Chapter 1

Review of Elementary Number Theory

In this chapter, we give a summary on elementary topics which are usually taught in a first course in number theory such as divisibility properties, prime numbers, and congruences. Many theorems in this chapter are given without proof but they can be found in standard texts such as those by Apostol [**18**], Hardy and Wright [**179**], Niven, Zuckerman, and Montgomery [**290**], and Rosen [**348**]. Nevertheless, if the results may be unfamiliar to some readers or if the idea might be useful later, we either give a proof or refer them to a specific reference. Throughout this chapter, the letters a, b, c, d, k, m, n denote integers.

1.1. Divisibility

For $a \neq 0$, we say that a *divides* b or b is *divisible* by a and we write $a \mid b$ if there exists c such that $b = ac$. If a does not divide b, we write $a \nmid b$. As usual, we exclude the division by zero. So if we write $a \mid b$, it is automatically assumed that a is a nonzero integer. Other languages for the divisibility $a \mid b$ are that a is a *divisor* of b, a is a *factor* of b, and that b is a *multiple* of a. In addition, if $a \mid b$ and $0 < a < b$, then a is called a *proper divisor* of b. We also write $a^k \parallel b$ and say that a^k *exactly divides* b or b is *exactly divisible* by a^k if $a^k \mid b$ and $a^{k+1} \nmid b$. Basic properties of divisibility are as follows.

Theorem 1.1. *The following statements hold.*

(i) $1 \mid a$, $a \mid 0$, *and* $a \mid a$.

(ii) $a \mid b$ *and* $b \mid c$ *imply* $a \mid c$.

(iii) $a \mid b$ *implies* $a \mid bx$ *for every* $x \in \mathbb{Z}$.

(iv) $a \mid b$ *if and only if* $ac \mid bc$.

(v) $a \mid b$ *and* $a \mid c$ *imply* $a \mid bx + cy$ *for every* $x, y \in \mathbb{Z}$.

(vi) $a \mid b$ *and* $b \neq 0$ *imply* $|a| \leq |b|$.

(vii) $a \mid b$ *and* $b \mid a$ *imply* $|a| = |b|$.

Theorem 1.2. (Division Algorithm) *Let* $a \in \mathbb{Z}$ *and* $b \in \mathbb{Z} \setminus \{0\}$. *Then there exists a unique pair of integers* q, r *such that* $a = bq + r$ *and* $0 \leq r < |b|$. (*The integer* q *is called the* quotient *and* r *is called the* remainder.)

The reader is perhaps familiar with Theorem 1.2 but there is a different version of the division algorithm as follows.

Theorem 1.3. (Division Algorithm Version 2) *Suppose* $a, b \in \mathbb{R}$ *and* $b \neq 0$. *Then there exists a unique pair* q, r *such that* $q \in \mathbb{Z}$ *and* $r \in \mathbb{R}$, $a = bq + r$, *and* $0 \leq r < |b|$. *In addition, if* $a, b \in \mathbb{Z}$, *then* $r \in \mathbb{Z}$.

Proof. For convenience, we assume that $b > 0$ (the proof is similar for $b < 0$). Since $a \in \mathbb{R} = \bigcup_{q \in \mathbb{Z}} [bq, b(q+1))$, there exists $q \in \mathbb{Z}$ such that $a \in [bq, b(q+1))$. Let $r = a - bq$. Then $a = bq + r$ and $0 \leq r < |b|$, as required. For the uniqueness, if $a = bq_1 + r_1 = bq_2 + r_2$ where $q_1, q_2 \in \mathbb{Z}$ and $0 \leq r_1, r_2 < |b|$, then $|q_1 - q_2| = |r_2 - r_1|/|b| < 1$, which implies $q_1 = q_2$ and $r_1 = r_2$. The rest is obvious. □

1.2. Greatest Common Divisor

If $d \mid a$, then we say that d is a divisor of a. If $d \mid a$ and $d \mid b$, then d is called a *common divisor* of a and b. Suppose that $a \neq 0$ or $b \neq 0$ and let A be the set of common divisors of a and b. Then A is nonempty because $1 \in A$. In addition, by Theorem 1.1(vi), the set A is finite. Therefore the maximum of A exists and we say that d is the *greatest common divisor* of a and b if $d = \max A$, that is, $d \mid a$, $d \mid b$, and $d \geq c$ for every common divisor c of a and b. In this case, we write $d = \gcd(a, b)$ or simply $d = (a, b)$ if no confusion arises. If $(a, b) = 1$, then we say that a and b are relatively prime (or a and b are coprime). We exclude the

case $a = b = 0$ in the definition of $\gcd(a, b)$ because zero is divisible by every positive integer, and hence there is no largest common divisor of a and b. So if we write $\gcd(a, b)$ or (a, b), it is automatically assumed that $a \neq 0$ or $b \neq 0$.

The Euclidean algorithm, a process in which we apply the division algorithm repeatedly, can be used to find $\gcd(a, b)$ for any pair of positive integers a, b and to explicitly obtain $x, y \in \mathbb{Z}$ such that $\gcd(a, b) = ax + by$. More precisely, we have the following result.

Theorem 1.4. (Euclidean Algorithm) *Assume that a, b are positive integers and $q_1, q_2, \ldots, q_{n-1}$, $r_1, r_2, \ldots, r_n$ are integers satisfying the following relations:*

$$\begin{aligned}
a &= bq_1 + r_1, \quad 0 < r_1 < b,\\
b &= r_1q_2 + r_2, \quad 0 < r_2 < r_1,\\
r_1 &= r_2q_3 + r_3, \quad 0 < r_3 < r_2,\\
&\vdots\\
r_{n-3} &= r_{n-2}q_{n-1} + r_{n-1}, \quad 0 < r_{n-1} < r_{n-2},\\
r_{n-2} &= r_{n-1}q_n + r_n, \quad r_n = 0.
\end{aligned}$$

Then r_{n-1}, the last nonzero remainder in these relations, is equal to $\gcd(a, b)$. *Furthermore, by writing the above relations backward as*

$$\begin{aligned}
r_{n-1} &= r_{n-3} - r_{n-2}q_{n-1} = r_{n-3} - (r_{n-4} - r_{n-3}q_{n-2})q_{n-1}\\
&= r_{n-4}(-q_{n-1}) + r_{n-3}(1 + q_{n-2}q_{n-1}) = f_3(r_{n-3}, r_{n-4})\\
&= f_4(r_{n-4}, r_{n-5}) = \cdots = f_{n-2}(r_2, r_1) = f_{n-1}(a, b),
\end{aligned}$$

we obtain $x, y \in \mathbb{Z}$ such that $r_{n-1} = ax + by$. Here for each $i = 3, \ldots, n-2$, we write $f_i(r_{n-i}, r_{n-i-1})$ and $f_{n-1}(a, b)$ to denote linear combinations of r_{n-i} and r_{n-i-1} and of a and b, respectively. In other words, if $d = (a, b)$, then there are $x, y \in \mathbb{Z}$ such that $d = ax + by$.

Example 1.5. Let $a = 372$ and $b = 48$. By the Euclidean algorithm, we obtain $372 = 48(7) + 36$, $48 = 36(1) + 12$, $36 = 12(3) + 0$. In addition, we have

$$12 = 48 - 36(1) = 48 - (372 - 48(7)) = 372(-1) + 48(8).$$

Therefore $(a, b) = 12$ and we can write $12 = ax + by$ where $x = -1$ and $y = 8$. Such a pair (x, y) is not unique. For instance, $12 = ax + by$ also holds when $x = 3$ and $y = -23$. In fact, there are infinitely many

1.13.8 If $n > 1$, prove that the sum

$$\sum_{k=1}^{n} \frac{1}{k}$$

is not an integer.

1.13.9 Show that there are infinitely many $n \in \mathbb{N}$ such that n, $n+1$, $n+2$ are sums of two squares. Show also that any set of four consecutive integers contain an element that is not a sum of two squares.

1.13.10 Let n be a positive integer and let $s(n)$ be the sum of digits of n in its decimal representation. Show that the following statements hold.

(i) $9 \mid s(n) - n$.
(ii) $s(m+n) \leq s(m) + s(n)$ (subadditivity property).
(iii) $s(mn) \leq \min(ms(n), ns(m))$.
(iv) $s(mn) \leq s(m)s(n)$ (submultiplicativity property).

1.13.11 Let $a, b, c \in \mathbb{Z}$, $m \in \mathbb{N}$, and $d = (a, b, m)$. Show that if the linear congruence in two variables $ax + by \equiv c \pmod{m}$ has a solution, then it has exactly dm incongruent solutions modulo m. Here we say that two solutions (x_1, y_1) and (x_2, y_2) are incongruent modulo m if $x_1 \not\equiv x_2 \pmod{m}$ and $y_1 \not\equiv y_2 \pmod{m}$.

1.13.12 Let $m_1, m_2, \ldots, m_k$ be pairwise relatively prime positive integers, $M = m_1 m_2 \cdots m_k$, and $M_j = M/m_j$ for $j = 1, 2, \ldots, k$. Show that $a_1 M_1 + a_2 M_2 + \cdots + a_k M_k$ runs through a complete residue system modulo M when $a_1, a_2, \ldots, a_k$ run through a complete residue system modulo $m_1, m_2, \ldots, m_k$, respectively. Show that the result also holds if

$$a_1 M_1 + a_2 M_2 + \cdots + a_k M_k$$

is replaced by

$$a_1 + a_2 m_1 + a_3 m_1 m_2 + \cdots + a_k m_1 m_2 \cdots m_{k-1}.$$

1.14. Notes

It is not difficult to show that every $n \geq 12$ can be written as a sum of two composite numbers (see Exercise 1.13.3). On the other hand, Goldbach conjectured in 1742 that every even number $n \geq 4$ is a sum of two primes but this problem is open and seems very difficult. Various partial results

have been obtained by many mathematicians. Here we mention a few. Vinogradov [**428**] proved that there exists a large number N such that every odd integer $n \geq N$ is a sum of three primes. Then about 76 years later, Helfgott [**184**] showed that we can take $N = 7$. Chen [**81**] obtained the result very close to Goldbach's conjecture by proving that every large even number can be written as a sum of a prime and a number that has at most two prime factors. For more details, we refer the reader to the books by Hua [**202**] and Vaughan [**422**].

Exercise 1.13.4 is connected with *Mersenne primes*, the primes of the form $2^p - 1$ where p is a prime. We know from Euclid's result (Theorem 1.12) that there exist infinitely many primes but we do not know whether or not the number of Mersenne primes is infinite. The sequence of primes and the sequence of those p such that $2^p - 1$ is prime are given, respectively, as A000040 and A000043 in the On-Line Encyclopedia of Integer Sequences (OEIS). Mersenne primes are also strongly related to *perfect numbers*, the positive integers that are equal to the sum of their proper divisors. In other words, if $\sigma(n)$ denotes the sum of all positive divisors of n, then n is perfect if and only if $\sigma(n) = 2n$. For instance, 6 and 28 are perfect as

$$\sigma(6) = 1 + 2 + 3 + 6 = 2 \times 6 \quad \text{and}$$
$$\sigma(28) = 1 + 2 + 4 + 7 + 14 + 28 = 2 \times 28.$$

Euler showed that an even number n is perfect if and only if

$$n = 2^{p-1}(2^p - 1),$$

where p and $2^p - 1$ are primes. We do not know whether or not there are infinitely many even perfect numbers. We cannot find an odd perfect number and we do not have a proof that such a number does not exist either.

As of November 2022, the largest known prime, which is a Mersenne prime, is $2^{82589933} - 1$ and thus the largest known perfect number is $2^{82589932}(2^{82589933} - 1)$. For more information on the search of Mersenne primes, we recommend the reader to follow the Great Internet Mersenne Prime Search (GIMPS). For the list of perfect numbers, see A000396 in OEIS.

Attempting to understand perfect numbers better, mathematicians have studied other closely related concepts: if $\sigma(n) < 2n$, then n is said to be deficient; if $\sigma(n) > 2n$, then n is abundant; if $\sigma(n) = 2n + 1$, then

n is quasiperfect; if $\sigma(n) = 2n - 1$, then n is almost perfect. For more information on this topic, see for example the online databases GIMPS [**157**] and OEIS [**374**].

Sierpiński [**368**] called n *pseudoperfect* if n can be written as a sum of some of its proper divisors. Pollack and Shevelev [**303**] initiated the study of a subclass of pseudoperfect numbers: n is *near-perfect* if n is the sum of all of its proper divisors except one of them; n is *exactly k-near-perfect* if n is expressible as a sum of all of its proper divisors with exactly k exceptions.

Tang, Ren, and Li [**403**] defined the notion of deficient-perfect numbers in a similar way: n is called a *deficient-perfect number with a deficient divisor d* if d is a proper divisor of n and $\sigma(n) = 2n - d$; n is *exactly k-deficient-perfect with deficient divisors $d_1, d_2, \ldots, d_k$* if $d_1, d_2, \ldots, d_k$ are distinct proper divisors of n and

$$\sigma(n) = 2n - (d_1 + d_2 + \cdots + d_k).$$

In 2012, Pollack and Shevelev [**303**] showed that if k is fixed and is large enough, then there are infinitely many exactly k-near-perfect numbers. A year later, Ren and Chen [**341**] determined all near-perfect numbers n that have $\omega(n) = 2$ and we can see from this classification that all such n are even. Here and throughout this book, $\omega(n)$ denotes the number of distinct prime divisors of n. Tang, Ren, and Li [**403**] proved that there is no odd near-perfect number n with $\omega(n) = 3$ and found all deficient-perfect numbers m with $\omega(m) \leq 2$. After that, Tang and Feng [**401**] extended it by showing that there is no odd deficient-perfect number n with $\omega(n) = 3$. Tang, Ma, and Feng [**402**] obtained in 2016 the only odd near-perfect number with $\omega(n) = 4$, namely, $n = 3^4 \cdot 7^2 \cdot 11^2 \cdot 19^2$, while Sun and He [**390**] asserted in 2019 that the only odd deficient-perfect number n with $\omega(n) = 4$ is $n = 3^2 \cdot 7^2 \cdot 11^2 \cdot 13^2$. Cohen et al. [**87**] improved the estimate of Pollack and Shevelev [**303**] on the number of near-perfect numbers $\leq x$. Hence, most results in the literature were devoted to characterizing, only when $k = 1$, the exactly k-near-perfect or exactly k-deficient-perfect numbers. Chen [**80**] started a slightly new direction by determining all 2-deficient-perfect numbers n with $\omega(n) \leq 2$. Finally, Aursukaree and the author of this book [**21**] have recently proved that the only odd exactly 3-deficient-perfect number with at most two distinct prime factors is $1521 = 3^2 \cdot 13^2$. We also plan to discover more about these numbers in the future.

Exercise 1.13.5 is about Fermat numbers. The number of the form $2^{2^n}+1$ is prime for $n = 1, 2, 3, 4$ and Fermat believed that it is a prime for all n. However, Euler showed that $2^{2^5}+1$ is composite. By using computer programming, it is known that $2^{2^n}+1$ is composite for $5 \leq n \leq 21$, and it is conjectured that there are only a finite number of n such that $2^{2^n}+1$ is prime.

Exercise 1.13.6 is a well known property of the Fibonacci numbers. More problems on these numbers are also given in later chapters. The books by Koshy [**230**] and Vajda [**418**] show various classical results on F_n. For more up-to-date information and research problems on F_n, its companion Lucas numbers, and other recurrence sequences, we refer the reader to the *Fibonacci Quarterly* and other publications of the Fibonacci Association. The Fibonacci and Lucas sequences are A000045 and A000032 in OEIS, respectively.

Exercise 1.13.7 shows that if $a, b \in \mathbb{N}$ and $(a, b) = 1$, then the largest positive integer that cannot be written as $ax + by$ for some $x, y \in \mathbb{N}$ is ab. This problem is actually related to a concept of Frobenius numbers. Suppose that $a_1, a_2, \ldots, a_n$ are positive integers and $(a_1, a_2, \ldots, a_n) = 1$. Then every positive integer m can be written as $m = a_1x_1 + a_2x_2 + \cdots + a_nx_n$ for some $x_1, x_2, \ldots, x_n \in \mathbb{Z}$. If we restrict our attention only to the case when $n \geq 2$ and $x_1, x_2, \ldots, x_n$ are nonnegative integers, then there is a finite number of $m \in \mathbb{N}$ that can not be written as $a_1x_1 + a_2x_2 + \cdots + a_nx_n$. The largest such integer is called the Frobenius number of $\{a_1, a_2, \ldots, a_n\}$ and is denoted by $g(a_1, a_2, \ldots, a_n)$. It is well known that $g(a, b) = ab - a - b$ for all relatively prime positive integers a, b. Tripathi [**414**] also obtained in 2017 formulas for $g(a, b, c)$ for all $a, b, c \in \mathbb{N}$ with $(a, b, c) = 1$. However, a general formula for the Frobenius number of more than three variables is not known. For other recent results on Frobenius numbers, see for instance [**284**, **346**, **385**, **413**].

By considering the highest power of 2, we obtain a proof of Exercise 1.13.8. A similar idea can be used to show that the sum $\sum_{m \leq k \leq n} \frac{1}{k}$ is not an integer for any $n > m \geq 1$. Erdös extended this to the sum of reciprocals of positive integers in an arithmetic progression. Belbachir and Khelladi [**42**] generalized Erdös' result further and obtained that for $a, d, k \in \mathbb{N}$ and $k \geq 2$, the sum

$$\frac{1}{a^{\alpha_0}} + \frac{1}{(a+d)^{\alpha_1}} + \cdots + \frac{1}{(a+(k-1)d)^{\alpha_{k-1}}}$$

is never an integer for all positive rational numbers $\alpha_0, \alpha_1, \ldots, \alpha_{k-1}$. In fact, the reciprocal sum of an integer sequence is of general interest in mathematics and theoretical physics as proposed by Bayless and Klyve [**39**], and by Roggero, Nardelli, and Di Noto [**347**]. See also the work of Nguyen and Pomerance [**288**] on the reciprocal sum of the amicable numbers, the preprint of Kinlaw, Kobayashi, and Pomerance [**226**] on the reciprocal sum of the positive integers n satisfying $\varphi(n) = \varphi(n+1)$, the article by Lichtman [**244**] on the reciprocal sum of primitive nondeficient numbers, and the recent paper by Phunphayap and Pongsriiam [**295**] on the reciprocal sum of b-adic palindromes. Here amicable numbers are the pairs of positive integers m, n such that $\sigma(m) = \sigma(n) = m+n$; φ is the Euler function, and b-adic palindromes are the positive integers n such that the representation of n in base b reads the same backward as forward. There are actually many results in the literature concerning sums of unit fractions and we refer the reader to [**19**, **94**, **112**, **148**–**150**, **408**] and references therein for more information.

Let A_k be the set of positive integers n such that n, $n+1$, …, $n+k-1$ are sums of two squares. By Exercise 1.13.9, we know that A_k is an infinite set for $k = 1, 2, 3$ and that $A_k = \emptyset$ for all $k \geq 4$. The integers in A_1, A_2, and A_3 are given, respectively, as sequences A001481, A140612, and A082982 in OEIS. In 1908, Landau [**239**] showed that the number of positive integers $\leq x$ that are a sum of two squares is asymptotic to $\frac{cx}{\sqrt{\log x}}$ where c is an explicitly given constant. That is,

$$A_1(x) := \sum_{\substack{n \leq x \\ n \in A_1}} 1 \sim \frac{cx}{\sqrt{\log x}}. \tag{1.5}$$

The concept of asymptotic relations will be explained in Chapter 3 but for now the reader can think of it as a good approximation. So (1.5) basically says that the left-hand side of (1.5) can be well approximated by $\frac{cx}{\sqrt{\log x}}$. In the following discussion, c with or without subscripts denotes a positive constant which does not depend on n or x. Rieger [**345**] showed in 1965 that there exists a constant $c_1 > 0$ such that for all $x \geq 2$

$$A_2(x) := \sum_{\substack{n \leq x \\ n \in A_2}} 1 \leq \frac{c_1 x}{\log x}.$$

About nine years later, Hooley [**191**, **192**] and Indlekofer [**207**] using different methods established that there is a constant $c_2 > 0$ such that

$$A_2(x) := \sum_{\substack{n \le x \\ n \in A_2}} 1 \ge \frac{c_2 x}{\log x}$$

for all $x \ge 2$. Therefore we say that the order of magnitude of $A_2(x)$ is $x/\log x$ and write $A_2(x) \asymp x/\log x$ for $x \ge 2$. Then in 1987, Cochrane and Dressler [**86**] used Selberg's sieve to obtain an upper bound

$$A_3(x) := \sum_{\substack{n \le x \\ n \in A_3}} 1 \le \frac{c_3 x}{(\log x)^{\frac{3}{2}}}.$$

However, the order of magnitude of $A_3(x)$ is not known. Although topics on squares might seem easy, they actually contain many open and difficult questions. Here we mention but a few. Let $(a_n)_{n\ge1} = (1, 2, 4, 5, 8, \ldots)$ be the increasing sequence of positive integers that can be written as a sum of two squares. In 1974, Bambah and Chowla [**28**] showed that there exists a constant $c_4 > 0$ such that for all $n \ge 1$, $a_{n+1} - a_n \le c_4 a_n^{1/4}$ and they believed that the exponent of the upper bound should be improved to a number smaller than 1/4 but it is still unsolved. Refining Lagrange's four-square theorem, Sun [**388**] showed that every positive integer can be written as $x^2 + y^2 + z^2 + w^2$ where $x, y, z, w \in \mathbb{Z}$ and $x+y+z$ is a square. He also posed several conjectures in his article [**388**] and on his homepage [**389**]. For example, his 1-3-5 conjecture states that any positive integer can be written as the sum of four squares of nonnegative integers x, y, z, w such that $x + 3y + 5z$ is also a square. He has offered 1,350 US dollars for the first solution to this problem, but it is still open. For partial answers, see the recent article by Wu and Sun [**438**]. Finally, a famous conjecture on the existence of primes between squares states that for each $n \in \mathbb{N}$, there is a prime p lying between n^2 and $(n+1)^2$. This has been verified by using a computer for $n \le 10^6$ but we can neither find a proof nor a counterexample.

Exercise 1.13.10 gives elementary properties of the sum of digits function and is easy to prove. However, the study of this function is not trivial. In fact, there are many interesting questions concerning this function; see for example, Gelfond's sum of digits problems as collected in Morgenbesser's thesis [**276**] and references therein.

It is well known that $(a,b)[a,b] = ab$ for every $a, b \in \mathbb{N}$, and generalizations of this are given in Theorem 1.17 and Exercise 1.13.1, respectively. The $\gcd(A)$ for any nonempty set A of nonzero integers is introduced at the end of Section 1.2 and in Exercise 1.13.2. If $\gcd(A) = 1$, then A is said to be a relatively prime set and if $\gcd(a_1, a_2) = 1$ for every distinct pair $a_1, a_2 \in A$, then A is called a pairwise relatively prime set. A similar concept was introduced by Erdös: A is called a primitive set if $a \nmid b$ for any distinct elements $a, b \in A$. So if A is the empty set or a singleton set, then A is a primitive set and if $|A| \geq 2$, then $1 \notin A$.

The number $f(n)$ of relatively prime subsets of $\{1, 2, \ldots, n\}$ was given by Nathanson [**282**] and generalized by various researchers including the author of this book. The sequence $(f(n))_{n\geq 1}$ is listed as A085945 in OEIS. See also A027375, A038199, and A224840 for related sequences. For more information on this topic, we refer the reader to Pongsriiam [**313**–**315**] and references therein.

On the other hand, a conjecture of Cameron and Erdös [**72**] on the number $g(n)$ of primitive subsets of $\{1, 2, \ldots, n\}$ has recently been solved by Angelo [**16**]. That is, $\lim_{n\to\infty} g(n)^{\frac{1}{n}}$ exists. There are other interesting theorems on primitive sets too. For instance, by Besicovitch's result [**52**], we know that the upper asymptotic density of a primitive set can be arbitrarily close to $1/2$ while the lower asymptotic density is always 0. The reciprocal sum of the elements of a primitive set can diverge but Erdös [**114**] showed that for any primitive set $A \subseteq \mathbb{N} \setminus \{1\}$,

$$\sum_{a\in A} \frac{1}{a \log a} \quad \text{converges.}$$

In fact, the proof shows that the sums are uniformly bounded on all primitive sets $A \subseteq \mathbb{N} \setminus \{1\}$. In fact, Erdös conjectured that for any primitive set $A \subseteq \mathbb{N} \setminus \{1\}$, we have

$$\sum_{a\in A} \frac{1}{a \log a} \leq \sum_{p} \frac{1}{p \log p},$$

where p runs over all prime numbers. Lichtman and Pomerance [**246**] made some contributions, and Lichtmann [**245**] has recently solved this problem.

Chapter 2

Arithmetic Functions I

2.1. Introduction

An *arithmetic function* (or a *number-theoretic function*) is a complex-valued function defined on the set of positive integers. In this section, we give the definitions of certain arithmetic functions which play an important role in the study of divisibility properties of integers and the distribution of prime numbers. Then we focus our attention on functions which have multiplicative properties, a concept to be defined in Section 2.2. We introduce in Section 2.3 the concept of Dirichlet convolution which enables us to prove various identities in Sections 2.4 and 2.5. Although many results in this chapter are known to undergraduate students, our presentation here is new. In particular, reading the definitions and proofs will help the readers get familiar with elementary calculations in analytic number theory.

Definition 2.1. The functions $\varphi, d, \sigma, 1, N, e, \mu, \lambda : \mathbb{N} \to \mathbb{C}$ are defined by

$$\begin{aligned}
\varphi(n) &= \text{ the number of integers } k \text{ such that } 1 \le k \le n \text{ and } (k,n) = 1,\\
d(n) &= \text{ the number of positive divisors of } n,\\
\sigma(n) &= \text{ the sum of positive divisors of } n,\\
1(n) &= 1 \text{ for every } n \in \mathbb{N},\\
N(n) &= n \text{ for every } n \in \mathbb{N},
\end{aligned}$$

Chapter 3

The Floor Function

3.1. Introduction

The origin of the greatest integer function is difficult to establish but it has been found quite commonly in the literature since the 1880s. Gauss, Dirichlet, Legendre, Sylvester, Kronecker, and many other mathematicians used it. A brief history of this function and a collection of its basic properties can also be found in the master theses by Murray [**279**] and by Haertel [**166**]. There were two popular symbols for the largest integer not exceeding x, namely $E(x)$ and $[x]$. Then Iverson [**210**] introduced in 1962 a new name and notation for this function which are now more popular and widely used in number theory and combinatorics. In this text, we follow Iverson and use $\lfloor x \rfloor$ instead of $E(x)$ or $[x]$, and call it the floor function. The definition of the floor and related functions are given as follows:

Definition 3.1. For each $x \in \mathbb{R}$, let $\lfloor x \rfloor$ be the largest integer less than or equal to x and let $\lceil x \rceil$ be the smallest integer larger than or equal to x. We call $\lfloor x \rfloor$ the *floor function* (or the *greatest integer function*) of x and call $\lceil x \rceil$ the *ceiling function* (or the *least integer function*) of x. In addition, we define $\{x\} = x - \lfloor x \rfloor$ and call $\{x\}$ the *fractional part* of x. Moreover, $\lfloor x \rfloor$ is sometimes called the *integer part* of x.

For instance, we have $\lfloor 2.5 \rfloor = 2$, $\lceil 2.5 \rceil = 3$, $\{2.5\} = 0.5$, $\lfloor -3.1 \rfloor = -4$, $\lceil -3.1 \rceil = -3$, $\{-3.1\} = 0.9$, $\lfloor \pi \rfloor = 3$, $\lceil \pi \rceil = 4$, and $\{\pi\} = \pi - 3$. Iverson

also introduced another notation using a bracket which is not used often in this book but is a very convenient tool in some calculations. See the notes in Section 3.6 for more details.

Definition 3.2. If P is a mathematical statement, then the *Iverson bracket* $[P]$ is defined by

$$[P] = \begin{cases} 1, & \text{if } P \text{ is true;} \\ 0, & \text{if } P \text{ is false.} \end{cases}$$

So, for example, [2 is a prime] $= 1$, [5 is composite] $= 0$, and [2+5 $=$ 7] $= 1$.

The following are basic properties of the floor and ceiling functions, which are applied throughout this chapter, sometimes without reference.

Theorem 3.3. *Let x, y be real numbers and let m, n be integers. Then the following statements hold.*

(i) $\lfloor x \rfloor \le x < \lfloor x \rfloor + 1$, $\lceil x \rceil - 1 < x \le \lceil x \rceil$, *and* $0 \le \{x\} < 1$. *In fact,* $\lfloor x \rfloor$ *is the unique integer* n *such that* $n \le x < n + 1$. *Similarly,* $\lceil x \rceil$ *is the unique integer satisfying*

$$\lceil x \rceil - 1 < x \le \lceil x \rceil .$$

(ii) $\lfloor x \rfloor = x \Leftrightarrow x \in \mathbb{Z} \Leftrightarrow \lceil x \rceil = x$,
$\lfloor x \rfloor = n \Leftrightarrow n \le x < n + 1 \Leftrightarrow x - 1 < n \le x$,
$\lceil x \rceil = n \Leftrightarrow n - 1 < x \le n \Leftrightarrow x \le n < x + 1$.

(iii) $\lfloor x + n \rfloor = \lfloor x \rfloor + n$, $\lceil x + n \rceil = \lceil x \rceil + n$, $\{x + n\} = \{x\}$.

(iv) $\lceil x \rceil - \lfloor x \rfloor = \begin{cases} 0, & \text{if } x \in \mathbb{Z}; \\ 1, & \text{if } x \notin \mathbb{Z}. \end{cases}$

(v) $\lfloor -x \rfloor = -\lceil x \rceil$, $\lceil -x \rceil = -\lfloor x \rfloor$,

$$\lfloor -x \rfloor = \begin{cases} -\lfloor x \rfloor, & \text{if } x \in \mathbb{Z}; \\ -\lfloor x \rfloor - 1, & \text{if } x \notin \mathbb{Z}, \end{cases}$$

$$\lceil -x \rceil = \begin{cases} -\lceil x \rceil, & \text{if } x \in \mathbb{Z}; \\ -\lceil x \rceil + 1, & \text{if } x \notin \mathbb{Z}. \end{cases}$$

$$\{-x\} = \begin{cases} 0, & \text{if } x \in \mathbb{Z}; \\ 1 - \{x\}, & \text{if } x \notin \mathbb{Z}. \end{cases}$$

$\left\lfloor x + \frac{1}{2} \right\rfloor$ *is the nearest integer to* x. *If two integers are equally near to* x, *it is the larger of the two. In addition,* $-\left\lfloor -x + \frac{1}{2} \right\rfloor$ *is*

the nearest integer to x and if two integers are equally near to x, it is the smaller of the two.

(vi) *The floor and ceiling functions are increasing on $\mathbb{R}$ (but are not strictly increasing on $\mathbb{R}$). That is,*

$$x < y \text{ implies } \lfloor x \rfloor \leq \lfloor y \rfloor \text{ and } \lceil x \rceil \leq \lceil y \rceil .$$

In addition, we have

$$\begin{aligned} x < n &\Leftrightarrow \lfloor x \rfloor < n, \\ x \geq n &\Leftrightarrow \lfloor x \rfloor \geq n, \\ x \leq n &\Leftrightarrow \lceil x \rceil \leq n, \\ x > n &\Leftrightarrow \lceil x \rceil > n. \end{aligned}$$

(vii) $0 \leq \lfloor x + y \rfloor - \lfloor x \rfloor - \lfloor y \rfloor \leq 1$. *More precisely,*

$$\lfloor x + y \rfloor = \begin{cases} \lfloor x \rfloor + \lfloor y \rfloor , & \text{if } \{x\} + \{y\} < 1; \\ \lfloor x \rfloor + \lfloor y \rfloor + 1, & \text{if } \{x\} + \{y\} \geq 1. \end{cases}$$

(viii) $\left\lfloor \frac{\lfloor x \rfloor}{n} \right\rfloor = \left\lfloor \frac{x}{n} \right\rfloor$ *and* $\left\lceil \frac{\lceil x \rceil}{n} \right\rceil = \left\lceil \frac{x}{n} \right\rceil$ *for* $n \geq 1$.

Proof. We begin with (i). By the definition of $\lfloor x \rfloor$, we immediately obtain the inequality $\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$ and by this and the definition of $\{x\}$, we see that $0 \leq \{x\} < 1$. Similarly, $\lceil x \rceil - 1 < x \leq \lceil x \rceil$. If n is an integer satisfying, $n \leq x < n + 1$, then n is the largest integer that is less than or equal to x, and so $n = \lfloor x \rfloor$. The uniqueness of $\lceil x \rceil$ can be obtained similarly. This proves (i). Then (ii) follows immediately from (i). Since (iii) to (vi) can be proved by using a similar idea, we only give a proof of (iv) and some parts of (v).

For (iv), if $x \in \mathbb{Z}$, then the result is easily verified. So suppose $x \notin \mathbb{Z}$. Then $m < x < m + 1$ for some $m \in \mathbb{Z}$. Then

$$\lceil x \rceil - \lfloor x \rfloor = (m + 1) - m = 1,$$

which proves (iv). In addition, $-m - 1 < -x < -m$, so

$$\lfloor -x \rfloor = -m - 1 = -\lfloor x \rfloor - 1, \quad \lceil -x \rceil = -m = -\lceil x \rceil + 1,$$

which proves some parts of (v). The rest of (iii) to (vi) is left to the reader.

For (vii), suppose that $m \leq x < m + 1$ and $n \leq y < n + 1$. Then $m + n \leq x + y < m + n + 2$. Therefore $\lfloor x + y \rfloor = m + n$ or $m + n + 1$,

Chapter 4

Summation Formulas

4.1. Introduction

The Riemann integral is defined as the limit of Riemann sums. In this sense, an integral can be approximated by a suitable sum and the readers might recall this from an exercise in calculus, real analysis, or numerical analysis courses. Conversely, a sum can also be estimated by a certain integral and we will do this in this chapter. Generally speaking, whenever we estimate A by B, we should also know how close A and B are, or how large (or small) the errors $|A-B|$ or $|(A-B)/B|$ are. Therefore it is convenient to use a specific notation to indicate the size of the error occurring in the approximation or to compare the order of magnitude of functions. For example, both $(\log x)^3$ and x^2 tend to ∞ as $x \to \infty$ but x^2 grows more rapidly than $(\log x)^3$. More precisely, $\lim_{x\to\infty} \frac{(\log x)^3}{x^2} = 0$, which can be written by using the little o notation as $(\log x)^3 = o(x^2)$. We will discuss this in more detail in the next section. Then we will give various basic summation formulas in subsequent sections. To prove such formulas conveniently, we also give a review on the Riemann-Stieltjes integral in Section 4.5. Finally, we remind the reader that $\log x$ is always the natural logarithm of x (not the common logarithm of x) throughout this text.

4.2. Big O, Little o, and Related Notations

To compare the order of magnitude of functions, the notations such as O, o, $\sim$, $\ll$, and $\gg$ are used regularly in the literature and they are explained in this section. The notations $\ll$ and $\gg$ are introduced by Vinogradov and are popular among number theorists. Other symbols are also standard in number theory (see also the notes in Section 4.9). However, we should remark that they may be used in physics and other branches of mathematics or computer science with a different meaning. For example, one sometimes writes $f(x) \prec g(x)$ to mean that $f(x) = o(g(x))$ but we do not use $f(x) \prec g(x)$ in this text.

4.2.1. Big O and Vinogradov notations. Let a be a nonnegative real number, $f, g : [a, \infty) \to \mathbb{R}$, and $g(x) > 0$ for all $x \in [a, \infty)$. Then we write $f(x) = O(g(x))$ if there exists a constant $M > 0$ such that

$$|f(x)| \le Mg(x) \quad \text{for all } x \in [a, \infty).$$

In particular, $f(x) = O(1)$ if f is bounded on $[a, \infty)$. The order of magnitude of functions is sometimes considered in a neighborhood of a real number or of infinity. We write $f(x) = O(g(x))$ as $x \to \infty$ if there exist $a_0 \ge a$ and $M > 0$ such that $|f(x)| \le Mg(x)$ for all $x \ge a_0$. If $c \in [a, \infty)$, then we write $f(x) = O(g(x))$ as $x \to c$ if there exist $\delta > 0$ and $M > 0$ such that

$$|f(x)| \le Mg(x) \text{ for all } x \in (c - \delta, c + \delta) \cap [a, \infty).$$

In this text, when we use the big O notation, we usually consider the functions in the whole domain. To make it clear, we sometimes write the statements such as

"uniformly for $x \ge a$, $f(x) = O(g(x))$"or
"$f(x) = O(g(x))$ for $x \ge a$"

to mean that there exists a constant $M > 0$ such that $|f(x)| \le Mg(x)$ for all $x \ge a$. As usual, if we write $O(g(x))$ it is assumed that $g(x) > 0$ for all x in the specified domain.

For Vinogradov's notation, $f(x) \ll g(x)$ is the same as $f(x) = O(g(x))$ and $f(x) \gg g(x)$ means $g(x) \ll f(x)$. Nevertheless, if we write $f(x) \gg g(x)$, then it is assumed that both $f(x)$ and $g(x)$ are positive for all x in the domains.

The advantage of using Vinogradov's notation is that it is more convenient when we have a chain of estimates such as

$$f(x) \ll f_1(x) \ll f_2(x) \ll f_3(x) \text{ or } g(x) \gg f_4(x) \gg f_5(x).$$

As in a regular inequality, $f(x) \ll f_1(x) \ll f_2(x)$ means that

$$f(x) \ll f_1(x) \text{ and } f_1(x) \ll f_2(x).$$

On the other hand, if $f(x) - g(x) \ll h(x)$, it is often better to write $f(x) = g(x) + O(h(x))$. Finally, if $f(x) \ll g(x)$ and $g(x) \ll f(x)$, then we say that f and g *have the same order of magnitude* and write $f(x) \asymp g(x)$.

4.2.2. Little o notation and asymptotic relation $\sim$. Again, let $f, g : [a, \infty) \to \mathbb{R}$, $a \geq 0$, and $g(x) > 0$ for all $x \in [a, \infty)$. We write $f(x) = o(g(x))$ as $x \to \infty$ if $\lim_{x\to\infty} \frac{f(x)}{g(x)} = 0$. If $c \in [a, \infty)$ is a fixed real number, then we write $f(x) = o(g(x))$ as $x \to c$ if $\lim_{x\to c} \frac{f(x)}{g(x)} = 0$. Nevertheless, in this text, we do not consider the relation $f(x) = o(g(x))$ as x approaches a point in $[a, \infty)$. So we simply write $f(x) = o(g(x))$ to mean $f(x) = o(g(x))$ as $x \to \infty$. In addition, we say that the functions f and g are *asymptotic* (or *asymptotically equivalent*) and we write

$$f(x) \sim g(x) \text{ if } \lim_{x\to\infty} \frac{f(x)}{g(x)} = 1.$$

As in the case of big O, when we write $f(x) = o(g(x))$, it is automatically assumed that $g(x) > 0$ for all x in the specified domain. For $f(x) \sim g(x)$, we only need $g(x) \neq 0$ for all large x (but we still focus only on the case $g(x) > 0$). To help the readers get familiar with these symbols, we provide several examples as follows.

Example 4.1. Uniformly for $x \geq 1$, we have

(i) $3x^4 + 5x^3 + 10x + 1 = O(x^4)$,
(ii) $\frac{2}{x^2} + \frac{1}{x} + 1 = O(1)$,
(iii) $3x + (\log 5x)^4 \ll x$,
(iv) $e^x \cos x \ll e^x$.

Solution. For all $x \geq 1$, we have

$$\left|3x^4 + 5x^3 + 10x + 1\right| \leq 3x^4 + 5x^4 + 10x^4 + x^4 \leq 19x^4.$$

So (i) is proved. For (ii) and (iv), we have

$$|2/x^2 + 1/x + 1| \leq 2 + 1 + 1 = 4 \text{ and } |e^x \cos x| \leq e^x.$$

Chapter 5

Arithmetic Functions II

5.1. Introduction

Previously, we obtained various identities for the arithmetic functions d, φ, σ, μ, e, N, and Λ. In this chapter, we give some analytic results concerning these functions and their combinations. Suppose f is an arithmetic function. Then some of the following questions may be considered. Does the limit $\lim_{n\to\infty} f(n)$ exist? If it exists, what is its value? If it does not exist, what is the value of $\liminf_{n\to\infty} f(n)$ and $\limsup_{n\to\infty} f(n)$? Can we obtain some nontrivial bounds for $f(n)$? Can we find an asymptotic formula for the sum $\sum_{n\le x} f(n)$?

Consider, for example, the divisor function. It is easy to see that $d(n) = 2$ for infinitely many n (when n is prime) and $d(n)$ can be arbitrarily large (for instance when n is a product of k distinct primes and k is large). Therefore

$$\liminf_{n\to\infty} d(n) = 2, \quad \limsup_{n\to\infty} d(n) = \infty,$$

and it is interesting to find a nontrivial upper bound $g(n)$ for $d(n)$ such that

$$0 < \limsup_{n\to\infty} d(n)/g(n) < \infty.$$

Similarly, for the Euler function, we have

$$\lim_{n\to\infty} \varphi(n) = +\infty, \quad \limsup_{n\to\infty} \varphi(n)/n = 1,$$

and if $f(n) = e^{-\gamma} n/\log\log n$ and γ is Euler's constant, then

$$\liminf_{n\to\infty} \varphi(n)/f(n) = 1.$$

We explain more about this in Section 5.4. Since $d(n)$ and the values of many arithmetic functions oscillate considerably as n increases, it is of interest to study their mean values or average orders (see Definition 5.1). For example, by calculating the partial sum $\sum_{n\le x} \omega(n)$ and using Turán's method, one can obtain that almost all positive integers n have $\log\log n$ prime factors. More precisely, if $\varepsilon > 0$ is given, then

$$\lim_{x\to\infty} \frac{1}{x} \#\left\{n \in \mathbb{N} \mid 2 \le n \le x \text{ and } \left|\frac{\omega(n)}{\log\log n} - 1\right| < \varepsilon\right\} = 1.$$

The precise definitions of mean value, average order, extremal order, and normal order are as follows.

Definition 5.1. Let f be an arithmetic function. Then the *mean value* (or the *average value*) of f over the interval $[1, x]$ is defined to be

$$F(x) = \frac{1}{x} \sum_{n\le x} f(n).$$

If $\lim_{x\to\infty} F(x)$ exists, then the limit is called the *asymptotic mean value* of f. In addition, if g is a monotone function such that

$$F(x) \sim \frac{1}{x} \sum_{n\le x} g(n),$$

then we say that $g(n)$ is an *average order* of $f(n)$.

If P is a mathematical property, then the statement "g is eventually P" means that $g(n)$ satisfies P for all large values of n. For example, g is eventually positive means that there exists $N \in \mathbb{N}$ such that $g(n) > 0$ for all $n \ge N$. We use the term "eventually P" in the following definitions.

Definition 5.2. Suppose that g is eventually positive and eventually monotone. Then g is a *maximal order* of f if

$$\limsup_{n\to\infty} f(n)/g(n) = 1,$$

and that g is a *minimal order* of f if $\liminf_{n\to\infty} f(n)/g(n) = 1$.

Definition 5.3. Suppose that g is eventually positive and eventually monotone. Then $f(n)$ has *normal order* $g(n)$ if for every $\varepsilon > 0$,

$$\lim_{x\to\infty} \left(\frac{1}{x} \#\{n \le x : |f(n) - g(n)| < \varepsilon g(n)\}\right) = 1.$$

(iii) $\sum_{2\le n\le x} (\Omega(n) - \log\log n)^2 \ll x \log\log x$.

(iv) If $\delta > 0$ is given, then

$$\#\left\{2 \le n \le x : |\Omega(n) - \log\log n| > (\log\log n)^{\frac{1}{2}+\delta}\right\} = o(x).$$

(v) $\Omega(n)$ has normal order $\log\log n$.

5.6.31 Let $\alpha > 1$. Show that the minimal order of $\sigma_\alpha(n)$ is n^α and a maximal order of $\sigma_\alpha(n)$ is $\zeta(\alpha)n^\alpha$.

5.6.32 Recall that $\log d(n)$ has normal order $(\log 2)(\log\log n)$. Show that $\log\varphi(n)$ has normal order $\log n$. If $k \ge 1$, prove that $\log\sigma_k(n)$ has normal order $k\log n$.

5.7. Notes

We first summarize the average orders, extremal orders, and normal orders of some arithmetic functions we have studied. We give the proofs for most of those given below but there are some exceptions. The exceptional case is either trivial or highly nontrivial. For example, the average orders of $d(n)$, $\varphi(n)$, $\sigma(n)$, $\omega(n)$, and $\Omega(n)$ are proved in Section 5.2. Those of $N(n)$, $1(n)$, and $e(n)$ are easy and are left as exercises. The estimate $\sum_{n\le x}\Lambda(n) \sim x$ is much more difficult and will be given in Chapter 9. The $**$ at the maximal order of $d(n)$ in the table indicates that this is not an accurate answer since we only obtain the maximal order for $\log d(n)$ but not for $d(n)$. The $o(1)$ term there only means that

$$d(n) \le n^{\frac{(1+\varepsilon)\log 2}{\log\log n}} \text{ for } n \text{ large and} \tag{5.22}$$

$$d(n) \ge n^{\frac{(1-\varepsilon)\log 2}{\log\log n}} \text{ for infinitely many } n, \tag{5.23}$$

and a better estimate is given in the work of Ramanujan ([**336**], [**339**, pp. 78–128]). For example, Ramanujan showed that ε in (5.22) and (5.23) can be replaced by $O\left((\log\log n)^{-1}\right)$. We recommend the interested reader to find more details in [**339**], and also in some of the subsequent articles and extensions by other mathematicians [**71**, **113**, **118**, **301**].

Since we require a normal order to be a positive and monotone function, $\Lambda(n)$ has no normal order. But $\Lambda(n) = 0$ for almost all n in $\mathbb{N}$, so we write $\Lambda(n) = 0$ a.e. in the table. Similarly, we proved that $\log d(n)$ has normal order $(\log 2)(\log\log n)$ and $d(n) = (\log n)^{\log 2+o(1)}$ a.e. but these do not imply that $(\log n)^{\log 2}$ is a normal order of $d(n)$. Therefore

we put $*$ in the column of normal order of $d(n)$ to mean that it is not actually a normal order. In fact, $d(n)$ has no normal order. Segal [**357**] showed that there does not exist an increasing function g such that $\varphi(n)$ has normal order $g(n)$. Then three years later, Birch [**54**] gave a general criterion implying that $d(n)$, $\varphi(n)$, $\sigma(n)$, and many other popular multiplicative functions have no normal order. The statement of his theorem is given below. See also Klazar's explanation notes [**228**] on the proof of Birch's theorem. The summary of orders is given in the following table.

	average order	minimal order
$d(n)$	$\log n$	2
$\varphi(n)$	$6n/\pi^2$	$\frac{e^{-\gamma}n}{\log\log n}$
$\sigma(n)$	$\pi^2 n/6$	n
$\omega(n)$	$\log\log n$	1
$\Omega(n)$	$\log\log n$	1
$\Lambda(n)$	1	does not exist
$N(n)$	n	n
$1(n)$	1	1
$e(n)$	$1/2^n$	does not exist

	maximal order	normal order
$d(n)$	$**n^{\frac{\log 2+o(1)}{\log\log n}}$	$*(\log n)^{\log 2+o(1)}$ a.e.
$\varphi(n)$	n	does not exist
$\sigma(n)$	$e^{\gamma}n\log\log n$	does not exist
$\omega(n)$	$\log n/\log\log n$	$\log\log n$
$\Omega(n)$	$\log n/\log 2$	$\log\log n$
$\Lambda(n)$	$\log n$	$\Lambda(n)=0$ a.e.
$N(n)$	n	$N(n)=n$ always
$1(n)$	1	$1(n)=1$ always
$e(n)$	does not exist	$e(n)=0$ a.e.

Theorem 5.30. (Birch [**54**]) *Let $f:\mathbb{N}\to[0,\infty)$ be a multiplicative function which is unbounded and has an increasing normal order. Then there exists a constant $\alpha>0$ such that $f(n)=n^{\alpha}$ for all $n\in\mathbb{N}$.*

to show that $\alpha < 517/1648 \approx 0.31371$, which is the best upper bound for α known to date. We summarize the time-line concerning the improvement on the size of $\Delta(x)$ below. For more information, see for example in [**59**, **60**, **204**, **205**, **213**, **354**, **437**]. In particular, we recommend the reader to read the survey article by Berndt, Kim, and Zaharescu [**50**] for a lot more details on both the Dirichlet divisor problem and the Gauss circle problem.

- Voronoï (1903) $\Delta(x) \ll x^{\frac{1}{3}+\varepsilon}$ $(0.33333\ldots)$
- Hardy and Landau (1916) $\Delta(x) \ll x^{\theta} \to \theta \geq \frac{1}{4}$
- van der Corput (1922) $\Delta(x) \ll x^{\frac{33}{100}+\varepsilon}$ (0.33)
- van der Corput (1928) $\Delta(x) \ll x^{\frac{27}{82}+\varepsilon}$ $(0.32926\ldots)$
- Chen (1963) $\Delta(x) \ll x^{\frac{12}{37}}$ $(0.32432\ldots)$
- Kolesnik (1982) $\Delta(x) \ll x^{\frac{35}{108}}$ $(0.32407\ldots)$
- Vinogradov (1985) $\Delta(x) \ll x^{\frac{17}{53}}$ $(0.32075\ldots)$
- Iwaniec and Mozzochi (1988) $\Delta(x) \ll x^{\frac{7}{22}+\varepsilon}$ $(0.31818\ldots)$
- Huxley (1993) $\Delta(x) \ll x^{\frac{23}{73}+\varepsilon}$ $(0.31506\ldots)$
- Huxley (2003) $\Delta(x) \ll x^{\frac{131}{416}+\varepsilon}$ $(0.31490\ldots)$
- Bourgain and Watt (2017) $\Delta(x) \ll x^{\frac{517}{1648}+\varepsilon}$ $(0.31371\ldots)$.

Exercises in this chapter are collected from various sources but we also put in something new. Specifically, the author designed Exercises 5.6.2 and 5.6.4 to give a proof, without involving the Euler product formula or the concept of infinite product, of the fact that

$$\sum_{n=1}^{\infty} \frac{\mu(n)}{n^{\alpha}} = \frac{1}{\zeta(\alpha)} \quad \text{for all } \alpha > 1.$$

Exercises 5.6.16 and 5.6.17 seem to be new too. Although the formula for the sum $\sum d(n)$ where n ranges over $n \leq x$ and $n \equiv 1 \pmod 2$ is not proved in this book, the reader can find a proof of a more general result in [**327**] where the condition $n \equiv 1 \pmod 2$ is replaced by $n \equiv a \pmod q$ for any $q \geq 2$ and $a \in \mathbb{Z}$. More precisely, Pongsriiam and Vaughan [**327**]