G(3) \leq 7$, $G(5) \leq 23$, $G(6) \leq 36$, $G(7) \leq 53$, and $G(8) \leq 73$. Hardy and Littlewood (1925) conjectures that $G(k) < 2k + 1$ when k is not a power of 2, and that $G(k) \leq 4k$ when k is a power of 2, but the most that is known (in 2009) is $G(k) < ck \log k$ for some constant c. A survey is given in Ellison (1971).

27.13(iv) Representation by Squares

For a given integer $k \geq 2$ the function $r_k(n)$ is defined as the number of solutions of the equation

27.13.3 $$n = x_1^2 + x_2^2 + \cdots + x_k^2,$$

where the x_j are integers, positive, negative, or zero, and the order of the summands is taken into account.

Jacobi (1829) notes that $r_2(n)$ is the coefficient of x^n in the square of the theta function $\vartheta(x)$:

27.13.4 $$\vartheta(x) = 1 + 2\sum_{m=1}^{\infty} x^{m^2}, \qquad |x| < 1.$$

(In §20.2(i), $\vartheta(x)$ is denoted by $\theta_3(0, x)$.) Thus,

27.13.5 $$(\vartheta(x))^2 = 1 + \sum_{n=1}^{\infty} r_2(n)x^n.$$

One of Jacobi's identities implies that

27.13.6 $$(\vartheta(x))^2 = 1 + 4\sum_{n=1}^{\infty} \left(\delta_1(n) - \delta_3(n)\right) x^n,$$

where $\delta_1(n)$ and $\delta_3(n)$ are the number of divisors of n congruent respectively to 1 and 3 (mod 4), and by equating coefficients in (27.13.5) and (27.13.6) Jacobi deduced that

27.13.7 $$r_2(n) = 4\left(\delta_1(n) - \delta_3(n)\right).$$

Hence $r_2(5) = 8$ because both divisors, 1 and 5, are congruent to 1 (mod 4). In fact, there are four representations, given by $5 = 2^2 + 1^2 = 2^2 + (-1)^2 = (-2)^2 + 1^2 = (-2)^2 + (-1)^2$, and four more with the order of summands reversed.

By similar methods Jacobi proved that $r_4(n) = 8\sigma_1(n)$ if n is odd, whereas, if n is even, $r_4(n) = 24$ times the sum of the odd divisors of n. Mordell (1917) notes that $r_k(n)$ is the coefficient of x^n in the power-series expansion of the kth power of the series for $\vartheta(x)$. Explicit formulas for $r_k(n)$ have been obtained by similar methods for $k = 6, 8, 10$, and 12, but they are more complicated. Exact formulas for $r_k(n)$ have also been found for $k = 3, 5$, and 7, and for all even $k \leq 24$. For values of $k > 24$ the analysis of $r_k(n)$ is considerably more complicated (see Hardy (1940)). Also, Milne (1996, 2002) announce new infinite families of explicit formulas extending Jacobi's identities. For more than 8 squares, Milne's identities are not the same as those obtained earlier by Mordell and others.

27.14 Unrestricted Partitions

27.14(i) Partition Functions

A fundamental problem studies the number of ways n can be written as a sum of positive integers $\leq n$, that is, the number of solutions of

27.14.1 $$n = a_1 + a_2 + \cdots, \quad a_1 \geq a_2 \geq \cdots \geq 1.$$

The number of summands is unrestricted, repetition is allowed, and the order of the summands is not taken into account. The corresponding *unrestricted partition function* is denoted by $p(n)$, and the summands are called *parts*; see §26.9(i). For example, $p(5) = 7$ because there are exactly seven partitions of 5: $5 = 4 + 1 = 3 + 2 = 3 + 1 + 1 = 2 + 2 + 1 = 2 + 1 + 1 + 1 = 1 + 1 + 1 + 1 + 1$.

The number of partitions of n into at most k parts is denoted by $p_k(n)$; again see §26.9(i).

27.14(ii) Generating Functions and Recursions

Euler introduced the reciprocal of the infinite product

$$f(x)=\prod_{m=1}^{\infty}(1-x^m),\qquad |x|<1, \tag{27.14.2}$$

as a generating function for the function $p(n)$ defined in §27.14(i):

$$\frac{1}{f(x)}=\sum_{n=0}^{\infty}p(n)x^n, \tag{27.14.3}$$

with $p(0)=1$. Euler's *pentagonal number theorem* states that

$$\begin{aligned}f(x)&=1-x-x^2+x^5+x^7-x^{12}-x^{15}+\cdots\\&=1+\sum_{k=1}^{\infty}(-1)^k\left(x^{\omega(k)}+x^{\omega(-k)}\right),\end{aligned} \tag{27.14.4}$$

where the exponents 1, 2, 5, 7, 12, 15, … are the *pentagonal numbers*, defined by

$$\omega(\pm k)=(3k^2\mp k)/2,\quad k=1,2,3,\ldots. \tag{27.14.5}$$

Multiplying the power series for $f(x)$ with that for $1/f(x)$ and equating coefficients, we obtain the recursion formula

$$\begin{aligned}p(n)&=\sum_{k=1}^{\infty}(-1)^{k+1}\left(p(n-\omega(k))+p(n-\omega(-k))\right)\\&=p(n-1)+p(n-2)-p(n-5)-p(n-7)+\cdots,\end{aligned} \tag{27.14.6}$$

where $p(k)$ is defined to be 0 if $k<0$. Logarithmic differentiation of the generating function $1/f(x)$ leads to another recursion:

$$n\,p(n)=\sum_{k=1}^{n}\sigma_1(n)\,p(n-k), \tag{27.14.7}$$

where $\sigma_1(n)$ is defined by (27.2.10) with $\alpha=1$.

27.14(iii) Asymptotic Formulas

These recursions can be used to calculate $p(n)$, which grows very rapidly. For example, $p(10)=42$, $p(100)=1905\,69292$, and $p(200)=397\,29990\,29388$. For large n

$$p(n)\sim e^{K\sqrt{n}}/(4n\sqrt{3}), \tag{27.14.8}$$

where $K=\pi\sqrt{2/3}$ (Hardy and Ramanujan (1918)). Rademacher (1938) derives a convergent series that also provides an asymptotic expansion for $p(n)$:

$$\begin{aligned}&p(n)\\&=\frac{1}{\pi\sqrt{2}}\sum_{k=1}^{\infty}\sqrt{k}A_k(n)\left[\frac{d}{dt}\frac{\sinh\left(K\sqrt{t}/k\right)}{\sqrt{t}}\right]_{t=n-(1/24)},\end{aligned} \tag{27.14.9}$$

where

$$A_k(n)=\sum_{\substack{h=1\\(h,k)=1}}^{k}\exp\left(\pi i s(h,k)-2\pi i n\frac{h}{k}\right), \tag{27.14.10}$$

and $s(h,k)$ is a *Dedekind sum* given by

$$s(h,k)=\sum_{r=1}^{k-1}\frac{r}{k}\left(\frac{hr}{k}-\left\lfloor\frac{hr}{k}\right\rfloor-\frac{1}{2}\right). \tag{27.14.11}$$

27.14(iv) Relation to Modular Functions

Dedekind sums occur in the transformation theory of the *Dedekind modular function* $\eta(\tau)$, defined by

$$\eta(\tau)=e^{\pi i\tau/12}\prod_{n=1}^{\infty}(1-e^{2\pi i n\tau}),\qquad \Im\tau>0. \tag{27.14.12}$$

This is related to the function $f(x)$ in (27.14.2) by

$$\eta(\tau)=e^{\pi i\tau/12}f\left(e^{2\pi i\tau}\right). \tag{27.14.13}$$

$\eta(\tau)$ satisfies the following functional equation: if a,b,c,d are integers with $ad-bc=1$ and $c>0$, then

$$\eta\left(\frac{a\tau+b}{c\tau+d}\right)=\varepsilon(-i(c\tau+d))^{\frac{1}{2}}\,\eta(\tau), \tag{27.14.14}$$

where $\varepsilon=\exp(\pi i(((a+d)/(12c))-s(d,c)))$ and $s(d,c)$ is given by (27.14.11).

For further properties of the function $\eta(\tau)$ see §§23.15–23.19.

27.14(v) Divisibility Properties

Ramanujan (1921) gives identities that imply divisibility properties of the partition function. For example, the Ramanujan identity

$$5\frac{\left(f\left(x^5\right)\right)^5}{(f(x))^6}=\sum_{n=0}^{\infty}p(5n+4)x^n \tag{27.14.15}$$

implies $p(5n+4)\equiv 0 \pmod 5$. Ramanujan also found that $p(7n+5)\equiv 0 \pmod 7$ and $p(11n+6)\equiv 0 \pmod{11}$ for all n. After decades of nearly fruitless searching for further congruences of this type, it was believed that no others existed, until it was shown in Ono (2000) that there are infinitely many. Ono proved that for every prime $q>3$ there are integers a and b such that $p(an+b)\equiv 0 \pmod q$ for all n. For example, $p(1575\,25693n+1\,11247)\equiv 0 \pmod{13}$.

27.14(vi) Ramanujan's Tau Function

The *discriminant function* $\Delta(\tau)$ is defined by

$$\Delta(\tau)=(2\pi)^{12}(\eta(\tau))^{24},\qquad \Im\tau>0, \tag{27.14.16}$$

and satisfies the functional equation

$$\Delta\left(\frac{a\tau+b}{c\tau+d}\right)=(c\tau+d)^{12}\,\Delta(\tau), \tag{27.14.17}$$

if a,b,c,d are integers with $ad-bc=1$ and $c>0$.

The 24th power of $\eta(\tau)$ in (27.14.12) with $e^{2\pi i\tau}=x$ is an infinite product that generates a power series in

x with integer coefficients called *Ramanujan's tau function* $\tau(n)$:

27.14.18
$$x\prod_{n=1}^{\infty}(1-x^n)^{24}=\sum_{n=1}^{\infty}\tau(n)x^n, \qquad |x|<1.$$

The tau function is multiplicative and satisfies the more general relation:

27.14.19
$$\tau(m)\,\tau(n)=\sum_{d|(m,n)}d^{11}\,\tau\Big(\frac{mn}{d^2}\Big), \quad m,n=1,2,\ldots.$$

Lehmer (1947) conjectures that $\tau(n)$ is never 0 and verifies this for all $n<21\,49286\,39999$ by studying various congruences satisfied by $\tau(n)$, for example:

27.14.20
$$\tau(n)\equiv\sigma_{11}(n) \pmod{691}.$$

For further information on partitions and generating functions see Andrews (1976); also §§17.2–17.14, and §§26.9–26.10.

Applications

27.15 Chinese Remainder Theorem

The Chinese remainder theorem states that a system of congruences $x\equiv a_1 \pmod{m_1},\ldots,x\equiv a_k \pmod{m_k}$, always has a solution if the moduli are relatively prime in pairs; the solution is unique (mod m), where m is the product of the moduli.

This theorem is employed to increase efficiency in calculating with large numbers by making use of smaller numbers in most of the calculation. For example, suppose a lengthy calculation involves many 10-digit integers. Most of the calculation can be done with five-digit integers as follows. Choose four relatively prime moduli m_1, m_2, m_3, and m_4 of five digits each, for example $2^{16}-3$, $2^{16}-1$, $2^{16}+1$, and $2^{16}+3$. Their product m has 20 digits, twice the number of digits in the data. By the Chinese remainder theorem each integer in the data can be uniquely represented by its residues (mod m_1), (mod m_2), (mod m_3), and (mod m_4), respectively. Because each residue has no more than five digits, the arithmetic can be performed efficiently on these residues with respect to each of the moduli, yielding answers $a_1 \pmod{m_1}$, $a_2 \pmod{m_2}$, $a_3 \pmod{m_3}$, and $a_4 \pmod{m_4}$, where each a_j has no more than five digits. These numbers, in turn, are combined by the Chinese remainder theorem to obtain the final result (mod m), which is correct to 20 digits.

Even though the lengthy calculation is repeated four times, once for each modulus, most of it only uses five-digit integers and is accomplished quickly without overwhelming the machine's memory. Details of a machine program describing the method together with typical numerical results can be found in Newman (1967). See also Apostol and Niven (1994, pp. 18–19).

27.16 Cryptography

Applications to cryptography rely on the disparity in computer time required to find large primes and to factor large integers.

For example, a code maker chooses two large primes p and q of about 100 decimal digits each. Procedures for finding such primes require very little computer time. The primes are kept secret but their product $n=pq$, a 200-digit number, is made public. For this reason, these are often called public key codes. Messages are coded by a method (described below) that requires only the knowledge of n. But to decode, both factors p and q must be known. With the most efficient computer techniques devised to date (2009), factoring a 200-digit number may require billions of years on a single computer. For this reason, the codes are considered unbreakable, at least with the current state of knowledge on factoring large numbers.

To code a message by this method, we replace each letter by two digits, say $A=01$, $B=02$, …, $Z=26$, and divide the message into pieces of convenient length smaller than the public value $n=pq$. Choose a prime r that does not divide either $p-1$ or $q-1$. Like n, the prime r is made public. To code a piece x, raise x to the power r and reduce x^r modulo n to obtain an integer y (the coded form of x) between 1 and n. Thus, $y\equiv x^r \pmod{n}$ and $1\le y<n$.

To decode, we must recover x from y. To do this, let s denote the reciprocal of r modulo $\phi(n)$, so that $rs=1+t\,\phi(n)$ for some integer t. (Here $\phi(n)$ is Euler's totient (§27.2).) By the Euler–Fermat theorem (27.2.8), $x^{\phi(n)}\equiv 1 \pmod{n}$; hence $x^{t\,\phi(n)}\equiv 1 \pmod{n}$. But $y^s\equiv x^{rs}\equiv x^{1+t\,\phi(n)}\equiv x \pmod{n}$, so y^s is the same as x modulo n. In other words, to recover x from y we simply raise y to the power s and reduce modulo n. If p and q are known, s and y^s can be determined (mod n) by straightforward calculations that require only a few minutes of machine time. But if p and q are not known, the problem of recovering x from y seems insurmountable.

For further information see Apostol and Niven (1994, p. 24), and for other applications to cryptography see Menezes *et al.* (1997) and Schroeder (2006).

27.17 Other Applications

Reed *et al.* (1990, pp. 458–470) describes a number-theoretic approach to Fourier analysis (called the *arithmetic Fourier transform*) that uses the Möbius inversion

(27.5.7) to increase efficiency in computing coefficients of Fourier series.

Congruences are used in constructing perpetual calendars, splicing telephone cables, scheduling round-robin tournaments, devising systematic methods for storing computer files, and generating pseudorandom numbers. Rosen (2004, Chapters 5 and 10) describes many of these applications. Apostol and Zuckerman (1951) uses congruences to construct magic squares.

There are also applications of number theory in many diverse areas, including physics, biology, chemistry, communications, and art. Schroeder (2006) describes many of these applications, including the design of concert hall ceilings to scatter sound into broad lateral patterns for improved acoustic quality, precise measurements of delays of radar echoes from Venus and Mercury to confirm one of the relativistic effects predicted by Einstein's theory of general relativity, and the use of primes in creating artistic graphical designs.

Computation

27.18 Methods of Computation: Primes

An overview of methods for precise counting of the number of primes not exceeding an arbitrary integer x is given in Crandall and Pomerance (2005, §3.7). T. Oliveira e Silva has calculated $\pi(x)$ for $x = 10^{23}$, using the combinatorial methods of Lagarias *et al.* (1985) and Deléglise and Rivat (1996); see Oliveira e Silva (2006). An analytic approach using a contour integral of the Riemann zeta function (§25.2(i)) is discussed in Borwein *et al.* (2000).

The *Sieve of Eratosthenes* (Crandall and Pomerance (2005, §3.2)) generates a list of all primes below a given bound. An alternative procedure is the *binary quadratic sieve* of Atkin and Bernstein (Crandall and Pomerance (2005, p. 170)).

For small values of n, primality is proven by showing that n is not divisible by any prime not exceeding $\sqrt{n}$.

Two simple algorithms for proving primality require a knowledge of all or part of the factorization of $n-1, n+1$, or both; see Crandall and Pomerance (2005, §§4.1–4.2). These algorithms are used for testing primality of *Mersenne numbers*, 2^n-1, and *Fermat numbers*, $2^{2^n}+1$.

The *APR (Adleman–Pomerance–Rumely)* algorithm for primality testing is based on Jacobi sums. It runs in time $O\big((\log n)^{c \log\log\log n}\big)$. Explanations are given in Cohen (1993, §9.1) and Crandall and Pomerance (2005, §4.4). A practical version is described in Bosma and van der Hulst (1990).

The *AKS (Agrawal–Kayal–Saxena)* algorithm is the first deterministic, polynomial-time, primality test. That is to say, it runs in time $O((\log n)^c)$ for some constant c. An explanation is given in Crandall and Pomerance (2005, §4.5).

The *ECPP (Elliptic Curve Primality Proving)* algorithm handles primes with over 20,000 digits. Explanations are given in Cohen (1993, §9.2) and Crandall and Pomerance (2005, §7.6).

27.19 Methods of Computation: Factorization

Techniques for factorization of integers fall into three general classes: *Deterministic algorithms*, *Type I probabilistic algorithms* whose expected running time depends on the size of the smallest prime factor, and *Type II probabilistic algorithms* whose expected running time depends on the size of the number to be factored.

Deterministic algorithms are slow but are guaranteed to find the factorization within a known period of time. Trial division is one example. Fermat's algorithm is another; see Bressoud (1989, §5.1).

Type I probabilistic algorithms include the *Brent–Pollard rho algorithm* (also called *Monte Carlo method*), the *Pollard* $p-1$ *algorithm*, and the *Elliptic Curve Method* (ECM). Descriptions of these algorithms are given in Crandall and Pomerance (2005, §§5.2, 5.4, and 7.4). As of January 2009 the largest prime factors found by these methods are a 19-digit prime for Brent–Pollard rho, a 58-digit prime for Pollard $p-1$, and a 67-digit prime for ECM.

Type II probabilistic algorithms for factoring n rely on finding a pseudo-random pair of integers (x, y) that satisfy $x^2 \equiv y^2 \pmod{n}$. These algorithms include the *Continued Fraction Algorithm* (CFRAC), the *Multiple Polynomial Quadratic Sieve* (MPQS), the *General Number Field Sieve* (GNFS), and the *Special Number Field Sieve* (SNFS). A description of CFRAC is given in Bressoud and Wagon (2000). Descriptions of MPQS, GNFS, and SNFS are given in Crandall and Pomerance (2005, §§6.1 and 6.2). As of January 2009 the SNFS holds the record for the largest integer that has been factored by a Type II probabilistic algorithm, a 307-digit composite integer. The SNFS can be applied only to numbers that are very close to a power of a very small base. The largest composite numbers that have been factored by other Type II probabilistic algorithms are a 63-digit integer by CFRAC, a 135-digit integer by MPQS, and a 182-digit integer by GNFS.

For further information see Crandall and Pomerance (2005) and §26.22.

For current records online, see http://dlmf.nist.gov/27.19.

27.20 Methods of Computation: Other Number-Theoretic Functions

To calculate a multiplicative function it suffices to determine its values at the prime powers and then use (27.3.2). For a completely multiplicative function we use the values at the primes together with (27.3.10). The recursion formulas (27.14.6) and (27.14.7) can be used to calculate the partition function $p(n)$. A similar recursion formula obtained by differentiating (27.14.18) can be used to calculate Ramanujan's function $\tau(n)$, and the values can be checked by the congruence (27.14.20).

For further information see Lehmer (1941, pp. 5–83) and Lehmer (1943, pp. 483–492).

27.21 Tables

Lehmer (1914) lists all primes up to 100 06721. Bressoud and Wagon (2000, pp. 103–104) supplies tables and graphs that compare $\pi(x)$, $x/\log x$, and $\mathrm{li}(x)$. Glaisher (1940) contains four tables: Table I tabulates, for all $n \leq 10^4$: (a) the canonical factorization of n into powers of primes; (b) the Euler totient $\phi(n)$; (c) the divisor function $d(n)$; (d) the sum $\sigma(n)$ of these divisors. Table II lists all solutions n of the equation $f(n) = m$ for all $m \leq 2500$, where $f(n)$ is defined by (27.14.2). Table III lists all solutions $n \leq 10^4$ of the equation $d(n) = m$, and Table IV lists all solutions n of the equation $\sigma(n) = m$ for all $m \leq 10^4$. Table 24.7 of Abramowitz and Stegun (1964) also lists the factorizations in Glaisher's Table I(a); Table 24.6 lists $\phi(n), d(n)$, and $\sigma(n)$ for $n \leq 1000$; Table 24.8 gives examples of primitive roots of all primes ≤ 9973; Table 24.9 lists all primes that are less than 1 00000.

The partition function $p(n)$ is tabulated in Gupta (1935, 1937), Watson (1937), and Gupta *et al.* (1958). Tables of the Ramanujan function $\tau(n)$ are published in Lehmer (1943) and Watson (1949). Lehmer (1941) gives a comprehensive account of tables in the theory of numbers, including virtually every table published from 1918 to 1941. Those published prior to 1918 are mentioned in Dickson (1919). The bibliography in Lehmer (1941) gives references to the places in Dickson's History where the older tables are cited. Lehmer (1941) also has a section that supplies errata and corrections to all tables cited.

No sequel to Lehmer (1941) exists to date, but many tables of functions of number theory are included in Unpublished Mathematical Tables (1944).

27.22 Software

See http://dlmf.nist.gov/27.22.

References

General References

The main references used in writing this chapter are Apostol (1976, 1990), and Apostol and Niven (1994). Further information can be found in Andrews (1976), Erdélyi *et al.* (1955, Chapter XVII), Hardy and Wright (1979), and Niven *et al.* (1991).

Sources

The following list gives the references or other indications of proofs that were used in constructing the various sections of this chapter. These sources supplement the references quoted in the text.

§27.2 Apostol (1976, Chapter 2). For (27.2.11) see Erdélyi *et al.* (1955, p. 168). Tables 27.2.1 and 27.2.2 are from Abramowitz and Stegun (1964, Tables 24.6 and 24.9).

§27.3 Apostol (1976, Chapter 2).

§27.4 Apostol (1976, Chapter 11). For (27.4.10) see Titchmarsh (1986b, p. 4).

§27.5 Apostol (1976, Chapter 2 and p. 228). For (27.5.7) use (27.5.2) and formal substitution.

§27.6 Apostol (1976, Chapter 2).

§27.7 Apostol (1990, Chapter 1).

§27.8 Apostol (1976, Chapter 6).

§27.9 Apostol (1976, Chapter 9).

§27.10 Apostol (1976, Chapter 8).

§27.11 Apostol (1976, Chapters 3, 4). For (27.11.12), (27.11.14), and (27.11.15) see Prachar (1957, pp. 71–74).

§27.12 Crandall and Pomerance (2005, pp. 131–152), Davenport (2000), Narkiewicz (2000), Rosser (1939). For (27.12.7) see Schoenfeld (1976) and Crandall and Pomerance (2005, pp. 37, 60). For the proof that there are infinitely many Carmichael numbers see Alford *et al.* (1994).

§27.13 Apostol (1976, Chapter 14), Ellison (1971), Grosswald (1985, pp. 8, 32). For (27.13.4) see (20.2.3).

§27.14(ii) Apostol (1976, Chapter 14), Apostol (1990, Chapters 3–5).