

M823

ANALYTIC NUMBER THEORY I

Course Notes

Prepared by

Robin Wilson

Contents

Introduction	2
Historical introduction and Chapter 1	
The fundamental theorem of arithmetic	3
Study Session 1: Historical introduction (pages 1–12)	3
Study Session 2: Sections 1.1–1.4 (pages 13–17)	6
Study Session 3: Sections 1.5–1.8 (pages 17–21)	8
Chapter 2 Arithmetical functions and Dirichlet multiplication	11
Study Session 1: Sections 2.1–2.5 (pages 24–28)	11
Study Session 2: Sections 2.6–2.8 (pages 29–33)	14
Study Session 3: Sections 2.9–2.11 (pages 33–37)	16
Study Session 4: Sections 2.12–2.14 (pages 37–40)	18
Chapter 3 Averages of arithmetical functions	20
Study Session 1: Sections 3.1–3.4 (pages 52–57)	20
Study Session 2: Sections 3.5–3.7 (pages 57–62)	24
Study Session 3: Sections 3.9–3.12 (pages 64–70)	26
Chapter 4 Some elementary theorems on the distribution of prime numbers	28
Study Session 1: Sections 4.1–4.3 (pages 74–79)	28
Study Session 2: Sections 4.4–4.5 (pages 79–85)	31
Study Session 3: Sections 4.6–4.8 (pages 85–91)	33
Study Session 4: Section 4.9 (pages 91–98)	34
Chapter 5 Congruences	37
Study Session 1: Sections 5.1–5.3 (pages 106–113)	37
Study Session 2: Sections 5.4–5.6 (pages 113–117)	39
Study Session 3: Sections 5.7–5.9 (pages 117–122)	41
Chapter 6 Finite abelian groups and their characters	43
Study Session 1: Sections 6.1–6.4 (pages 129–133)	43
Study Session 2: Sections 6.5–6.8 (pages 133–140)	45
Study Session 3: Sections 6.9–6.10 (pages 140–143)	47
Chapter 7 Dirichlet’s theorem on primes in arithmetic progressions	49
Study Session 1: Sections 7.1–7.3 (pages 146–150)	49
Study Session 2: Sections 7.4–7.6 (pages 150–152)	50
Study Session 3: Sections 7.7–7.9 (pages 153–155)	52
Chapter 9 Quadratic residues and the quadratic reciprocity law	54
Study Session 1: Sections 9.1–9.3 (pages 178–182)	54
Study Session 2: Sections 9.4–9.6 (pages 182–187)	56
Study Session 3: Sections 9.7–9.8 (pages 187–192)	59
Further reading	61
Solutions to the Self-assessment questions	62
Solutions to the Problems	83

Introduction

Number theory can be categorized into at least four interrelated areas. In previous courses on number theory you will probably have studied *elementary number theory*, in which all concepts and proofs arise from the subject matter itself and do not involve results from other branches of mathematics. (The word *elementary* does not refer to the simplicity of the material — some ‘elementary’ proofs are highly complicated and difficult to follow.) In this course we study *analytic number theory*, in which extensive use is made of techniques from analysis — in particular, the summation of series in real analysis.

This course is based on Chapters 1–7 and 9 of *Introduction to Analytic Number Theory* by T. M. Apostol. These Course Notes will guide you through Apostol’s book, telling you which sections to read, explaining difficult points, and setting Self-assessment Questions (SAQs) and Problems to test your understanding of the material. You should attempt all of the SAQs and as many Problems as you have time for; full solutions will be found at the end of the Course Notes. (You will need a pocket calculator for several of the problems, so please make sure you have one available.)

To help you organize your work, we have divided each chapter into three or four study sessions, each covering several sections of the book and each planned to correspond to about three hours’ work — although the time spent may vary widely from student to student. Do not become unduly discouraged if some of the material seems difficult or time-consuming. In particular, you may find that Chapters 3 and 4 are harder than Chapters 5 and 6, and that the material at the end of the course is rather heavy going. We have tried to alleviate the difficulties, in our commentaries, and we have made several of the sections in the book optional, but you should not expect this course to be an easy one.

In order to pace you through the course, we have set four Tutor-marked Assignments (TMAs). These are compulsory in that you cannot pass the course without obtaining a reasonable average grade on them.

It is possible that there are errors in these notes, and that we have not found all the errors in Apostol’s book. We should be grateful if you could inform us of any errors or misprints and of any suggested improvements to the Course Notes.

Historical introduction and Chapter 1

The fundamental theorem of arithmetic

The book starts with a historical introduction which is designed to set the scene for the work that follows. In Chapter 1, the basic notions of divisibility, greatest common divisor and prime number are introduced, and a number of important basic results are proved. These include the fundamental theorem of arithmetic, the Euclidean algorithm and the fact that there are infinitely many primes. Even if you are familiar with this material, you should read it carefully so as to accustom yourself to Apostol's style and notation.

This material splits into THREE study sessions.

Study Session 1: Historical introduction (pages 1–12)

Study Session 2: Sections 1.1–1.4 (pages 13–17)

Study Session 3: Sections 1.5–1.8 (pages 17–21)

Study Session 1: Historical introduction (pages 1–12)

Read pages 1–5

Commentary

1. *The top of page 2.* Note that here, as in much of this book, the words *integer* and *number* are taken to mean *positive integer*. The context will make it clear as to which meaning is intended.
2. *Figure I.1.* Note that, for each sequence, the n th term can be obtained by summing an arithmetic progression. For example, the n th square number is the sum of the arithmetic progression
$$1 + 3 + 5 + 7 + \cdots + (2n - 1) = n^2.$$
3. *Page 4, line 2.* We present Euclid's proof that there are infinitely many primes in Chapter 1.
4. *The bottom of page 4.* Since Apostol's book appeared, further Mersenne primes (and, hence, perfect numbers) have been discovered — for example, for $p = 216\,091$.
5. *The top of page 5.* It is now known that any odd perfect number (if it exists) must be greater than 10^{100} .

Self-assessment questions

- 1.1 Write down all the prime numbers between 100 and 150.
- 1.2 Find a formula for
 - (a) the n th triangular number;
 - (b) the n th pentagonal number.

- 1.3** (a) Verify that $x^2 + y^2 = z^2$ when
- (i) $x = n, y = \frac{1}{2}(n^2 - 1), z = \frac{1}{2}(n^2 + 1)$;
 - (ii) $x = 4n, y = 4n^2 - 1, z = 4n^2 + 1$;
 - (iii) $x = t(a^2 - b^2), y = 2tab, z = t(a^2 + b^2)$.
- (b) In part (iii), which numbers a, b and t give rise to the Pythagorean triples 12, 35, 37 and 9, 12, 15?
- 1.4** (a) Why does the formula $2^{p-1}(2^p - 1)$ fail to give a perfect number when $p = 11$?
- (b) Prove that $2^{p-1}(2^p - 1)$ is always a perfect number when p and $2^p - 1$ are primes.
- 1.5** Express each of the numbers 30, 35 and 40 as
- (a) a triangular number or a sum of 2 or 3 triangular numbers;
 - (b) a square or a sum of 2, 3 or 4 squares;
 - (c) a pentagonal number or a sum of 2, 3, 4 or 5 pentagonal numbers.
- 1.6** Express each of the prime numbers 53, 61 and 73 as a sum of two squares.

Read pages 6–12

Commentary

1. *Page 6, paragraph 3.* It is easy to produce a sequence of consecutive composite numbers with any required length. A method for doing this is given in SAQ 1.7.
2. *The top of page 7.* A proof that there are infinitely many primes of the form $4n + 3$ is given in the notes for Chapter 1. Dirichlet's theorem on primes in an arithmetic progression is proved in Chapter 7.
3. *The middle of page 7.* In connection with polynomials which represent infinitely many primes, it was proved in 1976 that there is a polynomial of degree 25 in twenty-six variables such that, whenever non-negative integers are substituted for the variables, the *positive* values taken by the polynomial are the prime numbers 2, 3, 5, 7, ...
4. *The greatest integer function.* Note that, for example, $[\pi] = [3] = 3$ and $[-1\frac{1}{2}] = -2$. The greatest integer function is of great importance in number theory, and some practice in using it is given in SAQ 1.10.
5. *The definition of $\pi(x)$.* Note, for example, that $\pi(10) = 4$ (corresponding to the primes 2, 3, 5 and 7) and $\pi(100) = 25$ (corresponding to the primes listed on page 2).
6. *The prime number theorem (page 9).* Riemann's 'zeta function' $\zeta(s)$ is introduced briefly in Chapter 2 and studied in depth in Chapters 11 and 12. The prime number theorem appears in Chapter 4 and is proved in Chapter 13. A brief sketch of an 'elementary proof' that does not involve $\zeta(s)$ is given in Chapter 4.
7. *Pages 10–11.* More recently, in connection with Goldbach's conjecture, Chen Jing-run and Wang Tian-ze have proved that every odd number $n > e^{e^{11.503}}$ is the sum of three primes, and R. C. Vaughan has proved that *every* number is the sum of at most nine primes. The important feature about the first result is that, in spite of the enormous number involved, the number of unsolved cases is *finite*.

8. *Fermat's conjecture (bottom of page 9).* Apart from 'trivial' solutions (such as when x or y is 0), no solutions of the equation $x^n + y^n = z^n$ are known for any value of $n \geq 3$, and Fermat believed that he could prove that *no non-trivial solutions exist*. But for many years no such proof was found, and the finding of a proof or counter-example remained one of the most famous unsolved problems in mathematics. Using techniques from algebraic number theory, one can prove it for infinitely many values of n , but it remained unproved in general. Eventually, a proof was announced by Andrew Wiles, but a gap was later found. This gap was filled in January 1995, and the proof is now complete; see the book by S. Singh for an informal introduction to Wiles's proof.
9. *The note on page 12.* LeVeque's *Reviews in Number Theory* has been updated by Richard Guy, providing a catalogue of the main discoveries in number theory right up to the 1980s.

Self-assessment questions

- 1.7 (a) Show that the following is a sequence of n consecutive composite numbers:

$$(n+1)! + 2, \quad (n+1)! + 3, \quad \dots, \quad (n+1)! + (n+1).$$
(b) Write down a sequence of 100 consecutive composite numbers.
- 1.8 Prove that the quadratic polynomial $x^2 + ax + b$ cannot give prime numbers for *all* values of $x = 0, 1, 2, \dots$.
- 1.9 In the statement of Dirichlet's theorem on primes in an arithmetic progression (page 7), why is it necessary to require that a and b have no prime factor in common?
- 1.10 If $[x]$ denotes the greatest integer $\leq x$, prove that:
(a) $[x + n] = [x] + n$, if n is an integer;
(b) $[2x] - 2[x] = 0$ or 1 .
- 1.11 Calculate $\pi(x) \div x / \log x$ when (a) $x = 50$, (b) $x = 150$.
- 1.12 The following problems relate to the list of unsolved problems on page 11.
- | | |
|--|--------------|
| (a) Verify the truth of the Goldbach conjecture when
$n = 30, 32, \dots, 40$. | (Problem 1) |
| (b) Express each of the even numbers $n = 30, 32, \dots, 40$ as
the difference of two primes. | (Problem 2) |
| (c) List five pairs of twin primes. | (Problem 3) |
| (d) List five primes of the form $x^2 + 1$, where x is an integer. | (Problem 8) |
| (e) List three primes of the form $x^2 + 2$, where x is an
integer. | (Problem 9) |
| (f) Find a prime between n^2 and $(n+1)^2$, for
$n = 6, 7, 8, 9, 10$. | (Problem 10) |
| (g) Find a prime between n^2 and $n^2 + n$, for
$n = 6, 7, 8, 9, 10$. | (Problem 11) |
-

Study Session 2: Sections 1.1–1.4 (pages 13–17)

Read Sections 1.1 and 1.2

Commentary

1. *The principle of induction.* When proving results by induction, it is usual to avoid any reference to Q and simply to *verify the result for $n = 1$* and *prove that if the result is true for n then it is true for $n + 1$* . The alternative version for (b) — ‘ $1, 2, 3, \dots, n \in Q$ implies $n + 1 \in Q$ ’ — is sometimes called *the principle of strong induction*, and states that if ‘the result is true for all $k \leq n$ ’, implies that ‘it is also true for $k = n + 1$ ’, then it is true for all n .
2. *The well-ordering principle.* Note that although the well-ordering principle is a property of the positive integers, it does not necessarily hold for some other sets, such as the sets of positive rational numbers and positive real numbers. For example, there is no smallest positive rational number and there is no smallest real number > 2 .
3. *Theorem 1.1.* In reading through these results you should convince yourself that each one is true and that you know how to prove it. An example of the type of proof required is as follows.
Proof of (b). If $d|n$ and $n|m$, then $n = rd$ and $m = sn$, for some integers r and s . So $m = (rs)d$, and hence $d|m$.

Self-assessment questions

- 1.13 Prove by induction that $2^n \leq \frac{(2n)!}{n!n!}$, for all n .
- 1.14 Deduce the principle of induction from the well-ordering principle.
[Hint: assume that the principle of induction is false and let $n + 1$ be the smallest number not in Q .]
- 1.15 Prove parts (c), (e), (j) and (k) of Theorem 1.1.

Read Section 1.3

Commentary

1. *The proof of Theorem 1.2.* This proof divides into two parts, corresponding to $a \geq 0, b \geq 0$ and to a and/or $b < 0$. The proof for $a \geq 0, b \geq 0$ uses the principle of strong induction, where we assume the result for $0, 1, 2, \dots, a + b - 1$ and prove it for $n = a + b$. By induction we can write $d = (a - b)x + by$ (since $(a - b) + b < n$) and we use the fact that if $d|(a - b)$ and $d|b$ then $d|a$.
2. *The definition of (a, b) .* As its name suggests, the greatest common divisor of a and b is the largest positive integer which divides both a and b . It is divisible by all other common divisors of a and b . The term *coprime* is sometimes used instead of *relatively prime*, when $(a, b) = 1$.

A general method for determining d is given in Section 1.7.

3. The proofs of Theorems 1.4 and 1.5. Note the use of the equation $d = ax + by$ in these proofs. Note also that this equation has a solution in integers x, y if and only if (a, b) divides d .

Self-assessment questions

- 1.16 Write down the following greatest common divisors $d = (a, b)$, and express your results in the form $d = ax + by$.
 (a) $(25, 5)$ (b) $(30, -18)$ (c) $(9, 25)$ (d) $(-21, -57)$
- 1.17 Prove part (b) of Theorem 1.4, and verify that it holds when $a = 42$, $b = 70$ and $c = 30$.
- 1.18 Prove that if $(a, b) = d$, then $(a/d, b/d) = 1$.

Read Section 1.4

Commentary

1. In order to find all the primes up to a given number x , we write down the numbers $2, 3, \dots, x$ and cross out all the multiples of 2 (other than 2 itself), of 3 (other than 3 itself), and so on through all the primes up to \sqrt{x} (see SAQ 1.19). The numbers that remain are the primes up to x . (This is called the *Sieve of Eratosthenes*.)
2. The proof of Theorem 1.7. Instead of taking $N = p_1 p_2 \dots p_n + 1$, we could have taken $N = p! + 1$, where p is the largest of the primes p_i , or
- $$N = p_2 p_3 \dots p_n + p_1 p_3 \dots p_n + \dots + p_1 p_2 \dots p_{n-1}$$
- (see SAQ 1.20).

Self-assessment questions

- 1.19 (a) Prove that if n is composite then it has a prime divisor that does not exceed \sqrt{n} . Deduce that in using the Sieve of Eratosthenes (see Commentary 1), we need check only the primes up to \sqrt{x} .
 (b) Use the Sieve of Eratosthenes to find all the primes between 150 and 200.
- 1.20 Show that in Euclid's proof of Theorem 1.7 we can replace $N = p_1 p_2 \dots p_n + 1$ by the displayed expression in Commentary 2.
- 1.21 Explain why $n^4 + 4$ is composite for $n > 1$.

Problems for Sections 1.1–1.4

- 1A Apostol, page 21, numbers 1 and 2.
 1B Apostol, page 21, number 7.
 1C Apostol, page 22, number 16.

- 1D** Let p_n be the n th prime (when arranged in increasing order). Prove that $p_{n+1} \leq p_1 \cdots p_n + 1$, and use this result to prove by induction that $p_n \leq 2^{2^{n-1}}$.
- 1E** By considering the number $4p_1 \cdots p_n - 1$, and imitating the proof of Theorem 1.7, prove that there are infinitely many primes of the form $4k + 3$.

Study Session 3: Sections 1.5–1.8 (pages 17–21)

Read Section 1.5

Commentary

- The fundamental theorem of arithmetic.* This theorem is, in some sense, the foundation on which the whole of number theory is built, and is sometimes expressed by saying that the integers form a unique factorization domain. Note that some number systems, such as the even integers, do not form a unique factorization domain (see Problem 1H).
- The proof of Theorem 1.10.* The proof relies heavily on Theorem 1.9. Note that in the last paragraph we can repeat the argument given earlier to deduce that $p_2 = q_2$ (after relabelling), $p_3 = q_3$, and so on. The induction step is used to make this informal argument precise.
- $n = p_1^{a_1} \cdots p_r^{a_r}$. If the p_i are arranged in increasing order, then this factorization of n is sometimes called the *canonical form* of the factorization. For example, if $n = 4200$, then the canonical form of the factorization is $4200 = 2^3 \cdot 3 \cdot 5^2 \cdot 7$.
- The statement of Theorem 1.12.* This result, and the Euclidean algorithm in Section 1.7, are the two principal methods for obtaining the greatest common divisor of a and b . We can find the *least common multiple* of a and b , denoted by $[a, b]$, by using the corresponding result in which $c_i = \max\{a_i, b_i\}$ (see SAQ 1.24 and Problem 1J).

Self-assessment questions

- 1.22** Express each of the following numbers as a product of primes, giving your answers in canonical form (see Commentary 3).
 (a) 1000 (b) 2310 (c) 4116 (d) 2187
- 1.23** (a) Verify the statement of Theorem 1.11 by writing down the prime factorizations of all the positive divisors of $60 = 2^2 \cdot 3 \cdot 5$.
 (b) Use Theorem 1.11 to prove that the number of positive divisors of $n = p_1^{a_1} \cdots p_r^{a_r}$ is

$$(a_1 + 1)(a_2 + 1) \cdots (a_r + 1).$$

 (c) Use part (b) to find the number of positive divisors of each of the numbers in SAQ 1.22.

- 1.24** (a) Use Theorem 1.12 and the results of SAQ 1.22 to evaluate the following gcfs.
- (i) (1000, 2310) (ii) (2310, 4116) (iii) (1000, 2187)
- (b) Use Commentary 4 and the results of SAQ 1.22 to evaluate the following lcfs.
- (i) [1000, 2310] (ii) [2310, 4116] (iii) [1000, 2187]

Read Section 1.6

Commentary

- 1.** *The statement of Theorem 1.13.* It is well known that $\sum_{n=1}^{\infty} \frac{1}{n}$ diverges, although a slight modification to $\sum_{n=1}^{\infty} n^{-1.0001}$ or $\sum_{n=1}^{\infty} \frac{1}{n(\log n)^2}$ produces a convergent series. Here we prove that if we throw away all the terms $1/n$ where n is composite (that is, we throw away ‘most’ of the terms), we still have a divergent series!
- 2.** *The proof of Theorem 1.13.* Having chosen a number k such that $\sum_{m=k+1}^{\infty} p_m^{-1} < \frac{1}{2}$, we consider the numbers $p_1 \dots p_k + 1$, $2p_1 \dots p_k + 1$, $3p_1 \dots p_k + 1, \dots$, none of which is divisible by p_1, \dots, p_k .

The main step is to add the reciprocals of these numbers, and write

$$\frac{1}{p_1 \dots p_k + 1} + \dots + \frac{1}{rp_1 \dots p_k + 1} \leq \sum_{m=k+1}^{\infty} \frac{1}{p_m} + \left(\sum_{m=k+1}^{\infty} \frac{1}{p_m} \right)^2 + \dots,$$

since each term on the left must appear somewhere on the right. So, by the comparison test, $\sum 1/(1 + nQ)$ converges. But

$$\begin{aligned} \frac{1}{Q+1} + \frac{1}{2Q+1} + \frac{1}{3Q+1} + \dots &> \frac{1}{2Q} + \frac{1}{3Q} + \frac{1}{4Q} + \dots \\ &= \frac{1}{Q} \left(\frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \dots \right), \end{aligned}$$

which diverges. This gives us the required contradiction.

- 3.** *The last sentence of Section 1.6.* The result referred to is Theorem 4.12 on page 90. It shows that the series diverges very slowly; for example, the smallest prime p_n for which $\frac{1}{p_1} + \dots + \frac{1}{p_n} > 2$ is $p_{59} = 277$.

Self-assessment questions

- 1.25** Find the smallest prime p_n for which $\frac{1}{p_1} + \frac{1}{p_2} + \dots + \frac{1}{p_n} > k$, where
- (a) $k = 1$, (b) $k = 1.5$.
- 1.26** Use Theorem 1.13 to deduce that there are infinitely many primes.

Commentary

1. *The proof of Theorem 1.14.* Note the use of the well-ordering principle in line 3 of the proof.
2. *The proof of Theorem 1.15.* Notice that to show that r_n is a common divisor of a and b we work from the bottom equation upwards, whereas to show that $d|r_n$ we work from the top equation downwards.

3. $d = ax + by$. To express the greatest common divisor in the form $ax + by$ (as in Theorem 1.2), we start from the last-but-one equation (ending with r_n) and work upwards. The following example will make the method clear.

Example Find $d = (82, 24)$, and write d in the form $82x + 24y$, where x and y are integers.

Solution

$$\begin{array}{llll} 82 = 3 \cdot 24 + 10 & (1) & 2 = 10 - 2 \cdot 4 & \text{from (3)} \\ 24 = 2 \cdot 10 + 4 & (2) & = 10 - 2 \cdot (24 - 2 \cdot 10) & \text{from (2)} \\ 10 = 2 \cdot 4 + 2 & (3) & = 5 \cdot 10 - 2 \cdot 24 & \text{(simplifying)} \\ 4 = 2 \cdot 2 & & = 5(82 - 3 \cdot 24) - 2 \cdot 24 & \text{from (1)} \\ \text{So } d = 2. & & \text{So } 2 = 5 \cdot 82 - 17 \cdot 24, \text{ and } x = 5, y = -17. & \end{array}$$

4. *The definition of relatively prime integers.* Note that 6, 10 and 15 are relatively prime, although *no two* of them are relatively prime.

Self-assessment questions

- 1.27 Use the Euclidean algorithm to find integers x and y such that $(544, 238) = 544x + 238y$.
- 1.28 Find the following greatest common divisors.
(a) $(87, 24, 45)$ (b) $(30, 42, 70, 135)$

Problems for Sections 1.5–1.8

- 1F Apostol, page 21, number 8.
 - 1G Prove that if p is prime then \sqrt{p} is irrational.
[Hint: try to write $pb^2 = a^2$, and count the number of prime factors on each side.]
 - 1H Consider the set of positive even integers. An even integer is *E-prime* if it cannot be written as a product of smaller even integers.
 - (a) List the E-primes up to 60, and write down an alternative description of them.
 - (b) Prove that every even integer is E-prime or a product of E-primes.
 - (c) Is factorization into E-primes unique?
 - 1I Apostol, page 22, number 20.
 - 1J Apostol, page 22, number 21, (a) and (b).
-

Chapter 2 Arithmetical functions and Dirichlet multiplication

In this chapter we study functions defined on the set of positive integers. Some of these, such as the Möbius function $\mu(n)$ and the Euler phi function $\phi(n)$, may already be familiar to you from previous courses. After investigating their properties and deriving identities connecting them, we show how such identities can sometimes be proved more simply by using the idea of ‘Dirichlet multiplication’. These identities are particularly interesting when the functions are ‘multiplicative’ — that is, $f(mn) = f(m)f(n)$ whenever m and n are relatively prime. We conclude with some results on ‘generalized convolutions’ which will be needed in Chapters 3 and 7.

This chapter splits into FOUR study sessions.

Study Session 1: Sections 2.1–2.5 (pages 24–28)

Study Session 2: Sections 2.6–2.8 (pages 29–33)

Study Session 3: Sections 2.9–2.11 (pages 33–37)

Study Session 4: Sections 2.12–2.14 (pages 37–40)

Sections 2.15–2.19 are NOT part of the course.

Study Session 1: Sections 2.1–2.5 (pages 24–28)

Read Sections 2.1 and 2.2

Commentary

1. Although arithmetical functions can take real or complex values, our attention in this chapter is entirely on real-valued functions. Complex numbers will not appear until Chapter 6.
2. *The definition of the Möbius function.* Note that the Möbius function $\mu(n)$ takes a non-zero value only when $n = 1$ or n is ‘squarefree’ (that is, a product of *distinct* prime numbers); in particular, if p_1, p_2, p_3 are prime numbers, then $\mu(p_1) = -1$, $\mu(p_1 p_2) = +1$ and $\mu(p_1 p_2 p_3) = -1$.
3. *The statement of Theorem 2.1.* Note that $\frac{1}{n} = 1$ if $n = 1$ and $\frac{1}{n} < 1$ if $n > 1$, so $\left[\frac{1}{n}\right] = 1$ or 0 according as $n = 1$ or $n > 1$. The reason for introducing the expression $\left[\frac{1}{n}\right]$ will become apparent in Section 2.4.
4. *The proof of Theorem 2.1.* The key feature of this proof is the use of the binomial expansion of $(1 - 1)^k$ in the last line. Recall that the binomial coefficient

$$\binom{k}{i} = \frac{k!}{i!(k-i)!}, \quad i \leq k,$$

represents the number of ways of selecting i of the k primes.

Self-assessment questions

- 2.1** Write down the values of $\mu(31)$, $\mu(32)$, \dots , $\mu(42)$.

2.2 Verify the statement of Theorem 2.1 when $n = 27, 28, 29$ and 30 .

2.3 Write out the proof of Theorem 2.1 in the case $n = 60$.

2.4 (a) Prove that if f is any arithmetical function, then

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

[Hint: if you have difficulty with this, write out both sides in the case $n = 10$.]

(b) Evaluate $\sum_{d|n} \mu(n/d)$ when $n > 1$.

Read Section 2.3

Commentary

1. *The definition of the Euler ϕ function.* An expression of the form $\sum_k 1$ means that we add 1 for each relevant value of k — that is, we *count* how many k s there are. So to find $\phi(n)$ we count those integers k such that $k \leq n$ and $(k, n) = 1$. For example, if $n = 12$, then $k = 1, 5, 7$ or 11 , so $\phi(12) = 4$.

2. *The proof of Theorem 2.2.* The set $A(d)$ is the set of integers k such that $k \leq n$ and $(k, n) = d$. For example, if $n = 10$, then $A(1) = \{1, 3, 7, 9\}$, $A(2) = \{2, 4, 6, 8\}$, $A(5) = \{5\}$ and $A(10) = \{10\}$. Note that each integer from 1 to 10 occurs in exactly one of these sets. Letting $f(d)$ be the number of integers in $A(d)$, we have $f(1) = f(2) = 4$, $f(5) = f(10) = 1$, and $\sum_{d|10} f(d) = 10$.

3. *The proof of Theorem 2.2 (continued).* If $n = 10$, the one-to-one correspondence referred to in the proof is

$$A(1) \longleftrightarrow \{1, 3, 7, 9\}, A(2) \longleftrightarrow \{1, 2, 3, 4\}, A(5) \longleftrightarrow \{1\}, A(10) \longleftrightarrow \{1\}.$$

Note that, for example, $A(2)$ corresponds to those integers q satisfying $0 < q \leq \frac{10}{2}$ and $(q, \frac{10}{2}) = 1$, and the number of such q is $\phi(5)$; so $f(2) = \phi(5) = 4$. The last two lines of the proof follow from SAQ 2.4 above.

Self-assessment questions

2.5 Write down the values of (a) $\sum_{q=1}^{10} 1$, (b) $\sum_{\substack{p \leq 20 \\ p \text{ prime}}} 1$, (c) $\sum_{\substack{k \leq 12 \\ (k, 12)=2}} 1$.

2.6 Write down the values of $\phi(11), \phi(12), \dots, \phi(20)$.

2.7 (a) Verify the statement of Theorem 2.2 when $n = 18$.

(b) What are the sets $A(d)$ in this case?

2.8 (a) Show that if p is prime, then $\phi(p) = p - 1$, and $\phi(p^\alpha) = p^\alpha - p^{\alpha-1}$.

(b) Use these results to prove Theorem 2.2 when $n = p^\alpha$.

2.9 Prove that $\phi(n) = \sum_{k=1}^n \left[\frac{1}{(n, k)} \right] = \sum_{k=1}^n \sum_{d|(n, k)} \mu(d)$.

Commentary

1. *The proof of Theorem 2.3.* The first part of the proof follows from SAQ 2.9 above. The second part, involving the rearrangement of a double summation, uses a standard technique in number theory and you should read it several times until you understand it — the main idea is to make the *first* of the summations into a summation over the divisors d of n , and to adjust the other sum accordingly.
2. *The statement of Theorem 2.4.* This is an important result which is very useful for computation. For example, if $n = 600 = 2^3 \cdot 3 \cdot 5^2$, then $\phi(n) = 600 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} = 160$.

3. *The proof of Theorem 2.4.* The main idea is to expand

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

and to express the result in the form $\sum \mu(d)/d$. By Theorem 2.3, this is equal to $\phi(n)/n$.

4. *The proof of Theorem 2.5(b).* If you have difficulty following this proof, consider first the case when $(m, n) = 1$ (which is part (c)). In this case the expressions in the denominators disappear.
5. *The proof of Theorem 2.5(e).* An alternative proof is to write $n = 2^k p_1^{a_1} \cdots p_r^{a_r}$ and to rewrite Theorem 2.4 in the form

$$\phi(n) = \begin{cases} 2^{k-1} p_1^{a_1-1} \cdots p_r^{a_r-1} (p_1 - 1) \cdots (p_r - 1), & \text{if } k \geq 1 \\ p_1^{a_1-1} \cdots p_r^{a_r-1} (p_1 - 1) \cdots (p_r - 1), & \text{if } k = 0. \end{cases}$$

Each of the terms $p_i - 1$ is even, and so contributes a factor of 2; the result follows.

Self-assessment questions

- 2.10 Verify the statement of Theorem 2.3 when $n = 18$.
- 2.11 Use Theorem 2.4 to evaluate $\phi(120)$ and $\phi(210)$.
- 2.12 (a) Prove that $\phi(3n) = 2\phi(n)$ if n is not a multiple of 3.
(b) What is the corresponding result when n is a multiple of 3?

Problems for Sections 2.1–2.5

- 2A Apostol, page 46, number 1.
 - 2B Apostol, page 47, number 4.
 - 2C Apostol, page 47, number 6.
-

Study Session 2: Sections 2.6–2.8 (pages 29–33)

Read Section 2.6

Commentary

1. The aim of this section and Section 2.7 is to define a ‘multiplication’ operation on a set of arithmetical functions (those functions f for which $f(1) \neq 0$) in such a way that we obtain an *abelian group*. The associative and commutative laws are proved in Theorem 2.6, the existence of an identity element is proved in Theorem 2.7, and the existence of inverses is discussed in Section 2.7.

If you are unfamiliar with group theory, do not worry at this stage; we shall study abelian groups in Chapter 6.

2. *The definition of Dirichlet product.* If you have studied Laplace or Fourier transforms, you may notice similarities between the definition of Dirichlet product and that of a convolution in transform theory. The reason for the name ‘Dirichlet product’ is that if we multiply together two Dirichlet series $\sum_{n=1}^{\infty} \frac{f(n)}{n^s}$ and $\sum_{n=1}^{\infty} \frac{g(n)}{n^s}$, we obtain another Dirichlet series $\sum_{n=1}^{\infty} \frac{h(n)}{n^s}$, where $h(n)$ is as given in the definition of Dirichlet product.

We study Dirichlet series in Chapter 11.

3. *The proof of Theorem 2.7.* It is easier to omit the square-bracket term, and argue as follows: since $I(n/d) = 1$ only when $d = n$, all but one of the terms in the sum disappear, giving

$$\sum_{d|n} f(d)I\left(\frac{n}{d}\right) = f(n), \quad \text{as required.}$$

In the following questions, the arithmetical functions I and N are defined in the text and u , σ_0 and σ_1 are defined by:

$$u(n) = 1, \text{ for all } n;$$

$$\sigma_0(n) = \text{the number of divisors of } n \text{ — for example, } \sigma_0(6) = 4;$$

$$\sigma_1(n) = \text{the sum of the divisors of } n \text{ — for example, } \sigma_1(6) = 12.$$

In M381, $\sigma_0(n)$ and $\sigma_1(n)$ are called $\tau(n)$ and $\sigma(n)$, respectively.

Self-assessment questions

- 2.13 Prove the following.

$$(a) \quad I * u = u \qquad (b) \quad \mu * u = I \qquad (c) \quad u * u = \sigma_0 \qquad (d) \quad N * u = \sigma_1$$

- 2.14 By considering $f * u$, prove that $\sum_{d|n} f(d) = \sum_{d|n} f(n/d)$ (see SAQ 2.4).

- 2.15 Prove that $\sum_{d|n} \frac{1}{d} = \frac{\sigma_1(n)}{n}$.

- 2.16 By considering $u * u * N$ and $u * N * N$, prove the following.

$$(a) \quad \sum_{d|n} \sigma_1(d) = n \sum_{d|n} \sigma_0(d)/d \qquad (b) \quad \sum_{d|n} d\sigma_0(d) = n \sum_{d|n} \sigma_1(d)/d$$

Commentary

1. Note that f^{-1} is the inverse of f with respect to $*$, and not the usual inverse function.
2. *The statement of Theorem 2.8.* This theorem shows you how to find the inverse of any arithmetical function f for which $f(1) \neq 0$. The basic idea is that $f^{-1}(n)$ can be expressed as a sum of terms involving the divisors d of n , other than n itself. For example, if p is prime, then

$$f^{-1}(p) = -\frac{1}{f(1)}(f(p)f^{-1}(1)) = -\frac{1}{f(1)^2}f(p),$$

and if p and q are distinct primes, then

$$\begin{aligned} f^{-1}(pq) &= -\frac{1}{f(1)} \{f(pq)f^{-1}(1) + f(q)f^{-1}(p) + f(p)f^{-1}(q)\} \\ &= \frac{1}{f(1)^3} \{2f(p)f(q) - f(1)f(pq)\}. \end{aligned}$$

These formulas simplify considerably when (as is usually the case) $f(1) = 1$.

3. *The proof of Theorem 2.8.* The main step in the proof is to consider the equation $(f * f^{-1})(n) = I(n)$, and to solve it for $f^{-1}(n)$.
4. *The Möbius inversion formula.* This important result states simply that $f = g * u$ if and only if $g = f * \mu$. Note that the equation for g can also be written in the form $g(n) = \sum_{d|n} \mu(d)f\left(\frac{n}{d}\right)$.

Self-assessment questions

- 2.17 If p and q are distinct primes, find $\phi^{-1}(1)$, $\phi^{-1}(p)$, $\phi^{-1}(p^2)$ and $\phi^{-1}(pq)$.
- 2.18 If p is a prime and f is an arithmetical function with $f(1) = 1$, find $f^{-1}(p^2)$ and $f^{-1}(p^3)$.
- 2.19 Prove that if $f(1) \neq 0$ and $g(1) \neq 0$, then $(f * g)^{-1} = f^{-1} * g^{-1}$.
- 2.20 Use SAQ 2.13 to prove that, for all n ,
(a) $\sum_{d|n} \sigma_0(d)\mu\left(\frac{n}{d}\right) = 1$, (b) $\sum_{d|n} \sigma_1(d)\mu\left(\frac{n}{d}\right) = n$.

Commentary

1. *The definition of $\Lambda(n)$.* Note that $\Lambda(n) = 0$ unless n is a prime power, so that the function Λ ‘picks out’ prime powers, and that *all logarithms are taken to base e* (sometimes written \ln).

The function $\Lambda(n)$ will be of great importance in Chapters 4 and 13.

2. *The proof of Theorem 2.10.* The main idea of this proof is to interpret $\sum_{d|n} \Lambda(d)$ as a sum involving $\log p_k$ for the primes p_k dividing n .
3. *The proof of Theorem 2.11.* Here we use the alternative version of the Möbius inversion formula (see Commentary 4 for Section 2.7). The reason is that we can then write $\log(n/d)$ as $\log n - \log d$, thereby splitting the sum into two parts, the first of which vanishes.

Self-assessment questions

- 2.21 Write down the values of $\Lambda(21)$, $\Lambda(22)$, \dots , $\Lambda(30)$.
- 2.22 Verify the statements of Theorems 2.10 and 2.11 when $n = 18$.

Problems for Sections 2.6–2.8

- 2D Apostol, page 48, number 17(a).
- 2E Apostol, page 47, number 13. [Hint: take logs.]

Study Session 3: Sections 2.9–2.11 (pages 33–37)

Read Section 2.9

Commentary

1. *Example 5.* To see that fg is multiplicative if f and g are, note that if $(m, n) = 1$, then

$$\begin{aligned}
 (fg)(mn) &= f(mn)g(mn) = f(m)f(n) \cdot g(m)g(n) \\
 &= f(m)g(m) \cdot f(n)g(n) \\
 &= (fg)(m) \cdot (fg)(n).
 \end{aligned}$$

Similar proofs hold for f/g and for the corresponding results for completely multiplicative functions.

2. *The statement of Theorem 2.13.* These results are very useful in practice: in proving results about multiplicative functions $f(n)$, it is often sufficient to restrict our attention to the case when $n = p^k$, a prime power, and then use multiplicativity for the general result; similarly, for completely multiplicative functions, we need consider only the values $f(p)$, where p is a prime.

Self-assessment questions

- 2.23 Let $f(n) = 1$ if n is a perfect square, and 0 otherwise. Prove that f is multiplicative. Is f completely multiplicative?
- 2.24 Let $g(1) = 1$, and $g(n) = 2^r$, where $n = p_1^{a_1} \dots p_r^{a_r}$. Is g multiplicative? Is g completely multiplicative?
- 2.25 Prove Theorem 2.13.

Commentary

1. *The statement of Theorem 2.14.* This result is extremely useful in practice. For example, knowing that u and N are multiplicative, we can deduce that $u * u = \sigma_0$ and $N * u = \sigma_1$ are both multiplicative. Note, however, that although u and N are both *completely* multiplicative, neither σ_0 nor σ_1 has this property:

$$\sigma_0(2 \cdot 2) = 3, \text{ but } \sigma_0(2) \cdot \sigma_0(2) = 4; \quad \sigma_1(2 \cdot 2) = 7, \text{ but } \sigma_1(2) \cdot \sigma_1(2) = 9.$$

2. *The proof of Theorem 2.14.* Note how the divisors c of mn split into relatively prime divisors a and b of m and n , respectively. This enables each of the terms $f(ab)$ and $g(mn/ab)$ to be split into two parts.
3. *The proof of Theorem 2.15.* This is a proof by contradiction in which we let mn be the smallest number for which $f(mn) \neq f(m)f(n)$ with $(m, n) = 1$. To derive the contradiction, we argue as in Theorem 2.14, using the fact that $ab < mn$ to split the terms $f(ab)$ and $g(mn/ab)$ into two parts each.
4. *The statement of Theorem 2.17.* We saw earlier that finding the inverse of an arithmetical function can be somewhat tedious. However, if f is a completely multiplicative function, then $f^{-1}(n)$ takes on a particularly simple form — namely, $f^{-1}(n) = \mu(n)f(n)$.
5. *The proof of Theorem 2.17.* In line 2 of the proof we replace $f(d)f(n/d)$ by $f(n)$, since f is completely multiplicative. In line 7 we have rewritten the equation

$$\sum_{d|n} f^{-1}(d)f\left(\frac{n}{d}\right) = 0 \quad (\text{line 6 of page 31}).$$

All but two terms of this equation vanish, since $\mu(p^k) = 0$ if $k \geq 2$.

6. *The proof of Theorem 2.18.* To show that $g(n) = \sum_{d|n} \mu(d)f(d)$ is multiplicative, we observe that $g = (\mu f) * u$.

Self-assessment questions

- 2.26 Use the fact that μ and N are multiplicative to prove that ϕ is multiplicative.
- 2.27 Use Theorem 2.18 to evaluate the following expressions, when $n = p_1^{a_1} \cdots p_r^{a_r}$:

$$(a) \sum_{d|n} \mu(d)\sigma_0(d) \quad (b) \sum_{d|n} \mu(d)\sigma_1(d) \quad (c) \sum_{d|n} \mu(d)/d \quad (d) \sum_{d|n} d\mu(d)$$

Problems for Sections 2.9–2.11

2F Apostol, page 49, number 26.

2G Apostol, page 49, number 27.

Study Session 4: Sections 2.12–2.14 (pages 37–40)

Read Sections 2.12 and 2.13

Commentary

1. *The proof of Theorem 2.19.* In the last line, the equation $\lambda^{-1}(n) = \mu(n)\lambda(n)$ follows from Theorem 2.17 since λ is completely multiplicative. The equation $\mu(n)\lambda(n) = \mu^2(n)$ follows since both sides are 0 if n is not squarefree, and $\lambda(n) = \mu(n)$ if n is a product of distinct primes. Finally, the equation $\mu^2(n) = |\mu(n)|$ follows from the definition of μ .
2. *The definition of $\sigma_\alpha(n)$.* You have already met the divisor functions $\sigma_0(n)$ and $\sigma_1(n)$ in the SAQs.

Self-assessment questions

2.28 Write down the values of $\lambda(n)$, $\sigma_0(n)$ and $\sigma_1(n)$ for $n = 11, 12, \dots, 20$.

2.29 Prove that $\sigma_0(n)$ is odd if and only if n is a perfect square.

2.30 By considering $u * u * N^2$, prove that $\sum_{d|n} \sigma_2(d) = n^2 \sum_{d|n} \sigma_0(d)/d^2$.

Read Section 2.14

Commentary

1. In Chapter 3 we are concerned with sums of the form $\sum_{n \leq x} \alpha(n)$, where α is an arithmetical function, and we shall need to refer to Theorem 2.21. The generalized Möbius inversion formula (Theorem 2.23) is needed in Chapter 7.
2. *The equation $(\alpha \circ F)(m) = (\alpha * F)(m)$.* If $F(x) = 0$ whenever x is not an integer, then $F(m/n)$ can be non-zero only when m is an integer and $n|m$. Thus
$$(\alpha \circ F)(m) = \sum_{n \leq m} \alpha(n)F(m/n) = \sum_{n|m} \alpha(n)F(m/n) = (\alpha * F)(m).$$
3. *Proof of Theorem 2.21.* This proof is another illustration of how to rearrange a double summation. By putting $k = mn$, we replace $mn \leq x$ by $k \leq x$ and $n|k$.

Self-assessment questions

2.31 Use Theorem 2.21 to evaluate $\sum_{n \leq x} \mu(n) \sum_{m \leq x/n} [x/mn]$.

2.32 Use Theorem 2.23 to prove that if $x \geq 1$, then $\sum_{n \leq x} \mu(n) [x/n] = 1$.
[Hint: take $F(x) = 1$ for $x \geq 1$.]

2.33 Verify the statement of Theorem 2.23 when $x = 1$ and $x = 2$.

Problems for Sections 2.12–2.14

2H Apostol, page 48, number 18. (Recall that n is perfect if $\sigma_1(n) = 2n$.)

2I Apostol, page 48, number 19.

Chapter 3 Averages of arithmetical functions

As we have seen, some arithmetical functions $f(n)$ fluctuate wildly as n increases — for example, Mangoldt’s function $\Lambda(n)$ is 0 when $x = 100$ or 102, but $\log 101$ when $n = 101$. One method for ‘smoothing out’ such fluctuations is to average the values of $f(n)$, and this leads to the study of $\sum f(n)$, where the summation is taken over all integers n up to a given number x ; by this means we can determine how ‘big’ a function is, on the average. In this chapter we investigate this problem when $f(n) = d(n)$, $\sigma_\alpha(n)$, $\phi(n)$, $\mu(n)$ and $\Lambda(n)$. The two principal techniques that we use are Euler’s summation formula and the counting of lattice points in a hyperbolic region.

This chapter splits into THREE study sessions.

Study Session 1: Sections 3.1–3.4 (pages 52–57)

Study Session 2: Sections 3.5–3.7 (pages 57–62)

Study Session 3: Sections 3.9–3.12 (pages 64–70)

Section 3.8 is NOT part of the course.

Study Session 1: Sections 3.1–3.4 (pages 52–57)

Read Sections 3.1 and 3.2

Commentary

1. From now on we shall use $d(n)$, rather than $\sigma_0(n)$, to denote the number of divisors of n . In Chapter 2 we used σ_0 so as to avoid expressions like $\sum_{d|n} d(d)d(n/d)$.
2. Most of this chapter is concerned with approximate expressions for $\sum_{n \leq x} f(n)$, where $f(n) = d(n)$, $\phi(n)$, $\mu(n)$ and $\Lambda(n)$. The method used may seem difficult and technical at first, but will become quite straightforward and routine once you have had practice in using it.
3. *Equations (2) and (3).* Equation (2) is the main result of Study Session 2, and says that $\sum_{k \leq x} d(k)$ is ‘about’ $x \log x$ — or, more accurately, ‘about’ $x \log x + (2C - 1)x$; the error in this approximation is not more than $K\sqrt{x}$, for some constant K . The proof that the right-hand side of Equation (3) converges is a standard application of the integral test, and may be found in any Analysis book; the value of C is about 0.57.

4. *The definition of ‘big oh’.* This definition is extremely useful when we want to approximate a function f by a simpler positive function g . For example, $x^2 + 3x + 2 = O(x^3)$ for $x \geq 1$, since $|x^2 + 3x + 2| \leq 10x^3$ when $x \geq 1$. (We could have chosen other constants M instead of 10.) Usually we are not concerned with the value of a , and simply write ‘ $f(x) = O(g(x))$ ’ to mean ‘ $|f(x)| \leq Mg(x)$ when $x \geq a$, for some value of a ’: for example, $x^2 + 3x + 2 = O(x^3)$.

Note that $\sin x = O(1)$ since $|\sin x| \leq 1$, and (more generally) $f(x) = O(1)$ whenever f is bounded. Note also that Equation (2) implies that

$$\sum_{k \leq x} d(k) = x \log x + O(x),$$

although this is less informative than Equation (2).

Note also that $O(f(n))$ makes sense only for *positive* functions $f(n)$; otherwise, we have to write $O(|f(n)|)$.

5. *Combining ‘big oh’ terms.* Some ‘big oh’ terms are smaller than others, and can be omitted. For example, we can replace $f(x) + O(x) + O(x^3)$ by $f(x) + O(x^3)$, since the $O(x)$ term is ‘swallowed up’ by the $O(x^3)$ term. You will soon get used to combining ‘big oh’ terms in this way.
6. *The definition of $f(x) \sim g(x)$.* To say that $f(x) \sim g(x)$ means that the ‘relative error’, rather than the ‘absolute error’, tends to 0 as $x \rightarrow \infty$. An example of this asymptotic behaviour was given in the Introduction of the book (page 9) where we stated the prime number theorem in the form

$$\lim_{x \rightarrow \infty} \frac{\pi(x) \log x}{x} = 1.$$

This is often written in the form $\pi(x) \sim \frac{x}{\log x}$, and implies that if x is large then $\pi(x)$ is approximately equal to, or ‘behaves like’, $x/\log x$.

Self-assessment questions

- 3.1 Which of the following statements are true?

- (a) $2x^2 = O(x^3)$ (b) $2x^3 = O(x^2)$ (c) $3 \sin(2x^2) = O(x^2)$
 (d) $3 \sin(2x^2) = O(1)$ (e) $5[x] = O(x)$ (f) $5x = O([x])$
 (g) $x + O(x^2) = O(x^2)$ (h) $x^2 + O(x) = O(x)$

- 3.2 Prove that if $g(x) > 0$ for all x , and $f(x) = O(g(x))$, then

$$\int_a^x f(t) dt = O\left(\int_a^x g(t) dt\right).$$

- 3.3 Prove that if $f(x) \sim g(x)$ and $g(x) \sim h(x)$, then $f(x) \sim h(x)$.

Read Section 3.3

Commentary

1. *The statement of Theorem 3.1.* This is the main tool to be used in this chapter. Basically, the idea is to replace the sum $\sum_{y < n \leq x} f(n)$ by the integral $\int_y^x f(t) dt$, and then calculate the error in doing so. (The last three terms will generally be small compared with the first term.)

2. *A special case of Theorem 3.1.* A useful form of Euler's summation formula, which will be needed in Section 3.4, is as follows.

$$\sum_{1 \leq n \leq x} f(n) = \int_1^x f(t) dt + \int_1^x (t - [t])f'(t) dt + f(1) - (x - [x])f(x)$$

It is obtained from Theorem 3.1 by letting $y \rightarrow 1$ from below; it is NOT obtained by substituting $y = 1$. Alternatively, we can write

$$\sum_{1 \leq n \leq x} f(n) = f(1) + \sum_{1 < n \leq x} f(n),$$

and substitute $y = 1$ in Theorem 3.1.

3. *The proof of Theorem 3.1.* The proof given, although straightforward, is a little confusing to follow. Here is an alternative proof, given for the special case of Commentary 2 above.

We let $N = [x]$, and consider the term

$$\int_1^x (t - [t])f'(t) dt = \int_1^x tf'(t) dt - \int_1^x [t]f'(t) dt.$$

Integrating by parts, we have

$$\int_1^x tf'(t) dt = [tf(t)]_1^x - \int_1^x f(t) dt = xf(x) - f(1) - \int_1^x f(t) dt.$$

Also,

$$\begin{aligned} \int_1^x [t]f'(t) dt &= \int_1^2 f'(t) dt + 2 \int_2^3 f'(t) dt + \cdots \\ &\quad + (N-1) \int_{N-1}^N f'(t) dt + N \int_N^x f'(t) dt \\ &= \{f(2) - f(1)\} + 2\{f(3) - f(2)\} + \cdots \\ &\quad + (N-1)\{f(N) - f(N-1)\} + N\{f(x) - f(N)\} \\ &= -f(1) - f(2) - \cdots - f(N-1) - f(N) + Nf(x). \end{aligned}$$

So

$$\begin{aligned} \int_1^x (t - [t])f'(t) dt &= xf(x) - f(1) - \int_1^x f(t) dt \\ &\quad + f(1) + f(2) + \cdots + f(N) - Nf(x) \\ &= \sum_{1 \leq n \leq x} f(n) - \int_1^x f(t) dt - f(1) + (x - [x])f(x). \end{aligned}$$

Rearranging this equation gives the required result.

Self-assessment questions

- 3.4 Verify the statement of Euler's summation formula in Commentary 2, when $f(x) = 1$ and $f(x) = x$.
- 3.5 Write out the above form of Euler's summation formula in the following cases.
- $f(x) = 1/x$
 - $f(x) = 1/x^s$ ($s > 0, s \neq 1$)
 - $f(x) = x^\alpha$ ($\alpha \geq 0$)

These results will be needed in Section 3.4.

Read Section 3.4

Commentary

1. *The Riemann zeta function.* We shall study the Riemann zeta function $\zeta(s)$ in detail in Chapters 11 and 12. For the time being, note that $\zeta(1)$ is undefined (since $\sum \frac{1}{n}$ diverges) and $\zeta(2) = \sum \frac{1}{n^2}$, which equals $\frac{\pi^2}{6}$.

2. *The proof of Theorem 3.2(a).* The first step after using Euler's summation formula is to notice that $x - [x] < 1$, and hence $(x - [x])/x = O(1/x)$. The second step is to write

$$\int_1^x (t - [t])/t^2 dt = \int_1^\infty (t - [t])/t^2 dt - \int_x^\infty (t - [t])/t^2 dt.$$

The first integral on the right is a constant, and the second integral is $O\left(\int_x^\infty 1/t^2 dt\right) = O(1/x)$.

So $\sum_{n \leq x} \frac{1}{n} = \log x + A + O(1/x)$, where $A = 1 - \int_1^\infty (t - [t])/t^2 dt$,

and the last part of the proof shows that $A = C$, using Equation (3).

3. *The proof of Theorem 3.2(b).* This proof is very similar to that of part (a).

In the second line the integral $\int_1^x (t - [t])/t^{s+1} dt$ has been replaced by $\int_1^\infty (t - [t])/t^{s+1} dt + O(x^{-s})$, since

$$\int_x^\infty (t - [t])/t^{s+1} dt = O\left(\int_x^\infty 1/t^{s+1} dt\right) = O(x^{-s}).$$

4. *The proof of Theorem 3.2(d).* The last line follows since

$$\alpha \int_1^x t^{\alpha-1} dt = x^\alpha - 1 = O(x^\alpha) \quad \text{and} \quad 1/(\alpha + 1) = O(1) = O(x^\alpha).$$

Self-assessment questions

3.6 Use Theorem 3.2 to write down asymptotic formulas for the following.

$$\begin{array}{lll} \text{(a)} \sum_{n \leq x} n & \text{(b)} \sum_{n \leq x} n^2 & \text{(c)} \sum_{n \leq x} n^3 \\ \text{(d)} \sum_{n \leq x} n^{-2} & \text{(e)} \sum_{n \leq x} n^{-1/2} & \text{(f)} \sum_{n > x} n^{-2} \end{array}$$

3.7 Compare the values of $\sum_{n \leq x} n^2$ and $\sum_{n \leq x} n^{-2}$ with the approximations obtained in SAQ 3.6 parts (b) and (d), when $x = 10$.

Problems for Sections 3.1–3.4

3A Apostol, page 70, number 1(a).

3B Apostol, page 70, number 1(b).

Study Session 2: Sections 3.5–3.7 (pages 57–62)

Read Section 3.5

Commentary

1. *The proof of Theorem 3.3.* This proof is in two parts. The first part proves the weaker result $\sum d(n) \sim x \log x$ and the second part refines the method to prove the result in full.

The method used is a standard one which recurs later in the chapter.

Basically, the idea is to replace the sum $\sum_{n \leq x} d(n)$ by a sum $\sum 1$, summed over

all q and d such that $qd \leq x$. To determine this sum, we count the number of ‘integer points’ on the hyperbolas $qd = 1, qd = 2, \dots, qd = [x]$, and this is done by fixing d and letting q range from 1 to x/d .

2. *The equation $\sum_{q \leq x/d} 1 = x/d + O(1)$.* It is not necessary to use

Theorem 3.2(d) to prove this, since the left-hand side is $[x/d]$ which differs from x/d by less than 1. In the following lines of mathematics, note the way we write $\sum_{d \leq x} O(1) = O(x)$ and $xO(1/x) + O(x) = O(1) + O(x) = O(x)$, to

deal with the ‘big oh’ terms.

3. *Figure 3.2.* On the horizontal line with height d there are $[x/d]$ lattice points, d of which do not lie in the shaded region; so there are $[x/d] - d$ lattice points on the line segment shown. The number of lattice points on the bisecting diagonal line is $[\sqrt{x}]$: these points are $(1, 1), (2, 2), \dots, ([\sqrt{x}], [\sqrt{x}])$.

4. At the end of the proof, notice again how we deal with the ‘big oh’ terms:

$$2 \sum_{d \leq \sqrt{x}} O(1) = O(\sqrt{x}) \quad \text{and} \quad 2xO(1/\sqrt{x}) = O(\sqrt{x}).$$

Self-assessment question

- 3.8 Without looking at the book or the above commentary, write down *in words* the method of proof of Theorem 3.3.

Read Section 3.6

Commentary

1. *The proof of Theorem 3.4.* The method of proof is exactly the same as before, with the results of Section 3.4 again giving the required estimates. Notice how the first term $-x/2$ in the last line is absorbed into the $O(x \log x)$ term.

2. *The proof of Theorem 3.5.* Again, the method of proof is the same as for the weak version of Theorem 3.3. To obtain the last line, notice that $\frac{x^{\alpha+1}}{\alpha+1} \cdot \frac{x^{-\alpha}}{-\alpha} = O(x)$, $\frac{x^{\alpha+1}}{\alpha+1} O(x^{-\alpha-1}) = O(1)$, $O\left(x^\alpha \cdot \frac{x^{1-\alpha}}{1-\alpha}\right) = O(x)$, $O(x^\alpha \zeta(\alpha)) = O(x^\alpha)$, $O(x^\alpha O(x^{-\alpha})) = O(1)$, and the $O(1)$ term is absorbed into the other ‘big oh’ terms.
3. *The proof of Theorem 3.6.* Again, this is much as before, using parts (a) and (d) of Theorem 3.2 to provide the required estimates. Notice how the terms $x^{1-\beta}/(-\beta) + O(x^{-\beta})$ are replaced by $O(x^{1-\beta})$ in the last line.

Self-assessment question

3.9 Use Theorems 3.4–3.6 to write down asymptotic formulas for the following.

- (a) $\sum_{n \leq x} \sigma_2(n)$ (b) $\sum_{n \leq x} \sigma_{1/2}(n)$
(c) $\sum_{n \leq x} \sigma_{-2}(n)$ (d) $\sum_{n \leq x} \sigma_{-1/2}(n)$

Read Section 3.7

Commentary

1. The result $\sum_{n=1}^{\infty} \frac{\mu(n)}{n^2} = \frac{1}{\zeta(2)} = \frac{6}{\pi^2}$ will be proved in Chapter 11.
2. *The proof of Theorem 3.7.* This proof starts with the expression for $\phi(n)$ proved in Theorem 2.3, and proceeds just as in the previous two sections.
3. *The ‘big oh’ terms.* Notice how the term $\sum_{d \leq x} \mu(d) O\left(\frac{x}{d}\right)$ is replaced by $O\left(x \sum_{d \leq x} \frac{1}{d}\right)$, since $|\mu(d)| \leq 1$ for all d . In the last line, the term $\frac{1}{2}x^2 O\left(\frac{1}{x}\right)$, which is $O(x)$, is ‘swallowed up’ by the $O(x \log x)$ term.

Self-assessment question

3.10 Compare the value of $\sum_{n \leq x} \phi(n)$ with the approximation $3x^2/\pi^2$, when $x = 10$.

Problems for Sections 3.5–3.7

- 3C Write out the proof of Theorem 3.5 in the case $\alpha = 2$.
- 3D Apostol, page 70, number 2.
- 3E Apostol, page 71, number 6.
-

Study Session 3: Sections 3.9–3.12 (pages 64–70)

Read Sections 3.9, 3.10 and 3.12

Commentary

1. In this reading section we prove a result on the partial sums of a Dirichlet product in Section 3.10, and generalize it in Section 3.12. The proof of Theorem 3.10 uses the associative law (Theorem 2.21) in the form $f \circ (g \circ U) = (f * g) \circ U = h \circ U = H$.

2. *The statement of Theorem 3.17.* Putting $a = 1$ gives $b = x$, and so the right-hand side of (24) reduces to

$$f(1)G(x) + \sum_{n \leq x} g(n)F\left(\frac{x}{n}\right) - F(1)G(x) - \sum_{n \leq x} g(n)F\left(\frac{x}{n}\right),$$

since $F(1) = f(1)$. Similarly, putting $b = 1$ gives $a = x$, and the right-hand side reduces to $\sum_{n \leq x} f(n)G\left(\frac{x}{n}\right)$.

Thus Theorem 3.17 is a generalization of Theorem 3.10.

3. *The proof of Theorem 3.17.* To see that the expression for $H(x)$ is the same as (24), we write

$$\begin{aligned} H(x) &= \sum_{n \leq a} f(n) \sum_{q \leq x/n} g(q) + \sum_{n \leq b} g(n) \sum_{d \leq x/n} f(d) - \sum_{d \leq a} f(d) \sum_{q \leq b} g(q) \\ &= \sum_{n \leq a} f(n)G\left(\frac{x}{n}\right) + \sum_{n \leq b} g(n)F\left(\frac{x}{n}\right) - F(a)G(b), \quad \text{as required.} \end{aligned}$$

Self-assessment questions

3.11 Use the method of proof of Theorem 3.17 to prove Theorem 3.10.

3.12 Verify Theorem 3.17 when $x = 4$ in the cases

- (a) $a = 1, b = 4$; (b) $a = b = 2$.

Read Section 3.11

Commentary

1. *The proof of Theorem 3.12.* Recall that $\sum_{d|n} \mu(d) = [1/n]$ (Theorem 2.1) and

$\sum_{d|n} \Lambda(d) = \log n$ (Theorem 2.10). Note also that

$$\sum_{n \leq x} \log n = \log 1 + \log 2 + \cdots + \log [x] = \log(1 \cdot 2 \cdot \cdots \cdot [x]) = \log([x]!).$$

2. *Line 3 of page 67.* Note that we have split the term $\{x\}$ away from the remaining terms. The inequality follows since

$$\sum_{2 \leq n \leq x} \{x/n\} < \sum_{2 \leq n \leq x} 1 = [x] - 1.$$

3. *The statement of Theorem 3.14.* This theorem tells us the highest power of p that divides $[x]!$. For example, if $x = 100$ and $p = 3$, then the highest power of 3 that divides $100!$ is $3^{\alpha(3)}$, where

$$\alpha(3) = \left[\frac{100}{3}\right] + \left[\frac{100}{9}\right] + \left[\frac{100}{27}\right] + \left[\frac{100}{81}\right] = 33 + 11 + 3 + 1 = 48.$$

Note that this is a finite sum: all succeeding terms $(\left[\frac{100}{243}\right], \left[\frac{100}{729}\right], \dots)$ are zero.

4. *The proof of Theorem 3.16.* In this proof we first replace the summation over n by a summation over prime powers p^m , all other terms being zero. We then split off the main term, corresponding to the sum over primes p (that is, $m = 1$), and show that the remaining terms (with $m \geq 2$) are $O(x)$.

This involves summing the geometric series $\sum_{m=2}^{\infty} p^{-m}$ and replacing the resulting sum over p by the corresponding (larger) sum over n . Since this latter sum converges (and is therefore $O(1)$), the result follows.

Self-assessment questions

3.13 Verify the statements of Theorem 3.12 and 3.13 when $x = 4\frac{1}{2}$.

3.14 Find the highest power of 7 dividing $500!$.

3.15 By calculating $\alpha(2)$, $\alpha(3)$, $\alpha(5)$ and $\alpha(7)$, factorize $10!$.

3.16 Verify that $\sum_{n \leq x} \Lambda(n) \left[\frac{x}{n}\right] = \sum_p \sum_{m=1}^{\infty} \left[\frac{x}{p^m}\right] \log p$, when $x = 10\frac{1}{2}$.

Problems for Sections 3.9–3.12

3F Apostol, page 70, number 4. [Hint: $[x/n] = x/n + O(1)$.]

3G Apostol, page 70, number 5.

Solutions to the Self-assessment questions

Historical introduction and Chapter 1

1.1 101, 103, 107, 109, 113, 127, 131, 137, 139, 149.

1.2 On summing the appropriate arithmetic progressions, we have:

(a) $1 + 2 + 3 + \cdots + n = \frac{1}{2}n(n+1)$;

(b) $1 + 4 + 7 + \cdots + (3n-2) = \frac{1}{2}n(3n-1)$.

1.3 (a) (i) $n^2 + \left\{\frac{1}{2}(n^2-1)\right\}^2 = \frac{1}{4}\{4n^2 + (n^4 - 2n^2 + 1)\}$
 $= \frac{1}{4}(n^4 + 2n^2 + 1) = \left\{\frac{1}{2}(n^2 + 1)\right\}^2$.

(ii) $(4n)^2 + (4n^2-1)^2 = 16n^2 + (16n^4 - 8n^2 + 1)$
 $= 16n^4 + 8n^2 + 1 = (4n^2 + 1)^2$.

(iii) $\{t(a^2 - b^2)\}^2 + (2tab)^2 = t^2\{(a^4 - 2a^2b^2 + b^4) + 4a^2b^2\}$
 $= t^2(a^4 + 2a^2b^2 + b^4) = \{t(a^2 + b^2)\}^2$.

(b) $t = 1, a = 6, b = 1$ and $t = 3, a = 2, b = 1$.

1.4 (a) $2^{11} - 1$ is not prime: $2047 = 23 \cdot 89$.

(b) The proper divisors of $2^{p-1}P$, where $P = 2^p - 1$ is prime, are $1, 2, 2^2, \dots, 2^{p-1}$ and $P, 2P, 2^2P, \dots, 2^{p-2}P$. Their sum is

$$(1 + 2 + 2^2 + \cdots + 2^{p-1}) + P(1 + 2 + \cdots + 2^{p-2})$$
$$= (2^p - 1) + P(2^{p-1} - 1) = 2^{p-1}(2^p - 1).$$

1.5 There are several possible answers — for example:

(a) $30 = 15 + 15$; $35 = 1 + 6 + 28$; $40 = 1 + 3 + 36$;

(b) $30 = 1 + 4 + 25$; $35 = 1 + 9 + 25$; $40 = 4 + 36$;

(c) $30 = 1 + 5 + 12 + 12$; 35 is pentagonal; $40 = 5 + 35$.

1.6 $53 = 7^2 + 2^2$; $61 = 6^2 + 5^2$; $73 = 8^2 + 3^2$.

1.7 (a) $(n+1)! + 2$ is divisible by 2, $(n+1)! + 3$ is divisible by 3, \dots , $(n+1)! + (n+1)$ is divisible by $n+1$. So the given n numbers are all composite.

(b) $101! + 2, 101! + 3, \dots, 101! + 101$.

1.8 Since $x^2 + ax + b$ is a prime number when $x = 0$ and $x = 1$, b and $1 + a + b$ are prime. But then, when $x = b$, $x^2 + ax + b = b(1 + a + b)$, which is composite.

1.9 If a and b are both divisible by the prime p , then so is every number of the form $ax + b$, for $x = 1, 2, \dots$, and hence there can be no prime numbers of this form.

1.10 (a) If $x = [x] + \theta$, where $0 \leq \theta < 1$, then $x + n = [x] + n + \theta$, and so $[x + n] = [x] + n$.

(b) Let $x = [x] + \theta$. If $0 \leq \theta < \frac{1}{2}$, then $2x = 2[x] + 2\theta$ gives $[2x] = 2[x]$; if $\frac{1}{2} \leq \theta < 1$, then $2x = 2[x] + 2\theta$ gives $[2x] = 2[x] + 1$.

1.11 (a) $\pi(50) = 15$, $x/\log x = 12.781$, so $\pi(x) \div x/\log x = 1.174$.

(b) $\pi(150) = 35$, $x/\log x = 29.936$, so $\pi(x) \div x/\log x = 1.169$.

- 1.12** (a) $30 = 23 + 7$, $32 = 29 + 3$, $34 = 29 + 5$, $36 = 29 + 7$, $38 = 31 + 7$,
 $40 = 37 + 3$.
 (b) $30 = 37 - 7$, $32 = 37 - 5$, $34 = 37 - 3$, $36 = 43 - 7$, $38 = 43 - 5$,
 $40 = 43 - 3$.
 (c) 3, 5; 5, 7; 11, 13; 17, 19; 29, 31.
 (d) 2, 5, 17, 37, 101.
 (e) 3, 11, 83.
 (f) 37, 53, 67, 83, 101.
 (g) 37, 53, 67, 83, 101.

1.13 The result is clearly true when $n = 1$. So assume that $\frac{(2n)!}{n!n!} \geq 2^n$. Then

$$\frac{(2(n+1))!}{(n+1)!(n+1)!} = \frac{(2n+2)(2n+1)}{(n+1)(n+1)} \cdot \frac{(2n)!}{n!n!} \geq \frac{2(2n+1)}{n+1} \cdot 2^n \geq 2^{n+1}.$$

The result follows by induction.

1.14 If the principle of induction is false, then there exist some positive integers that do not belong to Q . Let A be the set of such integers. By the well-ordering principle, A contains a smallest number — call it $n + 1$. (By (a), it cannot be 1.) Then $n \in Q$. This contradiction establishes the result.

- 1.15** (c) If $d|n$ and $d|m$, then $n = rd$, $m = sd$ for some integers r and s .
 So $an + bm = ard + bsd = (ar + bs)d$, so $d|(an + bm)$.
 (e) If $ad|an$, then $an = r \cdot ad$ for some integer r .
 Dividing by a ($\neq 0$) gives $n = rd$, so $d|n$.
 (j) If $d|n$ and $n|d$, then $n = rd$, $d = sn$ for some integers r and s .
 So $n = r \cdot sn$, giving $rs = 1$. This is possible only if $r = \pm 1$ and $s = r$,
 so $|d| = |n|$.
 (k) If $d|n$, then $n = rd$ for some integer r .
 So $r = n/d$ and $r|n$, and hence $(n/d)|n$.

- 1.16** (a) $d = 5$; $5 = (0 \times 25) + (1 \times 5)$.
 (b) $d = 6$; $6 = ((-1) \times 30) + ((-2) \times (-18))$.
 (c) $d = 1$; $1 = ((-11) \times 9) + (4 \times 25)$.
 (d) $d = 3$; $3 = (8 \times (-21)) + ((-3) \times (-57))$.

1.17 Let $d = (a, (b, c))$. Then $d|a$ and $d|(b, c)$, so $d|a$ and $d|b$ and $d|c$.

So $d|(a, b)$ and $d|c$, and hence $d|((a, b), c)$.

A similar argument proves that $((a, b), c)|(a, (b, c))$, and so

$$(a, (b, c)) = ((a, b), c).$$

When $a = 42$, $b = 70$ and $c = 30$, the left-hand side is $(42, 10) = 2$ and the right-hand side is $(14, 30) = 2$.

1.18 If $(a, b) = d$, then $d|a$, $d|b$ and $d = ax + by$ for some integers x and y .
 So $1 = (a/d)x + (b/d)y$. It follows that $(a/d, b/d) = 1$, since if c were a common factor of a/d and b/d , then c would also be a factor of $(a/d)x + (b/d)y = 1$, by Theorem 1.1(c).

- 1.19** (a) If n is composite, then it has at least two prime divisors (not necessarily different). If each prime divisor of n exceeds \sqrt{n} , then their product exceeds n , which is a contradiction.

- (b) Omitting the multiples of 2, 3 and 5 leaves the list

151, 157, 161, 163, 167, 169, 173, 179, 181, 187, 191, 193, 197, 199.

The only multiples of 7, 11 and 13 in this list are 161, 187 and 169, respectively, and we need go no further since 13 is the largest prime $\leq \sqrt{200}$. Removing these three numbers leaves the primes

151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199.

- 1.20** Clearly no $p_i | N$ since each p_i divides *all but one* of the terms in the sum — for example, p_1 does not divide $p_2 \dots p_n$. So N is prime or a product of primes, which is impossible if p_1, \dots, p_n are the only primes.

- 1.21** $n^4 + 4 = (n^2 - 2n + 2)(n^2 + 2n + 2)$, and both terms are > 1 if $n > 1$.

- 1.22** (a) $2^3 \cdot 5^3$ (b) $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11$ (c) $2^2 \cdot 3 \cdot 7^3$ (d) 3^7

- 1.23** (a) $1 = 2^0 \cdot 3^0 \cdot 5^0$; $2 = 2^1 \cdot 3^0 \cdot 5^0$; $3 = 2^0 \cdot 3^1 \cdot 5^0$; $4 = 2^2 \cdot 3^0 \cdot 5^0$;
 $5 = 2^0 \cdot 3^0 \cdot 5^1$; $6 = 2^1 \cdot 3^1 \cdot 5^0$; $10 = 2^1 \cdot 3^0 \cdot 5^1$; $12 = 2^2 \cdot 3 \cdot 5^0$;
 $15 = 2^0 \cdot 3^1 \cdot 5^1$; $20 = 2^2 \cdot 3^0 \cdot 5^1$; $30 = 2^1 \cdot 3^1 \cdot 5^1$; $60 = 2^2 \cdot 3^1 \cdot 5^1$.

- (b) There are $a_1 + 1$ possibilities for the power of p_1 , $a_2 + 1$ possibilities for the power of p_2 , \dots , $a_r + 1$ possibilities for the power of p_r . The total number of possibilities is therefore $(a_1 + 1)(a_2 + 1) \dots (a_r + 1)$, and each corresponds to just one positive divisor of n .

- (c) For the numbers in SAQ 1.22,

(a) $4 \cdot 4 = 16$, (b) $2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 32$, (c) $3 \cdot 2 \cdot 4 = 24$, (d) 8.

- 1.24** (a) (i) $2^1 \cdot 3^0 \cdot 5^1 \cdot 7^0 \cdot 11^0 = 10$; (ii) $2^1 \cdot 3^1 \cdot 5^0 \cdot 7^1 \cdot 11^0 = 42$;
 (iii) $2^0 \cdot 3^0 \cdot 5^0 = 1$.
 (b) (i) $2^3 \cdot 3^1 \cdot 5^3 \cdot 7^1 \cdot 11^1 = 231\,000$; (ii) $2^2 \cdot 3^1 \cdot 5^1 \cdot 7^3 \cdot 11^1 = 226\,380$;
 (iii) $2^3 \cdot 3^7 \cdot 5^3 = 2\,187\,000$.

- 1.25** (a) $p_3 = 5$ (since $\frac{1}{2} + \frac{1}{3} + \frac{1}{5} > 1$). (b) $p_{10} = 29$.

- 1.26** If there were only finitely many primes, then $\sum p^{-1}$ would be a finite sum, and hence convergent. This contradicts Theorem 1.13.

- 1.27** $544 = 2 \cdot 238 + 68$ $34 = 238 - 3 \cdot 68$
 $238 = 3 \cdot 68 + 34$ $= 238 - 3 \cdot (544 - 2 \cdot 238)$
 $68 = 2 \cdot 34$ $= 7 \cdot 238 - 3 \cdot 544$
 So $d = 34$. So $x = -3$, $y = 7$.

- 1.28** (a) 3 (b) 1

Chapter 2

- 2.1**

n	31	32	33	34	35	36	37	38	39	40	41	42
$\mu(n)$	-1	0	1	1	1	0	-1	1	1	0	-1	-1

- 2.2** $\sum_{d|27} \mu(d) = \mu(1) + \mu(3) + \mu(9) + \mu(27) = 1 + (-1) + 0 + 0 = 0$;

$$\sum_{d|28} \mu(d) = \mu(1) + \mu(2) + \mu(4) + \mu(7) + \mu(14) + \mu(28) \\ = 1 + (-1) + 0 + (-1) + 1 + 0 = 0;$$

$$\sum_{d|29} \mu(d) = \mu(1) + \mu(29) = 1 + (-1) = 0;$$

$$\sum_{d|30} \mu(d) = \mu(1) + \mu(2) + \mu(3) + \mu(5) + \mu(6) + \mu(10) + \mu(15) + \mu(30) \\ = 1 + (-1) + (-1) + (-1) + 1 + 1 + 1 + (-1) = 0.$$

2.3 $60 = 2^2 \cdot 3 \cdot 5$, so we can ignore $\mu(d)$ whenever d is divisible by 2^2 ; so

$$\begin{aligned}\sum_{d|60} \mu(d) &= \mu(1) + \{\mu(2) + \mu(3) + \mu(5)\} + \{\mu(2 \cdot 3) + \mu(2 \cdot 5) + \mu(3 \cdot 5)\} + \mu(2 \cdot 3 \cdot 5) \\ &= 1 + \binom{3}{1}(-1) + \binom{3}{2}(-1)^2 + (-1)^3 \\ &= (1-1)^3 = 0.\end{aligned}$$

2.4 (a) If $n = 10$, the left-hand side is $f(1) + f(2) + f(5) + f(10)$, and the right-hand side is $f(10) + f(5) + f(2) + f(1)$, which is the same. In general, as d runs through all the divisors of n , so does n/d , and so each term $f(d)$ on the left-hand side occurs exactly once on the right-hand side, and vice versa.

(b) By part (a) and Theorem 2.1,

$$\sum_{d|n} \mu(n/d) = \sum_{d|n} \mu(d) = 0, \quad \text{since } n > 1.$$

2.5 (a) 10 (b) 8 (c) 2

2.6

n	11	12	13	14	15	16	17	18	19	20
$\phi(n)$	10	4	12	6	8	8	16	6	18	8

2.7 (a) $\sum_{d|18} \phi(d) = \phi(1) + \phi(2) + \phi(3) + \phi(6) + \phi(9) + \phi(18)$
 $= 1 + 1 + 2 + 2 + 6 + 6 = 18.$

(b) $A(1) = \{1, 5, 7, 11, 13, 17\}$, $A(2) = \{2, 4, 8, 10, 14, 16\}$,
 $A(3) = \{3, 15\}$, $A(6) = \{6, 12\}$, $A(9) = \{9\}$, $A(18) = \{18\}.$

2.8 (a) If $1 \leq a \leq p$, then $(a, p) = 1$ except when $a = p$; thus $\phi(p) = p - 1$.
If $1 \leq a \leq p^\alpha$, then $(a, p^\alpha) = 1$ except when a is a multiple of p , and there are $p^{\alpha-1}$ such multiples; thus $\phi(p^\alpha) = p^\alpha - p^{\alpha-1}$.

(b) $\sum_{d|p^\alpha} \phi(d) = \phi(1) + \phi(p) + \phi(p^2) + \cdots + \phi(p^\alpha)$
 $= 1 + (p-1) + (p^2-p) + \cdots + (p^\alpha - p^{\alpha-1}) = p^\alpha.$

2.9 $\left[\frac{1}{(n, k)} \right] = 1$ only when $(n, k) = 1$, so $\sum_{k=1}^n \left[\frac{1}{(n, k)} \right] = \sum_{k=1}^n 1 = \phi(n).$

But $\left[\frac{1}{(n, k)} \right] = \sum_{d|(n, k)} \mu(d)$, by Theorem 2.1, so $\phi(n) = \sum_{k=1}^n \sum_{d|(n, k)} \mu(d).$

2.10 $\sum_{d|18} \mu(d) \frac{18}{d} = 18\mu(1) + 9\mu(2) + 6\mu(3) + 3\mu(6) + 2\mu(9) + 1\mu(18)$
 $= 18 - 9 - 6 + 3 + 0 + 0 = 6 = \phi(18).$

2.11 $120 = 2^3 \cdot 3 \cdot 5$, so $\phi(120) = 120 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} = 32$.
 $210 = 2 \cdot 3 \cdot 5 \cdot 7$, so $\phi(210) = 210 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} \cdot \frac{6}{7} = 48$.

2.12 (a) If n is not a multiple of 3, then (by Theorem 2.5(c))

$$\phi(3n) = \phi(3)\phi(n) = 2\phi(n).$$

(b) If n is a multiple of 3, then $n = 3^k m$, where $3 \nmid m$. Then (by Theorem 2.5(c))

$$\phi(3n) = \phi(3^{k+1})\phi(m) = 2 \cdot 3^k \phi(m) = 3(2 \cdot 3^{k-1} \phi(m)) = 3\phi(n).$$

2.13 (a) This follows from Theorem 2.7.

(b) $(\mu * u)(n) = \sum_{d|n} \mu(d) = I(n)$, by Theorem 2.1.

(c) $(u * u)(n) = \sum_{d|n} 1 = \sigma_0(n)$.

(d) $(N * u)(n) = \sum_{d|n} d = \sigma_1(n)$.

2.14 $\sum_{d|n} f(d) = (f * u)(n) = (u * f)(n) = \sum_{d|n} f\left(\frac{n}{d}\right)$.

2.15 $\sigma_1(n) = (N * u)(n) = (u * N)(n) = \sum_{d|n} \frac{n}{d} = n \sum_{d|n} \frac{1}{d}$.

2.16 (a) $\sum_{d|n} \sigma_1(d) = (\sigma_1 * u)(n) = ((N * u) * u)(n) = ((u * u) * N)(n)$
 $= (\sigma_0 * N)(n) = \sum_{d|n} \sigma_0(d) \cdot \frac{n}{d} = n \sum_{d|n} \sigma_0(d)/d$.

(b) $\sum_{d|n} d\sigma_0(d) = ((N * N) * u)(n)$ (since $(N * N)(n) = \sum_{d|n} d \cdot \frac{n}{d} = n\sigma_0(n)$)
 $= ((N * u) * N)(n)$
 $= \sum_{d|n} \sigma_1(d) \cdot \frac{n}{d} = n \sum_{d|n} \sigma_1(d)/d$.

2.17 Since $\phi(1) = 1$, $\phi(p) = p - 1$, $\phi(q) = q - 1$, $\phi(pq) = (p - 1)(q - 1)$, and $\phi(p^2) = p^2 - p$, we have

$$\begin{aligned}\phi^{-1}(1) &= 1, \\ \phi^{-1}(p) &= -\phi(p)\phi^{-1}(1) = 1 - p, \\ \phi^{-1}(p^2) &= -\{\phi(p^2)\phi^{-1}(1) + \phi(p)\phi^{-1}(p)\} \\ &= -\{(p^2 - p) + (p - 1)(1 - p)\} = 1 - p\end{aligned}$$

and

$$\phi^{-1}(pq) = 2\phi(p)\phi(q) - \phi(1)\phi(pq) = (p - 1)(q - 1),$$

by the formula in Commentary 2.

2.18 $f^{-1}(1) = 1$ and $f^{-1}(p) = -f(p)$. So

$$\begin{aligned}f^{-1}(p^2) &= -\{f(p^2)f^{-1}(1) + f(p)f^{-1}(p)\} = f(p)^2 - f(p^2), \\ f^{-1}(p^3) &= -\{f(p^3)f^{-1}(1) + f(p^2)f^{-1}(p) + f(p)f^{-1}(p^2)\} \\ &= -f(p)^3 + 2f(p)f(p^2) - f(p^3).\end{aligned}$$

2.19 $(f * g) * (f^{-1} * g^{-1}) = (f * f^{-1}) * (g * g^{-1}) = I$, so $(f * g)^{-1} = f^{-1} * g^{-1}$.

2.20 By SAQ 2.13 parts (c) and (d), $u * u = \sigma_0$ and $N * u = \sigma_1$. So

(a) $u = \sigma_0 * \mu$ — that is, $\sum_{d|n} \sigma_0(d)\mu\left(\frac{n}{d}\right) = 1$;

(b) $N = \sigma_1 * \mu$ — that is, $\sum_{d|n} \sigma_1(d)\mu\left(\frac{n}{d}\right) = n$.

2.21

n	21	22	23	24	25	26	27	28	29	30
$\Lambda(n)$	0	0	$\log 23$	0	$\log 5$	0	$\log 3$	0	$\log 29$	0

$$\begin{aligned}
2.22 \quad \sum_{d|18} \Lambda(d) &= \Lambda(1) + \Lambda(2) + \Lambda(3) + \Lambda(6) + \Lambda(9) + \Lambda(18) \\
&= 0 + \log 2 + \log 3 + 0 + \log 3 + 0 = \log 18. \\
-\sum_{d|18} \mu(d) \log d &= -\mu(1) \log 1 - \mu(2) \log 2 - \mu(3) \log 3 - \mu(6) \log 6 \\
&\quad - \mu(9) \log 9 - \mu(18) \log 18 \\
&= 0 + \log 2 + \log 3 - \log 6 + 0 + 0 = 0 = \Lambda(18).
\end{aligned}$$

2.23 $f(mn) = 1$ if mn is a perfect square, and 0 otherwise. If $(m, n) = 1$, this means that $f(mn) = 1$ if m and n are perfect squares, and 0 otherwise. So $f(mn) = f(m)f(n)$ if $(m, n) = 1$, and hence f is multiplicative. But f is not completely multiplicative, since $f(4) = 1$ but $f(2)f(2) = 0$.

2.24 If $m = p_1^{a_1} \dots p_r^{a_r}$, $n = q_1^{b_1} \dots q_s^{b_s}$ and $(m, n) = 1$, then $g(m, n) = 2^{r+s} = 2^r \cdot 2^s = g(m)g(n)$, so g is multiplicative. But g is not completely multiplicative, since $g(4) = 2$ but $g(2)g(2) = 4$.

2.25 (a) If f is multiplicative, then

$$\begin{aligned}
f(p_1^{a_1} p_2^{a_2} \dots p_r^{a_r}) &= f(p_1^{a_1}) f(p_2^{a_2} \dots p_r^{a_r}) \\
&= \dots = f(p_1^{a_1}) f(p_2^{a_2}) \dots f(p_r^{a_r}).
\end{aligned}$$

Conversely, if $m = p_1^{a_1} \dots p_r^{a_r}$, $n = q_1^{b_1} \dots q_s^{b_s}$ and $(m, n) = 1$, then

$$f(mn) = \prod f(p_k^{a_k}) \prod f(q_l^{b_l}) = f(m)f(n).$$

(b) If f is completely multiplicative, then

$$f(p^a) = f(p \cdot p^{a-1}) = f(p)f(p^{a-1}) = \dots = f(p)^a.$$

Conversely, if $m = p_1^{a_1} \dots p_r^{a_r}$, $n = q_1^{b_1} \dots q_s^{b_s}$, then

$$f(mn) = \prod f(p_k)^{a_k} f(q_l)^{b_l} = f(m)f(n).$$

2.26 Since $\phi = \mu * N$, and μ and N are multiplicative, the result follows from Theorem 2.14.

$$\begin{aligned}
2.27 \quad (a) \quad \sum_{d|n} \mu(d) \sigma_0(d) &= \prod_{p|n} (1 - \sigma_0(p)) = \prod_{p|n} (-1) = (-1)^r \\
(b) \quad \sum_{d|n} \mu(d) \sigma_1(d) &= \prod_{p|n} (1 - \sigma_1(p)) = \prod_{p|n} (-p) = (-1)^r p_1 p_2 \dots p_r \\
(c) \quad \sum_{d|n} \mu(d)/d &= \prod_{p|n} (1 - 1/p) = (1 - 1/p_1)(1 - 1/p_2) \dots (1 - 1/p_r) \\
&= \phi(n)/n, \text{ by Theorem 2.4.} \\
(d) \quad \sum_{d|n} d\mu(d) &= \prod_{p|n} (1 - p) = (1 - p_1)(1 - p_2) \dots (1 - p_r) \\
&= \phi^{-1}(n), \text{ by the Example on page 37 of Apostol.}
\end{aligned}$$

2.28

n	11	12	13	14	15	16	17	18	19	20
$\lambda(n)$	-1	-1	-1	1	1	1	-1	-1	-1	-1
$\sigma_0(n)$	2	6	2	4	4	5	2	6	2	6
$\sigma_1(n)$	12	28	14	24	24	31	18	39	20	42

2.29 If $n = p_1^{a_1} \dots p_r^{a_r}$, then $\sigma_0(n) = (a_1 + 1) \dots (a_r + 1)$. If $\sigma_0(n)$ is odd, then each term $a_k + 1$ is odd, so that each a_k is even and n is a perfect square. Conversely, if n is a perfect square, then each a_k is even, so that $\sigma_0(n)$ is odd.

Alternatively, pair off the divisors d and n/d . Then d pairs with itself if and only if $n = d^2$. The result now follows easily.

$$\begin{aligned} 2.30 \quad \sum_{d|n} \sigma_2(d) &= (\sigma_2 * u)(n) = \{(N^2 * u) * u\}(n) = \{(u * u) * N^2\}(n) \\ &= \sum_{d|n} \sigma_0(d)(n/d)^2 = n^2 \sum_{d|n} \sigma_0(d)/d^2. \end{aligned}$$

2.31 Take $\alpha = \mu$, $\beta = u$ and $F(x) = [x]$; then

$$\begin{aligned} \sum_{n \leq x} \mu(n) \sum_{m \leq x/n} \left[\frac{x}{mn} \right] &= \{\mu \circ (u \circ F)\}(x) \\ &= \{(\mu * u) \circ F\}(x) = (I \circ F)(x) = F(x) = [x]. \end{aligned}$$

2.32 If $\alpha = u$ and $F(x) = 1$ for $x \geq 1$, then $G(x) = \sum_{n \leq x} 1 = [x]$.

So, by Theorem 2.23, $1 = \sum_{n \leq x} \mu(n)[x/n]$, as required.

2.33 Putting $x = 1$ gives

$$G(1) = \alpha(1)F(1) \iff F(1) = \mu(1)\alpha(1)G(1),$$

which is true since $\mu(1) = \alpha(1) = 1$.

Putting $x = 2$ gives

$$G(2) = \alpha(1)F(2) + \alpha(2)F(1) \iff F(2) = \mu(1)\alpha(1)G(2) + \mu(2)\alpha(2)G(1),$$

which is true since $\mu(1) = \alpha(1) = 1$, $\mu(2) = -1$ and $F(1) = G(1)$.

Chapter 3

3.1 All are true except (b) and (h).

3.2 $|f(x)| \leq Mg(x)$, so

$$\left| \int_a^x f(t) dt \right| \leq \int_a^x |f(t)| dt \leq \int_a^x Mg(t) dt = M \int_a^x g(t) dt,$$

as required.

3.3 $\lim_{x \rightarrow \infty} f(x)/g(x) = 1$ and $\lim_{x \rightarrow \infty} g(x)/h(x) = 1$, so

$$\begin{aligned} \lim_{x \rightarrow \infty} \frac{f(x)}{h(x)} &= \lim_{x \rightarrow \infty} \frac{f(x)}{g(x)} \cdot \frac{g(x)}{h(x)} \\ &= \lim_{x \rightarrow \infty} \frac{f(x)}{g(x)} \cdot \lim_{x \rightarrow \infty} \frac{g(x)}{h(x)} = 1. \end{aligned}$$

3.4 When $f(x) = 1$, the left-hand side is $[x]$, and the right-hand side is $(x-1) + 0 + 1 - (x - [x]) = [x]$.

When $f(x) = x$, the left-hand side is $1 + 2 + \cdots + [x] = \frac{1}{2}[x]([x] + 1)$, and the right-hand side is

$\frac{1}{2}(x^2 - 1) + \frac{1}{2}(x^2 - 1) - (1 + 2 + \cdots + [x - 1] + [x](x - [x])) + 1 - (x - [x])x$, which reduces to $\frac{1}{2}[x]([x] + 1)$.

$$3.5 \quad (a) \quad \sum_{1 \leq n \leq x} \frac{1}{n} = \log x - \int_1^x (t - [t])/t^2 dt + 1 - (x - [x])/x$$

$$(b) \quad \sum_{1 \leq n \leq x} \frac{1}{n^s} = \frac{(x^{1-s} - 1)}{1-s} - s \int_1^x (t - [t])/t^{s+1} dt + 1 - (x - [x])/x^s$$

$$(c) \quad \sum_{1 \leq n \leq x} n^\alpha = \frac{(x^{\alpha+1} - 1)}{\alpha + 1} + \alpha \int_1^x (t - [t])t^{\alpha-1} dt + 1 - (x - [x])x^\alpha$$

- 3.6** (a) $\frac{1}{2}x^2 + O(x)$, by part (d).
 (b) $\frac{1}{3}x^3 + O(x^2)$, by part (d).
 (c) $\frac{1}{4}x^4 + O(x^3)$, by part (d).
 (d) $-\frac{1}{x} + \zeta(2) + O(x^{-2})$, by part (b).
 (e) $2\sqrt{x} + \zeta(\frac{1}{2}) + O(x^{-1/2})$, by part (b).
 (f) $O(x^{-1})$, by part (c).

- 3.7** (b) $\sum_{n \leq 10} n^2 = 385$; $\frac{1}{3}x^3 = 333$.
 (d) $\sum_{n \leq 10} n^{-2} = 1.5498$; $-\frac{1}{10} + \zeta(2) = 1.5449$.

- 3.8** The first step is to write $\sum d(n)$ as a sum involving the lattice points on the hyperbolas $qd = 1, \dots, qd = [x]$. To count these lattice points we fix d and let q range from 1 to x/d , using the results of the previous section to give us the required estimates. This yields the weak version $\sum d(n) \sim x \log x$. To obtain Dirichlet's form of the result, we use the symmetry of the hyperbolas about the diagonal, again using the results of the previous section to give us the required estimates.

- 3.9** (a) $\frac{1}{3}\zeta(3)x^3 + O(x^2)$
 (b) $\frac{2}{3}\zeta(\frac{3}{2})x^{3/2} + O(x)$
 (c) $\zeta(3)x + O(1)$
 (d) $\zeta(\frac{3}{2})x + O(x^{1/2})$

- 3.10** $\sum_{n \leq 10} \phi(n) = 1 + 1 + 2 + 2 + 4 + 2 + 6 + 4 + 6 + 4 = 32$; $300/\pi^2 = 30.396\dots$

- 3.11** Summing over the lattice points in the hyperbolic region shown, we have

$$H(x) = \sum_{\substack{q,d \\ qd \leq x}} f(d)g(q) = \sum_{d \leq x} f(d) \sum_{q \leq x/d} g(q) = \sum_{n \leq x} f(n)G\left(\frac{x}{n}\right).$$

Similarly,

$$H(x) = \sum_{\substack{q,d \\ qd \leq x}} f(d)g(q) = \sum_{q \leq x} g(q) \sum_{d \leq x/q} f(d) = \sum_{n \leq x} g(n)F\left(\frac{x}{n}\right).$$

- 3.12** $\sum_{\substack{q,d \\ qd \leq 4}} f(d)g(q) = f(1)g(1) + f(2)g(1) + f(3)g(1) + f(4)g(1) + f(1)g(2) \\ + f(2)g(2) + f(1)g(3) + f(1)g(4).$

- (a) The right-hand side of (24) is

$$\begin{aligned} & f(1)G(4) + \sum_{n \leq 4} g(n)F\left(\frac{x}{n}\right) - F(1)G(4) \\ &= \sum_{n \leq 4} g(n)F\left(\frac{x}{n}\right) \\ &= g(1)F(4) + g(2)F(2) + g(3)F(4/3) + g(4)F(1) \\ &= g(1)\{f(1) + f(2) + f(3) + f(4)\} + g(2)\{f(1) + f(2)\} \\ &\quad + g(3)f(1) + g(4)f(1), \end{aligned}$$

which agrees with the above sum.

(b) The right-hand side of (24) is

$$\begin{aligned} & \{f(1)G(4) + f(2)G(2)\} + \{g(1)F(4) + g(2)F(2)\} - F(2)G(2) \\ &= f(1)\{g(1) + g(2) + g(3) + g(4)\} + f(2)\{g(1) + g(2)\} \\ & \quad + g(1)\{f(1) + f(2) + f(3) + f(4)\} + g(2)\{f(1) + f(2)\} \\ & \quad - \{f(1)g(1) + f(1)g(2) + f(2)g(1) + f(2)g(2)\}, \end{aligned}$$

which simplifies to the above sum.

$$\mathbf{3.13} \quad \sum_{n \leq 4\frac{1}{2}} \mu(n) \left[\frac{4\frac{1}{2}}{n} \right] = 4\mu(1) + 2\mu(2) + 1\mu(3) + 1\mu(4) = 4 - 2 - 1 + 0 = 1.$$

$$\begin{aligned} \sum_{n \leq 4\frac{1}{2}} \Lambda(n) \left[\frac{4\frac{1}{2}}{n} \right] &= 4\Lambda(1) + 2\Lambda(2) + 1\Lambda(3) + 1\Lambda(4) \\ &= 0 + 2\log 2 + \log 3 + \log 2 = \log 24 = \log([4\frac{1}{2}]!). \\ \left| \sum_{n \leq 4\frac{1}{2}} \frac{\mu(n)}{n} \right| &= \left| \frac{\mu(1)}{1} + \frac{\mu(2)}{2} + \frac{\mu(3)}{3} + \frac{\mu(4)}{4} \right| = \left| 1 - \frac{1}{2} - \frac{1}{3} + 0 \right| = \frac{1}{6} \leq 1. \end{aligned}$$

$$\mathbf{3.14} \quad \alpha(7) = \left[\frac{500}{7} \right] + \left[\frac{500}{49} \right] + \left[\frac{500}{343} \right] = 71 + 10 + 1 = 82,$$

so the highest power is 7^{82} .

$$\begin{aligned} \mathbf{3.15} \quad \alpha(2) &= \left[\frac{10}{2} \right] + \left[\frac{10}{4} \right] + \left[\frac{10}{8} \right] = 5 + 2 + 1 = 8; \\ \alpha(3) &= \left[\frac{10}{3} \right] + \left[\frac{10}{9} \right] = 3 + 1 = 4; \quad \alpha(5) = \left[\frac{10}{5} \right] = 2; \quad \alpha(7) = \left[\frac{10}{7} \right] = 1. \\ \text{So } 10! &= 2^8 3^4 5^2 7. \end{aligned}$$

$$\begin{aligned} \mathbf{3.16} \quad \sum_{n \leq 10\frac{1}{2}} \Lambda(n) \left[\frac{10\frac{1}{2}}{n} \right] &= 10\Lambda(1) + 5\Lambda(2) + 3\Lambda(3) + 2\Lambda(4) + 2\Lambda(5) + 1\Lambda(6) + 1\Lambda(7) \\ & \quad + 1\Lambda(8) + 1\Lambda(9) + 1\Lambda(10) \\ &= 0 + 5\log 2 + 3\log 3 + 2\log 2 + 2\log 5 + 0 + \log 7 + \log 2 + \log 3 + 0 \\ &= 8\log 2 + 4\log 3 + 2\log 5 + \log 7. \\ \sum_p \sum_{m=1}^{\infty} \left[\frac{10\frac{1}{2}}{p^m} \right] \log p &= \left(\left[\frac{10\frac{1}{2}}{2} \right] + \left[\frac{10\frac{1}{2}}{4} \right] + \left[\frac{10\frac{1}{2}}{8} \right] \right) \log 2 + \left(\left[\frac{10\frac{1}{2}}{3} \right] + \left[\frac{10\frac{1}{2}}{9} \right] \right) \log 3 \\ & \quad + \left(\left[\frac{10\frac{1}{2}}{5} \right] \right) \log 5 + \left[\frac{10\frac{1}{2}}{7} \right] \log 7 \\ &= (5 + 2 + 1) \log 2 + (3 + 1) \log 3 + 2\log 5 + \log 7 \\ &= 8\log 2 + 4\log 3 + 2\log 5 + \log 7. \end{aligned}$$

Chapter 4

- 4.1** (a) 10, 11.
 (b) $3\log 2 + 2\log 3 + \log 5 + \log 7 + \log 11$;
 $4\log 2 + 2\log 3 + \log 5 + \log 7 + \log 11 + \log 13$.
 (c) $\log 2 + \log 3 + \log 5 + \log 7 + \log 11 + \log 13$ (for both answers).

4.2