Solutions to
Introduction to Analytic Number Theory
Tom M. Apostol

Greg Hurst
ghurst588@gmail.com

Preface

This is a solution manual for Tom Apostol's *Introduction to Analytic Number Theory*. Since graduating, I decided to work out all solutions to keep my mind sharp and act as a refresher. There are many problems in this book that are challenging and worth doing on your own, so I recommend referring to this manual as a last resort. The most up to date manual can be found at gregoryhurst.com. Please report any errors you may find.

Clearly some problems are harder than others so I used the following markers to indicate exercises I found hard:

(+) denotes problems I found particularly challenging.

(++) denotes what I considered to be the most challenging problem of the chapter.

Furthermore I kept track of the exercises from which I learned the most, which are naturally the ones I recommend the most:

Exercise 1.24	Exercise 1.30	Exercise 2.8	Exercise 3.12	Exercise 4.24
Exercise 4.25	Exercise 4.26	Exercise 4.27	Exercise 4.28	Exercise 4.29
Exercise 4.30	Exercise 5.13	Exercise 5.18	Exercise 5.19	Exercise 5.20
Exercise 6.18	Exercise 10.8	Exercise 10.9	Exercise 10.13	Exercise 11.15
Exercise 11.16	Exercise 12.12	Exercise 12.19	Exercise 13.10	Exercise 14.5

Contents

Chapter 1
The Fundamental Theorem of Arithmetic

In there exercises lower case latin letters $a, b, c, \ldots, x, y, z$ represent integers.
Prove each of the statements in Exercises 1 through 6.

Exercise 1.1. If $(a, b) = 1$ and if $c \mid a$ and $d \mid b$, then $(c, d) = 1$.

Proof. Since a and b are relatively prime, there are integers x and y such that $ax + by = 1$. Also because $c \mid a$ and $d \mid b$, we have $a = cn$ and $b = dm$ for some integers n and m. Thus $c(nx) + d(my) = 1$, which implies $(c, d) = 1$. □

Exercise 1.2. If $(a, b) = (a, c) = 1$, then $(a, bc) = 1$.

Proof. Since a is relatively prime to both b and c, there are integers x_1, x_2, y_1, y_2 such that

$$ax_1 + by_1 = 1 \quad \text{and} \quad ax_2 + cy_2 = 1.$$

Multiplying gives

$$\begin{aligned}(ax_1 + by_1)(ax_2 + cy_2) = 1 &\implies a^2x_1x_2 + acx_1y_2 + abx_2y_1 + bcy_1y_2 = 1 \\ &\implies a(ax_1x_2 + cx_1y_2 + bx_2y_1) + (bc)(y_1y_2) = 1 \\ &\implies (a, bc) = 1.\end{aligned}$$

□

Exercise 1.3. If $(a, b) = 1$, then $(a^n, b^k) = 1$ for all $n \geq 1, k \geq 1$.

Proof. Suppose $p \mid a^n$ and $p \mid b^k$ for some prime p. Then $p \mid a$ and $p \mid b$, as p is prime. This implies $p \mid (a, b)$, a contradiction. □

Exercise 1.4. If $(a, b) = 1$, then $(a + b, a - b)$ is either 1 or 2.

Proof. Since $(a, b) = 1$, there are integers x and y such that $ax + by = 1$. Then

$$\begin{aligned}(a + b)(x + y) + (a - b)(x - y) &= (ax + bx + ay + by) + (ax - bx - ay + by) \\ &= 2ax + 2by = 2.\end{aligned}$$

Thus $(a + b, a - b) \leq 2$, i.e. $(a + b, a - b)$ is either 1 or 2. □

Exercise 1.5. If $(a, b) = 1$, then $(a + b, a^2 - ab + b^2)$ is either 1 or 3.

Proof. Let $g = (a+b, a^2-ab+b^2)$. Since $(a+b)^2-(a^2-ab+b^2) = 3ab$, we have $g \mid 3ab$. This means each prime factor p of g must divide 3, a, or b. However without loss of generality , if $p \mid a$ then $p \mid (a+b)-a = b$. This contradicts $(a, b) = 1$, and so $p \nmid ab$. Therefore $(g, ab) = 1$, which means $g \mid 3$, i.e. $g = 1$ or $g = 3$. □

Exercise 1.6. If $(a, b) = 1$ and if $d \mid a + b$, then $(a, d) = (b, d) = 1$.

Proof. Let $g = (a, d)$, which means $g \mid a$ and $g \mid d$. Additionally, $d \mid a + b$ implies $b = nd - a$ for some integer n, and so $g \mid b$. Thus $g \mid (a, b)$, which forces $g = 1$. The same argument shows $(b, d) = 1$. □

Exercise 1.7. A rational number a/b with $(a, b) = 1$ is called a *reduced fraction*. If the sum of two reduced fractions in an integer, say $(a/b) + (c/d) = n$, prove that $|b| = |d|$.

Proof. Since $n = (ad + bc)/(bd)$, both b and d divide $ad + bc$. This means $b \mid ad$ and $d \mid bc$, but since $(a, b) = (c, d) = 1$ we must have $b \mid d$ and $d \mid b$. Therefore $|b| = |d|$. □

Exercise 1.8. An integer is called *squarefree* if it is not divisible by the square of any prime. Prove that for every $n \geq 1$ there exist uniquely determined $a > 0$ and $b > 0$ such that $n = a^2 b$, where b is squarefree.

Proof. Suppose $n \geq 1$ and $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$. Define

$$a = p_1^{\lfloor \alpha_1/2 \rfloor} \cdots p_k^{\lfloor \alpha_k/2 \rfloor} \quad \text{and} \quad b = p_1^{\alpha_1 \bmod 2} \cdots p_k^{\alpha_k \bmod 2}.$$

We then have $n = a^2 b$ since $\alpha_i = 2\lfloor \alpha_i/2 \rfloor + (\alpha_i \bmod 2)$. Moreover, b is square free.

Now suppose $n = c^2 d$ for $c > 0$ and $d > 0$. Then $a^2 b = c^2 d$ which means $a^2 \mid c^2 d$. However, d is squarefree so it follows that $a^2 \mid c^2$. Similarly $c^2 \mid a^2$, thus $|a^2| = |c^2|$. This forces $a = c$ as they are both positive. Substituting $a = c$ into $a^2 b = c^2 d$ shows $b = d$. Hence this decomposition is unique. □

Exercise 1.9. For each of the following statements, either give a proof or exhibit a counter example.
(a) If $b^2 \mid n$ and $a^2 \mid n$ and $a^2 \leq b^2$, then $a \mid b$.
(b) If b^2 is the largest square divisor of n, then $a^2 \mid n$ implies $a \mid b$.

Solution.
(a) False: Let $n = 36$, $a = 2$, and $b = 3$.
(b) If $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ and b^2 is the largest square divisor of n, then by Exercise 1.8,

$$b = p_1^{\lfloor \alpha_1/2 \rfloor} \cdots p_k^{\lfloor \alpha_k/2 \rfloor}.$$

If $a^2 \mid n$, then $a = p_1^{\beta_1} \cdots p_k^{\beta_k}$, where $\beta_i \leq \lfloor \alpha_i/2 \rfloor$. Thus $a \mid b$.

Exercise 1.10. Given x and y, let $m = ax + by$, $n = cx + dy$, where $ad - bc = \pm 1$. Prove that $(m, n) = (x, y)$.

Proof. Observe m and n are expressed as linear combinations of x and y. This means $(x, y) \mid m$ and $(x, y) \mid n$, which implies $(x, y) \mid (m, n)$.

Treating $m = ax + by$ and $n = cx + dy$ as a system of linear equations, solving gives

$$x = \frac{dm - bn}{ad - bc} \quad \text{and} \quad y = \frac{an - cm}{ad - bc}.$$

Furthermore, since $ad - bc = \pm 1$, then $x = \pm(dm - bn)$ and $y = \pm(an - cm)$. So applying the exact argument from above, we conclude $(m, n) \mid (x, y)$. This can only happen when $|(x, y)| = |(m, n)|$, and since gcd's are positive, $(x, y) = (m, n)$. □

Exercise 1.11. Prove that $n^4 + 4$ is composite if $n > 1$.

Proof. Factoring shows

$$\begin{aligned} n^4 + 4 &= (n^4 + 4n^2 + 4) - 4n^2 \\ &= (n^2 + 2)^2 - (2n)^2 \\ &= (n^2 + 2n + 2)(n^2 - 2n + 2). \end{aligned}$$

Observe for $n > 1$, both factors are larger than 1 and so $n^4 + 4$ is composite. □

In Exercises 12, 13, and 14, a, b, c, m, n denote *positive* integers.

Exercise 1.12. For each of the following statements, either give a proof or exhibit a counter example.
(a) If $a^n \mid b^n$ then $a \mid b$.
(b) If $n^n \mid m^m$ then $n \mid m$.
(c) If $a^n \mid 2b^n$ and $n > 1$, then $a \mid b$.

Solution.
(a) True: Suppose $a = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$. Then $a^n \mid b^n$ implies $b^n = p_1^{n\alpha_1} \cdots p_k^{n\alpha_k} \cdot q_1^{n\beta_1} \cdots q_l^{n\beta_l}$. This means $b = p_1^{\alpha_1} \cdots p_k^{\alpha_k} \cdot q_1^{\beta_1} \cdots q_l^{\beta_l}$, i.e. $a \mid b$.
(b) False: Let $n = 8$ and $m = 12$.
(c) True: If a is odd then $(a, 2) = 1$ and $a^n \mid b^n$, hence (a) implies $a \mid b$.

Now suppose $a = 2^s d$ where $s > 0$ and d is odd. Since $a^n \mid 2b^n$,

$$2b^n = 2^{ns} d^n m$$

for some integer m. Thus

$$b^n = 2^{n(s-1)+(n-1)} d^n m.$$

Since $n - 1 > 0$, $2^{n(s-1)+(n-1)}$ is not an nth power, which means m must be even. Therefore

$$b^n = 2^{ns} d^n (m')^n = a^n (m')^n,$$

and so $a \mid b$.

Exercise 1.13. If $(a, b) = 1$ and $(a/b)^m = n$, prove that $b = 1$.
If n is not the mth power of a positive integer, prove that $n^{1/m}$ is irrational.

Proof. If $(a/b)^m = n$, then $a^m/b^m - n/1 = 0$. Thus by Exercise 1.7, $|b^m| = 1$, and so $b = 1$.

Next suppose $n^{1/m} = a/b$ where $(a, b) = 1$. Then $n = (a/b)^m$, which we now know implies $b = 1$. Therefore $n = a^m$, i.e. n is an mth power. □

Exercise 1.14. If $(a, b) = 1$ and $ab = c^n$, prove that $a = x^n$ and $b = y^n$ for some x and y. [*Hint*: Consider $d = (a, c)$.]

Proof. Suppose $a = p_1^{a_1} \cdots p_k^{a_k}$ and $b = q_1^{b_1} \cdots q_l^{b_l}$ where all p_i and q_j are distinct. Then

$$c^n = p_1^{a_1} \cdots p_k^{a_k} \cdot q_1^{b_1} \cdots q_l^{b_l},$$

and so

$$c = p_1^{a_1/n} \cdots p_k^{a_k/n} \cdot q_1^{b_1/n} \cdots q_l^{b_l/n}.$$

Since each p_i and q_j are distinct, $n \mid a_i$ and $n \mid b_j$. Therefore a and b are nth powers. □

Exercise 1.15. Prove that every $n \geq 12$ is the sum of two composite numbers.

Proof. If n is even, then $n = 4 + (n - 4)$ and $n - 4 > 2$ is even. On the other hand, if n is odd, then $n = 9 + (n - 9)$ and $n - 9 > 2$ is even. □

Exercise 1.16. Prove that if $2^n - 1$ is prime, then n is prime.

Proof. Suppose n is composite and $n = ab$ for some $a > 1$ and $b > 1$. Then

$$2^n - 1 = (2^a)^b - 1 = (2^a - 1)(2^{a(b-1)} + 2^{a(b-2)} + \cdots + 2^a + 1).$$

Since both factors are greater than one, $2^n - 1$ must be composite. □

Exercise 1.17. Prove that if $2^n + 1$ is prime, then n is a power of 2.

Proof. Suppose $n = 2^s d$ where d is odd and $d > 1$. Then

$$2^n + 1 = (2^{2^s})^d + 1 = (2^{2^s} + 1)(2^{2^s(d-1)} - 2^{2^s(d-2)} + \cdots + 2^{2^s \cdot 2} - 2^{2^s} + 1).$$

Furthermore since $d > 1$ is odd,

$$(2^{2^s(d-1)} - 2^{2^s(d-2)}) + \cdots + (2^{2^s \cdot 2} - 2^{2^s}) + 1 > 0 + \cdots + 0 + 1 = 1.$$

Hence both factors are larger than 1 and so $2^n + 1$ is composite. Thus if $2^n + 1$ is prime, then $d = 1$, i.e. n is a power of 2. □

Exercise 1.18. If $m \neq n$ compute the gcd $(a^{2^m} + 1, a^{2^n} + 1)$ in terms of a. [*Hint*: Let $A_n = a^{2^n} + 1$ and show that $A_n \mid (A_m - 2)$ if $m > n$.]

Solution. Let $g = (A_m, A_n)$, where $m > n$ and define $A_k = a^{2^k} + 1$. Now

$$\begin{aligned} A_m - 2 &= a^{2^m} - 1 \\ &= (a^{2^n})^{2^{m-n}} - 1 \\ &= (a^{2^n} + 1)(a^{2^n(2^{m-n}-1)} - a^{2^n(2^{m-n}-2)} + \cdots + a^{2^n} - 1) \\ &= A_n \cdot (a^{2^n(2^{m-n}-1)} - a^{2^n(2^{m-n}-2)} + \cdots + a^{2^n} - 1), \end{aligned}$$

and hence $A_n \mid (A_m - 2)$. This shows $g \mid A_m - 2$ and $g \mid A_m$, thus by linearity $g \mid 2$. If a is even, then A_k is odd and hence $g = 1$. On the other hand, if a is odd, then A_k is even, giving $g = 2$.

Exercise 1.19. The *Fibonacci sequence* $1, 1, 2, 3, 5, 8, 13, 21, 34, \ldots$ is defined by the recursion formula $a_{n+1} = a_n + a_{n-1}$, with $a_1 = a_2 = 1$. Prove that $(a_n, a_{n+1}) = 1$ for each n.

Proof. Induct on n. It's clear $(a_1, a_2) = 1$. Let $n > 1$ and assume $(a_{n-1}, a_n) = 1$. Then

$$(a_n, a_{n+1}) = (a_n, a_n + a_{n-1}) = (a_n, a_{n-1}) = 1.$$

□

Exercise 1.20. Let $d = (826, 1890)$. Use the Euclidean algorithm to compute d, then express d as a linear combination of 826 and 1890.

Solution. Applying the Euclidean algorithm,

$$\begin{aligned} 1890 &= 2 \cdot 826 + 238 \\ 826 &= 3 \cdot 238 + 112 \\ 238 &= 2 \cdot 112 + 14 \\ 112 &= 8 \cdot 14 + 0, \end{aligned}$$

hence $d = 14$. Through back substitution,

$$\begin{aligned} 14 &= 238 - 2 \cdot 112 \\ &= (1890 - 2 \cdot 826) - 2(826 - 3 \cdot 238) \\ &= (1890 - 2 \cdot 826) - 2(826 - 3 \cdot (1890 - 2 \cdot 826)) \\ &= 7 \cdot 1890 - 16 \cdot 826. \end{aligned}$$

Exercise 1.21. The least common multiple (lcm) of two integers a and b is denoted by $[a, b]$ or by aMb, and is defined as follows.

$$\begin{aligned} [a, b] &= |ab|/(a, b) \quad \text{if } a \neq 0 \text{ and } b \neq 0 \\ [a, b] &= 0 \quad \text{if } a = 0 \text{ or } b = 0. \end{aligned}$$

Prove that the lcm has the following properties:
(a) If $a = \prod_{i=1}^{\infty} p_i^{a_i}$ and $b = \prod_{i=1}^{\infty} p_i^{b_i}$ then $[a, b] = \prod_{i=1}^{\infty} p_i^{c_i}$, where $c_i = \max\{a_i, b_i\}$.
(b) $(aDb)Mc = (aMc)D(bMc)$.
(c) $(aMb)Dc = (aDc)M(bDc)$.
(D and M are distributive with respect to each other.)

Proof.
(a) If $c_i = \max\{a_i, b_i\}$ and $m_i = \min\{a_i, b_i\}$, then by definition $[a, b] = \prod_{i=1}^{\infty} p_i^{a_i+b_i-m_i}$. Now it's easy to see $a_i + b_i = c_i + m_i$, and hence $[a, b] = \prod_{i=1}^{\infty} p_i^{c_i}$.

For the next parts assume $a = \prod_{i=1}^{\infty} p_i^{a_i}$, $b = \prod_{i=1}^{\infty} p_i^{b_i}$, and $c = \prod_{i=1}^{\infty} p_i^{c_i}$.
(b) We have

$$[(a, b), c] = \left[\prod p_i^{\min\{a_i,b_i\}}, \prod p_i^{c_i}\right] = \prod p_i^{\max\{\min\{a_i,b_i\},c_i\}}$$

and

$$([a, c], [b, c]) = \left(\prod p_i^{\max\{a_i,c_i\}}, \prod p_i^{\max\{b_i,c_i\}}\right) = \prod p_i^{\min\{\max\{a_i,c_i\},\max\{b_i,c_i\}\}}.$$

To show these exponents are equal, we will compare the two in a table.

ordering	$\max\{\min\{a_i, b_i\}, c_i\}$	$\min\{\max\{a_i, c_i\}, \max\{b_i, c_i\}\}$
$a_i \geq b_i \geq c_i$	b_i	b_i
$a_i \geq c_i \geq b_i$	b_i	b_i
$b_i \geq a_i \geq c_i$	b_i	b_i
$b_i \geq c_i \geq a_i$	a_i	a_i
$c_i \geq a_i \geq b_i$	b_i	b_i
$c_i \geq b_i \geq a_i$	a_i	a_i

This shows $\max\{\min\{a_i, b_i\}, c_i\} = \min\{\max\{a_i, c_i\}, \max\{b_i, c_i\}\}$ and the result follows.
(c) We have

$$([a, b], c) = \left(\prod p_i^{\max\{a_i,b_i\}}, \prod p_i^{c_i}\right) = \prod p_i^{\min\{\max\{a_i,b_i\},c_i\}}$$

and

$$[(a, c), (b, c)] = \left[\prod p_i^{\min\{a_i,c_i\}}, \prod p_i^{\min\{b_i,c_i\}}\right] = \prod p_i^{\max\{\min\{a_i,c_i\},\min\{b_i,c_i\}\}}.$$

To show these exponents are equal, we will compare the two in a table.

ordering	$\min\{\max\{a_i, b_i\}, c_i\}$	$\max\{\min\{a_i, c_i\}, \min\{b_i, c_i\}\}$
$a_i \geq b_i \geq c_i$	c_i	c_i
$a_i \geq c_i \geq b_i$	b_i	b_i
$b_i \geq a_i \geq c_i$	c_i	c_i
$b_i \geq c_i \geq a_i$	b_i	b_i
$c_i \geq a_i \geq b_i$	b_i	b_i
$c_i \geq b_i \geq a_i$	b_i	b_i

This shows $\min\{\max\{a_i, b_i\}, c_i\} = \max\{\min\{a_i, c_i\}, \min\{b_i, c_i\}\}$ and the result follows. □

Exercise 1.22. Prove that $(a, b) = (a + b, [a, b])$.

Lemma 1.22. If $(c, d) = 1$, then $(c + d, cd) = 1$.

Proof of Lemma. Suppose $p \mid c + d$ and $p \mid cd$ for some prime p. Then without loss of generality $p \mid c$, and so $p \mid (c + d) - c = d$. This means $p \mid (c, d)$, a contradiction. □

Proof of Exercise. Note by Theorem 1.4 (c) if $c > 0$, then $(ac, bc) = c(a, b)$. Now if $g = (a, b)$, then $a = gn$ and $b = gm$ for some integers n and m. By Lemma 1.22,

$$\begin{aligned}(a + b, [a, b]) &= (a + b, |ab|/g)\\ &= (g(n + m), \pm gnm)\\ &= g(n + m, nm)\\ &= g.\end{aligned}$$

□

Exercise 1.23. The sum of two positive integers is 5264 and their least common multiple is 200 340. Determine the two integers.

Solution. We have $a + b = 5264$ and $[a, b] = 200\,340$. So by Exercise 1.22,

$$200\,340 = ab/(5264, 200\,340) = ab/28,$$

and therefore

$$a + b = 5264 \quad \text{and} \quad ab = 5\,609\,520.$$

Assuming $a < b$, solving the system gives $a = 1484$ and $b = 3780$.

Exercise 1.24.(++) Prove the following multiplicative property of the gcd:

$$(ah, bk) = (a, b)(h, k)\left(\frac{a}{(a, b)}, \frac{k}{(h, k)}\right)\left(\frac{b}{(a, b)}, \frac{h}{(h, k)}\right).$$

In particular this shows that $(ah, bk) = (a, k)(b, h)$ whenever $(a, b) = (h, k) = 1$.

Lemma 1.24. If n, m, and $g > 0$ are integers, then $g = (n, m)$ if and only if $(n/g, m/g) = 1$.

Proof of Lemma. By Theorem 1.4 (c),

$$(n, m) = g \iff (g(n/g), g(m/g)) = g \iff g(n/g, m/g) = g \iff (n/g, m/g) = 1.$$

□

Proof of Exercise. Let $a_1 = a/(a, b), b_1 = b/(a, b), h_1 = h/(h, k), k_1 = k/(h, k)$. Then applying Lemma 1.24,

$$\begin{aligned}&(ah, bk) = (a, b)(h, k)\left(\frac{a}{(a, b)}, \frac{k}{(h, k)}\right)\left(\frac{b}{(a, b)}, \frac{h}{(h, k)}\right)\\ \iff\ &(a_1h_1, b_1k_1) = (a_1, k_1)(b_1, h_1)\\ \iff\ &\left(\frac{a_1}{(a_1, k_1)}\frac{h_1}{(b_1, h_1)}, \frac{b_1}{(b_1, h_1)}\frac{k_1}{(a_1, k_1)}\right) = 1.\end{aligned}$$

Now define $\alpha = \frac{a_1}{(a_1,k_1)}, \gamma = \frac{h_1}{(b_1,h_1)}, \beta = \frac{b_1}{(b_1,h_1)}, \delta = \frac{k_1}{(a_1,k_1)}$. Then by Lemma 1.24,

$$(\alpha, \delta) = 1 \quad \text{and} \quad (\gamma, \beta) = 1.$$

Additionally, note

$$\alpha = \frac{a}{d_1(a,b)} \quad \text{and} \quad \beta = \frac{b}{d_2(a,b)}$$

for some d_1 and d_2, so Lemma 1.24 shows $(\alpha, \beta) = 1$ and similarly $(\gamma, \delta) = 1$. This means $\alpha\gamma$ and $\beta\delta$ can share no positive divisors other than 1, that is $(\alpha\gamma, \beta\delta) = 1$. □

Prove each of the following statements in Exercises 25 through 28. All integers are positive.

Exercise 1.25. If $(a, b) = 1$ there exist $x > 0$ and $y > 0$ such that $ax - by = 1$.

Proof. If $a = 1$ then take $x = b + 1$ and $y = 1$, so we can assume $a > 1$ and $b > 1$. Since $(a, b) = 1$, there are x and y such that $ax+by = 1$. If $x > 0$ and $y < 0$, we're done. Otherwise we make a few quick observations.

- $x \neq 0$ and $y \neq 0$ because $a \neq 1$ and $b \neq 1$.
- x and y can't both be negative since this implies $ax + by < 0$.
- x and y can't both be positive since this implies $ax + by > 1$.

So at this stage we must conclude $x < 0$ and $y > 0$. Define $x_n = x + bn$ and $y_n = y - an$ for some integer n. Then

$$ax_n + by_n = ax + abn + by - abn = ax + by = 1,$$

so choosing n large enough to force $x_n > 0$ and $y_n < 0$ gives the result. □

Exercise 1.26. If $(a, b) = 1$ and $x^a = y^b$ then $x = n^b$ and $y = n^a$ for some n. [*Hint*: Use Exercises 25 and 13.]

Proof. Suppose $(a, b) = 1$. Then by Exercise 1.25, there are positive c and d such that $ac - bd = 1$. We then have

$$x^{ad} = y^{bd} = y^{ac-1}.$$

Raising both sides to the power $1/a$, yields $x^d = y^c \cdot y^{-1/a}$, or in other words $y^{1/a} = y^c/x^d \in \mathbb{Q}$.

By Exercise 1.13, this implies y is an ath power and so $y = n^a$ for some positive n. Finally

$$x^a = y^b = n^{ab} = (n^b)^a,$$

hence raising both sides to the power $1/a$ gives $x = n^b$. □

Exercise 1.27.(+)
(a) If $(a, b) = 1$ then for every $n > ab$ there exist positive x and y such that $n = ax + by$.
(b) If $(a, b) = 1$ there are no positive x and y such that $ab = ax + by$.

Proof.
(a) Let $n > ab$ and consider the sequence

$$S = \{n - ib \mid 1 \leq i \leq a\}.$$

Each member of S will have a different remainder when divided by a, since $(a, b) = 1$ and adding n simplify shifts the conjugacy classes. Since $|S| = a$, we deduce there is a unique element in S that is divisible by a. That is to say there is $n - yb \in S$ such that $n - yb = ax$. Since $1 \leq y \leq a$ we have $ax = n - yb > 0$, which means $x > 0$.

(b) Suppose $ab = ax + by$, where $x > 0$ and $y > 0$. Then $a(b - x) = by$ which means $a \mid by$, but since $(a, b) = 1$ we have $a \mid y$. If $y = az$, dividing through by a gives $b = x + bz$. Thus $b(1 - z) = x$, which means $1 > z$ as $x > 0$. This is a contradiction since $y > 0$ implies $z > 0$. Thus $ab = ax + by$ has no solution for $x > 0$ and $y > 0$. □

Exercise 1.28.(+) If $a > 1$ then $(a^m - 1, a^n - 1) = a^{(m,n)} - 1$.

Proof. If $m = n$, the result is immediate. Suppose $m > n$ and $m = qn + r$ with $0 \leq r < n$. Then

$$\begin{aligned} a^m - 1 &= a^{qn+r} - 1 \\ &= a^r(a^{qn} - 1) + (a^r - 1) \\ &= a^r(a^{q-1} + \cdots + a + 1)(a^n - 1) + (a^r - 1). \end{aligned}$$

Since $0 \leq r < n$, we have $0 \leq a^r - 1 < a^n - 1$. By the Euclidean algorithm, if we continue this process, we'll arrive at the gcd. But this process is also performing the Euclidean algorithm on the exponents, starting with m and n. From here we see $(a^m - 1, a^n - 1) = a^{(m,n)} - 1$. □

Exercise 1.29. Given $n > 0$, let S be a set whose elements are positive integers $\leq 2n$ such that if a and b are in S and $a \neq b$ then $a \nmid b$. What is the maximum number of integers that S can contain? [*Hint*: S can contain at most one of the integers $1, 2, 2^2, 2^3, \ldots$, at most one of $3, 3 \cdot 2, 3 \cdot 2^2, \ldots$, etc.]

Solution. Define

$$S_m = \{m, 2 \cdot m, 2^2 \cdot m, \ldots\} \quad \text{for } 1 \leq m \leq n.$$

Notice we can only have at most one element from each S_m in S, since if $x, y \in S_m$ and $x < y$, then $x \mid y$. This means $|S| \leq n$. Now let

$$S = \{k \mid n + 1 \leq k \leq 2n\}.$$

Note $|S| = n$ and no element divides another since a nontrivial multiple of any element is not in S. Thus for any n, the maximum size of S is n.

Exercise 1.30.(+) If $n > 1$ prove the sum

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

is not an integer.

Proof. Rewrite H_n as

$$H_n = \frac{(n!/1) + (n!/2) + \cdots + (n!/n)}{n!}.$$

Let m be the exponent of the highest power of 2 in $\{1, 2, \ldots, n\}$. If 2^l is the largest power of 2 that divides $n!$, then $l \geq m$. Thus the highest power of 2 that divides the integer $n!/2^m$ is 2^{l-m}. If $n > 1$, for any $k \neq 2^m$, the highest power of 2 that divides the integer $n!/k$ is at least 2^{l-m+1}. So we can factor out 2^{l-m} from the numerator of H_n, leaving the $k = 2^m$ term odd and every other term even. Thus after cancelation, the numerator of H_n is odd, while the denominator stays even. This means $H_n \notin \mathbb{Z}$ for $n > 1$. □

Chapter 2
Arithmetical Functions and Dirichlet Multiplication

Exercise 2.1. Find all integers n such that

$$\text{(a) } \varphi(n) = n/2, \qquad \text{(b) } \varphi(n) = \varphi(2n), \qquad \text{(c) } \varphi(n) = 12$$

Solution.
(a) Suppose $n = 2^s d$, where d is odd. If $\varphi(n) = n/2$, then $2 \mid n$, which forces $s > 0$. Thus $\varphi(n) = \varphi(2^s)\varphi(d) = 2^{s-1}\varphi(d)$. This means $2^{s-1}\varphi(d) = n/2$, which implies $\varphi(d) = d$. This can only happen when $d = 1$, since $\varphi(d) \leq d - 1$ for $d > 1$. Therefore $\varphi(n) = n/2$ if and only if $n = 2^s$ for some $s > 0$.

(b) Again suppose $n = 2^s d$, where d is odd. If $s = 0$, then $\varphi(n) = \varphi(d)$ and $\varphi(2n) = \varphi(2)\varphi(d) = \varphi(d)$. If $s > 0$, then $\varphi(n) = 2^{s-1}\varphi(d)$ and $\varphi(2n) = 2^s\varphi(d)$. So we see $\varphi(n) = \varphi(2n)$ if and only if n is odd.

(c) Suppose $\varphi(n) = 12$, then $\prod_{p|n}(p^a - p^{a-1}) = 2 \cdot 2 \cdot 3$. Note, it could happen that $p^a - p^{a-1} = 1$. This can only happen when $p = 2$ and $a = 1$. So if we find an odd n that satisfies our problem, $2n$ will satisfy it too.

- Solve $p^a - p^{a-1} = 12$: This can only happen for $p = 13$ and $a = 1$. Thus $n = 13$ and $n = 26$ are solutions.
- Solve $p^a - p^{a-1} = 3$: Then $p^{a-1}(p - 1) = 3$, and since 3 is prime, either $p^{a-1} = 1$ or $p - 1 = 1$. From here it's easy to see there is no solution.
- Solve $p^a - p^{a-1} = 2$ and $q^b - q^{b-1} = 6$: By inspection, the solutions are

  $$\{p, a\} = \{2, 2\} \quad \text{or} \quad \{p, a\} = \{3, 1\}$$

  and

  $$\{q, b\} = \{3, 2\} \quad \text{or} \quad \{q, b\} = \{7, 1\}.$$

  Grouping distinct primes above, solutions are $n = 36$, $n = 28$, $n = 21$, and $n = 42$.

Exercise 2.2. For each of the following statements either give a proof or exhibit a counter example.
(a) If $(m, n) = 1$ then $(\varphi(m), \varphi(n)) = 1$.
(b) If n is composite, then $(n, \varphi(n)) > 1$.
(c) If the same primes divides m and n, then $n\varphi(m) = m\varphi(n)$.

Solution.
(a) False: Take $m = 3$ and $n = 5$, then $(\varphi(m), \varphi(n)) = (2, 4) = 2$.
(b) False: Take $n = 15$, then $(n, \varphi(n)) = (15, 8) = 1$.
(c) True: Since $p \mid m$ if and only if $p \mid n$,

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

Exercise 2.3. Prove that

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

Proof. Suppose $n = p_1^{a_1} \cdots p_k^{a_k}$ where $a_i > 0$. Then since $\frac{\mu^2}{\varphi} * u$ is multiplicative,

$$\begin{aligned}
\sum_{d|n} \frac{\mu^2(d)}{\varphi(d)} &= \prod_{i=1}^{k} \sum_{j=0}^{a_i} \frac{\mu^2(p_i^j)}{\varphi(p_i^j)} \\
&= \prod_{i=1}^{k} \left(1 + \frac{1}{p_i - 1}\right) \\
&= \prod_{i=1}^{k} \frac{1}{1 - 1/p_i} = \frac{n}{\varphi(n)}.
\end{aligned}$$

□

Exercise 2.4. Prove that $\varphi(n) > n/6$ for all n with at most 8 distinct prime factors.

Proof. Note $\varphi(1) = 1 > 1/6$. Now suppose $n > 1$ has at most 8 distinct prime factors, then

$$\begin{aligned}
\frac{\varphi(n)}{n} &= \prod_{p|n} \frac{p-1}{p} \\
&\geq \frac{2-1}{2} \cdot \frac{3-1}{3} \cdot \frac{5-1}{5} \cdot \frac{7-1}{7} \cdot \frac{11-1}{11} \cdot \frac{13-1}{13} \cdot \frac{17-1}{17} \cdot \frac{19-1}{19} \\
&= \frac{55296}{323323} > \frac{55296}{331776} = \frac{1}{6}.
\end{aligned}$$

□

Exercise 2.5.(+) Define $\nu(1) = 0$, and for $n > 1$ let $\nu(n)$ be the number of distinct prime factors of n. Let $f = \mu * \nu$ and prove that $f(n)$ is either 0 or 1.

Proof. Note that $f(1) = \mu(1)\nu(1) = 0$. We will now show $f(n) = I(k)$ for $n = p_1 \cdots p_k$, $k > 0$, and p_i distinct. Suppose n is the product of $k > 0$ distinct primes. Then $n = pm$ for some prime $p \nmid m$ and thus

$$\begin{aligned}
f(n) &= \sum_{d|n} \mu(d)\nu\left(\frac{n}{d}\right) \\
&= \sum_{d|m} \mu(d)\nu\left(\frac{n}{d}\right) + \sum_{(pd)|n} \mu(pd)\nu\left(\frac{n}{pd}\right) \\
&= \sum_{d|m} \mu(d)\nu\left(p \cdot \frac{m}{d}\right) + \sum_{d|m} \mu(pd)\nu\left(\frac{m}{d}\right) \\
&= \sum_{d|m} \mu(d)\left(1 + \nu\left(\frac{m}{d}\right)\right) + \sum_{d|m} -\mu(d)\nu\left(\frac{m}{d}\right) \\
&= \sum_{d|m} \mu(d) + \sum_{d|m} \mu(d)\nu\left(\frac{m}{d}\right) - \sum_{d|m} \mu(d)\nu\left(\frac{m}{d}\right) \\
&= I(m).
\end{aligned}$$

Here we used $\mu(pd) = \mu(p)\mu(d) = -\mu(d)$ and $\nu(px) = 1+\nu(x)$ for $(p, d) = (p, x) = 1$. Finally suppose $n = p^a m$ for some $a > 1$. Then partitioning the divisors of n by the power of p in their factorizations,

$$\begin{aligned}
\sum_{d|n} \mu(d)\nu\left(\frac{n}{d}\right) &= \sum_{i=0}^{a} \sum_{\substack{p^i d|n \\ (p,d)=1}} \mu(p^i d)\nu\left(\frac{n}{d}\right) \\
&= \sum_{i=0}^{1} \sum_{d|m} \mu(p^i d)\nu\left(p^{a-i} \cdot \frac{m}{d}\right) \\
&= \sum_{d|m} \mu(d)\nu\left(p^a \cdot \frac{m}{d}\right) + \sum_{d|m} \mu(pd)\nu\left(p^{a-1} \cdot \frac{m}{d}\right) \\
&= \sum_{d|m} \mu(d)\nu\left(p^a \cdot \frac{m}{d}\right) + \sum_{d|m} -\mu(d)\nu\left(p^{a-1} \cdot \frac{m}{d}\right) \\
&= \sum_{d|m} \mu(d)\left(1 + \nu\left(\frac{m}{d}\right)\right) - \sum_{d|m} \mu(d)\left(1 + \nu\left(\frac{m}{d}\right)\right) \\
&= 0,
\end{aligned}$$

In the final steps we again used $\mu(pd) = \mu(p)\mu(d) = -\mu(d)$ for $(p, d) = 1$ and

$$\nu\left(p^a \cdot \frac{m}{d}\right) = 1 + \nu\left(\frac{m}{d}\right) = \nu\left(p^{a-1} \cdot \frac{m}{d}\right)$$

for $(p, m) = 1$ and $a > 1$.

□

Exercise 2.6. Prove that

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

and, more generally,

$$\sum_{d^k \mid n} \mu(d) = \begin{cases} 0 & \text{if } m^k \mid n \text{ for some } m > 1, \\ 1 & \text{otherwise.} \end{cases}$$

The last sum is extended over all positive divisors d of n whose kth power also divide n.

Proof. If all prime factors of n have an exponent is less than k, then $\sum_{d^k \mid n} \mu(d) = \mu(1) = 1$. Otherwise suppose exactly r prime factors have an exponent greater than or equal to k. Since $\mu(d)$ is zero when d is not squarefree,

$$\sum_{d^k \mid n} \mu(d) = \sum_{\substack{d^k \mid n \\ d \ \square\text{-free}}} \mu(d) = \binom{r}{0} + \binom{r}{1}(-1) + \binom{r}{2}(-1)^2 + \cdots + \binom{r}{r}(-1)^r = (1-1)^r = 0.$$

□

Exercise 2.7. Let $\mu(p, d)$ denote the value of the Möbius function at the gcd of p and d. Prove that for every prime p we have

$$\sum_{d \mid n} \mu(d)\mu(p, d) = \begin{cases} 1 & \text{if } n = 1, \\ 2 & \text{if } n = p^a, a \geq 1, \\ 0 & \text{otherwise.} \end{cases}$$

Lemma 2.7. For p prime, $\mu(p, \cdot)$ is multiplicative.

Proof of Lemma. Let $d = p^a \cdot q_1^{\beta_1} \cdots q_k^{\beta_k}$. If $a \geq 1$ then $(p, d) = p$ and thus

$$\mu(p, d) = -1 = -1 \cdot 1 \cdots 1 = \mu(p, p^a) \prod_{i=1}^{k} \mu(p, q_i^{\beta_i}).$$

If $a = 0$ then $(p, d) = 1$ and thus

$$\mu(p, d) = 1 = 1 \cdots 1 = \prod_{i=1}^{k} \mu(p, q_i^{\beta_i}).$$

Therefore $\mu(p, \cdot)$ is multiplicative. □

Proof of Exercise. If $n = 1$, $\sum_{d \mid n} \mu(d)\mu(p, d) = \mu(1)\mu(p, 1) = 1$. If $n = p^a$ where $a \geq 1$, then

$$\sum_{d \mid n} \mu(d)\mu(p, d) = \sum_{i=0}^{a} \mu(p^i)\mu(p, p^i) = \mu(1)\mu(p, 1) + \mu(p)\mu(p, p) = 2.$$

Otherwise by the Lemma 2.7, the sum in question is multiplicative, so

$$\sum_{d \mid n} \mu(d)\mu(p, d) = (2 \text{ or } 1) \prod_{i=1}^{k} \sum_{d \mid q_i^{\beta_i}} \mu(d) = 0.$$

□

Exercise 2.8.(++) Prove that

$$\sum_{d|n} \mu(d) \log^m(d) = 0$$

if $m \geq 1$ and n has more than m distinct prime factors. [*Hint*: Induction.]

Proof. If $m = 0$, then n must have at least one prime factor, so as the sum in question equals $I(n)$, it must be zero. Now assume the claim holds for all natural numbers less than $m+1$ and consider the case where n has $k > m+1$ distinct prime factors. Since $\mu(d) = 0$ when d is not square free, assume $n = p_1 \cdots p_k$. Then

$$\begin{aligned}\sum_{d|n} \mu(d) \log^{m+1}(d) &= \sum_{d|n} [\mu(d) \log^m(d)] \log(d) \\ &= \sum_{d|n} \sum_{p_i|d} \log(p_i) \left[\mu(d) \log^m(d)\right].\end{aligned}$$

Here we are summing over all d and p_i such that $d \mid n$, $p_i \mid d$, and hence $p_i \mid n$. Instead, first sum over $p_i \mid n$, then over each divisor d where $p_i \mid d$. This gives

$$\begin{aligned}\sum_{d|n} \sum_{p_i|d} \log(p_i) \left[\mu(d) \log^m(d)\right] &= \sum_{p_i|n} \sum_{\substack{d|n \\ p_i|d}} \log(p_i) \left[\mu(d) \log^m(d)\right] \\ &= \sum_{p_i|n} \log(p_i) \sum_{\substack{d|n \\ p_i|d}} \mu(d) \log^m(d) \\ &= \sum_{p_i|n} \log(p_i) \sum_{d|(n/p_i)} \mu(p_i d) \log^m(p_i d) \\ &= -\sum_{p_i|n} \log(p_i) \sum_{d|(n/p_i)} \mu(d) \sum_{j=0}^{m} \binom{m}{j} \log^{m-j}(p_i) \log^j(d) \\ &= -\sum_{p_i|n} \log(p_i) \sum_{j=0}^{m} \binom{m}{j} \log^{m-j}(p_i) \sum_{d|(n/p_i)} \mu(d) \log^j(d).\end{aligned}$$

By the induction hypothesis the innermost sum is zero, hence the claim is proven. □

Exercise 2.9.(+) If x is real, $x \geq 1$, let $\varphi(x, n)$ denote the number of positive integers $\leq x$ that are relatively prime to n. [Note that $\varphi(n, n) = \varphi(n)$.] Prove that

$$\varphi(x, n) = \sum_{d|n} \mu(d) \left[\frac{x}{d}\right] \quad \text{and} \quad \sum_{d|n} \varphi\left(\frac{x}{d}, \frac{n}{d}\right) = [x].$$

Proof. We have

$$\begin{aligned}\sum_{d|n}\mu(d)\left\lfloor\frac{x}{d}\right\rfloor &= \sum_{d|n}\sum_{k=1}^{\lfloor x/d\rfloor}\mu(d)\\ &= \sum_{k=1}^{\lfloor x\rfloor}\sum_{d|(n,k)}\mu(d) \qquad (1)\\ &= \sum_{k=1}^{\lfloor x\rfloor} I\left((n,k)\right)\\ &= \varphi(x,n).\end{aligned}$$

The change in order of summation at (1) is justified in the proof of Theorem 2.3.

Now let

$$S_x = \{1,2,\ldots,\lfloor x\rfloor\}, \quad A_{x,n}(d) = \{k\in S_x \mid (k,n)=d\}, \quad \text{and} \quad f_{x,n}(d) = |A_{x,n}(d)|.$$

Then $\sum_{d|n} f_{x,n}(d) = \lfloor x\rfloor$, since $\{A_{x,n}(d)\}$ partitions S_x. Moreover

$$\begin{aligned}f_{x,n}(d) &= \#\{k \mid 0<k\le x \text{ and } (k,n)=d\}\\ &= \#\{k/d \mid 0<k/d\le x/d \text{ and } (k/d,n/d)=1\}\\ &= \#\{q \mid 0<q\le x/d \text{ and } (q,n/d)=1\}\\ &= \varphi(x/d,n/d).\end{aligned}$$

Therefore $\sum_{d|n}\varphi\left(\frac{x}{d},\frac{n}{d}\right) = \lfloor x\rfloor$. □

In Exercises 10, 11, 12, $d(n)$ denotes the number of positive divisors of n.

Exercise 2.10. Prove that $\prod_{t|n} t = n^{d(n)/2}$.

Proof. $n^{d(n)} = \displaystyle\prod_{t|n} n = \prod_{t|n} t\cdot\left(\frac{n}{t}\right) = \left(\prod_{t|n} t\right)\left(\prod_{t|n}\frac{n}{t}\right) = \left(\prod_{t|n} t\right)^2.$ □

Exercise 2.11. Prove that $d(n)$ is odd if, and only if, n is a square.

Proof. Count divisors of n in pairs: t and n/t. Each pair will have distinct members unless $t = n/t$. Thus $d(n)$ is odd if and only if there is a divisor t such that $t = n/t$, i.e. $n = t^2$. □

Exercise 2.12. Prove that $\sum_{t|n} d(t)^3 = \left(\sum_{t|n} d(t)\right)^2$.

Proof. Letting $n = p_1^{a_1} \cdots p_s^{a_s}$, then since d is multiplicative,

$$\begin{aligned}(d^3 * u)(n) &= \prod_{i=1}^{s} (d^3 * u)(p_i^{a_i}) = \prod_{i=1}^{s} \sum_{k=0}^{a_i} (k_i + 1)^3 \\ &= \prod_{i=1}^{s} \left(\sum_{k=0}^{a_i} (k_i + 1) \right)^2 = \prod_{i=1}^{s} \left((d * u)(p_i^{a_i}) \right)^2 \\ &= \big((d * u)(n) \big)^2,\end{aligned}$$

where we used the identity $\sum_{i=1}^{n} i^3 = \left(\sum_{i=1}^{n} i\right)^2$. □

Exercise 2.13. *Product form of the Möbius inversion formula.* If $f(n) > 0$ for all n and if $a(n)$ is real, $a(1) \neq 0$, prove that

$$g(n) = \prod_{d|n} f(d)^{a(n/d)} \text{ if, and only if, } f(n) = \prod_{d|n} g(d)^{b(n/d)},$$

where $b = a^{-1}$, the Dirichlet inverse of a.

Proof. Suppose $g(n) = \prod_{d|n} f(d)^{a(n/d)}$. Since $f > 0$ (and hence $g > 0$), we can take logs of both sides. Since log takes products to sums, we have

$$g(n) = \prod_{d|n} f(d)^{a(n/d)} \iff \log g = (\log f) * a.$$

Now because $a(1) \neq 0$, there is an inverse $b = a^{-1}$, which tells us

$$\log g = (\log f) * a \iff (\log g) * b = \log f.$$

Taking the exponential of both sides completes the proof. □

Exercise 2.14. Let $f(x)$ be defined for all rational x in $0 \leq x \leq 1$ and let

$$F(n) = \sum_{k=1}^{n} f\left(\frac{k}{n}\right) \quad \text{and} \quad F^*(n) = \sum_{\substack{k=1 \\ (k,n)=1}}^{n} f\left(\frac{k}{n}\right).$$

(a) Prove that $F^* = \mu * F$, the Dirichlet product of μ and F.
(b) Use (a) or some other means to prove that $\mu(n)$ is the sum of the primitive nth roots of unity:

$$\mu(n) = \sum_{\substack{k=1 \\ (k,n)=1}}^{n} e^{2\pi i k/n}.$$

Lemma 2.14. For $n \geq 1$, the set

$$S = \{kn/d \mid d \text{ divides } n,\ 1 \leq k \leq d,\ (k,d) = 1\},$$

is equal to $\{1, \ldots, n\}$.

Proof of Lemma. If $1 \le m \le n$, let $m/n = k/d$ where $(k,d) = 1$. Then $m = kn/d$ and thus $\{1,\dots,n\} \subseteq S$.

Next, suppose $k_1 n/d_1 \in S$ and $k_2 n/d_2 \in S$ where $k_1 n/d_1 = k_2 n/d_2$. This implies $k_1 d_2 = k_2 d_1$, and so since $(k_i, d_i) = 1$, the d's must divide each other and the k's must divide each other. Therefore $d_1 = d_2$ and $k_1 = k_2$, so each element of S is unique. Since $1 \le kn/d \le n$, this shows $S \subseteq \{1,\dots,n\}$. □

Proof of Exercise.
(a) We have

$$(u * F^*)(n) = \sum_{d|n} F^*(d) = \sum_{d|n} \sum_{\substack{k=1 \\ (k,d)=1}}^{d} f\left(\frac{k}{d}\right) = \sum_{d|n} \sum_{\substack{k=1 \\ (k,d)=1}}^{d} f\left(\frac{kn/d}{n}\right).$$

By Lemma 2.14,

$$\sum_{d|n} \sum_{\substack{k=1 \\ (k,d)=1}}^{d} f\left(\frac{kn/d}{n}\right) = \sum_{k=1}^{n} f\left(\frac{k}{n}\right) = F(n).$$

Through Möbius inversion we find $F^* = \mu * F$.
(b) Letting $f(x) = e^{2\pi i x}$, then $F(n) = \sum_{k=1}^{n} e^{2\pi i k/n} = I(n)$ (a well known identity). Thus

$$\mu(n) = (\mu * I)(n) = (\mu * F)(n) = F^*(n).$$

Remark. An alternate proof is to apply Lemma 3.12 on $F^*(n)$. □

Exercise 2.15. Let $\varphi_k(n)$ denote the sum of the kth powers of the numbers $\le n$ and relatively prime to n. Note that $\varphi_0(n) = \varphi(n)$. Use Exercise 14 or some other means to prove that

$$\sum_{d|n} \frac{\varphi_k(d)}{d^k} = \frac{1^k + \cdots + n^k}{n^k}.$$

Proof. Let $F(n) = \sum_{m=1}^{n} \left(\frac{m}{n}\right)^k$. Then by Exercise 2.14,

$$F(n) = (u * F^*)(n) = \sum_{d|n} \sum_{\substack{m=1 \\ (m,d)=1}}^{d} \left(\frac{m}{d}\right)^k$$

$$= \sum_{d|n} \frac{1}{d^k} \sum_{\substack{m=1 \\ (m,d)=1}}^{d} m^k = \sum_{d|n} \frac{\varphi_k(d)}{d^k}.$$

□

Exercise 2.16. Invert the formula in Exercise 15 to obtain, for $n > 1$,

$$\varphi_1(n) = \frac{1}{2} n\varphi(n), \quad \text{and} \quad \varphi_2(n) = \frac{1}{3} n^2 \varphi(n) + \frac{n}{6} \prod_{p|n} (1-p).$$

Derive a corresponding formula for $\varphi_3(n)$.

Solution. Letting $N_1(n) = n(n+1)/2$, then by Exercise 2.15 we have $\varphi_1 * N = N_1$, which implies $\varphi_1 = N_1 * N^{-1} = N_1 * (\mu N)$. Thus

$$\begin{aligned}\varphi_1(n) &= \frac{1}{2}\sum_{d|n} d(d+1)\mu\left(\frac{n}{d}\right)\left(\frac{n}{d}\right)\\ &= \frac{1}{2}n\sum_{d|n} d\mu\left(\frac{n}{d}\right) + \frac{1}{2}n\sum_{d|n}\mu\left(\frac{n}{d}\right)\\ &= \frac{1}{2}n\varphi(n) + \frac{1}{2}nI(n).\end{aligned}$$

Since $I(n) = 0$ for $n > 1$, the result follows.

Letting $N_2(n) = n(n+1)(2n+1)/6$, then by Exercise 2.15 we have $\varphi_2 * N^2 = N_2$, which implies $\varphi_2 = N_2 * (N^2)^{-1} = N_2 * (\mu N^2)$. So

$$\begin{aligned}\varphi_2(n) &= \frac{1}{6}\sum_{d|n} d(d+1)(2d+1)\mu\left(\frac{n}{d}\right)\left(\frac{n}{d}\right)^2\\ &= \frac{1}{3}n^2\sum_{d|n} d\mu\left(\frac{n}{d}\right) + \frac{1}{2}n^2\sum_{d|n}\mu\left(\frac{n}{d}\right) + \frac{1}{6}n\sum_{d|n}\left(\frac{n}{d}\right)\mu\left(\frac{n}{d}\right)\\ &= \frac{1}{3}n^2\varphi(n) + \frac{1}{2}n^2 I(n) + \frac{1}{6}n\prod_i (N\mu * u)(p_i^{a_i})\\ &= \frac{1}{3}n^2\varphi(n) + \frac{1}{2}n^2 I(n) + \frac{1}{6}n\prod_{p|n}(1-p),\end{aligned}$$

Since $I(n) = 0$ for $n > 1$, the result follows.

Letting $N_3(n) = n^2(n+1)^2/4$, then by Exercise 2.15 we have $\varphi_3 * N^3 = N_3$, which implies $\varphi_3 = N_3 * (N^3)^{-1} = N_3 * (\mu N^3)$. So

$$\begin{aligned}\varphi_3(n) &= \frac{1}{4}\sum_{d|n} d^2(d+1)^2\mu\left(\frac{n}{d}\right)\left(\frac{n}{d}\right)^3\\ &= \frac{1}{4}n^3\sum_{d|n} d\mu\left(\frac{n}{d}\right) + \frac{1}{2}n^3\sum_{d|n}\mu\left(\frac{n}{d}\right) + \frac{1}{4}n^2\sum_{d|n}\left(\frac{n}{d}\right)\mu\left(\frac{n}{d}\right)\\ &= \frac{1}{4}n^3\varphi(n) + \frac{1}{2}n^3 I(n) + \frac{1}{4}n^2\prod_i (N\mu * u)(p_i^{a_i})\\ &= \frac{1}{4}n^3\varphi(n) + \frac{1}{2}n^3 I(n) + \frac{1}{4}n^2\prod_{p|n}(1-p),\\ &= \frac{1}{4}n^3\varphi(n) + \frac{1}{4}n^2\prod_{p|n}(1-p), \quad \text{for } n > 1.\end{aligned}$$

Exercise 2.17. Jordan's totient J_k is a generalization of Euler's totient defined by

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

(a) Prove that

$$J_k(n) = \sum_{d|n} \mu(d) \left(\frac{n}{d}\right)^k \quad \text{and} \quad n^k = \sum_{d|n} J_k(d).$$

(b) Determine the Bell series for J_k.

Proof.
(a) The claim is trivial for $n = 1$, so assume $n > 1$. Since both J_k and $\mu * N^k$ are multiplicative, we only need to look at prime powers:

$$\begin{aligned}\sum_{d|p^a} \mu(d) \left(\frac{p^a}{d}\right)^k &= \mu(1)(p^a)^k + \mu(p)(p^{a-1})^k \\ &= p^{ak} - p^{(a-1)k} \\ &= p^{ak}(1 - p^{-k}) \\ &= J_k(p^a).\end{aligned}$$

The second identity follows directly through Möbius inversion.
(b) Since $J_k = \mu * N^k$, $(J_k)_p(x) = \mu_p(x)N_p^k(x)$. Using

$$\mu_p(x) = 1 - x \quad \text{and} \quad N_p^k(x) = \sum_{n=0}^{\infty} \left(p^k\right)^n x^n = \frac{1}{1 - p^k x},$$

we have

$$(J_k)_p(x) = \frac{1 - x}{1 - p^k x}.$$

□

Exercise 2.18. Prove that every number of the form $2^{a-1}(2^a - 1)$ is perfect if $2^a - 1$ is prime.

Proof. Verifying directly, $\sigma(n) = \sum_{i=0}^{a-1} 2^i + (2^a - 1) \sum_{i=0}^{a-1} 2^i = 2^a \sum_{i=0}^{a-1} 2^i = 2^a \cdot \frac{2^a - 1}{2 - 1} = 2n.$ □

Exercise 2.19. Prove that if n is *even* and perfect then $n = 2^{a-1}(2^a - 1)$ for some $a \geq 2$. It is not known if any odd perfect numbers exist. It is known that there are no odd perfect numbers with less then 7 prime factors.

Proof. Suppose $n = 2^{a-1}d$ for $a \geq 2$ and n is perfect, i.e. n is even and $\sigma(n) = 2n$. Then

$$2^a d = \sigma(n) = \sigma(2^{a-1})\sigma(d) = (2^a - 1)\sigma(d).$$

Since $(2^a - 1, 2^a) = 1$, we have $2^a - 1 \mid d$ and so $d = (2^a - 1)m$. Substituting for d shows

$$(2^a - 1)\sigma(d) = 2^a(2^a - 1)m,$$

which implies $\sigma(d) = 2^a m$. Now since m and d are both divisors of d, $2^a m = \sigma(d) \geq m + d$, but $m + d = m + (2^a - 1)m = 2^a m$, which forces $\sigma(d) = m + d$. This means d can't have any other divisors, and so $m = 1$. We conclude that $d = 2^a - 1$ is prime, and $n = 2^{a-1}(2^a - 1)$. □

Exercise 2.20. Let $P(n)$ be the product of the positive integers which are $\leq n$ and relatively prime to n. Prove that

$$P(n) = n^{\varphi(n)} \prod_{d|n} \left(\frac{d!}{d^d}\right)^{\mu(n/d)}.$$

Proof. By Exercise 2.13, since $\mu^{-1} = u$,

$$\frac{P(n)}{n^{\varphi(n)}} = \prod_{d|n} \left(\frac{d!}{d^d}\right)^{\mu(n/d)} \iff \frac{n!}{n^n} = \prod_{d|n} \frac{P(d)}{d^{\varphi(d)}}.$$

Now

$$\begin{aligned}
\prod_{d|n} \frac{P(d)}{d^{\varphi(d)}} &= \prod_{d|n} \frac{1}{d^{\varphi(d)}} \prod_{\substack{k=1 \\ (k,d)=1}}^{d} k \\
&= \prod_{d|n} \prod_{\substack{k=1 \\ (k,d)=1}}^{d} \frac{k}{d} \\
&= \prod_{d|n} \prod_{\substack{k=1 \\ (k,d)=1}}^{d} \frac{kn/d}{n}.
\end{aligned}$$

By Lemma 2.14, kn/d attains the values $1, 2, \ldots, n$ exactly once, and so

$$\prod_{d|n} \frac{P(d)}{d^{\varphi(d)}} = \prod_{k=1}^{n} \frac{k}{n} = \frac{n!}{n^n}.$$

□

Exercise 2.21. Let $f(n) = [\sqrt{n}] - [\sqrt{n-1}]$. Prove that f is multiplicative but not completely multiplicative.

Lemma 2.21. f is the square indicator. That is $f(n) = 1$ if n is a square and $f(n) = 0$ otherwise.

Proof of Lemma. Suppose n is not a square and m^2 is the largest square less than n. Let $n = m^2 + k$, then

$$m^2 \leq m^2 + k - 1 < m^2 + k < (m+1)^2.$$

Therefore

$$m \leq \sqrt{n-1} < \sqrt{n} < m + 1,$$

which means $m = \lfloor \sqrt{n-1} \rfloor = \lfloor \sqrt{n} \rfloor$, i.e. $f(n) = 0$.

Now suppose $n = m^2$ is a square, then $(m-1)^2 \leq m^2 - 1 < m^2$. Therefore

$$m - 1 \leq \sqrt{n-1} < \sqrt{n} = m,$$

which means $\lfloor \sqrt{n-1} \rfloor = m - 1$ and $\lfloor \sqrt{n} \rfloor = m$, i.e. $f(n) = 1$. □

Proof of Exercise. Since f is the square indicator, by Theorem 2.19, $f = \lambda * u$ and hence is multiplicative. Now $f(4) = 1$ and $f(2)f(2) = 0$, so f is multiplicative but not completely multiplicative. □

Exercise 2.22. Prove that

$$\sigma_1(n) = \sum_{d|n} \varphi(d)\sigma_0\left(\frac{n}{d}\right),$$

and derive a generalization involving $\sigma_\alpha(n)$. (More than one generalization is possible.)

Proof. Since $\sigma_\alpha = u * N^\alpha$ and $N = \varphi * u$, we have

$$\begin{aligned}\sum_{d|n} \varphi(d)\sigma_\alpha\left(\frac{n}{d}\right) &= \varphi * \sigma_\alpha = \varphi * (u * N^\alpha) \\ &= (\varphi * u) * N^\alpha = N * N^\alpha \\ &= \sum_{d|n} d\left(\frac{n}{d}\right)^\alpha = n^\alpha \sum_{d|n} d^{1-\alpha} \\ &= n^\alpha \sigma_{1-\alpha}(n).\end{aligned}$$

Letting $1 - \alpha \mapsto \alpha$,

$$\sigma_\alpha(n) = n^{\alpha-1} \sum_{d|n} \varphi(d)\sigma_{1-\alpha}\left(\frac{n}{d}\right).$$

Taking $\alpha = 1$ gives us the result. □

Exercise 2.23. Prove the following statement or exhibit a counter example. If f is multiplicative, then $F(n) = \prod_{d|n} f(d)$ is multiplicative.

Solution. False: Let $f(n) = \varphi(n)$, then $F(6) = 4$ and $F(2)F(3) = 2$.

Exercise 2.24. Let $A(x)$ and $B(x)$ be formal power series. If the product $A(x)B(x)$ is the zero series, prove that at least one factor is zero. In other words, the ring of formal power series has no zero divisors.

Proof. Suppose $B(x) \neq 0$ and let b_k be the first non-zero term in the series expansion of B. Then $B(x) = x^k \sum_{i=0}^{\infty} b_{i+k}x^i = x^k\tilde{B}(x)$. Since $A(x)B(x) \equiv 0$ if and only if $A(x)\tilde{B}(x) \equiv 0$, without loss of generality assume $b_0 \neq 0$.

Now $A(x)B(x) \equiv 0$ tells us each series coefficient is zero, i.e. $\sum_{k=0}^{n} a_k b_{n-k} = 0$ for all $n \geq 0$. We shall show $a_i \equiv 0$ via strong induction. For $n = 0$ we have $a_0b_0 = 0$, which implies $a_0 = 0$, as we know $b_0 \neq 0$. Now suppose $a_k = 0$ for all $0 < k < n$. Then

$$0 = \sum_{k=0}^{n} a_k b_{n-k} = a_n b_0,$$

which again since $b_0 \neq 0$, tells us $a_n = 0$. Therefore $A(x) \equiv 0$. □

Exercise 2.25. Assume f is multiplicative. Prove that:
(a) $f^{-1}(n) = \mu(n)f(n)$ for every squarefree n.
(b) $f^{-1}(p^2) = f(p)^2 - f(p^2)$ for every prime p.

Proof.
(a) Since n is squarefree, then for any divisor d, $(d, n/d) = 1$. Hence

$$\begin{aligned}(f * (\mu f))(n) &= \sum_{d|n} \mu(d)f(d)f\left(\frac{n}{d}\right) \\ &= \sum_{d|n} \mu(d)f(n) \\ &= f(n)I(n) \\ &= I(n).\end{aligned}$$

(b) We will compute $f^{-1}(p^2)$ by the method described in Theorem 2.8.

1. Since f is multiplicative, $f(1) = 1$, which tells us $f^{-1}(1) = 1$.
2. $f^{-1}(p) = -f(p)f^{-1}(1) = -f(p)$.
3. $f^{-1}(p^2) = -(f(p^2)f^{-1}(1) + f(p)f^{-1}(p)) = f(p)^2 - f(p^2)$.

□

Exercise 2.26. Assume f is multiplicative. Prove that f is completely multiplicative if, and only if, $f^{-1}(p^a) = 0$ for all primes p and $a \geq 2$.

Proof. Suppose f is completely multiplicative. Then $f^{-1}(p^a) = \mu(p^a)f(p^a) = 0$ for $a \geq 2$.

Now suppose $f^{-1}(p^a) = 0$ for all primes p and $a \geq 2$. Then by Exercise 2.25 (b) $f(p)^2 - f(p^2) = 0$, i.e. $f(p^2) = f(p)^2$. Inductively, for $a > 2$ we have

$$\begin{aligned}f^{-1}(p^a) &= -\sum_{\substack{d|p^a \\ d<p^a}} f\left(\frac{p^a}{d}\right) f^{-1}(d) \\ &= -\sum_{i=0}^{a-1} f(p^{a-i})f^{-1}(p^i) \\ &= -(f(p^a)f^{-1}(1) + f(p^{a-1})f^{-1}(p)) \\ &= -(f(p^a) + f(p)^{a-1}(-f(p))) \\ &= f(p)^a - f(p^a).\end{aligned}$$

Therefore $f(p^a) = f(p)^a$ and hence f is completely multiplicative. □

Exercise 2.27.
(a) If f is completely multiplicative, prove that

$$f \cdot (g * h) = (f \cdot g) * (f \cdot h)$$

for all arithmetical functions g and h, where $f \cdot g$ denotes the product, $(f \cdot g)(n) = f(n)g(n)$.
(b) If f is multiplicative and if the relation in (a) holds for $g = \mu$ and $h = \mu^{-1}$, prove that f is completely multiplicative.

Proof.
(a) By the definition of Dirichlet convolution,

$$\begin{aligned}((f\cdot g)*(f\cdot h))(n) &= \sum_{d|n} f(d)g(d)f\left(\frac{n}{d}\right)h\left(\frac{n}{d}\right)\\ &= f(n)\sum_{d|n} g(d)h\left(\frac{n}{d}\right)\\ &= f(n)(g*h)(n).\end{aligned}$$

(b) Supposing

$$f\cdot(\mu*\mu^{-1}) = (f\cdot\mu)*(f\cdot\mu^{-1}),$$

then $fI = (\mu f)*f$. Now since $f(1)=1$, $(\mu f)*f = I$. This means $f^{-1}=\mu f$, and hence by Theorem 2.17, f is completely multiplicative. □

Exercise 2.28.
(a) If f is completely multiplicative, prove that

$$(f\cdot g)^{-1} = f\cdot g^{-1}$$

for every arithmetical function g with $g(1)\neq 0$.
(b) If f is multiplicative and the relation in (a) holds for $g=\mu^{-1}$, prove that f is completely multiplicative.

Proof.
(a) Suppose $g(1)\neq 0$. Then g^{-1} exists and

$$\begin{aligned}((f\cdot g)*(f\cdot g^{-1}))(n) &= \sum_{d|n} f(d)g(d)f\left(\frac{n}{d}\right)g^{-1}\left(\frac{n}{d}\right)\\ &= f(n)\sum_{d|n} g(d)g^{-1}\left(\frac{n}{d}\right)\\ &= f(n)(g*g^{-1})(n)\\ &= f(n)I(n)\\ &= I(n).\end{aligned}$$

Therefore $(f\cdot g)^{-1} = f\cdot g^{-1}$.
(b) Supposing $(f\cdot u)^{-1} = f\cdot\mu$, then $(\mu f)*f = I$. Hence by Theorem 2.17, f is completely multiplicative. □

Exercise 2.29. Prove that there is a multiplicative arithmetical function g such that

$$\sum_{k=1}^{n} f((k,n)) = \sum_{d|n} f(d)g\left(\frac{n}{d}\right)$$

for every arithmetical function f. Here (k,n) is the gcd of n and k. Use this identity to prove that

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

Proof. Using the second part of this problem for intuition, take $g = \varphi$. Partitioning k via it's gcd with n gives

$$\begin{aligned}\sum_{k=1}^{n} f((k,n)) &= \sum_{d|n} \sum_{\substack{1\le k\le n\\(k,n)=d}} f((k,n)) \\ &= \sum_{d|n} f(d) \sum_{\substack{1\le k\le n\\(k,n)=d}} 1.\end{aligned}$$

The proof of Theorem 2.2 shows

$$\sum_{\substack{1\le k\le n\\(k,n)=d}} 1 = \varphi\left(\frac{n}{d}\right)$$

and hence

$$\sum_{k=1}^{n} f((k,n)) = \sum_{d|n} f(d)\varphi\left(\frac{n}{d}\right).$$

Finally, let $f(n) = n\mu(n)$ and apply the above identity:

$$\sum_{k=1}^{n}(k,n)\mu((k,n)) = ((N\mu) * \varphi)(n) = (N^{-1} * \varphi)(n) = \mu(n).$$

□

Exercise 2.30. Let f be multiplicative and let g be any arithmetical function. Assume that

(a) $$f(p^{n+1}) = f(p)f(p^n) - g(p)f(p^{n-1}) \text{ for all primes } p \text{ and all } n \ge 1.$$

Prove that for each prime p the Bell series for f has the form

(b) $$f_p(x) = \frac{1}{1 - f(p)x + g(p)x^2}.$$

Conversely, prove that (b) implies (a).

Proof. By the uniqueness theorem of Bell series of multiplicative functions,

$$\begin{aligned}&f(p^{n+1}) = f(p)f(p^n) - g(p)f(p^{n-1}) \\ &\iff f_p(x) = 1 + f(p)x + \sum_{n=2}^{\infty}(f(p)f(p^{n-1}) - g(p)f(p^{n-2})x^n \\ &\iff f_p(x) = 1 + f(p)x + f(p)x\sum_{n=1}^{\infty} f(p^n)x^n - g(p)x^2\sum_{n=0}^{\infty} f(p^n)x^n \\ &\iff f_p(x) = 1 + f(p)xf_p(x) - g(p)x^2 f_p(x) \\ &\iff f_p(x) = \frac{1}{1 - f(p)x + g(p)x^2}.\end{aligned}$$

□

Exercise 2.31.(+) (Continuation of Exercise 2.30.) If g is completely multiplicative prove that statement (a) of Exercise 2.30 implies

$$f(m)f(n) = \sum_{d|(m,n)} g(d) f\left(\frac{mn}{d^2}\right),$$

where the sum is extended over the positive divisors of the gcd (m, n). [*Hint*: Consider first the case $m = p^a$, $n = p^b$.]

Proof. First, assume $m = p^a$ and $n = p^b$ for some prime p and $a \geq b$. Then $(m, n) = p^b$ and so

$$\sum_{d|(m,n)} g(d) f\left(\frac{mn}{d^2}\right) = \sum_{i=0}^{b} g(p)^i f(p^{a+b-2i}).$$

To prove the identity in the problem statement, fix a and induct on b. Suppose $b = 1$, then by assumption

$$\sum_{i=0}^{b} g(p)^i f(p^{a+b-2i}) = g(1)f(p^{a+1}) + g(p)f(p^{a-1}) = f(p^a)f(p).$$

Assume the identity is true for $1, \ldots, b-1$, then

$$\begin{aligned}
f(p^a)f(p^b) &= f(p^a)\left[f(p)f(p^{b-1}) - g(p)f(p^{b-2})\right] \\
&= \left[f(p^a)f(p)\right] f(p^{b-1}) - g(p)f(p^a)f(p^{b-2}) \\
&= \left[f(p^{a+1}) + g(p)f(p^{a-1})\right] f(p^{b-1}) - g(p)f(p^a)f(p^{b-2}) \\
&= f(p^{a+1})f(p^{b-1}) + g(p)f(p^{a-1})f(p^{b-1}) - g(p)f(p^a)f(p^{b-2}) \\
&= \sum_{i=0}^{b-1} g(p)^i f(p^{a+b-2i}) + g(p)\sum_{i=0}^{b-1} g(p)^i f(p^{a+b-2i-2}) - g(p)\sum_{i=0}^{b-2} g(p)^i f(p^{a+b-2i-2}) \\
&= \sum_{i=0}^{b-1} g(p)^i f(p^{a+b-2i}) + g(p)^b f(p^{a+b-2(b-1)-2}) \\
&= \sum_{i=0}^{b} g(p)^i f(p^{a+b-2i}).
\end{aligned}$$

So by induction, the identity holds for prime powers. What remains to be shown is that the right hand side is multiplicative with respect to m and n.

Let $m = p_1^{a_1} \cdots p_k^{a_k}$, $n = p_1^{b_1} \cdots p_k^{b_k}$ where $a_i, b_i \geq 0$, and define $c_i = \max\{a_i, b_i\}$. Then

$$\begin{aligned}
\sum_{d|(m,n)} g(d) f\left(\frac{mn}{d^2}\right) &= \sum_{i_1=0}^{c_1} \cdots \sum_{i_k=0}^{c_k} g(p_1^{i_1} \cdots p_k^{i_k}) f(p_1^{a_1+b_1-2i_1} \cdots p_k^{a_k+b_k-2i_k}) \\
&= \sum_{i_1=0}^{c_1} \cdots \sum_{i_k=0}^{c_k} g(p_1^{i_1}) \cdots g(p_k^{i_k}) f(p_1^{a_1+b_1-2i_1}) \cdots f(p_k^{a_k+b_k-2i_k}) \\
&= \prod_{j=1}^{k} \sum_{i_j=0}^{c_j} g(p_j^{i_j}) f(p_j^{a_j+b_j-2i_j}) \\
&= \prod_{j=1}^{k} \sum_{d|(p_j^{a_j}, p_j^{b_j})} g(d) f(mn/d^2),
\end{aligned}$$

hence the both sides are multiplicative with respect to m and n and the result follows. □

Exercise 2.32. Prove that

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

Proof. Since N^α is completely multiplicative and σ_α is multiplicative, by Exercise 2.31 it's enough to show

$$\sigma_\alpha(p^{n+1}) = \sigma_\alpha(p)\sigma_\alpha(p^n) - p^\alpha \sigma_\alpha(p^{n-1}).$$

For $\alpha = 0$,

$$\sigma_0(p)\sigma_0(p^n) - \sigma_0(p^{n-1}) = 2(n+1) - n = n + 2 = \sigma_0(p^{n+1}).$$

Otherwise

$$\begin{aligned}
\sigma_\alpha(p)\sigma_\alpha(p^n) - p^\alpha \sigma_\alpha(p^{n-1}) &= \frac{p^{2\alpha}-1}{p^\alpha - 1} \cdot \frac{p^{(n+1)\alpha}-1}{p^\alpha - 1} - p^\alpha \cdot \frac{p^{n\alpha}-1}{p^\alpha - 1} \\
&= \frac{(p^\alpha+1)(p^{(n+1)\alpha}-1) - p^\alpha(p^{n\alpha}-1)}{p^\alpha - 1} \\
&= \frac{p^{(n+2)\alpha} + p^{(n+1)\alpha} - p^\alpha - 1 - p^{(n+1)\alpha} - p^\alpha}{p^\alpha - 1} \\
&= \frac{p^{(n+2)\alpha}-1}{p^\alpha - 1} \\
&= \sigma_\alpha(p^{n+1}).
\end{aligned}$$

□

Exercise 2.33. Prove that Liouville's function is given by the formula

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

Proof. By Theorem 2.19, $f = \lambda * u$, where f is the square indicator function. Thus

$$\begin{aligned}\lambda(n) &= (f * \mu)(n) \\ &= \sum_{d|n} f(d)\mu\left(\frac{n}{d}\right) \\ &= \sum_{d^2|n} \mu\left(\frac{n}{d^2}\right).\end{aligned}$$

□

Exercise 2.34. This exercise describes an alternate proof to Theorem 2.16 which states that the Dirichlet inverse of a multiplicative function is multiplicative. Assume g is multiplicative and let $f = g^{-1}$.
(a) Prove that if p is prime then for $k \geq 1$ we have

$$f(p^k) = -\sum_{t=1}^{k} g(p^t) f(p^{k-t}).$$

(b) Let h be the uniquely determined multiplicative function which agrees with f at the prime powers. Show that $h * g$ agrees with the identity function I at the prime powers and deduce that $h * g = I$. This shows that $f = h$ so f is multiplicative.

Proof.
(a) Since $f = g^{-1}$, we have $f * g = I$. Thus for p prime and $k \geq 1$,

$$\begin{aligned}\sum_{d|p^k} g(d) f\left(\frac{p^k}{d}\right) = 0 \implies \sum_{t=0}^{k} g(p^t) f(p^{k-t}) = 0 \\ \implies f(p^k) + \sum_{t=1}^{k} g(p^t) f(p^{k-t}) = 0.\end{aligned}$$

(b) Suppose p is prime and $k \geq 1$. Then since $f = g^{-1}$,

$$0 = \sum_{t=0}^{k} g(p^t) f(p^{k-t}) = \sum_{t=0}^{k} g(p^t) h(p^{k-t}) = (h * g)(p^k).$$

Because h and g are multiplicative, $(h * g)(1) = 1$, and so $h * g$ agrees with the identity function at prime powers. Since h and g are multiplicative, so is $h * g$, and hence $h * g = I$. Finally since Dirchlet inverses are unique, $f = h$ and is therefore multiplicative. □

Exercise 2.35. If f and g are multiplicative and if a and b are positive integers with $a \geq b$, prove that the function h given by

$$h(n) = \sum_{d^a|n} f\left(\frac{n}{d^a}\right) g\left(\frac{n}{d^b}\right)$$

is also multiplicative. The sum is extended over those divisors d of n for which d^a divides n.

Proof. Let $(m,n)=1$. For all $c \mid m$ and $d \mid n$, $(m/c, n/d)=1$ and thus

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

In the second to last step we used the one-to-one correspondence between the divisors $(cd)^a \mid mn$ and $t^a \mid mn$ for $(m,n)=1$. □

MÖBIUS FUNCTIONS OF ORDER k.
If $k \geq 1$ we define μ_k, as follows:

$$\begin{aligned} &\mu_k(1) = 1, \\ &\mu_k(n) = 0 \text{ if } p^{k+1} \mid n \text{ for some prime } p, \\ &\mu_k(n) = (-1)^r \text{ if } n = p_1^k \cdots p_r^k \prod_{i>r} p_i^{a_i}, \quad 0 \leq a_i < k, \\ &\mu_k(n) = 1 \text{ otherwise.} \end{aligned}$$

In other words, $\mu_k(n)$ vanishes if n is divisible by the $(k+1)$st power of some prime; otherwise, $\mu_k(n)$ is 1 unless the prime factorization of n contains the kth powers of exactly r distinct primes, in which case $\mu_k(n) = (-1)^r$. Note that $\mu_1 = \mu$, the usual Möbius function.

Prove the properties of the functions μ_k described in the following exercises.

Exercise 2.36. If $k \geq 1$ then $\mu_k(n^k) = \mu(n)$.

Proof. We will show $\mu_k(n^k) = \mu_{k-1}(n^{k-1})$ for $k > 1$, then inductively the result follows. Assuming $k > 1$, consider the following cases.

- If $n = 1$, then $\mu_k(1^k) = 1 = \mu_{k-1}(1^{k-1})$.
- If $\mu_k(n^k) = 0$, then there is a prime p such that $p^{k+1} \mid n^k$, which implies $p^k \mid n^{k-1}$. This means $\mu_{k-1}(n^{k-1}) = 0$.
- If $\mu_k(n^k) = (-1)^r$, then $n^k = p_1^k \cdots p_r^k \prod_{i>r} p_i^{a_i}$ for $0 \leq a_i < k$. Now since n^k is a kth power, we must have $a_i = 0$. Thus $n^k = p_1^k \cdots p_r^k$, which means $n^{k-1} = p_1^{k-1} \cdots p_r^{k-1}$ and hence $\mu_{k-1}(n^{k-1}) = (-1)^r$.

□

Exercise 2.37. Each function μ_k is multiplicative.

Proof. Suppose $(m,n) = 1$ and $m, n > 1$, as the claim is trivial for m or n equal to 1. If $p^{k+1} \mid m$ for some prime p, then $p^{k+1} \mid mn$ and so $\mu_k(mn) = 0 = \mu_k(m)\mu_k(n)$. Otherwise suppose

$$m = p_1^k \cdots p_{r_1}^k \prod_{i>r_1} p_i^{a_i} \quad \text{and} \quad n = q_1^k \cdots q_{r_2}^k \prod_{i>r_2} q_i^{b_i}$$

for $0 \leq a_i, b_i < k$, $r_1, r_2 \geq 0$. Since $(m,n) = 1$, all kth prime powers are distinct and $a_i \neq 0$ implies $b_i = 0$ and vice versa. Therefore

$$\mu_k(mn) = (-1)^{r_1+r_2} = (-1)^{r_1}(-1)^{r_2} = \mu_k(m)\mu_k(n).$$

□

Exercise 2.38. If $k \geq 2$ we have

$$\mu_k(n) = \sum_{d^k \mid n} \mu_{k-1}\left(\frac{n}{d^k}\right) \mu_{k-1}\left(\frac{n}{d}\right).$$

Proof. By Exercise 2.37 the left hand side is multiplicative and by Exercise 2.35 the right hand side is multiplicative, so it suffices to prove this for prime powers. Denote the right hand side by *rhs*, and consider the three cases.

- Suppose $n = p^a$ for $0 \leq a < k$. Then since 1 is the only kth power to divide p^a, $\mu_k(p^a) = 1$ and $rhs = \mu_{k-1}(p^a)^2 = (\pm 1)^2 = 1$.
- Since 1 and p^k are the only kth powers to divide p^k, observe $\mu_k(p^k) = -1$ and

$$rhs = \mu_{k-1}(p^k)^2 + \mu_{k-1}(1)\mu_{k-1}(p^{k-1}) = 0 + 1(-1) = -1.$$

- Suppose $n = p^a$ for $a > k$. Then $\mu_k(p^a) = 0$ and

$$rhs = \sum_{i=0}^{\lfloor a/k \rfloor} \mu_{k-1}(p^{a-ki})\mu_{k-1}(p^{a-i}).$$

  Now

$$\begin{aligned} a - i &\geq a - \lfloor a/k \rfloor \geq a - a/k \\ &= \frac{a(k-1)}{k} \\ &> k - 1, \end{aligned}$$

  hence $a - i \geq k$. Therefore $\mu_{k-1}(p^{a-i}) = 0$, which forces $rhs = 0$.

□

Exercise 2.39. If $k \geq 1$ we have

$$|\mu_k(n)| = \sum_{d^{k+1}|n} \mu(d).$$

Proof. Since $m^k \mid n$ for some $m > 1$ if and only if $p^k \mid n$ for some prime p, by Exercise 2.6

$$\sum_{d^{k+1}|n} \mu(d) = \begin{cases} 0 & \text{if } p^{k+1} \mid n \text{ for some prime } p, \\ 1 & \text{otherwise.} \end{cases}$$

By definition it's clear this is exactly $|\mu_k(n)|$. □

Exercise 2.40. For each prime p the Bell series for μ_k is given by

$$(\mu_k)_p(x) = \frac{1 - 2x^k + x^{k+1}}{1 - x}.$$

Proof. Evaluating μ_k at prime powers, we see

$$(\mu_k)_p(x) = \sum_{n=0}^{k-1} x^n - x^k = \frac{x^k - 1}{x - 1} - x^k = \frac{1 - 2x^k + x^{k+1}}{1 - x}.$$

□

Chapter 3
Averages of Arithmetical Functions

Exercise 3.1. Use Euler's summation formula to deduce the following for $x \geq 2$.

(a) $\displaystyle\sum_{n\leq x} \frac{\log n}{n} = \frac{1}{2}\log^2 x + A + O\left(\frac{\log x}{x}\right)$, where A is a constant.

(b) $\displaystyle\sum_{n\leq x} \frac{1}{n\log n} = \log(\log x) + B + O\left(\frac{1}{x\log x}\right)$, where B is a constant.

Proof.
(a) Given $\frac{d}{dt}(\frac{\log t}{t}) = \frac{1-\log t}{t^2}$, then by Euler summation

$$\begin{aligned}\sum_{n\leq x} \frac{\log n}{n} &= \int_1^x \frac{\log t}{t}dt + \int_1^x (t-\lfloor t\rfloor)\frac{1-\log t}{t^2}dt + (x-\lfloor x\rfloor)\frac{\log x}{x} \\ &= \frac{1}{2}\log^2 x + \left(\int_1^\infty - \int_x^\infty\right)(t-\lfloor t\rfloor)\frac{1-\log t}{t^2}dt + O\left(\frac{\log x}{x}\right).\end{aligned}$$

Now

$$\begin{aligned}\left|\int_x^\infty (t-\lfloor t\rfloor)\frac{1-\log t}{t^2}dt\right| &\leq 2\int_x^\infty \frac{\log t}{t^2}dt \\ &= 2\cdot\frac{\log x+1}{x} \\ &= O\left(\frac{\log x}{x}\right),\end{aligned}$$

hence the result follows.

(b) Given $\frac{d}{dt}(\frac{1}{t\log t}) = \frac{-\log t-1}{t^2\log^2 t}$, then by Euler summation

$$\begin{aligned}\sum_{n\leq x} \frac{1}{n\log n} &= \int_1^x \frac{1}{t\log t}dt - \int_1^x (t-\lfloor t\rfloor)\frac{\log t+1}{t^2\log^2 t}dt + (x-\lfloor x\rfloor)\frac{1}{x\log x} \\ &= \log(\log x) - \left(\int_1^\infty - \int_x^\infty\right)(t-\lfloor t\rfloor)\frac{\log t+1}{t^2\log^2 t}dt + O\left(\frac{1}{x\log x}\right).\end{aligned}$$

Now

$$\begin{aligned}\left|\int_x^\infty (t-\lfloor t\rfloor)\frac{\log t+1}{t^2\log^2 t}dt\right| &\le \int_x^\infty \frac{\log t+1}{t^2\log^2 t}dt\\ &= \frac{1}{x\log x}\\ &= O\left(\frac{1}{x\log x}\right),\end{aligned}$$

hence the result follows.

□

Exercise 3.2. If $x \ge 2$ prove that

$$\sum_{n\le x}\frac{d(n)}{n} = \frac{1}{2}\log^2 x + 2C\log x + O(1), \text{ where } C \text{ is Euler's constant.}$$

Proof. Changing order of summation as in Theorem 3.3 and using Exercise 3.1 (a),

$$\begin{aligned}\sum_{n\le x}\frac{d(n)}{n} &= \sum_{d\le x}\frac{1}{d}\sum_{q\le x/d}\frac{1}{q}\\ &= \sum_{d\le x}\frac{1}{d}\left(\log\left(\frac{x}{d}\right)+C+O\left(\frac{d}{x}\right)\right)\\ &= \sum_{d\le x}\left(\frac{\log x+C}{d}-\frac{\log d}{d}+O\left(\frac{1}{x}\right)\right)\\ &= (\log x+C)\sum_{d\le x}\frac{1}{d}-\sum_{d\le x}\frac{\log d}{d}+O(1)\\ &= (\log x+C)\left(\log x+C+O\left(\frac{1}{x}\right)\right)-\left(\frac{1}{2}\log^2 x+O(1)\right)+O(1)\\ &= \log^2 x+C\log x+O\left(\frac{\log x}{x}\right)+C\log x+C^2+O\left(\frac{1}{x}\right)-\frac{1}{2}\log^2 x+O(1)\\ &= \frac{1}{2}\log^2 x+2C\log x+O(1).\end{aligned}$$

□

Exercise 3.3. If $x \ge 2$ and $\alpha > 0, \alpha \ne 1$, prove that

$$\sum_{n\le x}\frac{d(n)}{n^\alpha} = \frac{x^{1-\alpha}\log x}{1-\alpha}+\zeta(\alpha)^2+O(x^{1-\alpha}).$$

Proof. Changing order of summation as in Theorem 3.3 and using Theorem 3.2 (b),

$$\begin{aligned}
\sum_{n\le x}\frac{d(n)}{n^\alpha} &= \sum_{d\le x}\frac{1}{d^\alpha}\sum_{q\le x/d}\frac{1}{q^\alpha}\\
&= \sum_{d\le x}\frac{1}{d^\alpha}\left(\frac{(x/d)^{1-\alpha}}{1-\alpha}+\zeta(\alpha)+O\left(\frac{1}{(x/d)^\alpha}\right)\right)\\
&= \frac{x^{1-\alpha}}{1-\alpha}\sum_{d\le x}\frac{1}{d}+\zeta(\alpha)\sum_{d\le x}\frac{1}{d^\alpha}+O(x^{1-\alpha})\\
&= \frac{x^{1-\alpha}}{1-\alpha}\left(\log x+C+O\left(\frac{1}{x}\right)\right)+\zeta(\alpha)\left(\frac{x^{1-\alpha}}{1-\alpha}+\zeta(\alpha)+O(x^{-\alpha})\right)+O(x^{1-\alpha})\\
&= \frac{x^{1-\alpha}\log x}{1-\alpha}+C\cdot\frac{x^{1-\alpha}}{1-\alpha}+O(x^{-\alpha})+\zeta(\alpha)\cdot\frac{x^{1-\alpha}}{1-\alpha}+\zeta(\alpha)^2+O(x^{-\alpha})+O(x^{1-\alpha})\\
&= \frac{x^{1-\alpha}\log x}{1-\alpha}+\zeta(\alpha)^2+O(x^{1-\alpha}).
\end{aligned}$$

□

Exercise 3.4. If $x\ge 2$ prove that:

(a) $\displaystyle\sum_{n\le x}\mu(n)\left\lfloor\frac{x}{n}\right\rfloor^2=\frac{x^2}{\zeta(2)}+O(x\log x).$

(b) $\displaystyle\sum_{n\le x}\frac{\mu(n)}{n}\left\lfloor\frac{x}{n}\right\rfloor=\frac{x}{\zeta(2)}+O(\log x).$

Proof.
(a) Using Theorem 3.2 (a)(c),

$$\begin{aligned}
\sum_{n\le x}\mu(n)\left\lfloor\frac{x}{n}\right\rfloor^2 &= \sum_{n\le x}\mu(n)\left(\frac{x}{n}\right)^2-2\sum_{n\le x}\mu(n)\left(\frac{x}{n}\right)\left\{\frac{x}{n}\right\}+\sum_{n\le x}\mu(n)\left\{\frac{x}{n}\right\}^2\\
&= x^2\sum_{n=1}^{\infty}\frac{\mu(n)}{n^2}-x^2\sum_{n>x}\frac{\mu(n)}{n^2}+O\left(x\sum_{n\le x}\frac{1}{n}\right)+O\left(\sum_{n\le x}1\right)\\
&= x^2\sum_{n=1}^{\infty}\frac{\mu(n)}{n^2}-x^2\cdot O\left(\sum_{n>x}\frac{1}{n^2}\right)+O(x\log x)\\
&= \frac{x^2}{\zeta(2)}+x^2\cdot O\left(\frac{1}{x}\right)+O(x\log x)\\
&= \frac{x^2}{\zeta(2)}+O(x\log x).
\end{aligned}$$

(b) Again, using Theorem 3.2 (a)(c),

$$\begin{aligned}\sum_{n\le x}\frac{\mu(n)}{n}\left\lfloor\frac{x}{n}\right\rfloor &= x\sum_{n\le x}\frac{\mu(n)}{n^2}-\sum_{n\le x}\frac{\mu(n)}{n}\left\{\frac{x}{n}\right\}\\ &= x\sum_{n=1}^{\infty}\frac{\mu(n)}{n^2}-x\sum_{n>x}\frac{\mu(n)}{n^2}+O\left(\sum_{n\le x}\frac{1}{n}\right)\\ &= \frac{x}{\zeta(2)}+x\cdot O\left(\frac{1}{x}\right)+O(\log x)\\ &= \frac{x}{\zeta(2)}+O(\log x).\end{aligned}$$

□

Exercise 3.5. If $x\ge 1$ prove that:

(a) $\displaystyle\sum_{n\le x}\varphi(n)=\frac{1}{2}\sum_{n\le x}\mu(n)\left\lfloor\frac{x}{n}\right\rfloor^2+\frac{1}{2}.$

(b) $\displaystyle\sum_{n\le x}\frac{\varphi(n)}{n}=\sum_{n\le x}\frac{\mu(n)}{n}\left\lfloor\frac{x}{n}\right\rfloor.$

These formulas, together with those in Exercise 4, show that, for $x\ge 2$,

$$\sum_{n\le x}\varphi(n)=\frac{1}{2}\frac{x^2}{\zeta(2)}+O(x\log x)\text{ and }\sum_{n\le x}\frac{\varphi(n)}{n}=\frac{x}{\zeta(2)}+O(\log x).$$

Proof.
(a) Changing order of summation as in Theorem 3.3,

$$\begin{aligned}\sum_{n\le x}\varphi(n) &= \sum_{n\le x}\sum_{d\mid n}\mu(d)\frac{n}{d}\\ &= \sum_{\substack{q,d\\ q,d\le x}}\mu(d)q\\ &= \sum_{d\le x}\mu(d)\sum_{q\le x/d}q\\ &= \sum_{d\le x}\mu(d)\cdot\frac{\lfloor x/d\rfloor\,(\lfloor x/d\rfloor+1)}{2}\\ &= \frac{1}{2}\sum_{d\le x}\mu(d)\left\lfloor\frac{x}{d}\right\rfloor^2+\frac{1}{2}\sum_{d\le x}\mu(d)\left\lfloor\frac{x}{d}\right\rfloor\\ &= \frac{1}{2}\sum_{n\le x}\mu(n)\left\lfloor\frac{x}{n}\right\rfloor^2+\frac{1}{2}.\end{aligned}$$

(b) Changing order of summation as in Theorem 3.3,

$$\begin{aligned}\sum_{n\le x}\frac{\varphi(n)}{n} &= \sum_{n\le x}\sum_{d\mid n}\frac{\mu(d)}{d}\\ &= \sum_{\substack{q,d\\ q,d\le x}}\frac{\mu(d)}{d}\\ &= \sum_{d\le x}\frac{\mu(d)}{d}\sum_{q\le x/d}1\\ &= \sum_{d\le x}\frac{\mu(d)}{d}\left\lfloor\frac{x}{d}\right\rfloor.\end{aligned}$$

□

Exercise 3.6. If $x \ge 2$ prove that

$$\sum_{n\le x}\frac{\varphi(n)}{n^2} = \frac{1}{\zeta(2)}\log x + \frac{C}{\zeta(2)} - A + O\left(\frac{\log x}{x}\right),$$

where C is Euler's constant and

$$A = \sum_{n=1}^{\infty}\frac{\mu(n)\log n}{n^2}.$$

Proof. Changing order of summation as in Theorem 3.3 and using Theorem 3.2 (c),

$$\begin{aligned}\sum_{n\le x}\frac{\varphi(n)}{n^2} &= \sum_{n\le x}\frac{1}{n^2}\sum_{d\mid n}\mu(d)\frac{n}{d} = \sum_{\substack{q,d\\ qd\le x}}\frac{\mu(d)}{qd^2}\\ &= \sum_{d\le x}\frac{\mu(d)}{d^2}\sum_{q\le x/d}\frac{1}{q}\\ &= \sum_{d\le x}\frac{\mu(d)}{d^2}\left(\log x - \log d + C + O\left(\frac{1}{x}\right)\right)\\ &= (\log x + C)\sum_{d\le x}\frac{\mu(d)}{d^2} - \sum_{d\le x}\frac{\mu(d)\log d}{d^2} + O\left(\frac{1}{x}\right)\\ &= \frac{\log x + C}{\zeta(2)} - \sum_{d=1}^{\infty}\frac{\mu(d)\log d}{d^2} - (\log x + C)\sum_{d>x}\frac{\mu(d)}{d^2} + \sum_{d>x}\frac{\mu(d)\log d}{d^2} + O\left(\frac{1}{x}\right)\\ &= \frac{\log x + C}{\zeta(2)} - A + O\left(\frac{\log x + C}{x}\right) + O\left(\sum_{d>x}\frac{1}{d^{3/2}}\right)\\ &= \frac{\log x + C}{\zeta(2)} - A + O\left(\frac{\log x + C}{x}\right) + O\left(\frac{1}{\sqrt{x}}\right).\end{aligned}$$

Since $\log(x)/x$ is the main error term, we are done. □

Exercise 3.7. In a later chapter we will prove that $\sum_{n=1}^{\infty}\mu(n)n^{-\alpha} = 1/\zeta(\alpha)$ if $\alpha > 1$. Assuming this, prove that for $x \geq 2$ and $\alpha > 1, \alpha \neq 2$, we have

$$\sum_{n\leq x}\frac{\varphi(n)}{n^\alpha} = \frac{x^{2-\alpha}}{2-\alpha}\frac{1}{\zeta(2)} + \frac{\zeta(\alpha-1)}{\zeta(\alpha)} + O(x^{1-\alpha}\log x).$$

Proof. Changing order of summation as in Theorem 3.3 and using Theorem 3.2 (b),

$$\begin{aligned}
\sum_{n\leq x}\frac{\varphi(n)}{n^\alpha} &= \sum_{n\leq x}\frac{1}{n^\alpha}\sum_{d\mid n}\mu(d)\frac{n}{d} = \sum_{\substack{q,d\\ qd\leq x}}\frac{\mu(d)}{d^\alpha q^{\alpha-1}}\\
&= \sum_{d\leq x}\frac{\mu(d)}{d^\alpha}\sum_{q\leq x/d}\frac{1}{q^{\alpha-1}}\\
&= \sum_{d\leq x}\frac{\mu(d)}{d^\alpha}\left(\frac{(x/d)^{2-\alpha}}{2-\alpha} + \zeta(\alpha-1) + O\big((x/d)^{1-\alpha}\big)\right)\\
&= \frac{x^{2-\alpha}}{2-\alpha}\sum_{d\leq x}\frac{\mu(d)}{d^2} + \zeta(\alpha-1)\sum_{d\leq x}\frac{\mu(d)}{d^\alpha} + O\left(x^{1-\alpha}\sum_{d\leq x}\frac{\mu(d)}{d}\right)\\
&= \frac{x^{2-\alpha}}{2-\alpha}\frac{1}{\zeta(2)} + \frac{x^{2-\alpha}}{2-\alpha}\sum_{d>x}\frac{\mu(d)}{d^2} + \frac{\zeta(\alpha-1)}{\zeta(\alpha)} + \zeta(\alpha-1)\sum_{d>x}\frac{\mu(d)}{d^\alpha} + O\big(x^{1-\alpha}\log x\big)\\
&= \frac{x^{2-\alpha}}{2-\alpha}\frac{1}{\zeta(2)} + O\big(x^{1-\alpha}\big) + \frac{\zeta(\alpha-1)}{\zeta(\alpha)} + \zeta(\alpha-1)O(1) + O\big(x^{1-\alpha}\log x\big).
\end{aligned}$$

□

Exercise 3.8. If $\alpha \leq 1$ and $x \geq 2$ prove that

$$\sum_{n\leq x}\frac{\varphi(n)}{n^\alpha} = \frac{x^{2-\alpha}}{2-\alpha}\frac{1}{\zeta(2)} + O(x^{1-\alpha}\log x).$$

Proof. Starting off just as in the proof of Exercise 3.7 and using Theorem 3.2 (c)(d),

$$\begin{aligned}
\sum_{n\leq x}\frac{\varphi(n)}{n^\alpha} &= \sum_{d\leq x}\frac{\mu(d)}{d^\alpha}\sum_{q\leq x/d}\frac{1}{q^{\alpha-1}}\\
&= \sum_{d\leq x}\frac{\mu(d)}{d^\alpha}\left(\frac{(x/d)^{2-\alpha}}{2-\alpha} + O\big((x/d)^{1-\alpha}\big)\right)\\
&= \frac{x^{2-\alpha}}{2-\alpha}\sum_{d\leq x}\frac{\mu(d)}{d^2} + O\left(x^{1-\alpha}\sum_{d\leq x}\frac{\mu(d)}{d}\right)\\
&= \frac{x^{2-\alpha}}{2-\alpha}\frac{1}{\zeta(2)} - \frac{x^{2-\alpha}}{2-\alpha}\sum_{d>x}\frac{\mu(d)}{d^2} + O\big(x^{1-\alpha}\log x\big)\\
&= \frac{x^{2-\alpha}}{2-\alpha}\frac{1}{\zeta(2)} + O\big(x^{1-\alpha}\big) + O\big(x^{1-\alpha}\log x\big).
\end{aligned}$$

□

Exercise 3.9. In a later chapter we will prove that the infiite product $\prod_p(1-p^{-2})$, extended over all primes, converges to the value $1/\zeta(2) = 6/\pi^2$. Assuming this result, prove that

(a) $\dfrac{\sigma(n)}{n} < \dfrac{n}{\varphi(n)} < \dfrac{\pi^2}{6}\dfrac{\sigma(n)}{n}$ if $n \geq 2$.

[*Hint*: Use the formula $\varphi(n) = n\prod_{p|n}(1-p^{-1})$ and the relation

$$1 + x + x^2 + \cdots = \frac{1}{1-x} = \frac{1+x}{1-x^2} \quad \text{with } x = \frac{1}{p}.\Big]$$

(b) If $x \geq 2$ prove that

$$\sum_{n\leq x} \frac{n}{\varphi(n)} = O(x).$$

Proof.
(a) Let $n = p_1^{\alpha_1}\cdots p_k^{\alpha_k}$ for $k > 0$, then

$$\begin{aligned}
\frac{n}{\varphi(n)} &= \prod_{p|n}\frac{1}{1-1/p} = \prod_{p|n}\frac{1+1/p}{1-1/p^2} \\
&< \prod_{p}\left(1-1/p^2\right)^{-1}\prod_{p|n}(1+1/p) \\
&= \frac{\pi^2}{6}\prod_{p|n}(1+1/p) = \frac{\pi^2}{6}\cdot\frac{1}{n}\prod_{p_i|n}\left(p^{\alpha_i}+p^{\alpha_i-1}\right) \\
&\leq \frac{\pi^2}{6}\cdot\frac{1}{n}\prod_{p_i|n}\left(p_i^{\alpha_i}+p^{\alpha_i-1}+\cdots+1\right) \\
&\leq \frac{\pi^2}{6}\cdot\frac{1}{n}\prod_{p_i|n}\frac{p_i^{\alpha_i}-1}{p_i-1} = \frac{\pi^2}{6}\frac{\sigma(n)}{n}.
\end{aligned}$$

Also

$$\begin{aligned}
\frac{n}{\varphi(n)} &= \prod_{p|n}\frac{1}{1-1/p} = \prod_{p|n}\left(1+\frac{1}{p}+\frac{1}{p^2}+\cdots\right) \\
&> \prod_{p_i|n}\left(1+p_i^{-1}+\cdots p_i^{-\alpha_i}\right) \\
&= \frac{1}{n}\prod_{p_i|n}\left(p_i^{\alpha_i}+\cdots p_i+1\right) = \frac{\sigma(n)}{n}.
\end{aligned}$$

(b) Using the above upper bound and changing order of summation as in Theorem 3.3,

$$\begin{aligned}\frac{6}{\pi^2}\sum_{n\le x}\frac{n}{\varphi(n)} &< \sum_{n\le x}\frac{\sigma(n)}{n} = \sum_{\substack{q,d\\ qd\le x}}\frac{d}{qd}\\ &= \sum_{d\le x}\sum_{q\le x/d}\frac{1}{q}\\ &= \sum_{d\le x}\left(\log x - \log d + C + O\left(\frac{d}{x}\right)\right)\\ &= (\log x + C)\lfloor x\rfloor - \sum_{d\le x}\log d + O\left(\sum_{d\le x}\frac{d}{x}\right).\end{aligned}$$

Applying Theorem 3.15 gives

$$\begin{aligned}\frac{6}{\pi^2}\sum_{n\le x}\frac{n}{\varphi(n)} &< (\log x + C)\lfloor x\rfloor - x\log x + O(x)\\ &= -\{x\}\log x + C\lfloor x\rfloor + O(x)\\ &= O(x).\end{aligned}$$

□

Exercise 3.10. If $x \ge 2$ prove that

$$\sum_{n\le x}\frac{1}{\varphi(n)} = O(\log x).$$

Proof. Using the same approach in the proof of Exercise 3.9 (b) and Theorem 3.2 (a)(b),

$$\begin{aligned}\frac{6}{\pi^2}\sum_{n\le x}\frac{1}{\varphi(n)} &< \sum_{n\le x}\frac{\sigma(n)}{n^2} = \sum_{d\le x}\frac{1}{d}\sum_{q\le x/d}\frac{1}{q^2}\\ &= \sum_{d\le x}\frac{1}{d}\left(\frac{(x/d)^{-1}}{-1} + \zeta(2) + O\Big((d/x)^2\Big)\right)\\ &= \sum_{d\le x}\left(-\frac{1}{x} + \frac{\zeta(2)}{d} + \frac{O(d)}{x^2}\right)\\ &= O(1) + O(\log x) + O(1)\\ &= O(\log x).\end{aligned}$$

□

Exercise 3.11. Let $\varphi_1(n) = n\sum_{d|n}|\mu(d)|/d$.
(a) Prove that φ_1 is multiplicative and that $\varphi_1(n) = n\prod_{p|n}(1+p^{-1})$.
(b) Prove that

$$\varphi_1(n) = \sum_{d^2|n}\mu(d)\sigma\left(\frac{n}{d^2}\right)$$

where the sum is over those divisors of n for which $d^2 \mid n$.
(c) Prove that

$$\sum_{n\le x}\varphi_1(n) = \sum_{d\le\sqrt{x}}\mu(d)S\left(\frac{x}{d^2}\right), \text{ where } S(x) = \sum_{k\le x}\sigma(k),$$

then use Theorem 3.4 to deduce that, for $x \ge 2$,

$$\sum_{n\le x}\varphi_1(n) = \frac{\zeta(2)}{2\zeta(4)}x^2 + O(x\log x).$$

As in Exercise 7, you may assume the result $\sum_{n=1}^{\infty}\mu(n)n^{-\alpha} = 1/\zeta(\alpha)$ for $\alpha > 1$.

Proof. Let $n = p_1^{\alpha_1}\cdots p_k^{\alpha_k}$.
(a) Notice $\varphi_1 = |\mu| * N$, and since both $|\mu|$ and N are multiplicative, so is φ_1. Therefore since

$$\varphi_1(p^\alpha) = p^\alpha(1+p^{-1}),$$

we have $\varphi_1(n) = n\prod_{p\mid n}(1+p^{-1})$.
(b) Since φ_1 is multiplicative, if we can show the right hand side is multiplicative then it suffices to show the claim holds for prime powers.

So suppose $(m,n) = 1$. If $q \mid m$ and $d \mid n$ then $(q,d) = 1$ and so

$$\left(\sum_{q^2\mid m}\mu(q)\sigma\left(\frac{m}{q^2}\right)\right)\left(\sum_{d^2\mid n}\mu(d)\sigma\left(\frac{n}{d^2}\right)\right) = \sum_{q^2\mid m}\sum_{d^2\mid n}\mu(qd)\sigma\left(\frac{mn}{q^2d^2}\right). \tag{2}$$

Next, observe $(d,m) = 1$ and $(q,n) = 1$, hence $q^2 \mid m$ and $d^2 \mid n$ if and only if $(qd)^2 \mid nm$. Additionally since $(qd)^2$ spans over all square divisors of mn, (2) is equal to

$$\sum_{t^2\mid mn}\mu(t)\sigma\left(\frac{mn}{t^2}\right),$$

which shows the sum is multiplicative.

Now let $F(n)$ be the right hand side of the claim. Then

$$\varphi_1(1) = 1 = F(1) \quad \text{and} \quad \varphi_1(p) = p+1 = \sigma(p) = F(p)$$

for any prime p. For $\alpha > 1$, $\varphi_1(p) = p^\alpha + p^{\alpha-1}$ and

$$F(p^\alpha) = \mu(1)\sigma(p^\alpha) + \mu(p)\sigma(p^{\alpha-2}) = p^\alpha + p^{\alpha-1},$$

since μ is zero for any higher prime power. Thus both sides agree on prime powers.
(c) From (b) we have

$$\sum_{n\le x}\varphi_1(n) = \sum_{n\le x}\sum_{d^2\mid n}\mu(d)\sigma\left(\frac{n}{d^2}\right).$$

Since $d^2 \mid n$ implies $n = qd^2$, we can extend the sum over all pairs q, d with $qd^2 \le x$. Thus

$$\begin{aligned}\sum_{n\le x}\varphi_1(n) &= \sum_{\substack{q,d\\ qd^2\le x}}\mu(d)\sigma(q)\\ &= \sum_{d^2\le x}\mu(d)\sum_{q\le x/d^2}\sigma(q)\\ &= \sum_{d^2\le x}\mu(d)S\left(\frac{x}{d^2}\right)\\ &= \sum_{d\le\sqrt{x}}\mu(d)S\left(\frac{x}{d^2}\right).\end{aligned}$$

Applying Theorem 3.4 and Theorem 3.2 (c), we have

$$\begin{aligned}\sum_{n\le x}\varphi_1(n) &= \sum_{d\le\sqrt{x}}\mu(d)S\left(\frac{x}{d^2}\right)\\ &= \sum_{d\le\sqrt{x}}\mu(d)\left(\frac{\zeta(2)}{2}\frac{x^2}{d^4}+O\Big(\frac{x}{d^2}\log\left(\frac{x}{d^2}\right)\Big)\right)\\ &= \frac{\zeta(2)x^2}{2}\sum_{d\le\sqrt{x}}\frac{\mu(d)}{d^4}+O\left(x\log x\sum_{d\le\sqrt{x}}\frac{\mu(d)}{d^2}\right)+O\left(x\sum_{d\le\sqrt{x}}\frac{\mu(d)\log d}{d^2}\right)\\ &= \frac{\zeta(2)x^2}{2\zeta(4)}+\frac{\zeta(2)x^2}{2}\sum_{d>\sqrt{x}}\frac{\mu(d)}{d^4}+O(x\log x)+O(x)\\ &= \frac{\zeta(2)x^2}{2\zeta(4)}+O\left(x^2\sum_{d>\sqrt{x}}\frac{1}{d^4}\right)+O(x\log x)\\ &= \frac{\zeta(2)x^2}{2\zeta(4)}+O\big(x^2\cdot x^{-3/2}\big)+O(x\log x)\\ &= \frac{\zeta(2)x^2}{2\zeta(4)}+O(x\log x).\end{aligned}$$

□

Exercise 3.12.(+) For real $s > 0$ and integer $k \ge 1$ find an asymptotic formula for the partial sums

$$\sum_{\substack{n\le x\\ (n,k)=1}}\frac{1}{n^s}$$

with an error term that tends to 0 as $x \to \infty$. Be sure to include the case $s = 1$.

Lemma 3.12. If f is an arithmetical function, then

$$\sum_{\substack{n\le x\\ (n,k)=1}}f(n)=\sum_{d\mid k}\mu(d)\sum_{q\le x/d}f(qd).$$

Proof of Lemma. We have

$$\begin{aligned}\sum_{\substack{n\le x\\(n,k)=1}} f(n) &= \sum_{n\le x} I((n,k))f(n)\\ &= \sum_{n\le x}\sum_{d\mid(n,k)} \mu(d)f(n)\\ &= \sum_{n\le x}\sum_{\substack{d\mid n\\ d\mid k}} \mu(d)f(n).\end{aligned}$$

For a fixed divisor d of k we must sum over all those n in the range $1 \le n \le x$ which are multiples of d. If we write $n = qd$, it's equivalent to sum over all q where $1 \le q \le x/d$. Therefore

$$\sum_{n\le x}\sum_{\substack{d\mid n\\ d\mid k}} \mu(d)f(n) = \sum_{d\mid k}\sum_{q\le x/d} \mu(d)f(qd).$$

□

Proof of Exercise. By Lemma 3.12

$$\sum_{\substack{n\le x\\(n,k)=1}} \frac{1}{n^s} = \sum_{d\mid k} \frac{\mu(d)}{d^s} \sum_{n\le x/d} \frac{1}{n^s}.$$

If $s = 1$ then by Theorem 3.2 (a),

$$\begin{aligned}\sum_{\substack{n\le x\\(n,k)=1}} \frac{1}{n} &= \sum_{d\mid k} \frac{\mu(d)}{d}\left(\log x - \log d + C + O\left(\frac{d}{x}\right)\right)\\ &= (\log x + C)\sum_{d\mid k}\frac{\mu(d)}{d} - \sum_{d\mid k}\frac{\mu(d)\log d}{d} + O\left(\frac{1}{x}\right)\\ &= \frac{\varphi(k)}{k}(\log x + C) + M_{k,1} + O\left(\frac{1}{x}\right),\end{aligned}$$

where $M_{k,1}$ is a constant dependent on k.

If $s \ne 1$ then by Theorem 3.2 (b),

$$\begin{aligned}\sum_{\substack{n\le x\\(n,k)=1}} \frac{1}{n^s} &= \sum_{d\mid k} \frac{\mu(d)}{d^s}\left(\frac{(x/d)^{1-s}}{1-s} + \zeta(s) + O\left(\frac{d^s}{x^s}\right)\right)\\ &= \frac{x^{1-s}}{1-s}\sum_{d\mid k}\frac{\mu(d)}{d} + \zeta(s)\sum_{d\mid k}\frac{\mu(d)}{d^s} + O\big(x^{-s}\big)\\ &= \frac{\varphi(k)}{k}\frac{x^{1-s}}{1-s} + \zeta(s)M_{k,s} + O\big(x^{-s}\big),\end{aligned}$$

where $M_{k,s}$ is a constant dependent on k and s. □

PROPERTIES OF THE GREATEST-INTEGER FUNCTION

For each real x the symbol $[x]$ denotes the greatest integer $\leq x$. Exercises 13 through 26 describe some properties of the greatest-integer function. In these exercises x and y denote real numbers, n denotes an integer.

Exercise 3.13. Prove each of the following statements:
(a) If $x = k + y$ where k is an integer and $0 \leq y < 1$, then $k = [x]$.
(b) $[x + n] = [x] + n$.
(c) $[-x] = \begin{cases} -[x] & \text{if } x = [x], \\ -[x] - 1 & \text{if } x \neq [x]. \end{cases}$
(d) $[x/n] = [[x]/n]$ if $n \geq 1$.

Proof.
(a) Since $0 \leq y < 1$, it's clear $k \leq x < k+1$. Thus k is the greatest integer $\leq x$, i.e. $k = \lfloor x \rfloor$.
(b) Let $k = \lfloor x \rfloor$, $y = x - k$, and $z = x + n = (k + n) + y$. By (a) $\lfloor z \rfloor = k + n$, and so

$$\lfloor x + n \rfloor = \lfloor z \rfloor = k + n = \lfloor x \rfloor + n.$$

(c) Suppose $x = \lfloor x \rfloor$, then since $\lfloor x \rfloor$ is an integer, so is x and hence so is $-x$. From here it's easy to see

$$\lfloor -x \rfloor = -x = -\lfloor x \rfloor.$$

Now suppose $x \neq \lfloor x \rfloor$. Let $k = \lfloor x \rfloor$ and $y = x - k$, where $0 < y < 1$. Then since $0 < 1 - y < 1$, by (a) we have

$$\lfloor -x \rfloor = \lfloor -k - y \rfloor = \lfloor (-k - 1) + (1 - y) \rfloor = -k - 1 = -\lfloor x \rfloor - 1.$$

(d) Letting $\lfloor x \rfloor = qn + r$ for an integer $0 \leq r < n$ implies $x = qn + (r + y)$ for some $0 \leq y < 1$. Since $0 \leq (r + y)/n < 1$, by (a)

$$\lfloor x/n \rfloor = \lfloor q + (r + y)/n \rfloor = q.$$

Also since $0 \leq r/n < 1$, again by (a)

$$\lfloor \lfloor x \rfloor / n \rfloor = \lfloor q + r/n \rfloor = q.$$

□

Exercise 3.14. If $0 < y < 1$, what are the possible values of $[x] - [x - y]$?

Solution. Let $\{x\} = x - \lfloor x \rfloor$ and $\{x - y\} = (x - y) - \lfloor x - y \rfloor$, where $0 \leq \{x\}, \{x - y\} < 1$. Then $\lfloor x \rfloor - \lfloor x - y \rfloor = y + \{x - y\} - \{x\}$. Adding the inequalities

$$0 < y < 1, \quad 0 \leq \{x - y\} < 1, \quad -1 < -\{x\} \leq 0$$

we see $-1 < \lfloor x \rfloor - \lfloor x - y \rfloor < 2$ and thus $0 \leq \lfloor x \rfloor - \lfloor x - y \rfloor \leq 1$.

If $x = 3/4$, $y = 1/2$ then $\lfloor x \rfloor - \lfloor x - y \rfloor = 0$. If $x = 1$, $y = 1/2$ then $\lfloor x \rfloor - \lfloor x - y \rfloor = 1$. Thus all possible values of $\lfloor x \rfloor - \lfloor x - y \rfloor$ are 0 or 1.

Exercise 3.15. The number $\{x\} = x - [x]$ is called the *fractional part* of x. It satisfies the inequalities $0 \leq \{x\} < 1$, with $\{x\} = 0$ if, and only if, x is an integer. What are the possible values of $\{x\} + \{-x\}$?

Solution. Assume the result from Exercise 3.13 (c). If $x = \lfloor x \rfloor$, then

$$\begin{aligned} \{x\} + \{-x\} &= x - [x] + (-x) - [-x] \\ &= x - [x] - x + [x] = 0. \end{aligned}$$

If $x \neq \lfloor x \rfloor$, then

$$\begin{aligned} \{x\} + \{-x\} &= x - [x] + (-x) - [-x] \\ &= x - [x] - x + [x] + 1 = 1. \end{aligned}$$

Exercise 3.16.
(a) Prove that $[2x] - 2[x]$ is either 0 or 1.
(b) Prove that $[2x] + [2y] \geq [x] + [y] + [x + y]$.

Proof.
(a) We have

$$[2x] - 2[x] = 2x - \{2x\} - 2(x - \{x\}) = 2\{x\} - \{2x\}.$$

Adding $0 \leq 2\{x\} < 2$ and $-1 < -\{2x\} \leq 0$ gives $-1 < [2x] - 2[x] < 2$. Thus

$$0 \leq [2x] - 2[x] \leq 1.$$

(b) Suppose $x = m + a$ and $y = n + b$ where $0 \leq a, b < 1$. By symmetry we have four cases to consider:

1. $a, b < 1/2$
2. $a < 1/2, b \geq 1/2,$ and $a + b < 1$
3. $a < 1/2, b \geq 1/2,$ and $a + b \geq 1$
4. $a, b \geq 1/2$

1. $\lfloor 2x \rfloor + \lfloor 2y \rfloor = 2m + 2n = m + n + (m + n) = \lfloor x \rfloor + \lfloor y \rfloor + \lfloor x + y \rfloor$
2. $\lfloor 2x \rfloor + \lfloor 2y \rfloor = 2m + (2n + 1) > m + n + (m + n) = \lfloor x \rfloor + \lfloor y \rfloor + \lfloor x + y \rfloor$
3. $\lfloor 2x \rfloor + \lfloor 2y \rfloor = 2m + (2n + 1) = m + n + (m + n + 1) = \lfloor x \rfloor + \lfloor y \rfloor + \lfloor x + y \rfloor$
4. $\lfloor 2x \rfloor + \lfloor 2y \rfloor = (2m + 1) + (2n + 1) > m + n + (m + n + 1) = \lfloor x \rfloor + \lfloor y \rfloor + \lfloor x + y \rfloor$

□

Exercise 3.17. Prove that $[x] + \left[x + \frac{1}{2}\right] = [2x]$ and, more generally,

$$\sum_{k=0}^{n-1} \left[x + \frac{k}{n}\right] = [nx].$$

Proof. Let i be the largest integer such that $\{x\} + \frac{i}{n} < 1$. Then $0 \leq i < n$ and

$$\begin{aligned}
\sum_{k=0}^{n-1} \left\lfloor x + \frac{k}{n} \right\rfloor &= \sum_{k=0}^{i} \left\lfloor x + \frac{k}{n} \right\rfloor + \sum_{k=i+1}^{n-1} \left\lfloor x + \frac{k}{n} \right\rfloor \\
&= \sum_{k=0}^{i} \left\lfloor \lfloor x \rfloor + \left(\{x\} + \frac{k}{n} \right) \right\rfloor + \sum_{k=i+1}^{n-1} \left\lfloor (\lfloor x \rfloor + 1) + \left(\{x\} + \frac{k}{n} - 1 \right) \right\rfloor \\
&= (i+1) \lfloor x \rfloor + (n-i-1)(\lfloor x \rfloor + 1) \\
&= n \lfloor x \rfloor + n - i - 1 \\
&= nx - n \{x\} + n - i - 1 \\
&= \lfloor nx \rfloor + \{nx\} - n \{x\} + n - i - 1.
\end{aligned}$$

Since $\{x\} + \frac{i}{n} < 1 \leq \{x\} + \frac{i+1}{n}$, then $-1 < -n\{x\} + n - i - 1 \leq 0$. Adding this to $0 \leq \{nx\} < 1$, we have

$$-1 < \{nx\} - n\{x\} + n - i - 1 < 1.$$

However it is evident from the above chain of equalities that $\{nx\} - n\{x\} + n - i - 1$ is an integer, and so it must equal 0. The result then follows. □

Exercise 3.18. Let $f(x) = x - [x] - \frac{1}{2}$. Prove that

$$\sum_{k=0}^{n-1} f\left(x + \frac{k}{n} \right) = f(nx)$$

and deduce that

$$\left| \sum_{n=1}^{m} f\left(2^n x + \frac{1}{2} \right) \right| \leq 1 \quad \text{for all } m \geq 1 \text{ and all real } x.$$

Proof. Using Exercise 3.17 we have

$$\begin{aligned}
\sum_{k=0}^{n-1} f\left(x + \frac{k}{n} \right) &= \sum_{k=0}^{n-1} \left(x + \frac{k}{n} \right) - \sum_{k=0}^{n-1} \left\lfloor x + \frac{k}{n} \right\rfloor - \sum_{k=0}^{n-1} \frac{1}{2} \\
&= nx + \frac{n-1}{2} - \lfloor nx \rfloor - \frac{n}{2} \\
&= nx - \lfloor nx \rfloor - \frac{1}{2} \\
&= f(nx).
\end{aligned}$$

This means $f\left(2^n x\right) + f\left(2^n x + \frac{1}{2}\right) = f\left(2(2^n x)\right)$ and so

$$\begin{aligned}
\sum_{n=1}^{m} f\left(2^n x + \frac{1}{2} \right) &= \sum_{n=1}^{m} \left(f\left(2^{n+1} x\right) - f\left(2^n x\right) \right) \\
&= f\left(2^{m+1} x\right) - f(2x) \\
&= 2^{m+1} x - \left\lfloor 2^{m+1} x \right\rfloor - \frac{1}{2} - 2x + \lfloor 2x \rfloor + \frac{1}{2} \\
&= \left\{ 2^{m+1} x \right\} - \{2x\}.
\end{aligned}$$

Adding the inequalities $0 \le \{2^{m+1}x\} < 1$ and $-1 < -\{2x\} \le 0$ we obtain

$$\left| \sum_{n=1}^{m} f\left(2^n x + \frac{1}{2}\right) \right| \le 1.$$

□

Exercise 3.19.(++) Given positive odd integers h and k, $(h,k) = 1$, let $a = (k-1)/2, b = (h-1)/2$.
(a) Prove that $\sum_{r=1}^{a} [hr/k] + \sum_{r=1}^{b} [kr/h] = ab$. [*Hint*: Lattice points.]
(b) Obtain a corresponding result if $(h,k) = d$.

Proof.
(a) Consider the line segment s in $\mathbb{R}^2$ with endpoints $(0,0)$ and (h,k). Since $(h,k) = 1$, by Theorem 3.8, s does not intersect any lattice points other then its endpoints.

Define the rectangle R to be the rectangle with corners at $(1,1)$ and (h,k). Counting, we see the number of lattice points with even entries inside R is ab. Now the first sum in question counts the number of lattice points with even entries in R on or above s, whereas the second sum counts the number of lattice points with even entries on or below the line. Since there are no lattice points on s, these sums add to ab.

(b) Define s and R as in (a) and let $d = (h,k)$. Looking at the proof of Theorem 3.8, we see s will cross a lattice point inside R precisely d times. Of these, $(d-1)/2$ will have even entries and so the technique in (a) would count these twice. Thus

$$\sum_{r=1}^{a} \left\lfloor \frac{hr}{k} \right\rfloor + \sum_{r=1}^{b} \left\lfloor \frac{kr}{h} \right\rfloor = ab + \frac{d-1}{2}.$$

□

Exercise 3.20. If n is a positive integer prove that $\left[\sqrt{n} + \sqrt{n+1}\,\right] = \left[\sqrt{4n+2}\,\right]$.

Proof. Note

$$\left(\sqrt{n} + \sqrt{n+1}\right)^2 = 2n + 2\sqrt{n^2+n} + 1,$$

so since $(n+1/2)^2 < n^2 + n \le (n+1)^2$ we have

$$4n + 2 < \left(\sqrt{n} + \sqrt{n+1}\right)^2 \le 4n + 3.$$

Moreover $\sqrt{4n+3} - \sqrt{4n+2} < 1$, which implies

$$\left\lfloor \sqrt{4n+2}\,\right\rfloor < \sqrt{n} + \sqrt{n+1} < \left\lfloor \sqrt{4n+2}\,\right\rfloor + 1.$$

We conclude $\left\lfloor \sqrt{n} + \sqrt{n+1}\,\right\rfloor = \left\lfloor \sqrt{4n+2}\,\right\rfloor$. □

Exercise 3.21. Determine all positive integers n such that $[\sqrt{n}\,]$ divides n.

Solution. Let k^2 be the greatest square $\leq n$ and $a = n - k^2$. Then $k^2 \leq n < (k+1)^2$ and so $0 \leq a < 2k+1$ and $k \leq \sqrt{n} < k+1$, which means $k = \lfloor \sqrt{n} \rfloor$. Now

$$\begin{aligned} \lfloor \sqrt{n} \rfloor \mid n &\iff k \mid n \\ &\iff k \mid (n - k^2) \\ &\iff k \mid a \\ &\iff a = 0 \text{ or } k \text{ or } 2k. \end{aligned}$$

Thus $\lfloor \sqrt{n} \rfloor$ divides n if and only if $n = k^2$, $n = k^2 + k$, or $n = k^2 + 2k$. Solving for k, then $\lfloor \sqrt{n} \rfloor$ divides n if and only if one of n, $4n+1$, or $4n+4$ is a square.

Exercise 3.22. If n is a positive integer, prove that

$$\left\lfloor \frac{8n+13}{25} \right\rfloor - \left\lfloor \frac{n - 12 - \left\lfloor \frac{n-17}{25} \right\rfloor}{3} \right\rfloor$$

is independent of n.

Proof. Let $f(n)$ be the expression in question. We can see $f(n)$ has period ≤ 25 by applying Exercise 3.13 (b):

$$\begin{aligned} f(n+25) &= \left\lfloor \frac{8(n+25)+13}{25} \right\rfloor - \left\lfloor \frac{(n+25) - 12 - \left\lfloor \frac{(n+25)-17}{25} \right\rfloor}{3} \right\rfloor \\ &= \left\lfloor \frac{8n+13}{25} + 8 \right\rfloor - \left\lfloor \frac{n+25-12 - \left\lfloor \frac{n-17}{25} + 1 \right\rfloor}{3} \right\rfloor \\ &= \left\lfloor \frac{8n+13}{25} + 8 \right\rfloor - \left\lfloor \frac{n+25-12 - \left\lfloor \frac{n-17}{25} \right\rfloor - 1}{3} \right\rfloor \\ &= \left\lfloor \frac{8n+13}{25} + 8 \right\rfloor - \left\lfloor \frac{n-12 - \left\lfloor \frac{n-17}{25} \right\rfloor}{3} + 8 \right\rfloor \\ &= \left\lfloor \frac{8n+13}{25} \right\rfloor + 8 - \left\lfloor \frac{n-12 - \left\lfloor \frac{n-17}{25} \right\rfloor}{3} \right\rfloor - 8 \\ &= f(n). \end{aligned}$$

Testing $n = 1, 2, \ldots, 25$ in Mathematica, we see $f(n)$ is constant over the integers.

```
In[1]:= f[n_] := Floor[(8n+13)/25]-Floor[(n-12-Floor[(n-17)/25])/3]

In[2]:= SameQ @@ f[Range[25]]
Out[2]= True
```

□

Exercise 3.23. Prove that

$$\sum_{n\leq x} \lambda(n) \left[\frac{x}{n}\right] = \left[\sqrt{x}\,\right].$$

Proof. Let $s(n)$ be the square indicator function, then by Theorem 2.19 $s(n) = \sum_{d|n} \lambda(d)$. We then have

$$\begin{aligned}\left\lfloor \sqrt{x} \right\rfloor &= \#\text{ of squares} \leq x \\ &= \sum_{n\leq x} s(n) \\ &= \sum_{n\leq x} \sum_{d|n} \lambda(d).\end{aligned}$$

Applying Theorem 3.11 shows

$$\sum_{n\leq x} \sum_{d|n} \lambda(d) = \sum_{n\leq x} \lambda(n) \left\lfloor \frac{x}{n} \right\rfloor.$$

□

Exercise 3.24. Prove that

$$\sum_{n\leq x} \left[\sqrt{\frac{x}{n}}\,\right] = \sum_{n\leq \sqrt{x}} \left[\frac{x}{n^2}\right].$$

Proof. Let $s(n)$ be the square indicator function and $S(x) = \sum_{n\leq x} s(n)$. Then

$$\left\lfloor \sqrt{x} \right\rfloor = \#\text{ of squares} \leq x = S(x).$$

By Theorem 3.11,

$$\sum_{n\leq x} \left\lfloor \sqrt{\frac{x}{n}} \right\rfloor = \sum_{n\leq x} S\left(\frac{x}{n}\right) = \sum_{n\leq x} s(n) \left\lfloor \frac{x}{n} \right\rfloor.$$

Now $s(n) = 1$ if $n = m^2$ and is 0 otherwise, thus

$$\sum_{n\leq x} s(n) \left\lfloor \frac{x}{n} \right\rfloor = \sum_{\substack{m^2\leq x \\ m>0}} \left\lfloor \frac{x}{m^2} \right\rfloor = \sum_{m\leq \sqrt{x}} \left\lfloor \frac{x}{m^2} \right\rfloor.$$

□

Exercise 3.25. Prove that

$$\sum_{k=1}^{n} \left[\frac{k}{2}\right] = \left[\frac{n^2}{4}\right]$$

and that

$$\sum_{k=1}^{n} \left[\frac{k}{3}\right] = \left[\frac{n(n-1)}{6}\right].$$

Proof. For the first sum, apply Exercise 3.26 with $a = 2$. Also by Exercise 3.26

$$\sum_{k=1}^{n} \left\lfloor \frac{k}{3} \right\rfloor = \left\lfloor \frac{n(n-1)}{6} + \frac{1}{24} \right\rfloor,$$

but the fractional part of $n(n-1)/6$ is either 0 or $1/3$ and so $1/24$ can be ignored. □

Exercise 3.26.(+) If $a = 1, 2, \ldots, 7$ prove that there exists and integer b (depending on a) such that

$$\sum_{k=1}^{n} \left\lfloor \frac{k}{a} \right\rfloor = \left\lfloor \frac{(2n+b)^2}{8a} \right\rfloor.$$

Proof. Let $n = qa + r$ where $0 \le r < a$. Then for any $0 < k < qa$, we have $k = ma + r'$ for some $m < q$ and $0 \le r' < a$. Thus

$$\left\lfloor \frac{k}{a} \right\rfloor = \left\lfloor m + \frac{r'}{a} \right\rfloor = m.$$

Also if $qa \le k \le qa + r$, then $\left\lfloor \frac{k}{a} \right\rfloor = q$. So summing over all quotients and remainders,

$$\begin{aligned}
\sum_{k=1}^{n} \left\lfloor \frac{k}{a} \right\rfloor &= \sum_{m=0}^{q-1} \sum_{i=0}^{a-1} \left\lfloor \frac{ma+i}{a} \right\rfloor + \sum_{i=0}^{r} \left\lfloor \frac{qa+i}{a} \right\rfloor \\
&= \sum_{m=0}^{q-1} \sum_{i=0}^{a-1} m + \sum_{i=0}^{r} q \\
&= \frac{a(q-1)q}{2} + q(r+1) \\
&= \frac{aq^2 - aq + 2qr + 2q}{2} \\
&= \frac{4a^2q^2 - 4a^2q + 8aqr + 8aq}{8a}. \qquad (3)
\end{aligned}$$

We now look for values of b such that $(2n+b)^2$ minus the numerator of (3) is positive for any q and r. To do this we see when this difference factored into a square in Mathematica.

```
In[3]:= squarePolyQ[poly_] :=
  MatchQ[FactorList[poly], {({_?Positive, _} | {_, _?EvenQ})..}]

In[4]:= Column@Reap[Do[
  If[squarePolyQ[(2q a+2r+b)^2-(4a^2q^2-4a^2q+8a q r+8a q)],
    Sow[Row[{"a = ", a, ", b = ", b}]]
  ],
  {a, 1, 7}, {b, -10, 10}
]][[-1,1]]
```

```
Out[4]= a = 1, b = 1
        a = 2, b = 0
        a = 3, b = -1
        a = 4, b = -2
        a = 5, b = -3
        a = 6, b = -4
        a = 7, b = -5
```

So choosing $b = 2 - a$ is our candidate. Mathematica already found

$$0 \leq 4a^2q^2 - 4a^2q + 8aqr + 8aq - (2n + b)^2,$$

but we need to show this difference is smaller than $8a$. In doing so,

$$0 \leq \frac{(2n + b)^2}{8a} - \frac{4a^2q^2 - 4a^2q + 8aqr + 8aq}{8a} < 1,$$

or rearranging terms,

$$\frac{4a^2q^2 - 4a^2q + 8aqr + 8aq}{8a} \leq \frac{(2n + b)^2}{8a} < \frac{4a^2q^2 - 4a^2q + 8aqr + 8aq}{8a} + 1,$$

forcing $(2n + b)^2/(8a)$ to have the desired floor.

Since $(a - 2r - 2)^2$ is maximized at $r = a - 1$ for $0 \leq r < a - 1$,

$$\begin{aligned}(2n + 2 - a)^2 - (4a^2q^2 - 4a^2q + 8aqr + 8aq) &= (a - 2r - 2)^2 \\ &\leq (a - 2(a - 1) - 2)^2 \\ &= a^2 \\ &= a \cdot a < 8a.\end{aligned}$$

So since their difference is small enough, we see choosing $b = 2 - a$ gives us the result. □

Chapter 4
Some Elementary Theorems on the Distribution of Prime Numbers

Exercise 4.1. Let $S = \{1, 5, 9, 13, 17, \ldots\}$ denote the set of all positive integers of the form $4n+1$. An element p of S is called an S-prime if $p > 1$ and if the only positive divisors of p, among the elements of S, are 1 and p. (For example, 49 is an S-prime.) An element $n > 1$ in S which is not an S-prime is called an S-composite.
(a) Prove that every S-composite is a product of S-primes.
(b) Find the smallest S-composite that can be expressed in more than one way as a product of S-primes.
This example shows that unique factorization does not hold in S.

Proof.
(a) By definition, if n is S-composite then there is a $d \in S$ such that $1 < d < n$ and $d \mid n$. Let $n = kd$ and since $n \equiv d \equiv 1 \bmod 4$, we see $k \equiv 1 \bmod 4$, i.e. $k \in S$. Applying this process on k, d, and so on, it will eventually terminate since there are only finitely many numbers between 1 and n. This shows n can be written as a product of S-primes.

(b) If $x \equiv y \equiv 3 \bmod 4$ then $xy \equiv 1 \bmod 4$. So the idea is to find the three smallest primes congruent to 3 mod 4 and taking their products. These primes are 3 and 7. To ensure this number is in S we need an even number of factors congruent to 3 mod 4, so we take $3^2 = 9$ instead of 3 and $7^2 = 49$ instead of 7. Hence the smallest S-composite that can be expressed in more than one way as a product of S-primes is

$$441 = 9 \cdot 49 = 21 \cdot 21.$$

□

Exercise 4.2. Consider the following finite set of integers:

$$T = \{1, 7, 11, 13, 17, 19, 23, 29\}.$$

(a) For each prime p in the interval $30 < p < 100$ determine a pair of integers m, n, where $m \geq 0$ and $n \in T$, such that $p = 30m + n$.
(b) Prove the following statement or exhibit a counter example:
Every prime $p > 5$ can be expressed in the form $30m + n$, where $m \geq 0$ and $n \in T$.

Proof.
(a) We show this in Mathematica.

```
In[1]:= With[{primes = Prime[Range[PrimePi[31], PrimePi[100]]]},
  apostolCh4Num2Format[QuotientRemainder[#, 30]& /@ primes]
]

Out[1]=
31=30*1+1      37=30*1+7      41=30*1+11     43=30*1+13     47=30*1+17
53=30*1+23     59=30*1+29     61=30*2+1      67=30*2+7      71=30*2+11
73=30*2+13     79=30*2+19     83=30*2+23     89=30*2+29     97=30*3+7
```

(b) Suppose $6 < p < 30$, then observe $p \in T$ and $p = 30 \cdot 0 + p$. Now assume $p > 30$ and let $p = 30n + r$ where $n > 0$ and $0 \leq r < 30$. Since p is prime and $n > 0$, we require $(30, r) = 1$. Observing $T = \{m \mid 0 \leq m < 30,\ (30, m) = 1\}$, we must have $r \in T$, and so the claim holds for all $p > 5$. □

Exercise 4.3. Let $f(x) = x^2 + x + 41$. Find the smallest integer $x \geq 0$ for which $f(x)$ is composite.

Proof. We show $x = 40$ using Mathematica.

```
In[2]:= f[x_] := x^2 + x + 41

In[3]:= VectorQ[f[Range[0, 39]], PrimeQ] && !PrimeQ[f[40]]
Out[3]= True
```

□

Exercise 4.4. Let $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ be a polynomial with integer coefficients, where $a_n > 0$ and $n \geq 1$. Prove that $f(x)$ is composite for infinitely many integers x.

Proof. Consider three cases:

- Suppose $a_0 = 0$. Then $f(x) = x(a_1 + \cdots + a_n x^{n-1})$ and so $x \mid f(x)$ which means $f(x)$ is composite whenever x is composite.
- Suppose $|a_0| \neq 1$. Then for any integer m,

  $$f(ma_0) = a_0 \cdot (1 + ma_1 + \cdots + ma_n (ma_0)^{n-1}),$$

  where the right factor is larger than 1 in absolute value for large enough m. From here we see $f(x)$ is composite infinitely often.
- Suppose $|a_0| = 1$. Pick an integer k such that $|f(k)| \neq 1$ and let $g(y) = f(y + k)$. Expanding gives a polynomial in terms of y with constant coefficient

  $$a_0 + a_1 k + \cdots + a_n k^n = f(k).$$

  Applying one of the above cases on g shows it is composite infinitely often, and since f is g shifted k units horizontally, it must also be composite infinitely often. □

Exercise 4.5. Prove that for every $n > 1$ there exist n consecutive composite numbers.

Proof. Define $C_n = \{(n+1)! + k \mid 2 \leq k \leq n+1\}$. Notice $|C_n| = n$ and each element is composite since $k \mid (n+1)! + k$. □

Exercise 4.6. Prove that there do not exist polynomials P and Q such that

$$\pi(x) = \frac{P(x)}{Q(x)} \text{ for } x = 1, 2, 3, \ldots$$

Proof. Suppose $\deg(P) = m$ and $\deg(Q) = n$, then $\frac{P(x)}{Q(x)} = \theta(x^{m-n})$. Theorem 4.6 implies $\pi(x)$ cannot be asymptotic to $\frac{P(x)}{Q(x)}$ as

$$\pi(x) = \theta\left(\frac{x}{\log x}\right) \neq \theta(x^{m-n}).$$

□

Exercise 4.7.(+) Let $a_1 < a_2 < \cdots < a_n \leq x$ be a set of positive integers such that no a_i divides the product of the others. Prove that $n \leq \pi(x)$.

Proof. Fix x and denote the hypothesis of the problem by H_x. Suppose $k = \pi(x)$ and

$$\begin{aligned} a_1 &= p_1^{\alpha_{11}} \cdot p_2^{\alpha_{12}} \cdots p_k^{\alpha_{1k}} \\ a_2 &= p_1^{\alpha_{21}} \cdot p_2^{\alpha_{22}} \cdots p_k^{\alpha_{2k}} \\ &\vdots \\ a_n &= p_1^{\alpha_{n1}} \cdot p_2^{\alpha_{n2}} \cdots p_k^{\alpha_{nk}}. \end{aligned}$$

Observe for each a_i that there must be a j such that $\alpha_{ij} > \sum_{l \neq j} \alpha_{il}$, otherwise $a_i \mid \prod_{l \neq i} a_l$. without loss of generality assume $\alpha_{nk} > \sum_{l \neq k} \alpha_{nl}$. If $a_i' = a_i / p_k^{\alpha_{ik}}$, then by this observation, $\{a_i'\}_{i=1}^{n-1}$ still satisfies H_x. Each time we apply this process, the new sequence will still satisfy H_x.

Assuming $n > k$ then applying the above process $k-1$ times would yield a sequence of of the form $\{p^{a_i}\}_{i=1}^{n-k+1}$ for some prime p. This clearly does not satisfy H_x since $n-k+1 > 1$ so we conclude $n \leq k$. □

Exercise 4.8. Calculate the highest power of 10 that divides 1000!.

Proof. Note we can reduce this to finding the highest power of 5 that divides 1000! since 2 appears more in factorial than 5. From Theorem 3.14 we have $\log 1000! = \sum_{p \leq 1000} \alpha(p) \log p$, where $\alpha(p)$ is the highest power of p to divide 1000! and is given by

$$\alpha(p) = \sum_{m=1}^{\left\lfloor \frac{\log 1000}{\log p} \right\rfloor} \left\lfloor \frac{1000}{p^m} \right\rfloor.$$

So

$$\begin{aligned}\alpha(5) &= \sum_{m=1}^{4} \left\lfloor \frac{1000}{5^m} \right\rfloor \\ &= \left\lfloor \frac{1000}{5} \right\rfloor + \left\lfloor \frac{1000}{25} \right\rfloor + \left\lfloor \frac{1000}{125} \right\rfloor + \left\lfloor \frac{1000}{625} \right\rfloor \\ &= 200 + 40 + 8 + 1 \\ &= 249.\end{aligned}$$

□

Exercise 4.9. Given an arithmetic progression of integers

$$h, h+k, h+2k, \ldots, h+nk, \ldots,$$

where $0 < k < 2000$. If $h + nk$ is prime for $n = t, t+1, \ldots, t+r$ prove that $r \leq 9$. In other words, at most 10 consecutive terms of this progression can be primes.

Proof. If $h + tk \leq 11$, direct verification shows the claim so assume $h + tk > 11$ and $r \geq 10$. Then for each prime $p \leq 11$ we have $p \nmid h + nk$ for $n = t, t+1, \ldots, t+r$. Now suppose $p \nmid k$ for some $p \leq 11$, which means $l := k^{-1} \bmod p$ exists. Choosing $i = -(h+tk)l \bmod p$ gives $0 \leq i \leq 10$ and

$$h + (t+i)k \equiv (h+tk) - (h+tk)lk \equiv (h+tk) - (h+tk) \equiv 0 \mod p,$$

a contradiction. Thus $p \mid k$ for all $p \leq 11$, which implies $k \geq 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 = 2310$, another contradiction, and so $r \leq 9$ since this only forces primes ≤ 10 to divide k. □

Exercise 4.10. Let s_n denote the nth partial sum of the series

$$\sum_{r=1}^{\infty} \frac{1}{r(r+1)}.$$

Prove that for every integer $k > 1$ there exist integers m and n such that $s_m - s_n = 1/k$.

Proof. Notice $\frac{1}{r(r+1)} = \frac{1}{r} - \frac{1}{r+1}$ and so $s_n = 1 - \frac{1}{n+1}$. If $k > 1$ then $k^2 - k - 1 > 0$, $k - 2 \geq 0$, and

$$s_{k^2-k-1} - s_{k-2} = \frac{1}{k-1} - \frac{1}{k^2-k} = \frac{1}{k}.$$

□

Exercise 4.11.(+) Let s_n denote the sum of the first n primes. Prove that for each n there exists an integer whose square lies between s_n and s_{n+1}.

Lemma 4.11. If $n > 3$, then

$$s_n < \left(\frac{p_{n+1} - 1}{2} \right)^2.$$

Proof of Lemma. Since s_n is a sum of primes, we can bound it by summing over 2, 3, and all odd numbers $\leq p_n$ not divisible by 3:

$$\begin{aligned} s_n &\leq 2+3+\sum_{k=1}^{\lfloor (p_{n+1}+1)/6 \rfloor}(6k-1)+\sum_{k=1}^{\lfloor (p_{n+1}+1)/6 \rfloor}(6k+1) \\ &= 5+6\left\lfloor \frac{p_{n+1}+1}{6} \right\rfloor + 6\left\lfloor \frac{p_{n+1}+1}{6} \right\rfloor^2 \\ &\leq 5+p_{n+1}+1+6\left(\frac{p_{n+1}+1}{6}\right)^2 \\ &= \frac{p_{n+1}^2+8p_{n+1}+37}{6}. \end{aligned}$$

Now for any $x \geq 25$, $(x^2+8x+37)/6 < (x-1)^2/4$ and so verifying by hand for $n = 4, \ldots, 9$ proves the claim. □

Proof of Exercise. Assume $n > 3$ and let $k = \lfloor \sqrt{s_n} \rfloor$. The goal is to show $2k+1 \leq p_{n+1}$, which would place $(k+1)^2$ between s_n and s_{n+1}. Now isolating p_{n+1} in the proof of Lemma 4.11, we have $2\sqrt{s_n}+1 \leq p_{n+1}$, and so

$$2k+1 \leq 2\sqrt{s_n}+1 < p_{n+1}.$$

Inductively (with base cases $n = 1$, 2, 3), assume there is a square between s_n and s_{n+1}. The above inequality then gives us the result. Verifying the base cases, $s_n = 2$, 5, 10, 17 and the squares in between are 4, 9, 16. Thus there is always a square between s_n and s_{n+1}. □

Remark. One should note that for any $m > 0$, eventually m squares will always lie between s_n and s_{n+1}. This is done by showing

$$s_n < \left(\frac{p_{n+1}-m}{2m}\right)^2$$

eventually holds, which can be proven through partial summation on s_n or a applying a tighter sieve (dependent on m) as in Lemma 4.11. The advantage to the sieve is it gives information as to when the inequality becomes starts to hold.

Prove each of the statements in Exercises 12 through 16. In this group of exercises you may use the prime number theorem.

Exercise 4.12. If $a > 0$ and $b > 0$, then $\pi(ax)/\pi(bx) \sim a/b$ as $x \to \infty$.

Proof. Assuming the prime number theorem we have

$$\frac{\pi(ax)}{\pi(bx)} \sim \frac{ax\log(bx)}{bx\log(ax)} \sim \frac{a}{b}.$$

□

Exercise 4.13. If $0 < a < b$, there exists an x_0 such that $\pi(ax) < \pi(bx)$ if $x \geq x_0$.

Proof. Notice for any $c > 0$ that

$$\lim_{x\to\infty} \frac{\log x}{\log cx} = 1$$

and so

$$\frac{1}{\log cx} = \frac{1}{\log x} + o(1)\,.$$

So assuming the prime number theorem we have

$$\pi(bx) - \pi(ax) = (b-a)\frac{x}{\log x} + o\left(\frac{x}{\log x}\right) = (b - a + o(1))\,\frac{x}{\log x}.$$

Now, choose x_0 such that for all $x \geq x_0$, the $o(1)$ term is less than $b - a$ in absolute value. This gives $\pi(ax) < \pi(bx)$ for all $x \geq x_0$. □

Exercise 4.14. If $0 < a < b$, there exists an x_0 such that for $x \geq x_0$ there is at least one prime between ax and bx.

Proof. Given $0 < a < b$, by Exercise 4.13 there is an x_0 such that $\pi(ax) < \pi(bx)$ for all $x \geq x_0$. Since π is an integer valued function, then $\pi(bx) - \pi(ax) \geq 1$ for all $x \geq x_0$, implying there is at least one prime between ax and bx. □

Exercise 4.15. Every interval $[a, b]$ with $0 < a < b$, contains a rational number of the form p/q, where p and q are primes.

Proof. Assume the result from Exercise 4.13 and pick x_0 such that $\pi(ax) < \pi(bx)$ for all $x \geq x_0$. Let q be any prime larger than x_0. Choose a prime p to lie in the interval $[aq, bq]$, which gives $p/q \in [a, b]$. □

Exercise 4.16.
(a) Given a positive integer n there exists a positive integer k and a prime p such that $10^k n < p < 10^k(n + 1)$.
(b) Given m integers $a_1, \ldots, a_m$ such that $0 \leq a_i \leq 9$ for $i = 1, 2, \ldots, m$, there exists a prime p whose decimal expansion has $a_1, \ldots, a_m$ for its first m digits.

Proof.
(a) By Exercise 4.13 there is an x_0 such that $\pi(nx) < \pi((n + 1)x)$ for all $x \geq x_0$. Let $k = \lceil \log_{10} x_0 \rceil$, then $10^k \geq x_0$ and so there is a prime p such that $10^k n < p < 10^k(n + 1)$.
(b) Let $n = \sum_{i=1}^{m} a_i 10^{m-i}$ and choose k and p as in (a). Then p will have the desired first m digits. □

Exercise 4.17. Given an integer $n > 1$ with two factorizations $n = \prod_{i=1}^{r} p_i$ and $n = \prod_{i=1}^{t} q_i$, where the p_i are primes (not necessarily distinct) and the q_i are arbitrary integers > 1. Let α be a nonnegative real number.
(a) If $\alpha \geq 1$ prove that

$$\sum_{i=1}^{r} p_i^{\alpha} \leq \sum_{i=1}^{t} q_i^{\alpha}.$$

(b) Obtain a corresponding inequality relating these sums if $0 \leq \alpha < 1$.

Proof.
(a) Suppose $q_i = p_{i_1} \cdots p_{i_j}$. It suffices to show

$$\sum_{k=1}^{j} p_{i_k}^{\alpha} \leq q_i = \prod_{k=1}^{j} p_{i_k}^{\alpha}.$$

Inducting on j, for $j = 2$ suppose without loss of generality $p_{i_1} \geq p_{i_2}$. Then

$$p_{i_1}^{\alpha} + p_{i_2}^{\alpha} \leq p_{i_1}^{\alpha} p_{i_2}^{\alpha} \quad \text{if and only if} \quad 1 \leq p_{i_2}^{\alpha} - \left(\frac{p_{i_2}}{p_{i_1}}\right)^{\alpha}.$$

Since $p_{i_1} \geq p_{i_2}$ and $p_{i_2} > 1$, it's clear the right hand side is larger than 1 and thus the claim holds for $j = 2$.

Now assume the claim holds for all $j \leq n$. Then

$$\begin{aligned}
\sum_{k=1}^{n+1} p_{i_k}^{\alpha} &= \sum_{k=1}^{n} p_{i_k}^{\alpha} + p_{i_{n+1}}^{\alpha} \\
&\leq \left(\prod_{k=1}^{n} p_{i_k}\right)^{\alpha} + p_{i_{n+1}}^{\alpha} \\
&\leq \left(\prod_{k=1}^{n} p_{i_k}\right)^{\alpha} \cdot p_{i_{n+1}}^{\alpha} \\
&= \prod_{k=1}^{n+1} p_{i_k}^{\alpha},
\end{aligned}$$

where we inductively assumed the claim held true for $j = n$ and $j = 2$. □

(b) Assume $r > t$, as the problem is trivial otherwise. Fix n and each q_i and define

$$f(\alpha) = \sum_{i=1}^{r} p_i^{\alpha} - \sum_{i=1}^{t} q_i^{\alpha},$$

and note $f(\alpha)$ is monotonic. The assumption $r > t$ gives $f(0) > 0$ and (a) gives $f(1) < 0$, hence f is a monotonically decreasing function. This means there is a *unique* α_0 (dependent on n and q_i) where the inequality in (a) flips.

Unfortunately, finding α_0 is very tough and perhaps is impossible to do as we demonstrate in Mathematica.

```
(* n = 840, q1 = 14, q2 = 60 *)
In[5]:= Reduce[2^α + 2^α + 2^α + 3^α + 5^α + 7^α == 14^α + 60^α, α]

During evaluation of In[5]:= Reduce::nsmet: This system cannot be
   solved with the methods available to Reduce. >>
Out[5]= Reduce[3*2^α + 3^α + 5^α + 7^α == 14^α + 60^α, α]
```

For this reason, we will explore some computational results instead. The code below will find α_0 for a given n by randomly choosing q_i.

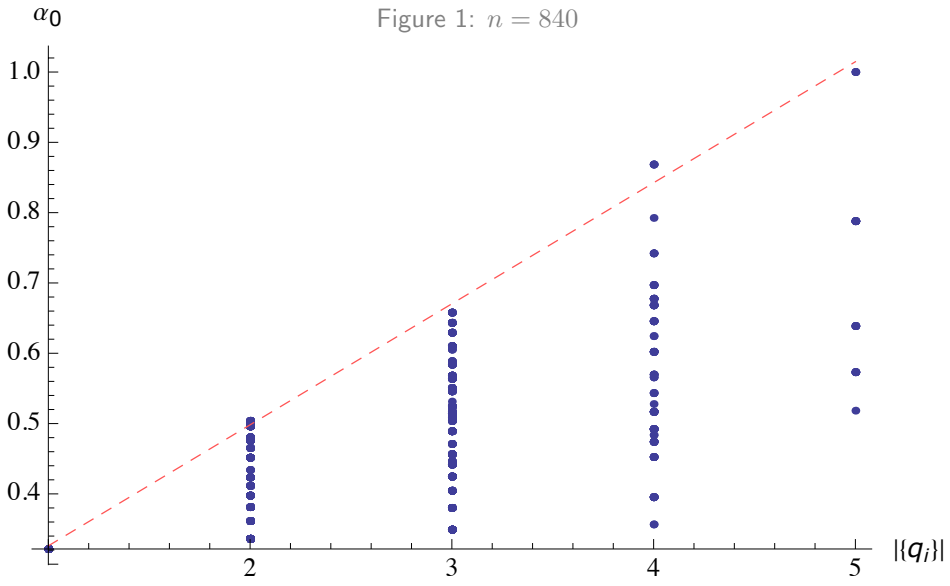
```
(* returns {{qi}, α0} *)
In[6]:= Apostol417[n_] := Module[{fac, rand},
  rand = fac = Flatten[ConstantArray @@@ FactorInteger[n]];
  While[Length[fac] == Length[rand],
    rand = Times @@@ RandomPartition[RandomSample[fac]]
  ];
  {rand, α /. FindRoot[Total[fac^α] == Total[rand^α], {α, .4},
     WorkingPrecision -> 10]}
]
RandomPartition[l_List] := SplitBy[l, RandomInteger[]&]
```

For $n = 840$ and $\{q_1, q_2, q_3\} = \{2, 5, 84\}$, the inequality flips at $\alpha_0 \approx 0.42466$:

```
In[7]:= Apostol417[840]
Out[7]= {{2, 5, 84}, 0.4246600508}
```

We can test many instances by plotting t versus α_0 for a fixed n, where a point (t, α_0) below represents a value of α_0 given t many random q_i.

Figure 1: $n = 840$




```
min: 0.3216421714, max: 1.000000000
line of best fit: y == 0.15395325 + 0.172134985 t
```

Avoiding prime numbers, we now hold n to be even. Plotting the smallest possible α_0 for a fixed n shows there's a nice downward trend as n increases, but is quite erratic as this is inherent to prime factorization.

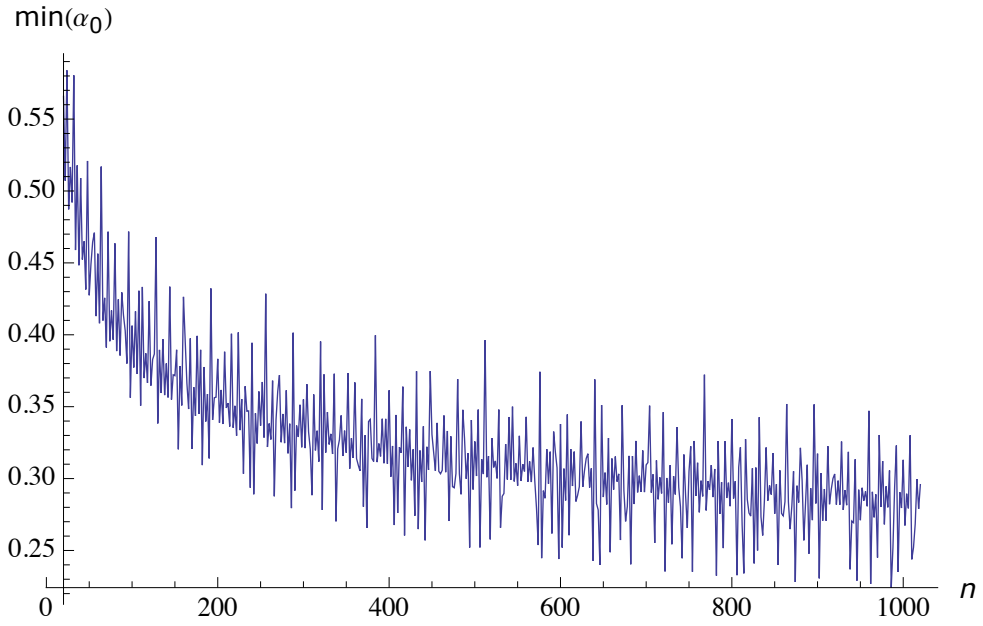


Figure 2: Plot of the smallest possible α_0 for a fixed n.

Exercise 4.18. Prove that the following two relations are equivalent:

(a) $$\pi(x) = \frac{x}{\log x} + O\left(\frac{x}{\log^2 x}\right).$$

(b) $$\vartheta(x) = x + O\left(\frac{x}{\log x}\right).$$

Proof. Assuming either relation implies the prime number theorem and so Theorem 4.4 yields $\pi(x) \sim \vartheta(x)/\log x$. The result follows directly from this assertion. □

Exercise 4.19. If $x \geq 2$, let

$$\mathrm{Li}(x) = \int_2^x \frac{dt}{\log t} \text{ (the } \textit{logarithmic integral} \text{ of } x).$$

(a) Prove that

$$\mathrm{Li}(x) = \frac{x}{\log x} + \int_2^x \frac{dt}{\log^2 t} - \frac{2}{\log 2},$$

and that, more generally,

$$\mathrm{Li}(x) = \frac{x}{\log x}\left(1 + \sum_{k=1}^{n-1} \frac{k!}{\log^k x}\right) + n! \int_2^x \frac{dt}{\log^{n+1} t} + C_n,$$

where C_n is independent of x.
(b) If $x \geq 2$ prove that

$$\int_2^x \frac{dt}{\log^n t} = O\left(\frac{x}{\log^n x}\right).$$

Proof.
(a) Integrating by parts with $u = \frac{1}{\log t}$ and $dv = dt$ gives

$$\mathrm{Li}(x) = \frac{x}{\log x} + \int_2^x \frac{dt}{\log^2 t} - \frac{2}{\log 2}.$$

Now inductively assume

$$\mathrm{Li}(x) = x\sum_{k=0}^{n-1} \frac{k!}{\log^{k+1} x} + n! \int_2^x \frac{dt}{\log^{n+1} t} + C_n,$$

with base case $n = 1$. Evaluating $\int_2^x \frac{dt}{\log^{n+1} t}$ by parts with $u = \frac{1}{\log^{n+1} t}$ and $dv = dt$ gives

$$\int_2^x \frac{dt}{\log^{n+1} t} = \frac{x}{\log^{n+1} x} - \frac{2}{\log^{n+1} 2} + (n+1)\int_2^x \frac{dt}{\log^{n+2} t}.$$

Thus

$$\begin{aligned}
\mathrm{Li}(x) &= x\sum_{k=0}^{n-1} \frac{k!}{\log^{k+1} x} + n! \int_2^x \frac{dt}{\log^{n+2} t} + C_n \\
&= x\sum_{k=0}^{n-1} \frac{k!}{\log^{k+1} x} + n! \left(\frac{x}{\log^{n+1} x} - \frac{2}{\log^{n+1} 2} + (n+1)\int_2^x \frac{dt}{\log^{n+2} t} \right) + C_n \\
&= x\sum_{k=0}^{n-1} \frac{k!}{\log^{k+1} x} + x\frac{n!}{\log^{n+1} x} + (n+1)! \int_2^x \frac{dt}{\log^{n+2} t} + C_n - \frac{2n!}{\log^{n+1} 2} \\
&= x\sum_{k=0}^{n} \frac{k!}{\log^{k+1} x} + (n+1)! \int_2^x \frac{dt}{\log^{n+2} t} + C_{n+1}.
\end{aligned}$$

(b) Applying L'Hôpital's rule we have

$$\begin{aligned}
\lim_{x\to\infty} \frac{\int_2^x dt/\log^n t}{x/\log^n x} &= \lim_{x\to\infty} \frac{1/\log^n x}{1/\log^n x - n/\log^{n+1} x} \\
&= \lim_{x\to\infty} \frac{1}{1 - n/\log x} \\
&= 1.
\end{aligned}$$

Hence

$$\int_2^x \frac{dt}{\log^n t} \sim \frac{x}{\log^n x}.$$

□

Exercise 4.20. Let f be an arithmetical function such that

$$\sum_{p\le x} f(p)\log p = (ax+b)\log x + cx + O(1) \text{ for } x \ge 2.$$

Prove that there is a constant A (depending of f) such that, if $x \geq 2$,

$$\sum_{p \leq x} f(p) = ax + (a+c)\left(\frac{x}{\log x} + \int_2^x \frac{dt}{\log^2 t}\right) + b\log(\log x) + A + O\left(\frac{1}{\log x}\right).$$

Proof. Let $h(x) = 1/\log x$ and $g(n) = f(n)\log n$ if n is prime and 0 otherwise. Define

$$G(x) = \sum_{n \leq x} g(n) = (ax+b)\log x + cx + R(x), \text{ where } R(x) = O(1).$$

Then by Abel's summation formula,

$$\sum_{p \leq x} f(p) = \sum_{n \leq x} g(n)h(n) = \frac{G(x)}{\log x} + \int_2^x \frac{G(t)}{t\log^2 t}dt.$$

Looking at both parts separately,

$$\frac{G(x)}{\log x} = \frac{(ax+b)\log x + cx + O(1)}{\log x} = ax + b + \frac{cx}{\log x} + O\left(\frac{1}{\log x}\right)$$

and

$$\begin{aligned}\int_2^x \frac{G(t)}{t\log^2 t}dt &= \int_2^x \frac{(at+b)\log t + ct + R(t)}{t\log^2 t}dt \\ &= a\int_2^x \frac{dt}{\log t} + b\int_2^x \frac{dt}{t\log t} + c\int_2^x \frac{dt}{\log^2 t} + \int_2^x \frac{R(t)}{t\log^2 t}dt.\end{aligned}$$

By Exercise 4.19, the first integral evaluates to

$$\frac{ax}{\log x} + a\int_2^x \frac{dt}{\log^2 t} - \frac{2a}{\log 2}$$

and the second integral evaluates to $b\log(\log x) - b\log(\log 2)$. The integral with the error term $R(t)$ can be rewritten as

$$\begin{aligned}\int_2^x \frac{R(t)}{t\log^2 t}dt &= \int_2^\infty \frac{R(t)}{t\log^2 t}dt + \int_x^\infty \frac{R(t)}{t\log^2 t}dt \\ &= C + O\left(\frac{1}{\log x}\right).\end{aligned}$$

Combining all constants into A, we see

$$\begin{aligned}\sum_{p \leq x} f(p) &= ax + (a+c)\left(\frac{x}{\log x} + \int_2^x \frac{dt}{\log^2 t}\right) + b\log(\log x) + A + O\left(\frac{1}{\log x}\right) \\ &= ax + (a+c)\mathrm{Li}(x) + b\log(\log x) + A + O\left(\frac{1}{\log x}\right).\end{aligned}$$

□

Exercise 4.21. Given two real-valued functions $S(x)$ and $T(x)$ such that

$$T(x) = \sum_{n \le x} S\left(\frac{x}{n}\right) \text{ for all } x \ge 1.$$

If $S(x) = O(x)$ and if c is a positive constant, prove that the relation

$$S(x) \sim cx \text{ as } x \to \infty$$

implies

$$T(x) \sim cx \log x \text{ as } x \to \infty.$$

Proof. We have $S(x) = cx + o(x)$ and so

$$\begin{aligned} T(x) &= \sum_{n \le x} \left(\frac{cx}{n} + o\left(\frac{x}{n}\right)\right) \\ &= cx \sum_{n \le x} \frac{1}{n} + o\left(x \sum_{n \le x} \frac{1}{n}\right) \\ &= cx \log x + o(x \log x)\,. \end{aligned}$$

Thus $T(x) \sim cx \log x$. □

Exercise 4.22. Prove that Selberg's formula, as expressed in Theorem 4.18, is equivalent to each of the following relations:

(a) $$\psi(x) \log x + \sum_{p \le x} \psi\left(\frac{x}{p}\right) \log p = 2x \log x + O(x)\,.$$

(b) $$\vartheta(x) \log x + \sum_{p \le x} \vartheta\left(\frac{x}{p}\right) \log p = 2x \log x + O(x)\,.$$

Proof. Let (c) denote the left hand sides of Selberg's formula. Using Theorem 4.9, which says $\psi(x) = O(x)$, we will show both $(c) - (a) = O(x)$ and $(c) - (b) = O(x)$. The first difference gives

$$\begin{aligned} (c) - (a) &= \sum_{p \le x} \sum_{m=2}^{\log_2 x} \psi\left(\frac{x}{p^m}\right) \log p \\ &= \sum_{p \le x} \log p \sum_{m=2}^{\log_2 x} \psi\left(\frac{x}{p^m}\right) \\ &= \sum_{p \le x} \log p \cdot O\left(\sum_{m=2}^{\infty} \frac{x}{p^m}\right) \\ &= O\left(x \sum_{p \le x} \frac{\log p}{p(p-1)}\right) \\ &= O(x)\,. \end{aligned}$$

Moving on to the second difference,

$$(c) - (b) = (\psi(x) - \vartheta(x)) \log x + \sum_{p \le x} \sum_{m=2}^{\log_2 x} \vartheta\left(\frac{x}{p^m}\right) \log p.$$

Applying Theorem 4.1, $\psi(x) - \vartheta(x) = O\big(\sqrt{x} \log^2 x\big)$, to the first part and applying the same technique as above to the second part, we have

$$(c) - (b) = O\big(\sqrt{x} \log^2 x\big) + O(x) = O(x)\,.$$

□

Exercise 4.23. Let $M(x) = \sum_{n \le x} \mu(n)$. Prove that

$$M(x) \log x + \sum_{n \le x} M\left(\frac{x}{n}\right) \Lambda(n) = O(x)\,.$$

and that

$$M(x) \log x + \sum_{p \le x} M\left(\frac{x}{p}\right) \log p = O(x)\,.$$

[*Hint*: Theorem 4.17.]

Proof. By Theorems 3.11 and 3.12,

$$\sum_{n \le x} M\Big(\frac{x}{n}\Big) = \sum_{n \le x} \mu(n) \left\lfloor \frac{x}{n} \right\rfloor = 1.$$

Coupling this with Theorem 4.17, to prove the first claim it's enough to show

$$\sum_{d \le x} \mu(d) \log\left(\frac{x}{d}\right) = O(x)\,.$$

This is evident through Stirling's approximation:

$$\begin{aligned}
\sum_{d \le x} \mu(d) \log\left(\frac{x}{d}\right) &= O\left(\sum_{d \le x} \log\left(\frac{x}{d}\right)\right) \\
&= O\left(\lfloor x \rfloor \log x - \sum_{d \le x} \log d\right) \\
&= O(x \log x + O(\log x) - x \log x + x + O(\log x)) \\
&= O(x)\,.
\end{aligned}$$

Next, to prove the second claim notice

$$\sum_{n \le x} M\left(\frac{x}{n}\right) \Lambda(n) = \sum_{p \le x} M\left(\frac{x}{p}\right) \log(p) + \sum_{\substack{p^m \le x \\ m > 1}} M\left(\frac{x}{p^m}\right) \log(p).$$

So it's enough to show

$$\sum_{\substack{p^m \le x \\ m>1}} M\left(\frac{x}{p^m}\right)\log(p) = O(x)\,.$$

Applying similar technique as in the proof of Exercise 4.22 we have

$$\begin{aligned}\sum_{\substack{p^m \le x \\ m>1}} M\left(\frac{x}{p^m}\right)\log(p) &= \sum_{p\le x}\log p \sum_{m=2}^{\log_2 x} M\left(\frac{x}{p^m}\right)\\ &= \sum_{p\le x}\log p\cdot O\left(\sum_{m=2}^{\infty}\frac{x}{p^m}\right)\\ &= O\left(x\sum_{p\le x}\frac{\log p}{p(p-1)}\right)\\ &= O(x)\,.\end{aligned}$$

□

Exercise 4.24.(+) Let $A(x)$ be defined for all $x > 0$ and assume that

$$T(x) = \sum_{n\le x} A\left(\frac{x}{n}\right) = ax\log x + bx + o\left(\frac{x}{\log x}\right) \text{ as } x\to\infty,$$

where a and b are constants. Prove that

$$A(x)\log x + \sum_{n\le x} A\left(\frac{x}{n}\right)\Lambda(n) = 2ax\log x + o(x\log x) \text{ as } x\to\infty.$$

Verify that Selberg's formula of Theorem 4.18 is a special case.

Lemma 4.24. For $x \ge 1$,

$$2\sum_{n\le x}\frac{1}{n}\log\left(\frac{x}{n}\right) = \log^2 x + 2C\log x + A + o(1)\,,$$

for some constants A and C.

Proof of Lemma. Applying Exercise 3.1 to estimate $\sum\log(n)/n$, we have

$$\begin{aligned}2\sum_{n\le x}\frac{1}{n}\log\left(\frac{x}{n}\right) &= 2\log x\sum_{n\le x}\frac{1}{n} - 2\sum_{n\le x}\frac{\log n}{n}\\ &= 2\log x\left(\log x + C + O\left(\frac{1}{x}\right)\right) - 2\left(\frac{1}{2}\log^2 x + A + o(1)\right)\\ &= \log^2 x + 2C\log x + A + o(1)\,.\end{aligned}$$

□

Proof of Exercise. By Theorem 4.17, it's enough to show

$$\sum_{d\le x}\mu(d)\log\left(\frac{x}{d}\right)T\left(\frac{x}{d}\right)=2ax\log x+o(x\log x)\,.$$

Expanding the left hand side we obtain

$$ax\sum_{d\le x}\frac{\mu(d)}{d}\log^2\left(\frac{x}{d}\right)+bx\sum_{d\le x}\frac{\mu(d)}{d}\log\left(\frac{x}{d}\right)+\sum_{d\le x}\mu(d)\log\left(\frac{x}{d}\right)o\left(\frac{x/d}{\log(x/d)}\right), \tag{4}$$

which will be analyzed in reverse order. Quickly looking at the error term, distributing gives a bound of

$$o\left(x\sum_{d\le x}\frac{1}{d}\right)=o(x\log x)\,.$$

Shifting focus to the second term, we will show $\sum_{d\le x}\frac{\mu(d)}{d}\log\left(\frac{x}{d}\right)=O(1)$ through a generalized Möbius inversion. Theorem 2.23 states for a completely multiplicative function $a(n)$,

$$G(x)=\sum_{n\le x}a(n)F\left(\frac{x}{n}\right)\text{ if and only if }F(x)=\sum_{n\le x}\mu(n)a(n)G\left(\frac{x}{n}\right).$$

Applying this with $a(n)=1/n$ and $F(x)=1$ we have

$$\sum_{n\le x}\frac{1}{n}=\log x+C+o(1)\text{ if and only if }\sum_{n\le x}\frac{\mu(n)}{n}\left(\log\left(\frac{x}{n}\right)+C+o(1)\right)=1.$$

Thus

$$\sum_{n\le x}\frac{\mu(n)}{n}\log\left(\frac{x}{n}\right)=1-(C+o(1))\sum_{n\le x}\frac{\mu(n)}{n}=O(1)\,,$$

where we used Theorem 3.13 which states $\sum\mu(n)/n$ is bounded.

We will now show $\sum_{d\le x}\frac{\mu(d)}{d}\log^2\left(\frac{x}{d}\right)=2\log x+O(1)$ through this generalized Möbius inversion. By Lemma 4.24,

$$2\sum_{n\le x}\frac{1}{n}\log\left(\frac{x}{n}\right)=\log^2 x+2C\log x+A+o(1)\,,$$

so through this generalized Möbius inversion we have

$$\begin{aligned}\sum_{n\le x}\frac{\mu(n)}{n}\log^2\left(\frac{x}{n}\right)&=2\log x-\sum_{n\le x}\frac{\mu(n)}{n}\left(2C\log\left(\frac{x}{n}\right)+A+o(1)\right)\\&=2\log x-2C\sum_{n\le x}\frac{\mu(n)}{n}\log\left(\frac{x}{n}\right)+(A+o(1))\sum_{n\le x}\frac{\mu(n)}{n}\\&=2\log x+O(1)+O(1)\,.\end{aligned}$$

From here we see

$$\sum_{d\le x}\mu(d)\log\left(\frac{x}{d}\right)T\left(\frac{x}{d}\right) = ax(2\log x + O(1)) + bxO(1) + o(x\log x)$$
$$= 2ax\log x + o(x\log x)\,.$$

Finally, from Theorem 4.11, ψ satisfies the hypothesis of the problem with $a = 1$ and $b = -1$. So substituting $A = \psi$ and $a = 1$ derives Selberg's formula. □

Exercise 4.25. Prove that the prime number theorem in the form $\psi(x) \sim x$ implies Selberg's asymptotic formula in Theorem 4.18 with an error term $o(x\log x)$ as $x \to \infty$.

Proof. Assuming the prime number theorem, $\psi(x) = x + o(x)$, then

$$\psi(x)\log x + \sum_{n\le x}\psi\left(\frac{x}{n}\right)\Lambda(n) = (x + o(x))\log x + \sum_{n\le x}\left(\frac{x}{n} + o\Big(\frac{x}{n}\Big)\right)\Lambda(n)$$
$$= x\log x + o(x\log x) + x\sum_{n\le x}\frac{\Lambda(n)}{n} + o\left(x\sum_{n\le x}\frac{\Lambda(n)}{n}\right)$$
$$= x\log x + x(\log x + O(1)) + o(x\log x)$$
$$= 2x\log x + o(x\log x)\,.$$

□

Remark. The prime number theorem implies a statement weaker than Selberg's formula, which is quite telling.

Exercise 4.26. In 1851 Chebyshev proved that if $\psi(x)/x$ tends to a limit as $x \to \infty$ then this limit equals 1. This exercise outlines a simple proof of this result based on the formula

$$\sum_{n\le x}\psi\left(\frac{x}{n}\right) = x\log x + O(x) \tag{5}$$

which follows from Theorem 4.11.
(a) Let $\delta = \limsup_{x\to\infty}(\psi(x)/x)$. Given $\varepsilon > 0$ choose $N = N(\varepsilon)$ so that $x \ge N$ implies $\psi(x) \le (\delta + \varepsilon)x$. Split the sum in (5) into two parts, one with $n \le x/N$, the other with $n > x/N$, and estimate each part to obtain the inequality

$$\sum_{n\le x}\psi\left(\frac{x}{n}\right) \le (\delta + \varepsilon)x\log x + x\psi(N).$$

Comparing this with (5), deduce that $\delta \ge 1$.
(b) Let $\gamma = \liminf_{x\to\infty}(\psi(x)/x)$ and use an argument similar to that in (a) to deduce that $\gamma \le 1$. Therefore, if $\psi(x)/x$ has a limit as $x \to \infty$ then $\gamma = \delta = 1$.

Proof. By Theorem 4.9, there are positive constants c_1, c_2 such that $c_2 x \le \psi(x) \le c_1 x$ eventually holds for all x. Thus both the liminf and limsup of $\psi(x)/x$ exist.

(a) Let $\delta = \limsup \psi(x)/x$ and $\varepsilon > 0$. By definition of limsup, there exists $N = N_\varepsilon$ such that for all $x \ge N$, $\psi(x) \le (\delta + \varepsilon)x$. Then

$$\begin{aligned}
\sum_{n \le x} \psi\left(\frac{x}{n}\right) &= \sum_{n \le x/N} \psi\left(\frac{x}{n}\right) + \sum_{x/N < n \le x} \psi\left(\frac{x}{n}\right) \\
&\le \sum_{n \le x/N} (\delta + \varepsilon)\frac{x}{n} + \sum_{x/N < n \le x} \psi\left(\frac{x}{x/N}\right) \\
&= (\delta + \varepsilon)x \sum_{n \le x/N} \frac{1}{n} + \sum_{n \le x} \psi(N) \\
&= (\delta + \varepsilon)x \left(\log \frac{x}{N} + C + O\left(\frac{1}{x}\right)\right) + x\psi(N) \\
&= (\delta + \varepsilon)x \log x + x\psi(N) - (\delta + \varepsilon)x \left(\log N - C + o(1)\right) \\
&\le (\delta + \varepsilon)x \log x + x\psi(N).
\end{aligned}$$

Applying Theorem 4.11 we have $x \log x + O(x) \le (\delta + \varepsilon)x \log x + x\psi(N)$ for a fixed $\varepsilon > 0$. Dividing by $x \log x$ gives $1 \le \delta + \varepsilon + O\left(\frac{1}{\log x}\right)$, and letting $x \to \infty$ gives $1 \le \delta + \varepsilon$. Finally, since ε can be as small as we like, $\delta \ge 1$.

(b) Let $\gamma = \liminf \psi(x)/x$ and $\varepsilon > 0$. By definition of liminf, there exists $N = N_\varepsilon$ such that for all $x \ge N$, $\psi(x) \ge (\gamma - \varepsilon)x$. Then

$$\begin{aligned}
\sum_{n \le x} \psi\left(\frac{x}{n}\right) &= \sum_{n \le x/N} \psi\left(\frac{x}{n}\right) + \sum_{x/N < n \le x} \psi\left(\frac{x}{n}\right) \\
&\ge \sum_{n \le x/N} (\gamma - \varepsilon)\frac{x}{n} \\
&= (\gamma - \varepsilon)x \sum_{n \le x/N} \frac{1}{n} \\
&= (\gamma - \varepsilon)x \left(\log \frac{x}{N} + C + O\left(\frac{1}{x}\right)\right) \\
&= (\gamma - \varepsilon)x \log x - (\gamma - \varepsilon)x \left(\log N - C + o(1)\right).
\end{aligned}$$

Applying Theorem 4.11 we have $x \log x + O(x) \ge (\gamma - \varepsilon)x \log x + O(x)$ for a fixed $\varepsilon > 0$. Dividing by $x \log x$ gives $1 \ge \gamma - \varepsilon + O\left(\frac{1}{\log x}\right)$, and letting $x \to \infty$ gives $1 \ge \gamma - \varepsilon$. Finally, since ε can be as small as we like, $\gamma \le 1$. □

In Exercises 27 through 30, let $A(x) = \sum_{n \le x} a(n)$, where $a(n)$ satisfies

$$a(n) \ge 0 \text{ for all } n \ge 1, \tag{6}$$

and

$$\sum_{n\le x} A\left(\frac{x}{n}\right) = \sum_{n\le x} a(n)\left[\frac{x}{n}\right] = ax\log x + bx + o\left(\frac{x}{\log x}\right) \text{ as } x\to\infty. \tag{7}$$

When $a(n)=\Lambda(n)$ these relations hold with $a=1$ and $b=-1$. The following exercises show that (6) and (7), together with the prime number theorem, $\psi(x)\sim x$, impliy $A(x)\sim ax$, a result due to Basil Gordon. This should be compared with Theorem 4.8 (Shapiro's Tauberian theorem) which assumes only (6) and the weaker condition $\sum_{n\le x} A(x/n) = ax\log x + O(x)$ and concludes that $Cx\le A(x)\le Bx$ for some positive constants C and B.

Exercise 4.27. Prove that

$$\text{(a)}\quad \sum_{n\le x} A\left(\frac{x}{n}\right)\Lambda(n) = \sum_{n\le\sqrt{x}} A\left(\frac{x}{n}\right)\Lambda(n) + \sum_{n\le\sqrt{x}} \psi\left(\frac{x}{n}\right)a(n) + O(x)$$

and use this to deduce the relation

$$\text{(b)}\quad \frac{A(x)}{x} + \frac{1}{x\log x}\sum_{n\le\sqrt{x}} A\left(\frac{x}{n}\right)\Lambda(n) + \frac{1}{x\log x}\sum_{n\le\sqrt{x}} \psi\left(\frac{x}{n}\right)a(n) = 2a + o(1)\,.$$

Proof.
(a) The left hand side can be rewritten as follows:

$$\sum_{n\le x}\Lambda(n)A\left(\frac{x}{n}\right) = \sum_{d\le x}\Lambda(d)\sum_{q\le x/d} a(q) = \sum_{qd\le x}\Lambda(d)a(q).$$

Applying the hyperbola method described in Theorem 3.17 with $a=b=\sqrt{x}$, then

$$\sum_{qd\le x}\Lambda(d)a(q) = \sum_{n\le\sqrt{x}} A\left(\frac{x}{n}\right)\Lambda(n) + \sum_{n\le\sqrt{x}}\psi\left(\frac{x}{n}\right)a(n) - \psi(\sqrt{x}\,)A(\sqrt{x}\,).$$

Looking at $\psi(\sqrt{x})A(\sqrt{x})$, assuming the prime number theorem then $\psi(\sqrt{x}\,)\sim\sqrt{x}$. Also by Theorem 4.8, $A(\sqrt{x}\,) = O(\sqrt{x}\,)$. This gives an error term that is $O(x)$.
(b) By Exercise 4.24,

$$A(x)\log x + \sum_{n\le x} A\left(\frac{x}{n}\right)\Lambda(n) = 2ax\log x + o(x\log x)\,.$$

Substituting the result of (a) and dividing both sides by $x\log x$ proves the claim. □

Exercise 4.28. Let $\alpha = \liminf_{x\to\infty}(A(x)/x)$ and let $\beta = \limsup_{x\to\infty}(A(x)/x)$.
(a) Choose any $\varepsilon>0$ and use the fact that

$$A\left(\frac{x}{t}\right) < (\beta+\varepsilon)\frac{x}{t} \quad\text{and}\quad \psi\left(\frac{x}{t}\right) < (1+\varepsilon)\frac{x}{t}$$

for all sufficiently large x/t to deduce, from Exercise 27(b), that

$$\alpha + \frac{\beta}{2} + \frac{a}{2} + \frac{\varepsilon}{2} + \frac{a\varepsilon}{2} > 2a.$$

Since ε is arbitrary this implies

$$\alpha + \frac{\beta}{2} + \frac{a}{2} \geq 2a.$$

[*Hint*: Let $x \to \infty$ in such a way that $A(x)/x \to \alpha$.]
(b) By a similar argument, prove that

$$\beta + \frac{\alpha}{2} + \frac{a}{2} \leq 2a$$

and deduce that $\alpha = \beta = a$. In other words, $A(x) \sim ax$ as $x \to \infty$.

Proof. By Theorem 4.8, there are positive constants b, c such that $cx \leq A(x) \leq bx$ eventually holds for all x. Thus both the liminf and limsup of $A(x)/x$ exist.

(a) Let $\varepsilon > 0$ then there is an N such that for all $x \geq N^2$, $A(x) < (\beta+\varepsilon)x$ and $\psi(x) < (1+\varepsilon)x$. Let $\{x_k\}_{k=1}^{\infty}$ be a sequence such that $A(x_k)/x_k \to \alpha$ as $k \to \infty$, which means

$$\frac{A(x_k)}{x_k} = \alpha + o(1)\,.$$

Now, for $x_k \geq N^2$ and any $n \leq \sqrt{x}_k$, then $x_k/n \geq \sqrt{x}_k \geq N$ and thus

$$\begin{aligned}
\frac{1}{x_k \log x_k} \sum_{n \leq \sqrt{x}_k} A\left(\frac{x_k}{n}\right) \Lambda(n) &< \frac{1}{x_k \log x_k} \sum_{n \leq \sqrt{x}_k} (\beta+\varepsilon)\left(\frac{x_k}{n}\right) \Lambda(n) \\
&= \frac{\beta+\varepsilon}{\log x_k} \sum_{n \leq \sqrt{x}_k} \frac{\Lambda(n)}{n} \\
&= \frac{\beta+\varepsilon}{\log x_k} (\log \sqrt{x}_k + O(1)) \\
&= (\beta+\varepsilon)\left(\frac{1}{2} + o(1)\right).
\end{aligned}$$

Similarly, applying Theorem 4.8,

$$\begin{aligned}
\frac{1}{x_k \log x_k} \sum_{n \leq \sqrt{x}_k} \psi\left(\frac{x_k}{n}\right) a(n) &< \frac{1}{x_k \log x_k} \sum_{n \leq \sqrt{x}_k} (1+\varepsilon)\left(\frac{x_k}{n}\right) a(n) \\
&= \frac{1+\varepsilon}{\log x_k} \sum_{n \leq \sqrt{x}_k} \frac{a(n)}{n} \\
&= \frac{1+\varepsilon}{\log x_k} (a \log \sqrt{x}_k + O(1)) \\
&= (1+\varepsilon)\left(\frac{a}{2} + o(1)\right).
\end{aligned}$$

Hence $\alpha + \frac{\beta}{2} + \frac{a}{2} + \frac{\varepsilon}{2} + \frac{a\varepsilon}{2} + o(1) > 2a + o(1)$. Letting $x \to \infty$ (but keeping ε fixed), then letting $\varepsilon \to 0$ gives us the result.
(b) Similar to (a), let $\varepsilon > 0$ and choose N such that for all $x \geq N^2$, $A(x) > (\alpha - \varepsilon)x$ and $\psi(x) > (1 - \varepsilon)x$. Let $\{x_k\}_{k=1}^{\infty}$ be a sequence such that $A(x_k)/x_k \to \beta$ as $k \to \infty$. Applying the same bounds as in (a) we get $\alpha + \frac{\beta}{2} + \frac{a}{2} - \frac{\varepsilon}{2} - \frac{a\varepsilon}{2} < 2a$. Letting $\varepsilon \to 0$ gives us $\alpha + \frac{\beta}{2} + \frac{a}{2} \leq 2a$. From here we have

$$\beta + \frac{\alpha}{2} + \frac{a}{2} \leq 2a \leq \alpha + \frac{\beta}{2} + \frac{a}{2}.$$

Rearranging terms and multiplying by 2 gives $\beta \leq 3a - \alpha - \beta \leq \alpha$. However by construction $\alpha \leq \beta$, and so $\beta = 3a - \alpha - \beta = \alpha$. This implies $\alpha = \beta = a$ and hence $A(x) \sim ax$. □

Exercise 4.29. Take $a(n) = 1 + \mu(n)$ and verify that (7) is satisfied with $a = 1$ and $b = 2C - 1$, where C is Euler's constant. Show that the result of Exercise 28 implies

$$\lim_{x\to\infty} \frac{1}{x} \sum_{n\leq x} \mu(n) = 0.$$

This gives an alternate proof of Theorem 4.14.

Proof. Let $M(x) = \sum_{n\leq x} \mu(n)$. We first derive bounds on three sums.

1. Just as in the proof of Theorem 3.3, by the hyperbola method,

$$\sum_{n\leq x} \left\lfloor \frac{x}{n} \right\rfloor = \sum_{n\leq x} \sum_{d\leq x/n} 1 = \sum_{m\leq x} d(m) = x \log x + (2C-1)x + O\left(\sqrt{x}\right).$$

2. By Theorem 3.12,

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

3. By Theorem 3.11,

$$\sum_{n\leq x} M\left(\frac{x}{n}\right) = \sum_{n\leq x} \mu(n) \left\lfloor \frac{x}{n} \right\rfloor = 1.$$

These give

$$\sum_{n\leq x} A\left(\frac{x}{n}\right) = \sum_{n\leq x} \left\lfloor \frac{x}{n} \right\rfloor + \sum_{n\leq x} M\left(\frac{x}{n}\right) = x \log x + (2C-1)x + O\left(\sqrt{x}\right)$$

and

$$\sum_{n\leq x} a(n) \left\lfloor \frac{x}{n} \right\rfloor = \sum_{n\leq x} \left\lfloor \frac{x}{n} \right\rfloor + \sum_{n\leq x} \mu(n) \left\lfloor \frac{x}{n} \right\rfloor = x \log x + (2C-1)x + O\left(\sqrt{x}\right).$$

Therefore (7) is satisfied with $a = 1$ and $b = 2C - 1$ and so by Exercise 4.28, $A(x) \sim x$. This means $\lfloor x \rfloor + M(x) = x + o(x)$ and thus $M(x) = o(x)$. □

Exercise 4.30.(++) Suppose that in Exercise 4.28, we do not assume the prime number theorem. Instead, let

$$\gamma = \liminf_{x\to\infty} \frac{\psi(x)}{x}, \quad \delta = \limsup_{x\to\infty} \frac{\psi(x)}{x}.$$

(a) Show that the argument suggested in Exercise 4.28 leads to the inequalities

$$\alpha + \frac{\beta}{2} + \frac{a\delta}{2} \geq 2a, \quad \beta + \frac{\alpha}{2} + \frac{a\gamma}{2} \leq 2a.$$

(b) From the inequalities in part (a) show that $\beta - \alpha \leq a\delta - a\gamma$ and deduce that

$$a\gamma \leq \alpha \leq \beta \leq a\delta.$$

This shows that among all numbers $a(n)$ satisfying (2) and (3) with a fixed a, the most widely separated limits of indetermination,

$$\liminf_{x\to\infty} \frac{A(x)}{x} \text{ and } \limsup_{x\to\infty} \frac{A(x)}{x},$$

occur when $a(n) = a\Lambda(n)$. Hence to deduce $A(x) \sim ax$ from (2) and (3) it suffices to treat only the special case $a(n) = a\Lambda(n)$.

Lemma 4.30. Selberg's formula implies $\gamma + \delta = 2$.

Proof of Lemma. Choose x to tend to infinity so that $\psi(x)/x \to \gamma$. Fix $\varepsilon > 0$ and choose $N = N_\varepsilon$ such that for all $x \geq N$, $\psi(x) < (\delta + \varepsilon)x$. Using a variation of Selberg's formula from Exercise 4.22 and the same idea in Exercise 4.26 we have

$$\begin{aligned}
2x\log x + o(x\log x) &= \psi(x)\log x + \sum_{p\leq x} \psi\left(\frac{x}{p}\right)\log p \\
&= \psi(x)\log x + \sum_{p\leq x/N} \psi\left(\frac{x}{p}\right)\log p + \sum_{x/N<p\leq x} \psi\left(\frac{x}{p}\right)\log p \\
&< \gamma x\log x + o(x\log x) + \sum_{p\leq x/N} \frac{(\delta+\varepsilon)x}{p}\log p + \sum_{x/N<p\leq x} \psi\left(\frac{x}{x/N}\right)\log p \\
&\leq \gamma x\log x + o(x\log x) + (\delta+\varepsilon)x\left(\log\frac{x}{N} + O(1)\right) + \psi(N)\vartheta(x) \\
&= (\gamma+\delta+\varepsilon)x\log x + o(x\log x)\,.
\end{aligned}$$

Here we used Theorem 4.10, which says $\sum_{p\leq x}\log(p)/p = \log x + O(1)$. Dividing by $x\log x$ gives $\gamma+\delta+\varepsilon+o(1) > 2+o(1)$, and letting $x\to\infty$ then $\varepsilon\to 0$ then shows $\gamma+\delta\geq 2$.

On the other hand we can choose x to tend to infinity so that $\psi(x)/x \to \delta$ and $N = N_\varepsilon$ such that for all $x \geq N$, $\psi(x) > (\gamma-\varepsilon)x$. Then mirroring the above argument,

$$(\delta+\gamma-\varepsilon)x\log x + o(x\log x) < 2x\log x + o(x\log x)\,,$$

which leads to $\gamma+\delta\leq 2$. We conclude

$$\gamma + \delta = 2.$$

□

Proof of Exercise.
(a) Replacing $1+\varepsilon$ with $\delta+\varepsilon$ and $1-\varepsilon$ with $\gamma-\varepsilon$ in the proof of Exercise 4.28 immediately implies these inequalities.
(b) Adding the inequalities from (a) we have

$$2a+\beta+\frac{\alpha}{2}+\frac{a\gamma}{2}\leq 2a+\alpha+\frac{\beta}{2}+\frac{a\delta}{2}.$$

Rearranging terms and multiplying by 2 gives $\beta-\alpha\leq a\delta-a\gamma$.

Now using Lemma 4.30, substituting $\delta=2-\gamma$ into $\alpha+\frac{\beta}{2}+\frac{a\delta}{2}\geq 2a$ shows

$$2\alpha+\beta+a(2-\gamma)\geq 4a.$$

Adding this to $\beta+\frac{\alpha}{2}+\frac{a\gamma}{2}\leq 2a$ gives

$$4a+\beta+\frac{\alpha}{2}+\frac{a\gamma}{2}\leq 2a+2\alpha+\beta+a(2-\gamma),$$

and solving for α, we have $a\gamma\leq\alpha$.

Substituting $\gamma=2-\delta$ into $\beta+\frac{\alpha}{2}+\frac{a\gamma}{2}\leq 2a$ shows

$$2\beta+\alpha+a(2-\delta)\leq 4a.$$

Adding this to $\alpha+\frac{\beta}{2}+\frac{a\delta}{2}\geq 2a$ gives

$$4a+\alpha+\frac{\beta}{2}+\frac{a\delta}{2}\geq 2a+2\beta+\alpha+a(2-\delta),$$

and solving for β, we have $\beta\leq a\delta$. By construction $\alpha\leq\beta$, and so $a\gamma\leq\alpha\leq\beta\leq a\delta$. □

Chapter 5
Congruences

Exercise 5.1. Let S be a set of n integers (not necessarily distinct). Prove that some nonempty subset of S has a sum which is divisible by n.

Proof. Let $S = \{s_1, s_2, \ldots, s_n\}$ and define $a_i = s_1 + s_2 + \cdots + s_i$ for $1 \leq i \leq n$. If a_k is divisible by n for some k, we are done. Otherwise, by the pigeonhole principle there exists i and j such that $i > j$ and $a_i \equiv a_j \bmod n$. Thus $a_i - a_j \equiv 0 \bmod n$, or in other words $s_{i+1} + \cdots + s_j \equiv 0 \bmod n$. □

Exercise 5.2. Prove that $5n^3 + 7n^5 \equiv 0 \bmod 12$ for all integers n.

Proof. By Theorem 5.2 (d), it's enough to show this holds for $n = 1, 2, \ldots, 11$. We show this in Mathematica.

```
In[1]:= f[n_] := 5n^3 + 7n^5

In[2]:= Mod[f[Range[12]], 12]
Out[2]= {0,0,0,0,0,0,0,0,0,0,0,0}
```

□

Exercise 5.3.
(a) Find all positive integers n for which $n^{13} \equiv n \bmod 1365$.
(b) Find all positive integers n for which $n^{17} \equiv n \bmod 4080$.

Solution.
(a) Since $1365 = 3 \cdot 5 \cdot 7 \cdot 13$, it's equivalent to solve $n^{13} \equiv n \bmod 3, 5, 7, 13$.

- Since $n^{13} = (n^2)^6 \cdot n \equiv n \bmod 3$, all n are solutions mod 3.
- Since $n^{13} = (n^4)^3 \cdot n \equiv n \bmod 5$, all n are solutions mod 5.
- Since $n^{13} = (n^6)^2 \cdot n \equiv n \bmod 7$, all n are solutions mod 7.
- By Fermat's little theorem, $n^{13} \equiv n \bmod 13$, thus all n are solutions mod 13.

Therefore all integers n satisfy $n^{13} \equiv n \bmod 1365$.
(b) Since $4080 = 2^4 \cdot 3 \cdot 5 \cdot 17$, it's equivalent to solve $n^{17} \equiv n \bmod 3, 5, 16, 17$.

- Since $n^{17} = (n^2)^8 \cdot n \equiv n \bmod 3$, all n are solutions mod 3.
- Since $n^{17} = (n^4)^4 \cdot n \equiv n \bmod 5$, all n are solutions mod 5.
- By Fermat's little theorem, $n^{17} \equiv n \bmod 17$, thus all n are solutions mod 17.

Therefore it's equivalent to solve $n^{17} \equiv n \bmod 16$. By inspection, all solutions are multiples of 16 and odd integers.

Exercise 5.4.
(a) Prove that $\varphi(n) \equiv 2 \bmod 4$ when $n = 4$ and when $n = p^a$, where p is a prime, $p \equiv 3 \bmod 4$.
(b) Find all n for which $\varphi(n) \equiv 2 \bmod 4$.

Proof.
(a) If $n = 4$ then $\varphi(n) = 2$. Instead suppose $n = p^a$, where p is a prime, $p \equiv 3 \bmod 4$. Then $\varphi(n) = p^{a-1}(p-1)$. Since $p^{a-1} \equiv 1, 3 \bmod 4$, then $\varphi(n)$ is either $1 \cdot 2$ or $3 \cdot 2 \bmod 4$. But $6 \equiv 2 \bmod 4$ and so $\varphi(n) \equiv 2 \bmod 4$.

(b) Consider the four cases.

- Suppose $n = p^a m$, where $p \equiv 1 \bmod 4$ and p is relatively prime to m. Then
$$\varphi(n) = p^{a-1}(p-1)\varphi(m) \equiv p^{a-1} \cdot 0 \cdot \varphi(m) \equiv 0 \mod 4.$$
Thus if n is divisible by a prime congruent to 1 mod 4 then $\varphi(n) \not\equiv 2 \bmod 4$.
- Suppose $n = p^a q^b m$ for primes $p, q \equiv 3 \bmod 4$ which are relatively prime to m. Then
$$\varphi(n) = \varphi(p^a)\varphi(q^b)\varphi(m) \equiv 2 \cdot 2 \cdot \varphi(m) \equiv 0 \mod 4.$$
So if n is divisible by more than one prime congruent to 3 mod 4 then $\varphi(n) \not\equiv 2 \bmod 4$.
- Suppose $n = 2^s p^a$, where $s > 0$, $a > 0$, and p is a prime, $p \equiv 3 \bmod 4$. Then
$$\varphi(n) = 2^{s-1}\varphi(p^a) \equiv 2^{s-1} \cdot 2 \equiv 2^s \mod 4.$$
Thus for $\varphi(n) \equiv 2 \bmod 4$ to hold we require $s = 1$.
- Suppose $n = 2^s$, where $s > 0$. Then $\varphi(n) = 2^{s-1}$ and thus for $\varphi(n) \equiv 2 \bmod 4$ to hold we require $n = 4$.

Hence $\varphi(n) \equiv 2 \bmod 4$ if and only if $n = 4$, $n = p^a$, or $n = 2p^a$ for $a > 0$ and some prime $p \equiv 3 \bmod 4$. □

Exercise 5.5. A yardstick divided into inches is again divided into 70 equal parts. Prove that among the four shortest divisions two have left endpoints corresponding to 1 and 19 inches. What are the right endpoints of the other two?

Solution. Take a yardstick marked at every inch. Next make a mark at every $\frac{36}{70}$th of an inch. The yardstick has now been non-uniformly partitioned. We are asked to find where the four shortest divisions lie.

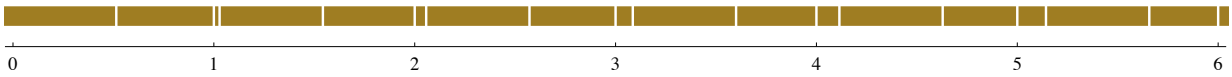


Figure 3: The first six inches of the marked yardstick.

Let x and y be integers such that x and $\frac{36}{70}y$ are endpoints of a division. Then $(36, 70) = 2$ implies

$$\left| x - \frac{36}{70}y \right| \geq \frac{2}{70} = \frac{1}{35}.$$

So the smallest possible division length is $1/35$. The goal now is to solve $|70x - 36y| = 2$. Note that $|70x - 36y| = 2$ can be rewritten as

$$70x - 36y = 2 \quad \text{or} \quad 70x - 36y = -2.$$

First, look at $70x - 36y = 2$. By inspection, $70(-1) - 36(-2) = 2$ and thus $x = -1$ and $y = -2$ is a solution. Next, to find all solutions, we solve $70(-1 + m) - 36(-2 + n) = 2$ for integers n and m. This gives $n = \frac{35}{18}m$ and thus $m = 18k$ and $n = 35k$ for some integer k. Hence the solutions are of the form

$$x = 18k - 1, \;\; y = 35k - 2, \quad \text{for some } k \in \mathbb{Z}.$$

Similarly, the solutions to $70x - 36y = -2$ are of the form

$$x = 1 + 18k, \;\; x = 2 + 35k, \quad \text{for some } k \in \mathbb{Z}.$$

Since x and $\frac{36}{70}y$ both lie on the yardstick, it must be that $0 < x < 36$ and $0 < y < 70$. Thus the only valid solutions are

$$(x, y) = (17, 33), (35, 68), (1, 2), (19, 37).$$

These correspond to the divisions

$$\left[\frac{594}{35}, 17\right], \left[\frac{1224}{35}, 35\right], \left[1, \frac{36}{35}\right], \left[19, \frac{666}{35}\right]$$

respectively.

Remark. This problem can also be solved using Mathematica

```
In[3]:= Block[{marklocs, divs},
  marklocs = Union[Join[Range[0, 36], Range[0, 36, 36/70]]];
  divs = Partition[marklocs, 2, 1];
  divs[[Ordering[divs, 4, Subtract @@ #1 > Subtract @@ #2&]]]
]
Out[3]= {{1224/35, 35}, {19, 666/35}, {594/35, 17}, {1, 36/35}}
```

Exercise 5.6. Find all x which simultaneously satisfy the system of congruences

$$x \equiv 1 \mod 3, \qquad x \equiv 2 \mod 4, \qquad x \equiv 3 \mod 5.$$

Solution. By the Chinese remainder theorem there is a unique solution mod 60. Following the method described in the proof of Theorem 5.26, we define the following.

Let $M_1 = 20$, $M_2 = 15$, and $M_3 = 12$. This gives $M_1' = 2$, $M_2' = 3$, and $M_3' = 3$. The solution mod 60 is thus

$$x = 1 \cdot 20 \cdot 2 + 2 \cdot 15 \cdot 3 + 3 \cdot 12 \cdot 3 \equiv 58 \mod 60.$$

So all solutions are $x = 60k + 58$ for all integers k.

Exercise 5.7. Prove the converse of Wilson's theorem: *If* $(n-1)! + 1 \equiv 0 \bmod n$*, then* n *is prime if* $n > 1$.

Lemma 5.7. If n is composite and $n \neq 4$ then $n \mid (n-1)!$.

Proof of Lemma. Suppose $n = ab$ for $1 < a < b < n$. Then

$$(n-1)! = (ab)(1)(2)\cdots(a-1)(a+1)\cdots(b-1)(b+1)\cdots(n-1),$$

hence $n \mid (n-1)!$. Otherwise $n = p^2$ for some prime $p > 2$. This means $p^2 - 1 > 2p$ and so

$$(p^2-1)! = (p^2)(1)(2)\cdots(p-1)(p+1)\cdots(2p-1)(2)(2p+1)\cdots(p^2-1).$$

Therefore $n \mid (n-1)!$. □

Proof of Exercise. Let n be composite. For $n = 4$, $(4-1)! + 1 \equiv 3 \bmod 4$. Otherwise, by Lemma 5.7, $(n-1)! + 1 \equiv 1 \bmod n$. Thus if n is composite then $(n-1)! + 1 \not\equiv 0 \bmod n$. □

Exercise 5.8. Find all positive integers n for which $(n-1)! + 1$ is a power of n.

Proof. By Exercise 5.7, $n \mid (n-1)!+1$ if and only if n is prime. Thus we may assume $n = p$ for some prime p. Suppose $(p-1)! + 1 = p^k$ for some prime $p > 5$. Then

$$\begin{aligned}(p-2)! &= p^{k-1} + \cdots + p + 1 \\ &= (p^{k-1} - 1) + \cdots + (p-1) + (1-1) + k.\end{aligned}$$

By Lemma 5.7, $p - 1 \mid (p-2)!$ and thus $p - 1 \mid k$. We conclude $k \geq p - 1$, a contradiction since $(p-1)! + 1 < p^{p-1}$.

Testing $p = 2$, 3, 5 then $(p-1)!+1$ is 2, 3, 25, respectively. Thus $(n-1)!+1$ is a power of n if and only if $n = 2$, 3, 5. □

Exercise 5.9. If p is an odd prime, let $q = (p-1)/2$. Prove that

$$(q!)^2 + (-1)^q \equiv 0 \mod p.$$

This gives $q!$ as an explicit solution to the congruence $x^2 + 1 \equiv 0 \bmod p$ when $p \equiv 1 \bmod 4$, and it shows $q! \equiv \pm 1 \bmod p$ if $p \equiv 3 \bmod 4$. No simple general rule is known for determining the sign.

Proof. Suppose $p = 4n + 1$, then $q = (2n)!$. By Wilson's theorem,

$$\begin{aligned} -1 &\equiv (p-1)! \\ &\equiv (1 \cdot 2 \cdots 2n)((2n+1) \cdots 4n) \\ &\equiv (1 \cdot 2 \cdots 2n)((p-2n) \cdots (p-1)) \\ &\equiv (1 \cdot 2 \cdots 2n)((-2n) \cdots (-1)) \\ &\equiv ((2n)!)^2(-1)^{2n} \\ &\equiv q^2 \mod p. \end{aligned}$$

On the other hand, if $p = 4n + 3$ then $q = (2n + 1)!$. Thus

$$\begin{aligned} -1 &\equiv (p-1)! \\ &\equiv (1 \cdot 2 \cdots 2n \cdot (2n+1))((2n+2) \cdots (4n+2)) \\ &\equiv (1 \cdot 2 \cdots 2n \cdot (2n+1))((p-2n-1) \cdots (p-1)) \\ &\equiv (1 \cdot 2 \cdots 2n \cdot (2n+1))((-2n-1) \cdots (-1)) \\ &\equiv ((2n+1)!)^2(-1)^{2n+1} \\ &\equiv -q^2 \mod p. \end{aligned}$$

Hence $(q!)^2 + (-1)^q \equiv 0 \bmod p$. □

Exercise 5.10. If p is odd, $p > 1$, prove that

$$1^2 3^2 5^2 \cdots (p-2)^2 \equiv (-1)^{(p+1)/2} \mod p$$

and

$$2^2 4^2 6^2 \cdots (p-1)^2 \equiv (-1)^{(p+1)/2} \mod p.$$

Proof. Suppose $p = 4n + 1$, then by Wilson's theorem,

$$\begin{aligned} -1 &\equiv (p-1)! \\ &\equiv (1 \cdot 3 \cdots (4n-1))(2 \cdot 4 \cdots 4n) \\ &\equiv (1 \cdot 3 \cdots (4n-1))((p-4n+1) \cdot (p-4n-3) \cdots (p-1)) \\ &\equiv (1 \cdot 3 \cdots (4n-1))((-4n+1) \cdot (-4n-3) \cdots (-1)) \\ &\equiv 1^2 3^2 5^2 \cdots (p-2)^2(-1)^{2n} \qquad (8) \\ &\equiv 1^2 3^2 5^2 \cdots (p-2)^2 \mod p. \end{aligned}$$

Instead, substituting $2k+1 = p-2k$ establishes $2^2 4^2 6^2 \cdots (p-1)^2 \equiv -1 \bmod p$ for $p = 4n+1$.

Now if $p = 4n + 3$, then the same exact methodology applies here, except there are now an odd number of even terms and an odd number of odd terms. Thus we have $(-1)^{2n+1}$ in (8) instead of $(-1)^{2n}$. The result then follows. □

Exercise 5.11. Let p be a prime, $p \geq 5$, and write

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p} = \frac{r}{ps}.$$

Prove that $p^3 \mid (r - s)$.

Proof. Let H_n be the nth harmonic number. By Theorem 5.25, $p!H_{p-1} \equiv 0 \bmod p^3$. Adding $(p-1)!$ to both sides gives $p!H_p \equiv (p-1)! \bmod p^3$, i.e. there is an integer k such that

$$p!H_p = (p-1)! + kp^3.$$

Thus

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p} = \frac{(p-1)! + kp^3}{p(p-1)!}.$$

Let $g = \gcd\big((p-1)! + kp^3, (p-1)!\big)$. Now $g \mid (p-1)!$, which means $g \nmid p$. Thus since $g \mid kp^3$ we have $g \mid k$. Defining $q = (p-1)!/g$ and $m = k/g$ gives

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p} = \frac{q + mp^3}{pq} = \frac{r}{ps},$$

where the right hand side is in lowest terms. Hence $r - s = mp^3 \equiv 0 \bmod p^3$. □

Exercise 5.12. If p is a prime, prove that

$$\binom{n}{p} \equiv \left[\frac{n}{p}\right] \mod p.$$

Also if $p^\alpha \mid [n/p]$ prove that

$$p^\alpha \left| \binom{n}{p} \right. .$$

Lemma 5.12. Suppose $b \mid a$ and $(b, n) = 1$. If $bc \equiv 1 \bmod n$ then $a/b \equiv ac \bmod n$.

Proof of Lemma. Let $a = bd$. Then $a/b = d$ and $ac = d(bc) \equiv d \bmod n$. □

Proof of Exercise. Suppose $n = pq + r$ where $0 \le r < p$. Then $\lfloor n/p \rfloor = q$ and

$$\begin{aligned}
\binom{n}{p} &= \frac{(pq+r)!}{p!(pq+r-p)!} \\
&= \frac{1}{p!} \prod_{i=0}^{p-1} (pq + r - i) \\
&= \frac{pq}{p!} \prod_{\substack{0 \le i < p \\ i \ne r}} (pq + r - i) \\
&= \frac{q}{(p-1)!} \prod_{\substack{0 \le i < p \\ i \ne r}} (pq + r - i). \qquad (9)
\end{aligned}$$

Notice $\{pq + r - i \mid 0 \le i < p \text{ and } i \ne r\}$ forms a reduced residue system mod p and so

$$\prod_{\substack{0 \le i < p \\ i \ne r}} (pq + r - i) \equiv (p-1)! \mod p.$$

Thus by Wilson's theorem and Lemma 5.12,

$$\binom{n}{p} \equiv q(-1)(-1) = q \mod p.$$

Next suppose $q = p^\alpha d$, then by (9)

$$\binom{n}{p} = p^\alpha \left(\frac{d}{(p-1)!} \prod_{\substack{0 \le i < p \\ i \neq r}} (pq + r - i) \right).$$

Since p^α is relatively prime to $(p-1)!$, the quantity on the right is an integer and hence $p^\alpha \mid \binom{n}{p}$. □

Exercise 5.13.(+) Let a, b, n be positive integers such that n divides $a^n - b^n$. Prove that n also divides $(a^n - b^n)/(a - b)$.

Proof. Let $n = p^\alpha m$ where $p \nmid m$ and $(a-b, n) = p^\beta g$ where $p \nmid g$. It's enough to show

$$p^{\alpha+\beta} \mid a^n - b^n.$$

Assume $\beta > 0$, as it is trivial otherwise. Since $p^\beta \mid a - b$, then $a = b + kp^\beta$ for some k. Consequently

$$\begin{aligned} a^n - b^n &= \sum_{j=1}^{n} \binom{n}{j} k^j p^{\beta j} b^{n-j} \\ &= \sum_{j=1}^{n} \frac{n(n-1)\cdots(n-j+1)}{j!} k^j p^{\beta j} b^{n-j} \\ &= \sum_{j=1}^{n} C_j \frac{np^{\beta j}}{j!}. \end{aligned}$$

Let M be the highest power of p dividing $a^n - b^n$, then

$$M \ge \min_{1 \le j \le n} \left\{ \alpha + \beta j - \left\lfloor \log_p j \right\rfloor \right\}.$$

Since $\beta > 0$,

$$\begin{aligned} M &\ge \alpha + \beta \min_{1 \le j \le n} \left\{ j - \left\lfloor \log_p j \right\rfloor \right\} \\ &\ge \alpha + \beta \min_{1 \le j \le n} \left\{ j - \log_2 j \right\}. \end{aligned}$$

Now $j - \log_2 j$ is minimized over the positive integers at $j = 1$ and $j = 2$ with value 1. This means $M \ge \alpha + \beta$, and hence $p^{\alpha+\beta} \mid a^n - b^n$. Therefore $n \mid (a^n - b^n)/(a - b)$. □

Exercise 5.14. Let a, b, and x_0 be positive integers and define

$$x_n = ax_{n-1} + b \quad \text{for } n = 1, 2, \ldots$$

Prove that not all x_n can be primes.

Proof. If x_1 is not prime, we are done. Otherwise suppose $p = ax_0 + b$ is prime. We have $p \nmid a$ and thus $a^{p-1} \equiv 1 \bmod p$. Then

$$\begin{aligned} x_{p(p-1)+1} &= a^{p(p-1)+1}x_0 + a^{p(p-1)}b + \cdots + a^2b + ab + b \\ &= a^{p(p-1)+1}x_0 + a^{p(p-1)}b + \sum_{i=0}^{p-1} \left(a^{i(p-1)+p-2} + \cdots + a^{i(p-1)+1} + a^{i(p-1)}\right)b \\ &\equiv ax_0 + b + p(a^{p-2} + \cdots + a^2 + a + 1)b \\ &\equiv ax_0 + b \equiv 0 \mod p, \end{aligned}$$

and since x_n is a monotonically increasing sequence, $x_{p(p-1)+1}$ must be composite. □

Exercise 5.15. Let n, r, a denote positive integers. The congruence $n^2 \equiv n \bmod 10^a$ implies $n^r \equiv n \bmod 10^a$ for all r. Find the values of r such that $n^r \equiv n \bmod 10^a$ implies $n^2 \equiv n \bmod 10^a$.

Solution. Consider the three possible cases on r.

- Let r be odd and choose n to satisfy $n \equiv -1 \bmod 10^a$. Then $n^r \equiv n \bmod 10^a$, but $n^2 \not\equiv n \bmod 10^a$.
- Let $r = 10k + 6$, $a = 2$, and $n = 16$. Inducting on k, note $n^{r-1} \equiv 1 \bmod 10^a$. Hence $n^r \equiv n \bmod 10^a$, but observe $n^2 \not\equiv n \bmod 10^a$.
- Let $r = 10k + m$, where $m \in \{0, 2, 4, 8\}$. If $n^{r-1} \equiv 1 \bmod 10^a$, then $|n| \mid 10k + m - 1$. However $|n| \mid \varphi(10^a) = 4 \cdot 10^{a-1}$, hence for $m \in \{0, 2, 4, 8\}$ it must be that $|n| = 1$. Therefore in this case, the only solutions to $n^r \equiv n \bmod 10^a$ are $n = 0$ or $n = 1$.

We conclude $n^r \equiv n \bmod 10^a$ implies $n^2 \equiv n \bmod 10^a$ if and only if r is even and not congruent to 1 mod 5.

Exercise 5.16. Let n, a, d be given integers with $(a, d) = 1$. Prove that there exists an integer m such that $m \equiv a \bmod d$ and $(m, n) = 1$.

Proof. Define $S = \{a + td \mid t = 1, 2, \ldots, (nd)/d\}$. Since $(a, d) = 1$, by Theorem 5.32 there is an $m \in S$ such that $(m, nd) = 1$. This implies $(m, n) = 1$. □

Exercise 5.17. Let f be an integer-valued arithmetical function such that

$$f(m + n) \equiv f(n) \mod m$$

for all $m \geq 1$, $n \geq 1$. Let $g(n)$ be the number of values (including repetitions) of $f(1), f(2), \ldots, f(n)$ divisible by n, and let $h(n)$ be the number of these values relatively prime to n. Prove that

$$h(n) = n \sum_{d \mid n} \mu(d) \frac{g(d)}{d}.$$

Proof. Let $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ and define $g(k, n)$ to be the number of values (including repetitions) of $f(1), f(2), \ldots, f(n)$ divisible by k. Through the principle of cross-classification,

$$h(n) = n - \sum_{1 \le i \le k} g(p_i, n) + \sum_{1 \le i < j \le k} g(p_i p_j, n) - \ldots + (-1)^k g(p_1 \cdots p_k, n).$$

Suppose $k \mid n$. By assumption we can partition $\{f(1), f(2), \ldots, f(n)\}$ into n/k subsets which are congruent mod k. This implies

$$g(k, n) = \frac{n}{k} g(k),$$

hence

$$h(n) = n - \sum_{1 \le i \le k} \frac{n}{p_i} g(p_i) + \sum_{1 \le i < j \le k} \frac{n}{p_i p_j} g(p_i p_j) - \ldots + (-1)^k \frac{n}{p_1 \cdots p_k} g(p_1 \cdots p_k).$$

Since μ is zero for all other factors of n, we have

$$h(n) = n \sum_{d \mid n} \mu(d) \frac{g(d)}{d}.$$

□

Exercise 5.18.(+) Given an odd integer $n > 3$, let k and t be the smallest positive integers such that both $kn + 1$ and tn are squares. Prove that n is prime if, and only if, both k and t are greater than $n/4$.

Proof. If n is prime, then $n^2 \mid tn$ which implies $n \mid t$. Thus $t \ge n > n/4$. Also, by Theorem 5.21, $x^2 \equiv 1 \mod n$ has exactly the two solutions $\pm 1 \mod n$. So if $kn + 1 = a^2$, then $a \equiv \pm 1 \mod n$. Thus $a \ge n - 1$, which implies $kn + 1 \ge (n-1)^2$. Isolating k, we see $k \ge n - 2$. Finally since $n > 3$, then $n - 2 > n/4$ and therfore $k > n/4$.

If n is composite, consider the three cases.

- Suppose $n = p^{2a}$ for a prime p. Taking $t = 1$ gives the smallest integer such that tn is a square and $t < n/4$, as $n > 4$.
- Suppose $n = p^{2a+1}$ for a prime p. Taking $t = p$ gives the smallest integer such that tn is a square. Since $p > 2$ then $t = p < p \cdot (p^2/4) = p^3/4 \le n/4$.
- Suppose $n = p^a m$ for $m > 2$ and $p \nmid m$. By the Chinese remainder theorem, there is a unique y such that

$$y \equiv 1 \mod p^a, \quad y \equiv -1 \mod m, \quad |y| < \frac{n}{2}.$$

This gives $y^2 \equiv 1 \mod n$. Now if $y = 1$ then $y \equiv 1 \mod m$, which is impossible since $m > 2$. Therefore $y \ne 1$ and similarly $y \ne -1$, so taking $k = (y^2 - 1)/n$ gives a positive integer such that $kn + 1$ is a square. Additionally, under the assumption $|y| < n/2$, we have $k < y^2/n < n/4$.

Thus if n is composite then at least one of k, t is less than $n/4$. □

Exercise 5.19.(++) Prove that each member of the set of $n-1$ consecutive integers

$$n!+2, n!+3, \ldots, n!+n$$

is divisible by a prime which does not divide any other member of the set.

Proof. For each $2 \leq k \leq n$, consider the three cases.

- Suppose k is prime and $k > n/2$. Then $k \mid n!+k$ and $k \nmid n!+j$ for $j \neq k$ since $n!+2k > n!+j$. In this case we are done.
- Suppose k is prime and $k \leq n/2$. Then since $2k \leq n$, for any prime $p \leq n$, $p \mid n!/k$ and hence $p \nmid n!/k+1$. It follows that $n!/k+1$ has a prime factor larger than n. This implies $n!+k$ does as well.
- Suppose k is composite. Similar to the above case, for any prime $p \leq n$, $p \mid n!/k$. Thus $p \nmid n!/k+1$ and so $n!+k$ has a prime factor larger than n.

Now suppose k is not a prime larger than $n/2$. Let $p_k > n$ be a prime dividing $n!+k$. Since $|(n!+j)-(n!+k)| < n$ we have

$$n!+j \not\equiv n!+k \mod p_k \quad \text{for } j \neq k.$$

Therefore $p_k \mid n!+k$ and $p_k \nmid n!+j$ for $j \neq k$. □

Exercise 5.20.(+) Prove that for any positive integers n and k, there exists a set of n consecutive integers such that each member of this set is divisible by k distinct prime factors no one of which divides any other member of the set.

Proof. Fix n and induct on k, where the base case $k = 1$ is proven in Exercise 5.19. Suppose

$$S_k = \{s_1, s_2, \ldots, s_n\}$$

satisfies the claim for k with corresponding primes $p_{i,j}$ for $1 \leq i \leq n$ and $1 \leq j \leq k$. Define

$$S_{k+1} = \{t_1, t_2, \ldots, t_n\}, \text{ where } t_i = s_n! + s_i,$$

a set of consecutive integers. It's clear each $p_{i,j}$ divides t_i and $p_{i,j}$ does not divide t_l for $l \neq i$. Applying the exact process in Exercise 5.19, since s_i is composite, there is a prime $P_i > s_n$ that divides t_i. Furthermore, since $|t_i - t_l| < n$ we have

$$t_i \not\equiv t_l \mod P_i \quad \text{for } l \neq i.$$

Thus each member of S_{k+1} is divisible by $k+1$ distinct prime factors no one of which divides any other member S_{k+1}. □

Remark. The last two exercises both prove there are infinitely many primes.

Exercise 5.21. Let n be a positive integer which is not a square. Prove that for every integer a relatively prime to n there exist integers x and y satisfying

$$ax \equiv y \mod n \quad \text{with } 0 < x < \sqrt{n} \text{ and } 0 < |y| < \sqrt{n}.$$

Proof. Consider $ax - y$ for $0 \leq x, y \leq \lfloor \sqrt{n} \rfloor$, which gives $(\lfloor \sqrt{n} \rfloor + 1)^2$ possible values for (x, y). Since $\sqrt{n} < \lfloor \sqrt{n} \rfloor + 1$, then $n < (\lfloor \sqrt{n} \rfloor + 1)^2$.

Now, there are at most n values $ax - y$ can attain mod n, so by the pigeonhole principle there must be at least two distinct expressions $ax - y$ that are congruent mod n. Suppose $ax_1 - y_1 \equiv ax_2 - y_2 \mod n$ for $\{x_1, y_1\} \neq \{x_2, y_2\}$. This gives

$$a(x_1 - x_2) \equiv y_1 - y_2 \mod n,$$

and so take $x = |x_1 - x_2|$ and $y = \pm|y_1 - y_2|$. Observe $0 \leq x \leq \sqrt{n}$ and $0 \leq |y| \leq \sqrt{n}$, so all that remains is to show the inequalities are strict.

- Supposing $x = 0$, then $x_1 = x_2$ and $y_1 - y_2 \equiv 0 \mod n$. So $y_1 = kn + y_2$ for some integer k. However since $0 \leq y_1, y_2 \leq \lfloor \sqrt{n} \rfloor$, we must have $k = 0$ and thus $y_1 = y_2$. This contradicts $\{x_1, y_1\} \neq \{x_2, y_2\}$.
- Supposing $y = 0$, then $y_1 = y_2$ and $a(x_1 - x_2) \equiv 0 \mod n$. Now since $(a, n) = 1$ we must have $x_1 - x_2 \equiv 0 \mod n$. We conclude $x_1 = x_2$, another contradiction.
- Since n is not a square and both x and y are integers, we have $x \neq \sqrt{n}$ and $|y| \neq \sqrt{n}$.

Therefore $0 < x < \sqrt{n}$ and $0 < |y| < \sqrt{n}$. □

Exercise 5.22. Let p be a prime, $p \equiv 1 \mod 4$, let $q = (p-1)/2$, and let $a = q!$.
(a) Prove that there exist positive integers x and y satisfying $0 < x < \sqrt{p}$ and $0 < y < \sqrt{p}$ such that

$$a^2x^2 - y^2 \equiv 0 \mod p.$$

(b) For the x and y in part (a), prove that $p = x^2 + y^2$. This shows that every prime $p \equiv 1 \mod 4$ is the sum of two squares.
(c) Prove that no prime $p \equiv 3 \mod 4$ is the sum of two squares.

Proof.
(a) Since $q!$ and p are relatively prime then by Exercise 5.21 there are integers x and y satisfying $0 < x < \sqrt{p}$ and $0 < |y| < \sqrt{p}$ such that $ax \equiv y \mod p$. Hence p divides $ax - y$, which divides $a^2x^2 - y^2$ and so $a^2x^2 - y^2 \equiv 0 \mod p$.
(b) By Exercise 5.9, $a^2 \equiv -1 \mod p$ and so $-x^2 - y^2 \equiv 0 \mod p$. This implies $p \mid x^2 + y^2$. However, since $0 < x < \sqrt{p}$ and $0 < y < \sqrt{p}$ then $0 < x^2 + y^2 < 2p$, forcing $p = x^2 + y^2$.
(c) Given any integers a and b then

$$a^2, b^2 \equiv 0, 1 \mod 4.$$

Thus

$$a^2 + b^2 \equiv 0, 1, 2 \not\equiv 3 \mod 4.$$

That is if $p \equiv 3 \mod 4$ then p cannot be expressed as the sum of two sqaures. □

Chapter 6
Finite Abelian Groups and Their Characters

Exercise 6.1. Let G be a set of nth roots of a nonzero complex number. If G is a group under multiplication, prove that G is the group of nth roots of unity.

Proof. For $x \neq 0$ define $G_x = \{z \in \mathbb{C} \mid z^n = x\}$ and assume G_x is a group. If $z, w \in G_x$, then by closure $z^n w^n = x$. Since $z^n = x = w^n$ we also have $z^n w^n = x^2$. Thus $x^2 = x$, and hence $x = 1$. Direct verification shows G_1 is a group. □

Exercise 6.2. Let G be a finite group of order n with identity element e. If $a_1, \ldots, a_n$ are n elements of G, not necessarily distinct, prove that there are integers p and q with $1 \leq p \leq q \leq n$ such that $a_p a_{p+1} \cdots a_q = e$.

Proof. Let $A = \{a_1, a_2, \ldots, a_n\}$ and define $b_i = a_1 a_2 \cdots a_i$ for $1 \leq i \leq n$. If $b_k = e$ for some k, we are done. Otherwise, by the pigeonhole principle there exists q and p such that $p < q$ and $b_q = b_p$. Thus $b_q b_p^{-1} = e$, or in other words $a_{p+1} \cdots a_q = e$. □

Remark. Taking $G = (\mathbb{Z}/n\mathbb{Z}, +)$ proves Exercise 5.1.

Exercise 6.3. Let G be the set of all 2×2 matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, where a, b, c, d are integers with $ad - bc = 1$. Prove that G is a group under matrix multiplcation. This group is sometimes called the *modular group*.

Proof. The condition $ad - bc = 1$ is equivalent to having determinant 1. We now show G satisfies the group axioms.

- *Closure*: If $A, B \in G$ then $\det(A) = \det(B) = 1$. Since the determinant is multiplicative, $\det(AB) = \det(A)\det(B) = 1$ and so $AB \in G$.
- *Associativity*: Matrix multiplication is associative, which can be verified directly.
- *Existence of identity*: Since $\det(I_2) = 1$, $I_2 \in G$.
- *Existence of inverses*: If $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$, let $B = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$. We have $\det(B) = ad - bc = 1$ and thus $B \in G$. Observe $AB = I_2$, which means $B = A^{-1} \in G$. □

Exercise 6.4. Let $G = \langle a \rangle$ be a cyclic group generated by a. Prove that every subgroup of G is cyclic. (It is not assumed G is finite.)

Proof. Let $1 < H \leq G$ and m be the smallest positive integer such that $a^m \in H$. If $b \in H$ then $b = a^n$ for some $n \in \mathbb{Z}$, as $b \in G$.

If $n = qm + r$, where $0 \leq r < m$, then $a^n = (a^m)^q a^r$. This implies $a^r = (a^m)^{-q} a^n \in H$. By the minimality of m, we must have $r = 0$ and so $a^n = (a^m)^q$. Therefore $H = \langle a^m \rangle$. □

Exercise 6.5. Let G be a finite group of order n and let G' be a subgroup of order m. Prove $m \mid n$ (Lagrange's theorem). Deduce that the order of every element of G divides n.

Lemma 6.5. For $G' \leq G$, the set $P = \{xG' \mid x \in G\}$ partitions G.

Proof of Lemma. Pick $x, y \in G$ such that $xG' \cap yG' \neq \emptyset$. This means there are $g_1, g_2 \in G'$ such that $xg_1 = yg_2$. Multiplying both sides by g_1^{-1} gives

$$x = g_1^{-1} y g_2 = y g_3, \quad \text{where } g_3 \in G'.$$

Now for any element $g \in G'$, $xg = y(g_3 g) \in yG'$, thus $xG' \subseteq yG'$. Similarly $yG' \subseteq xG'$ and hence $xG' = yG'$. This means either $xG' = yG'$ or $xG' \cap yG' = \emptyset$. □

Proof of Exercise. For any $x \in G$, since x is invertible, the set xG' has order $|G'|$. By Lemma 6.5 $\{xG' \mid x \in G\}$ partitions G, and thus $|G| = k|G'|$ for some integer k.

Now choose $x \in G$ and let $n = |x| = |\langle x \rangle|$. By Lagrange's theorem, $|\langle x \rangle|$ divides $|G|$. □

Exercise 6.6. Let G be a finite group of order 6 with identity element e. Prove that either G is cyclic, or else there are two elements a and b in G such that

$$G = \{a, a^2, a^3, b, ab, a^2 b\},$$

with $a^3 = b^2 = e$. Which of these elements is ba?

Proof. By Exercise 6.8 (Cauchy's theorem) there exists $a, b \in G$ such that $|a| = 3$ and $|b| = 2$. We have $b \notin \langle a \rangle$ since $2 \nmid |\langle a \rangle|$. Furthermore, $b \in \langle a \rangle b$ and so by Lemma 6.5 $\langle a \rangle \cap \langle a \rangle b = \emptyset$. This means $G = \langle a \rangle \cup \langle a \rangle b = \{e, a, a^2, b, ab, a^2 b\}$, whether G is cyclic or not.

Assuming G is not cyclic we now rule out cases to conclude $ba = a^2 b$.

- Supposing $ba = e$, then multiplying both sides by b yields $a = b$, a contradiction.
- Supposing $ba = a$, then multiplying both sides by a^2 yields $b = e$, a contradiction.
- Supposing $ba = a^2$, then multiplying both sides by a^2 yields $b = a$, a contradiction.
- Supposing $ba = b$, then multiplying both sides by b yields $a = e$, a contradiction.
- If $ba = ab$, then G is abelian. This would mean $(ab)^2 = a^2 b^2 = a^2$ and $(ab)^3 = a^3 b^3 = b$, which implies $|ab| = 6$. This is a contradiction since $G \neq \langle ab \rangle$. □

Exercise 6.7. A group table for a finite group $G = \{a_1, \ldots, a_n\}$ of order n is an $n \times n$ matrix whose ij-entry is $a_i a_j$. If $a_i a_j = e$ prove that $a_j a_i = e$. In other words, the identity element is symmetrically located in the group table. Deduce that if n is even the equation $x^2 = e$ has an even number of solutions.

Proof. Suppose $a_i a_j = e$. Then

$$a_i(a_j a_i) = (a_i a_j)a_i = a_i,$$

and multiplying both sides by a_i^{-1} shows $a_j a_i = e$.

Now given $a_i \in G$, there is a unique $a_j \in G$ such that $a_i a_j = e$, hence the number of times e appears in the group table is n. By symmetry, the number e's above the main diagonal is the same as the number of e's below the main diagonal. Adding these thus produces an even number. Since n is even, the number of e's on the main diagonal must be even too. That is to say the number of solutions to $x^2 = e$ is even. □

Exercise 6.8. Generalizing Exercise 6.7, let $f(p)$ denote the number of solutions of the equation $x^p = e$, where p is a prime divisor of n, the order of G. Prove that $p \mid f(p)$ (Cauchy's theorem). [*Hint*: Consider the set S of ordered p-tuples $(a_1, \ldots, a_p)$ such that $a_i \in G$ and $a_1 \cdots a_p = e$. There are n^{p-1} p-tuples in S. Call two such p-tuples equivalent if one is a cyclic permutation of the other. Show that $f(p)$ equivalence classes contain exactly one member and that each of the others contains exactly p members. Count the number of members of S in two ways and deduce $p \mid f(p)$.]

Proof. Following the hint, let $(a_1, \ldots, a_p) \in S$. Since every element of G is invertible, we can choose $a_1, \ldots, a_{p-1}$ freely, which forces $a_p = (a_1 \cdots a_{p-1})^{-1}$. This implies $|S| = n^{p-1}$, since there are n choices for each freely chosen a_i.

Define $\phi : S \to S$ such that $\phi\big((a_1, \ldots, a_p)\big) = (a_2, \ldots, a_p, a_1)$. For $A, B \in S$, we say $A \sim B$ if $B = \phi^m(A)$ for some m. Let $[A] = \{B \in S \mid A \sim B\}$.

Suppose for $A = (a_1, \ldots, a_p)$, $\phi^m(A) = A$ for some $0 < m < p$. By Exercise 1.25, there exists $x > 0$ and $y > 0$ such that $mx - py = 1$. Since $\phi^{-yp} = \mathrm{id}$,

$$\phi(A) = \phi^{mx-py}(A) = \phi^{mx}(\phi^{-py}(A)) = \phi^{mx}(A) = A.$$

Therefore

$$a_1 = a_2, a_2 = a_3, \ldots, a_p = a_1.$$

This means $A = (x, x, \ldots, x)$ for some $x \in G$, and so $|[A]| = 1$. Furthermore there are $f(p)$ many $[A]$ such that $|[A]| = 1$.

Now suppose $\phi^m(A) \neq A$ for all $0 < m < p$. If $1 \leq k \leq j < p$ and $\phi^j(A) = \phi^k(A)$, then $\phi^{j-k}(A) = A$. This means $j - k = 0$ and so each $\phi^i(A)$ is unique. This shows $|[A]| = p$.

Thus partitioning S by $\sim$ implies

$$n^{p-1} = ps + f(p).$$

Since $p \mid n$, we see $p \mid f(p)$. □

Exercise 6.9. Let G be a finite group of order n. Prove that n is odd if, and only if, each element of G is square. That is, for each a in G there is an element b in G such that $a = b^2$.

Proof. Let $n = 2m+1$, $x \in G$ and $y = x^{-1}$. Then by Exercise 6.5 (Lagrange's theorem), $|y|$ divides $2m+1$ and so

$$x = xy^{2m+1} = (y^m)^2 .$$

Conversely, suppose every element in G is a square. This means the map $\phi : G \to G$ defined by $\phi(g) = g^2$ is surjective. Therefore the only solution to $x^2 = e$ is $x = e$. Hence G does not contain an element of order 2, so by Exercise 6.8 (Cauchy's theorem) n is odd. □

Exercise 6.10. State and prove a generalization of Exercise 6.9 in which the condition "n is odd" is replaced by "n is relatively prime to k" for some $k \geq 2$.

Statement: Let G be a finite group of order n. Prove that n is relatively prime to k if and only if each element of G is a kth power.

Proof. Suppose $(n, k) = 1$ and $n = km + r$ for $0 < r < k$. Let $x \in G$ and $y = x^{-1}$. Then by Exercise 6.5 (Lagrange's theorem), $|y|$ divides $km + r$ and so

$$x^r = x^r y^{km+r} = (y^m)^k .$$

There are a and b such that $ar + bk = 1$ and so

$$x = x^{ar+bk} = (y^{am})^k (x^b)^k = (y^{am} x^b)^k = (x^{b-am})^k.$$

Conversely, suppose every element in G is a kth power. This means the map $\phi : G \to G$ defined by $\phi(g) = g^k$ is surjective. Therefore the only solution to $x^k = e$ is $x = e$. This implies for any prime divisor p of k, the only solution to $x^p = e$ is $x = e$. Hence G does not contain an element of order p, so by Exercise 6.8 (Cauchy's theorem), $p \nmid n$. We conclude $(n, k) = 1$. □

Exercise 6.11. Let G be a finite group of order n, and let S be a subset containing more than $n/2$ elements of G. Prove that for each g in G there exist elements a and b in S such that $ab = g$.

Proof. Suppose for some $g \in G$ that $ab \neq g$ for all $a, b \in S$. We have

$$G = \{g_1, \ldots, g_j, h_1, \ldots, h_k\}, \text{ where } g_i^2 = g \text{ and } h_i^2 \neq g.$$

By the hypothesis we have $g_i \notin S$ and so $S \subseteq \{h_i\}$. Now for each h_i there is a unique $h_j \neq h_i$ such that $h_i h_j = g$. Therefore if $h_i \in S$, then $h_j \notin S$. Thus pairing the h_i accordingly gives $|S| \leq |\{h_i\}|/2 \leq n/2$. □

Exercise 6.12. Let G be a group and let S be a subset of n distinct elements of G with the property that $a \in S$ implies $a^{-1} \notin S$. Consider the n^2 product (not necessarily distinct) of the form ab, where $a \in S$ and $b \in S$. Prove that at most $n(n-1)/2$ of these products belong to S.

Proof. Consider the $n^2 - n$ pairs $a, c \in S$ such that $a \neq c$. If there exists $b \in S$ such that $ab = c$, then $cb^{-1} = a$, where $b^{-1} \notin S$. That is to say if $ab = c$ for $a, b, c \in S$, then there is no element $x \in S$ such that $cx = a$. This means at most half of these pairs have $b \in S$ such that $ab = c$. Additionally note if $a = c$, then there is no $b \in S$ such that $ab = c$. □

Exercise 6.13. Let $f_1, \ldots, f_m$ be the characters of a finite group G of order m, and let a be an element of G of order n. Theorem 6.7 shows that each number $f_r(a)$ is an nth root of unity. Prove that every nth root of unity occurs equally often among the numbers $f_1(a), f_2(a), \ldots, f_m(a)$. [*Hint*: Evaluate the sum

$$\sum_{r=1}^{m} \sum_{k=1}^{n} f_r(a^k) e^{-2\pi i k/n}$$

in two ways to determine the number of times $e^{2\pi i/n}$ occurs.]

Proof. Define $e(x) = e^{2\pi i x}$ and let S be the sum from the hint. Changing order of summation we have

$$S = \sum_{k=1}^{n} e(-k/n) \sum_{r=1}^{m} f_r(a^k).$$

By Theorem 6.13, since $|a| = n$, the inner sum is 0 if $k < n$ and m if $k = n$. Hence

$$S = me(n/n) = m.$$

On the other hand if $f_r(a) = e(j_r/n)$, we have

$$S = \sum_{r=1}^{m} \sum_{k=1}^{n} e\left(\frac{j_r - 1}{n}\right)^k.$$

The inner sum is geometric and evaluates to n if $j_r = 1$ and 0 otherwise. Coupling this with $S = m$ tells us $e(1/n)$ occurs exactly m/n times within $f_1(a), f_2(a), \ldots, f_m(a)$.

Next, replace $e(-k/n)$ in S with $e(-kx/n)$ for $1 \leq x \leq n$. Applying the same technique shows $e(x/n)$ occurs exactly m/n times within $f_1(a), f_2(a), \ldots, f_m(a)$. □

Remark. This exercise provides an alternate proof that the order of any element of a finite group divides the order of the group.

Exercise 6.14. Construct tables showing the values of all the Dirichlet characters mod k for $k = 8$, 9, and 10.

Solution. We construct the tables in Mathematica.

```
apostolCh6Num14Format[Table[
  DirichletCharacter[#, j, Range[#]], {j, 1, EulerPhi[#]}
]& /@ {8, 9, 10}]
```

$\chi(n) \bmod 8$

1	0	1	0	1	0	1	0
1	0	−1	0	−1	0	1	0
1	0	−1	0	1	0	−1	0
1	0	1	0	−1	0	−1	0

$\chi(n) \bmod 9$

1	1	0	1	1	0	1	1	0
1	$e^{\frac{i\pi}{3}}$	0	$e^{\frac{2i\pi}{3}}$	$e^{-\frac{i\pi}{3}}$	0	$e^{-\frac{2i\pi}{3}}$	−1	0
1	$e^{\frac{2i\pi}{3}}$	0	$e^{-\frac{2i\pi}{3}}$	$e^{-\frac{2i\pi}{3}}$	0	$e^{\frac{2i\pi}{3}}$	1	0
1	−1	0	1	−1	0	1	−1	0
1	$e^{-\frac{2i\pi}{3}}$	0	$e^{\frac{2i\pi}{3}}$	$e^{\frac{2i\pi}{3}}$	0	$e^{-\frac{2i\pi}{3}}$	1	0
1	$e^{-\frac{i\pi}{3}}$	0	$e^{-\frac{2i\pi}{3}}$	$e^{\frac{i\pi}{3}}$	0	$e^{\frac{2i\pi}{3}}$	−1	0

$\chi(n) \bmod 10$

1	0	1	0	0	0	1	0	1	0
1	0	$-i$	0	0	0	i	0	−1	0
1	0	−1	0	0	0	−1	0	1	0
1	0	i	0	0	0	$-i$	0	−1	0

Exercise 6.15. Let χ be any nonprincipal character mod k. Prove that for all integers $a < b$ we have

$$\left|\sum_{n=a}^{b} \chi(n)\right| \leq \frac{1}{2}\varphi(k).$$

Proof. For this exercise assume $1 \leq a, b \leq k$, since the sum has period k. Suppose there are at most $\varphi(k)/2$ numbers relatively prime to k inclusively between a and b. Then

$$\begin{aligned}\left|\sum_{n=a}^{b} \chi(n)\right| &\leq \sum_{n=a}^{b} |\chi(n)| \\ &= \sum_{\substack{a\leq n\leq b \\ (n,k)=1}} 1 \\ &\leq \varphi(k)/2.\end{aligned}$$

Suppose there are more than $\varphi(k)/2$ numbers relatively prime to k inclusively between a and b. This means there are less than $\varphi(k)/2$ numbers n relatively prime to k where $1 \leq n < a$ or $b < n \leq k$. Since χ is nonprincipal we have $\sum_{n=1}^{k} \chi(n) = 0$, thus

$$\begin{aligned}\left|\sum_{n=a}^{b} \chi(n)\right| &= \left|-\sum_{n=1}^{a-1} \chi(n) - \sum_{n=b+1}^{k} \chi(n)\right| \\ &\leq \sum_{n=1}^{a-1} |\chi(n)| + \sum_{n=b+1}^{k} |\chi(n)| \\ &= \sum_{\substack{1\leq n<a \\ (n,k)=1}} 1 + \sum_{\substack{b<n\leq k \\ (n,k)=1}} 1 \\ &< \varphi(k)/2.\end{aligned}$$

□

Exercise 6.16. If χ is a real-valued character mod k then $\chi(n) = \pm 1$ or 0 for each n, so the sum

$$S = \sum_{n=1}^{k} n\chi(n)$$

is an integer. This exercise shows that $12S \equiv 0 \bmod k$.
(a) If $(a, k) = 1$ prove that $a\chi(a)S \equiv S \bmod k$.
(b) Write $k = 2^\alpha q$ where q is odd. Show that there is an integer a with $(a, k) = 1$ such that $a \equiv 3 \bmod 2^\alpha$ and $a \equiv 2 \bmod q$. Then use (a) to deduce that $12S \equiv 0 \bmod k$.

Proof.
(a) Given $(a, k) = 1$, for each $1 \leq m \leq k$ there is a unique n such that $am \equiv n \bmod k$ and $1 \leq n \leq k$. Moreover, since χ has period k, $\chi(am) = \chi(n)$. Thus summing over all am for $1 \leq m \leq k$ gives

$$\sum_{m=1}^{k} am\chi(am) \equiv \sum_{n=1}^{k} n\chi(n) \mod k.$$

Using the fact that χ is completely multiplicative implies $a\chi(a)S \equiv S \bmod k$.
(b) By the Chinese remainder theorem, there is an a such that $a \equiv 3 \bmod 2^\alpha$ and $a \equiv 2 \bmod q$. Additionally since a is relatively prime to 2^α and q, it must be relatively prime to $k = 2^\alpha q$.

By (a) we know $(a\chi(a) - 1)S \equiv 0 \bmod k$. We will use this to show 2^α and q both divide $12S$. If $\alpha < 3$, it's clear $2^\alpha \mid 12S$. Otherwise, we know $\alpha \geq 3$. Then since $a \equiv 3 \bmod 2^\alpha$,

$$(a\chi(a) - 1)S \equiv \begin{cases} 2S \mod 2^\alpha & \text{if } \chi(a) = 1 \\ -4S \mod 2^\alpha & \text{if } \chi(a) = -1. \end{cases}$$

Since $2^\alpha \mid (a\chi(a) - 1)S$, we must have $2^{\alpha-2} \mid S$. This implies $2^\alpha \mid 12S$.

From (a) we have $q \mid (a\chi(a) - 1)S$. Since $a \equiv 2 \bmod q$,

$$(a\chi(a) - 1)S \equiv \begin{cases} S \mod q & \text{if } \chi(a) = 1 \\ -3S \mod q & \text{if } \chi(a) = -1. \end{cases}$$

Thus if $3 \mid q$ we must have $(q/3) \mid S$ and if $3 \nmid q$ we have $q \mid S$. Both cases imply $q \mid 12S$.

By Theorem 5.9, $12S \equiv 0 \bmod 2^\alpha$ and $12S \equiv 0 \bmod q$ imply $12S \equiv 0 \bmod k$. □

Exercise 6.17. An arithmetical function f is called *periodic* mod k if $k > 0$ and $f(m) = f(n)$ whenever $m \equiv n \bmod k$. The integer k is called a *period* of f.
(a) If f is periodic mod k, prove that f has a smallest positive period k_0 and that $k_0 \mid k$.
(b) Let f be a periodic and completely multiplicative, and let k be the smallest positive period of f. Prove that $f(n) = 0$ if $(n, k) > 1$. This shows that f is a Dirichlet character mod k.

Proof.
(a) If f is periodic, by the well ordering principal there is a smallest positive period k_0. Let $g = (k, k_0)$. Since g can be expressed as a linear combination of k and k_0, f has a period of

g. The minimality of k_0, thus forces $g = k_0$. Hence $k_0 \mid k$.
(b) Suppose there is a prime p that divides both n and k. Then for any integer m,

$$f(p)f(m) = f(pm) = f(pm + k) = f(p)f(m + k/p).$$

This implies $f(p) = 0$ since otherwise f would have a smaller period k/p. Thus since $p \mid n$ and f is completely multiplicative, $f(n) = 0$. □

Exercise 6.18.(++)
(a) Let f be a Dirichlet character mod k. If k is squarefree, prove that k is the smallest positive period of f.
(b) Give an example of a Dirichlet character mod k for which k is not the smallest positive period of f.

Lemma 6.18. Let $\chi(n;k)$ denote $\chi(n)$ mod k. If $k = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ then there are characters χ_j mod $p_j^{\alpha_j}$ such that

$$\chi(n;k) = \prod_{j=1}^{r} \chi_j(n; p_j^{\alpha_j}) \quad \text{for all } n.$$

Proof of Lemma. For each j, by the Chinese remainder theorem there is a unique n_j mod k satisfying

$$n_j \equiv n \mod p_j^{\alpha_j} \quad \text{and} \quad n_j \equiv 1 \mod p_i^{\alpha_i} \quad \text{for } i \neq j.$$

Given a character $\chi(n;k)$, define $\chi_j(n) = \chi(n_j;k)$. It is clear χ_j is completely multiplicative. Furthermore since solving the simultaneous congruences

$$x \equiv n + p_j^{\alpha_j} \mod p_j^{\alpha_j} \quad \text{and} \quad n_j \equiv 1 \mod p_i^{\alpha_i}$$

gives $x \equiv n_j$ mod k, we have $\chi_j(n+p_j^{\alpha_j}) = \chi_j(n)$. Thus by Exercise 6.17 (b) χ_j is a Dirichlet character whose smallest period is at most $p_j^{\alpha_j}$. We then have

$$\prod_{j=1}^{r} \chi_j(n; p_j^{\alpha_j}) = \prod_{j=1}^{r} \chi(n_j;k) = \chi\left(\prod_{j=1}^{r} n_j; k\right).$$

By construction $\prod_{j=1}^{r} n_j \equiv n$ mod $p_j^{\alpha_j}$ for each j and so by Theorem 5.9 $\prod_{j=1}^{r} n_j \equiv n$ mod k, which proves the lemma. □

Proof of Exercise.
(a) Let $k = p_1 \cdots p_r$ be squarefree and choose a charachter χ mod k. By Lemma 6.18 there are characters χ_j mod p_j such that

$$\chi(n;k) = \prod_{j=1}^{r} \chi_j(n; p_j).$$

Let q be a proper divisor of k. Applying the Chinese remainder theorem, pick a such that $a \equiv 1$ mod p_j if $p_j \mid q$ and $a \equiv 0$ mod p_j otherwise. This gives $(a,k) > 1$ and so $\chi(a) = 0$. However if $(p_j, q) = 1$ then $(a+q, p_j) = 1$, i.e. $\chi_j(a+q; p_j) \neq 0$. Additionally if $p_j \mid q$ then

$$\chi_j(a+q; p_j) = \chi_j(a; p_j) = 1.$$

This implies $\chi(a+q;k) \neq 0$, so we conclude the smallest period of χ is k.
(b) It can be seen in Exercise 6.14 that χ_3 mod 8 has period 4. □

Chapter 7
Dirichlet's Theorem on Primes in Arithmetic Progressions

In Exercises 1 through 8, h and k are given positive integers, $(h,k)=1$, and $A(h,k)$ is the arithmetic progession $A(h,k)=\{h+kx \mid x=0,1,2,\ldots\}$. Exercises 1 through 4 are to be solved without Dirichlet's theorem.

Exercise 7.1. Prove that, for every integer $n \geq 1$, $A(h,k)$ contains infinitely many numbers relatively prime to n.

Proof. Let p denote a prime and define

$$\begin{aligned} A &= \{p : p \mid n,\ p \mid k\ \ (\Rightarrow p \nmid h)\},\\ B &= \{p : p \mid n,\ p \mid h\ \ (\Rightarrow p \nmid k)\},\\ C &= \{p : p \mid n,\ p \nmid kh\}. \end{aligned}$$

Notice A, B, and C partition the prime divisors of n. For a set S, define $P_S = \prod_{p\in S} p$, then by the Chinese remainder theorem there are infinitely many x simultaneously satisfying

$$\begin{aligned} x &\equiv 1 \mod P_A\\ x &\equiv 1 \mod P_B\\ x &\equiv 0 \mod P_C. \end{aligned}$$

We then have

$$kx+h \equiv \begin{cases} h \mod p & \text{if } p \in A\\ k \mod p & \text{if } p \in B\\ h \mod p & \text{if } p \in C. \end{cases}$$

This means if $p \mid n$ then $p \nmid kx+h$, which implies $(kx+h,n)=1$. □

Exercise 7.2. Prove that $A(h,k)$ contains an infinite subset $\{a_1,a_2,\ldots\}$ such that $(a_i,a_j)=1$ if $i \neq j$.

Proof. Construct this infinite subset S as follows. Let $a_1 = h$. Next suppose we have constructed $\{a_1,a_2,\cdots a_n\} \subset S$. By Exercise 7.1 there is a number $a_{n+1} \in A(h,k)$ such that

$$\left(a_{n+1}, \prod_{i=1}^{n} a_i\right) = 1.$$

This implies $(a_{n+1}, a_i) = (a_i, a_{n+1}) = 1$ for any $i \leq n$. We let a_{n+1} be a member of S and continue this process indefinitely. □

Exercise 7.3. Prove that $A(h,k)$ contains an infinite subset which forms a geometric progression (a set of numbers of the form ar^n, $n = 0, 1, 2, \ldots$). This implies $A(h,k)$ contains infinitely many numbers having the same prime factors.

Proof. Since $h(k+1)^n \equiv h \bmod k$, we see $h(k+1)^n \in A(h,k)$ for all $n \geq 0$. □

Exercise 7.4. Let S be any infinite subset of $A(h,k)$. Prove that for every positive integer n there is a number in $A(h,k)$ which can be expressed as a product of more than n different elements of S.

Proof. Let $S = \{s_1, s_2, \ldots\} \subseteq A(h,k)$. We have for any $m \in \mathbb{N}$ that

$$S_m := \prod_{i=1}^{m\varphi(k)+1} s_i \equiv \prod_{i=1}^{m\varphi(k)+1} h \equiv h \mod k.$$

Hence $S_m \in A(h,k)$ and taking any $m > (n-1)/\varphi(k)$ gives $m\varphi(k) + 1 > n$. □

Exercise 7.5. Dirichlet's theorem implies the following statement: If h and $k > 0$ are any two integers with $(h,k) = 1$, then there exists at least one prime number of the form $kn + h$. Prove that this statement also implies Dirichlet's theorem.

Proof. Assume the hypothesis of the exercise and suppose Dirichlet's theorem is false. Then there are integers h, k, and p such that $(h,k) = 1$ and p is the largest prime in $A(h,k)$. Defining $h' = k + p$ and $k' = pk$, it's clear $(h', p) = (h', k) = 1$ and so $(h', k') = 1$. Moreover observe $A(h', k') \subset A(h,k)$. Therefore since the smallest element in $A(h', k')$ is $k + p > p$, every element in $A(h', k')$ must be composite. This is a contradiction, which means Dirichlet's theorem must be true. □

Exercise 7.6. If $(h,k) = 1$, $k > 0$, prove that there is a constant A (depending on h and on k) such that, if $x \geq 2$,

$$\sum_{\substack{p \leq x \\ p \equiv h \bmod k}} \frac{1}{p} = \frac{1}{\varphi(k)} \log\log x + A + O\left(\frac{1}{\log x}\right).$$

Proof. Let $f(x) = 1/\log x$ and $a(n) = \log(n)/n$ if $n \equiv h \bmod k$ is prime and 0 otherwise. By Dirichlet's Theorem,

$$\sum_{n \leq x} a(n) = \frac{1}{\varphi(k)} \log x + R(x), \quad \text{where } R(x) = O(1).$$

Applying Abel's summation formula,

$$\begin{aligned}\sum_{\substack{p\le x\\ p\equiv h \mod k}}\frac{1}{p} &= \sum_{1<n\le x} a(n)f(n)\\ &= \frac{1}{\log x}\left(\frac{1}{\varphi(k)}\log x + O(1)\right) + \int_2^x \frac{1}{t\log^2 t}\left(\frac{1}{\varphi(k)}\log t + R(t)\right)dt\\ &= \frac{1}{\varphi(k)} + O\left(\frac{1}{\log x}\right) + \frac{1}{\varphi(k)}\int_2^x \frac{dt}{t\log t} + \int_2^\infty \frac{R(t)}{t\log^2 t}dt + \int_x^\infty \frac{R(t)}{t\log^2 t}dt\\ &= \frac{1}{\varphi(k)} + O\left(\frac{1}{\log x}\right) + \frac{\log\log x - \log\log 2}{\varphi(k)} + C + O\left(\int_x^\infty \frac{dt}{t\log^2 t}\right)\\ &= \frac{1}{\varphi(k)}\log\log x + A + O\left(\frac{1}{\log x}\right).\end{aligned}$$

□

Exercise 7.7. Construct an infinite set S of primes with the following property: If $p \in S$ and $q \in S$ then $(\frac{1}{2}(p-1), \frac{1}{2}(q-1)) = (p, q-1) = (p-1, q) = 1$.

Solution. Let $S = \{q_1, q_2, \ldots\}$ where $2 < q_1 < q_2 < \cdots$ and

$$q_{n+1} = 2t_n \prod_{\substack{p\le q_n\\ p \text{ prime}}} p \ - 1,$$

where t_n is chosen so that q_{n+1} is prime.

We now show S satisfies the required properties. Let $n > m$.

- Since $2 < q_m$ and $q_m \mid q_n + 1$, by linearity $q_m \nmid q_n - 1$, i.e. $(q_n - 1, q_m) = 1$.
- Since $q_m - 1 < q_n$, $q_n \nmid q_m - 1$, i.e. $(q_m - 1, q_n) = 1$.
- Let r be a prime divisor of $\frac{1}{2}(q_n - 1)$. Then by linearity r can't divide any prime less than or equal to q_{n-1}, and so $r > q_{n-1}$. This means $r \nmid \frac{1}{2}(q_m - 1)$ since

$$\frac{1}{2}(q_m - 1) < q_m \le q_{n-1}.$$

Therefore $(\frac{1}{2}(q_n - 1), \frac{1}{2}(q_m - 1)) = 1$.

Remark. Unfortunately, this is a very impractical solution. In a straightforward implementation, choosing $q_1 = 7$ means q_3 is a 170 digit integer! We show this in Mathematica.

```
In[1]:= q[1] = 7;
  Do[
    k = 2*Product[Prime[i], {i, 3, PrimePi[q[n - 1]]}];
    t = 1; While[!PrimeQ[k*t - 1], t++];
    q[n] = k*t - 1,
    {n, 2, 3}
  ];
  q /@ Range[3]
Out[1]= {7, 419, 41937675041365708 7≪134≫178028407044929539}
```

Exercise 7.8. Let f be an integer-coefficient polynomial of degree $n \geq 1$ with the following property: For each prime p there exists a prime q and an integer m such that $f(p) = q^m$. Prove that $q = p$, $m = n$ and $f(x) = x^n$ for all x. [*Hint*: If $q \neq p$ then q^{m+1} divides $f(p + tq^{m+1}) - f(p)$ for each $t = 1, 2, \ldots$.]

Proof. Suppose $f(p) = q^m$ for $p \neq q$ and $m > 0$ (we can find $m > 0$ since f can only equal 1 finitely many times). Applying binomial expansion,

$$q^{m+1} \mid f(p + tq^{m+1}) - f(p) \quad \text{for } t = 1, 2, \ldots \tag{10}$$

By Dirichlet's theorem, since $(p, q) = 1$, there are infinitely many primes of the form $p+tq^{m+1}$. Suppose $p + tq^{m+1}$ is prime, then $f(p + tq^{m+1}) = r^s$ for some prime r.

By (10), $r^s = q^m(aq+1)$ for some integer a. This means $q \mid r^s$, and so $q = r$. Furthermore, for both sides to have the same prime factorization, we require $a = 0$ which implies $s = m$. Thus $f(p + tq^{m+1}) = q^m$ for infinitely many t. This means $f \equiv q^m$, which contradicts $n \geq 1$. We conclude $p = q$, that is for any prime p, $f(p) = p^m$ for some m dependent on p.

Next, note

$$\lim_{k \to \infty} \frac{f(p_k)}{p_k^n} = C \quad \text{for some } C > 0,$$

and so for large enough p, $f(p) = p^n$. This implies $f(x) = x^n$, since a polynomial is determined by finitely many points. □

Chapter 8
Periodic Arithmetic Functions and Gauss Sums

Exercise 8.1. Let $x = e^{2\pi i/n}$ and prove that

$$\sum_{k=1}^{n-1} kx^k = \frac{n}{x-1}.$$

Lemma 8.1. If $x \neq 1$ then

$$\sum_{k=1}^{n-1} kx^k = \frac{n(x^{n+1} - x^n) - x^{n+1} + x}{(x-1)^2}.$$

Proof of Lemma. Given $x^n - 1 = (x-1)(x^{n-1} + \cdots + x + 1)$, then

$$\sum_{k=0}^{n-1} x^k = \frac{x^n - 1}{x - 1}.$$

Differentiating both sides with respect to x then multiplying both sides by x gives the result. □

Proof of Exercise. If $x = e^{2\pi i/n}$ then $x^n = 1$ and $x^{n+1} = x$. Thus by Lemma 8.1

$$\begin{aligned}\sum_{k=1}^{n-1} kx^k &= \frac{n(x^{n+1} - x^n) - x^{n+1} + x}{(x-1)^2} \\ &= \frac{n(x-1) - x + x}{(x-1)^2} \\ &= \frac{n}{x-1}.\end{aligned}$$

□

Exercise 8.2. Let $((x)) = x - [x] - \frac{1}{2}$ if x is not an integer, and let $((x)) = 0$ otherwise. Note that $((x))$ is a periodic function of x with period 1. If k and n are integers, with $n > 0$, prove that

$$\left(\left(\frac{k}{n}\right)\right) = -\frac{1}{2n} \sum_{m=1}^{n-1} \cot\frac{\pi m}{n} \sin\frac{2\pi km}{n}. \tag{11}$$

Lemma 8.2. If $k > 0$ then

$$\sin(2k+1)x = \sin x + 2\sin x \sum_{j=1}^{k} \cos 2jx.$$

Proof of Lemma. Applying a product to sum identity we have

$$2\sin x \sum_{j=1}^{k} \cos 2jx = \sum_{j=1}^{k} (\sin(2j+1)x - \sin(2j-1)x) = \sin(2k+1)x - \sin x,$$

where the intermediate sum telescopes. □

Proof of Exercise. If $n \mid k$ then both sides in (11) are 0, so we can assume $n \nmid k$. Now by Exercise 3.13 (c) $((k/n)) = -((-k/n))$, and since sin is also odd, we can reduce the problem to the case where $k > 0$.

Let $x = \frac{\pi m}{n}$ and assume $n \nmid k$ and $k > 0$. Applying a product to sum identity gives

$$\begin{aligned}
\cot x \sin 2kx &= \frac{\cos x \sin 2kx}{\sin x} \\
&= \frac{\sin(2k+1)x + \sin(2k-1)x}{2\sin x} \\
&= 1 - \cos 2kx + 2\sum_{j=1}^{k} \cos 2jx,
\end{aligned}$$

where Lemma 8.2 was applied. Furthermore, since $\cos 2\pi x = \operatorname{Re}(e^{2\pi i x})$ we have

$$\sum_{m=1}^{n-1} \cos \frac{2\pi jm}{n} = \begin{cases} n-1 & \text{if } n \mid j \\ -1 & \text{otherwise.} \end{cases}$$

Therefore

$$\begin{aligned}
\sum_{m=1}^{n-1} \cot \frac{\pi m}{n} \sin \frac{2\pi km}{n} &= \sum_{m=1}^{n-1} \left(1 - \cos \frac{2\pi km}{n} + 2\sum_{j=1}^{k} \cos \frac{2\pi jm}{n}\right) \\
&= (n-1) - (-1) + 2\sum_{j=1}^{k} \sum_{m=1}^{n-1} \cos \frac{2\pi jm}{n} \\
&= n + 2\left((n-1)\left\lfloor \frac{k}{n} \right\rfloor + (-1)\left(k - \left\lfloor \frac{k}{n} \right\rfloor\right)\right) \\
&= n + 2n\left\lfloor \frac{k}{n} \right\rfloor - 2k.
\end{aligned}$$

Dividing both sides by $-2n$ proves (11). □

Exercise 8.3. Let $c_k(n)$ denote Ramanujan's sum and let $M(x) = \sum_{n \le x} \mu(n)$, the partial sums of the Möbius function.
(a) Prove that

$$\sum_{k=1}^{n} c_k(m) = \sum_{d|m} dM\left(\frac{n}{d}\right).$$

In particular, when $n = m$, we have

$$\sum_{k=1}^{m} c_k(m) = \sum_{d|m} dM\left(\frac{m}{d}\right).$$

(b) Use (a) to deduce that

$$M(m) = m \sum_{d|m} \frac{\mu(m/d)}{d} \sum_{k=1}^{d} c_k(d).$$

(c) Prove that

$$\sum_{m=1}^{n} c_k(m) = \sum_{d|k} d\mu\left(\frac{k}{d}\right)\left[\frac{n}{d}\right].$$

Proof.
(a) By Theorem 8.6, $c_k(m) = \sum_{d|(m,k)} d\mu\left(\frac{k}{d}\right)$. Thus

$$\sum_{k=1}^{n} c_k(m) = \sum_{k=1}^{n} \sum_{d|(m,k)} d\mu\left(\frac{k}{d}\right) = \sum_{k=1}^{n} \sum_{\substack{d|m \\ d|k}} d\mu\left(\frac{k}{d}\right).$$

For a fixed divisor d of m we must sum over all those k in the range $1 \le k \le n$ which are multiples of d. If we write $k = qd$, it's equivalent to sum over all q where $1 \le q \le n/d$. Therefore

$$\sum_{k=1}^{n} \sum_{\substack{d|m \\ d|k}} d\mu\left(\frac{k}{d}\right) = \sum_{d|m} \sum_{q \le n/d} d\mu(q) = \sum_{d|m} dM\left(\frac{n}{d}\right).$$

(b) By (a)

$$\frac{1}{m} \sum_{k=1}^{m} c_k(m) = \sum_{d|m} \frac{1}{m/d} M\left(\frac{m}{d}\right).$$

Applying Möbius inversion gives

$$\frac{1}{m} M(m) = \sum_{d|m} \frac{\mu(m/d)}{d} \sum_{k=1}^{d} c_k(d).$$

(c) Just as in (a)

$$\sum_{m=1}^{n} c_k(m) = \sum_{m=1}^{n} \sum_{\substack{d|m \\ d|k}} d\mu\left(\frac{k}{d}\right).$$

This time fixing a divisor d of k, we must sum over all those m in the range $1 \leq m \leq n$ which are multiples of d. If we write $m = qd$, it's equivalent to sum over all q where $1 \leq q \leq n/d$. Therefore

$$\sum_{m=1}^{n} \sum_{\substack{d|m \\ d|k}} d\mu\left(\frac{k}{d}\right) = \sum_{d|k} \sum_{q \leq n/d} d\mu\left(\frac{k}{d}\right) = \sum_{d|k} d\mu\left(\frac{k}{d}\right) \left\lfloor \frac{n}{d} \right\rfloor.$$

□

Exercise 8.4. Let n, a, d be given integers with $(a, d) = 1$. Let $m = a + qd$ where q is the product (possibly empty) of all primes which divide n but not a. Prove that

$$m \equiv a \mod d \quad \text{and} \quad (m, n) = 1.$$

Proof. Since $m = a + qd$, by defnition $m \equiv a \mod d$. Now suppose $p \mid n$ for some prime p. If $p \mid a$, then by definition $p \nmid qd$ and so by linearity $p \nmid m$. If $p \nmid a$ then again by definition $p \mid qd$ and so by linearity $p \nmid m$. Therefore $(m, n) = 1$. □

Exercise 8.5. Prove there exists no real primitive character χ mod k if $k = 2m$, where m is odd.

Proof. We show each character mod k is not primitive. Let χ be a character mod k and pick a and b such that $(a, k) = (b, k) = 1$ and $a \equiv b \mod m$. This implies a and b are odd. Hence if $a = b + rm$ for some r, then r must be even. This means $k \mid rm$, and so $a \equiv b \mod k$. From here $\chi(a) = \chi(b)$, which by Theorem 8.16 means m is an induced modulus of χ. □

Exercise 8.6. Let χ be a character mod k. If k_1 and k_2 are induced moduli for χ prove that so too is (k_1, k_2), their gcd.

Lemma 8.6. Let a be an integer such that $(a, k) = 1$ and $a \equiv 1 \mod (k_1, k_2)$. Then there are integers x and y such that $a = 1 + xk_1 + yk_2$ and $(1 + xk_1, k) = 1$.

Proof of Lemma. Let $g = (k_1, k_2)$ and $k = d_1 d_2$, where d_2 is the product of all primes dividing k_2 and $(d_1 k_1, k_2) = g$. There are integers t, u, and v such that $a = 1 + tg$ and $g = ud_1 k_1 + vk_2$. Letting $x = tud_1$ and $y = tv$ gives

$$a = 1 + xk_1 + yk_2.$$

Now by linearity $(1 + xk_1, d_1) = 1$. Additionally, using $1 + xk_1 = a - yk_2$, linearity shows

$$(1 + xk_1, k_2) = (a - yk_2, k_2) = (a, k_2) = 1.$$

This means $(1 + xk_1, d_2) = 1$, since k_2 and d_2 share prime divisors and it follows that $(1 + xk_1, d_1 d_2) = 1$. □

Proof of Exercise. Let $g = (k_1, k_2)$ and choose a such that $(a, k) = 1$ and $a \equiv 1 \mod g$. Then by Lemma 8.6, there are integers x and y such that $a = 1 + xk_1 + yk_2$ and $(1 + xk_1, k) = 1$. Since k_1 and k_2 are both induced moduli, we then have

$$\chi(1 + xk_1 + yk_2) = \chi(1 + xk_1) = \chi(1) = 1.$$

Therefore by definition g is an induced modulus. □

Exercise 8.7. Prove that the conductor of χ divides every induced modulus for χ.

Proof. Let k_1 be the conductor of χ and k_2 be an induced modulus for χ. By Exercise 8.6, (k_1, k_2) is also an induced modulus. Since $(k_1, k_2) \leq k_1$, the minimality of k_1 forces $k_1 = (k_1, k_2)$. Therefore $k_1 \mid k_2$. □

In Exercises 8 through 12, assume that $k = k_1 k_2 \cdots k_r$, where the positive integers k_i are relatively prime in pairs: $(k_i, k_j) = 1$ if $i \neq j$.

Exercise 8.8.
(a) Given any integer a, prove that there is an integer a_i such that

$$a_i \equiv a \mod k_i \quad \text{and } a_i \equiv 1 \mod k_j \quad \text{for all } j \neq i.$$

(b) Let χ be a character mod k. Define χ_i by the equation

$$\chi_i(a) = \chi(a_i),$$

where a_i is the integer of part (a). Prove that χ_i is a character mod k_i.

Proof. Replace $p_i^{\alpha_i}$ with k_i in Lemma 6.18. □

Exercise 8.9. Prove that every character χ mod k can be factored uniquely as a product of the form $\chi = \chi_1 \chi_2 \cdots \chi_r$, where χ_i is a character mod k_i.

Proof. Replace $p_i^{\alpha_i}$ with k_i in Lemma 6.18. □

Exercise 8.10.(+) Let $f(\chi)$ denote the conductor of χ. If χ has the factorization in Exercise 8.9, prove that $f(\chi) = f(\chi_1) \cdots f(\chi_r)$.

Proof. Choose a such that $(a, k) = 1$ and $a \equiv 1 \mod f(\chi_1) \cdots f(\chi_r)$. This implies $a \equiv 1 \mod f(\chi_i)$, thus $\chi_i(a) = 1$. This means

$$\chi(a) = \chi_1(a) \cdots \chi_r(a) = 1.$$

Hence $f(\chi_1) \cdots f(\chi_r)$ is an induced modulus for χ and therefore $f(\chi) \mid f(\chi_1) \cdots f(\chi_r)$.

Now define $e(x) = e^{2\pi i x}$ and choose a such that $(a, k) = 1$ and $a \equiv 1 \mod f(\chi)$. Since $f(\chi)$ is an induced modulus for χ and χ_i is a k_ith root of unity, there are c_i such that

$$\begin{aligned} 1 = \chi(a) &= \chi_1(a) \cdots \chi_r(a) \\ &= e\left(\frac{c_1}{k_1}\right) \cdots e\left(\frac{c_r}{k_r}\right) \\ &= e\left(\frac{1}{k_1 \cdots k_r} \sum_{m=1}^{r} c_m \prod_{j \neq m} k_j\right). \end{aligned}$$

This implies $k_i \mid \sum_{m=1}^{r} c_m \prod_{j \neq m} k_j$, and by linearity $k_i \mid c_i \prod_{j \neq i} k_j$. Since $(k_i, k_j) = 1$ for $j \neq i$ we have $k_i \mid c_i$, and so

$$1 = e(c_i/k_i) = \chi_i(a).$$

Therefore $f(\chi)$ is an induced modulus for χ_i, hence $f(\chi_i) \mid f(\chi)$. Moreover $(f(\chi_i), f(\chi_j)) = 1$ for $j \neq i$ implies $f(\chi_1) \cdots f(\chi_r) \mid f(\chi)$. We conclude $f(\chi) = f(\chi_1) \cdots f(\chi_r)$. □

Exercise 8.11.(+) If χ has the factorization in Exercise 8.9, prove that for every integer a we have

$$G(a,\chi) = \prod_{i=1}^{r} \chi_i\left(\frac{k}{k_i}\right) G(a_i,\chi_i),$$

where a_i is the integer of Exercise 8.8.

Lemma 8.11. If $k = k_1 k_2 \cdots k_r$, where k_i are pairwise relatively prime, then the set

$$\left\{ \sum_{i=1} \frac{m_i k}{k_i} \,\middle|\, 1 \le m_i \le k_i \right\}$$

runs through a complete system of residues mod k.

Proof of Lemma. If $\sum_{i=1} m_i k/k_i \equiv \sum_{i=1} n_i k/k_i \bmod k$, then $k \mid \sum_{i=1}(m_i - n_i)k/k_i$. By linearity $k_i \mid m_i - n_i$. Since $1 \le m_i, n_i \le k_i$, we must have $m_i = n_i$. Thus for $1 \le m_i \le k_i$, all k numbers $\sum_{i=1} m_i k/k_i$ are incongruent and form a complete set of residues mod k. □

Proof of Exercise. Let $e(x) = e^{2\pi i x}$. By Lemma 8.11 we have

$$\begin{aligned}
G(a,\chi) &= \sum_{m=1}^{k} \chi(m) e\left(\frac{am}{k}\right) \\
&= \sum_{m_1=1}^{k_1} \cdots \sum_{m_r=1}^{k_r} \chi\left(\sum_{j=1} \frac{m_j k}{k_j}\right) e\left(\frac{a}{k}\sum_{j=1} \frac{m_j k}{k_j}\right) \\
&= \sum_{m_1=1}^{k_1} \cdots \sum_{m_r=1}^{k_r} \prod_{i=1}^{r} \chi_i\left(\sum_{j=1} \frac{m_j k}{k_j}\right) e\left(\frac{am_i}{k_i}\right) \\
&= \sum_{m_1=1}^{k_1} \cdots \sum_{m_r=1}^{k_r} \prod_{i=1}^{r} \chi_i\left(\frac{m_i k}{k_i}\right) e\left(\frac{am_i}{k_i}\right) \\
&= \prod_{i=1}^{r} \chi_i\left(\frac{k}{k_i}\right) \sum_{m_1=1}^{k_1} \cdots \sum_{m_r=1}^{k_r} \prod_{i=1}^{r} \chi_i(m_i) e\left(\frac{am_i}{k_i}\right).
\end{aligned}$$

Since the last sum is separable,

$$G(a,\chi) = \prod_{i=1}^{r} \chi_i\left(\frac{k}{k_i}\right) \sum_{m_i=1}^{k_i} \chi_i(m_i) e\left(\frac{am_i}{k_i}\right).$$

Finally, observe $a_i \equiv a \bmod k_i$ implies $e(am_i/k_i) = e(a_i m_i/k_i)$. Hence

$$\begin{aligned}
G(a,\chi) &= \prod_{i=1}^{r} \chi_i\left(\frac{k}{k_i}\right) \sum_{m_i=1}^{k_i} \chi_i(m_i) e\left(\frac{a_i m_i}{k_i}\right) \\
&= \prod_{i=1}^{r} \chi_i\left(\frac{k}{k_i}\right) G(a_i,\chi_i).
\end{aligned}$$

□

Exercise 8.12. If χ has the factorization in Exercise 8.9, prove that χ is primitive mod k if, and only if, each χ_i is primitive mod k_i. [*Hint*: Theorem 8.19 or Exercise 8.10.]

Proof. By Exercise 8.10, $f(\chi) = f(\chi_1)\cdots f(\chi_r)$, and so

$$k = f(\chi_1)\cdots f(\chi_r) \iff \prod_{i=1}^{r} \frac{k_i}{f(\chi_i)} = 1.$$

Now by Exercise 8.7, $f(\chi_i) \mid k_i$. Therefore

$$\begin{aligned}\prod_{i=1}^{r} \frac{k_i}{f(\chi_i)} = 1 &\iff \frac{k_i}{f(\chi_i)} = 1 \text{ for all } i \\ &\iff k_i = f(\chi_i) \text{ for all } i.\end{aligned}$$

□

Exercise 8.13. Let χ be a primitive character mod k. Prove that if $N < M$ we have

$$\left|\sum_{m=N+1}^{M} \frac{\chi(m)}{m}\right| < \frac{2}{N+1}\sqrt{k}\log k.$$

Proof. Since χ is primitive, by Theorem 8.21 $\left|\sum_{m\le x}\chi(m)\right| < \sqrt{k}\log k$. Therefore

$$\begin{aligned}\left|\sum_{m=N+1}^{M} \frac{\chi(m)}{m}\right| &\le \frac{1}{N+1}\left|\sum_{m=N+1}^{M}\chi(m)\right| \\ &\le \frac{1}{N+1}\left(\left|\sum_{m=1}^{M}\chi(m)\right| + \left|\sum_{m=1}^{N}\chi(m)\right|\right) \\ &< \frac{2}{N+1}\sqrt{k}\log k.\end{aligned}$$

□

Exercise 8.14. This exercise outlines a slight improvement in Pólya's inequality. Refer to the proof of Theorem 8.21. After inequality (26) write

$$\sum_{n\le k/2}|f(n)| \le \sum_{n\le k/2}\frac{1}{\sin\frac{\pi n}{k}} < \frac{1}{\sin\frac{\pi}{k}} + \int_1^{k/2}\frac{dt}{\sin\frac{\pi t}{k}}.$$

Show that the integral is less than $-(k/\pi)\log(\sin(\pi/(2k)))$ and deduce that

$$\left|\sum_{n\le x}\chi(n)\right| < \sqrt{k} + \frac{2}{\pi}\sqrt{k}\log k.$$

This improves Pólya's inequality by a factor of $2/\pi$ in the principal term.

Proof. Since $1/\sin x$ is monotonically decreasing when $0 < x < \pi/2$,

$$\begin{aligned}\sum_{n\le k/2}\frac{1}{\sin\frac{\pi n}{k}} &= \frac{1}{\sin\frac{\pi}{k}} + \sum_{2\le n\le k/2}\frac{1}{\sin\frac{\pi n}{k}}\\ &< \frac{1}{\sin\frac{\pi}{k}} + \sum_{2\le n\le k/2}\int_{n-1}^{n}\frac{dt}{\sin\frac{\pi t}{k}}\\ &\le \frac{1}{\sin\frac{\pi}{k}} + \int_1^{k/2}\frac{dt}{\sin\frac{\pi t}{k}}.\end{aligned}$$

Now

$$\int_1^{k/2}\frac{dt}{\sin\frac{\pi t}{k}} = \frac{k}{\pi}\log\left(\tan\left(\frac{\pi t}{2k}\right)\right)\Big]_{t=1}^{k/2} = -\frac{k}{\pi}\log\left(\tan\left(\frac{\pi}{2k}\right)\right),$$

and so

$$\begin{aligned}\frac{1}{\sin\frac{\pi}{k}} + \int_1^{k/2}\frac{dt}{\sin\frac{\pi t}{k}} &= \frac{1}{\sin\frac{\pi}{k}} - \frac{k}{\pi}\log\left(\sin\left(\frac{\pi}{2k}\right)\right) + \frac{k}{\pi}\log\left(\cos\left(\frac{\pi}{2k}\right)\right)\\ &< \frac{1}{\sin\frac{\pi}{k}} - \frac{k}{\pi}\log\left(\sin\left(\frac{\pi}{2k}\right)\right).\end{aligned}$$

Furthermore, just as in Theorem 8.21, the bound $\sin t \ge 2t/\pi$ for $0 < t < \pi/2$ gives

$$\sum_{n\le k/2}|f(n)| < \frac{1}{\sin\frac{\pi}{k}} - \frac{k}{\pi}\log\left(\sin\left(\frac{\pi}{2k}\right)\right) < \frac{k}{2} + \frac{k}{\pi}\log k.$$

Using this estimate in the proof of Theorem 8.21 then gives

$$\begin{aligned}\left|\sum_{n\le x}\chi(n)\right| &< \frac{2}{\sqrt{k}}\sum_{n<k/2}|f(n)| + \frac{|f(k/2)|}{\sqrt{k}} \qquad (12)\\ &\le \frac{2}{\sqrt{k}}\sum_{n\le k/2}|f(n)|\\ &< \sqrt{k} + \frac{2}{\pi}\sqrt{k}\log k.\end{aligned}$$

Note, just as in Theorem 8.21, $f(k/2)$ only appears in (12) if k is even. □

Exercise 8.15.(++) The Kloosterman sum $K(m,n;k)$ is defined as follows:

$$K(m,n;k) = \sum_{\substack{h \bmod k\\(h,k)=1}} e^{2\pi i(mh+nh')/k}$$

where h' is the reciprocal of h mod k. When $k \mid n$ this reduces to Ramanujan's sum $c_k(m)$. Derive the following properties of Kloosterman sums:
(a) $K(m,n;k) = K(n,m;k)$.
(b) $K(m,n;k) = K(1,mn;k)$ whenever $(m,k) = 1$.

(c) Given integers n, k_1, k_2 such that $(k_1, k_2) = 1$, show that there exists integers n_1 and n_2 such that

$$n \equiv n_1 k_2^2 + n_2 k_1^2 \mod k_1 k_2,$$

and that for those integers we have

$$K(m, n; k_1 k_2) = K(m, n_1; k_1) K(m, n_2; k_2).$$

This reduces the study of Kloosterman sums to the special case $K(m, n; p^\alpha)$, where p is prime.

Lemma 8.15. If $(k_1, k_2) = 1$, then the set

$$S = \{hk_1 + gk_2 \mid 1 \le g \le k_1, 1 \le h \le k_2, (g, k_1) = (h, k_2) = 1\}$$

runs through a complete system of residues relatively prime to $k_1 k_2$.

Proof of Lemma. By Lemma 8.11 the set

$$\{hk_1 + gk_2 \mid 1 \le g \le k_1, 1 \le h \le k_2\}$$

runs through a complete system of residues mod $k_1 k_2$. Next let $(g, k_1) = (h, k_2) = 1$. Since $(hk_1 + gk_2, k_1) = (hk_1 + gk_2, k_2) = 1$, we have $(hk_1 + gk_2, k_1 k_2) = 1$. This means every element of S is relatively prime to $k_1 k_2$. Since $|S| = \varphi(k_1)\varphi(k_2) = \varphi(k_1 k_2)$ and each elements are pairwise incongruent mod $k_1 k_2$, the lemma follows. □

Proof of Exercise.
(a) Since $(h', k) = 1$, we see $(h')^2 h \bmod k$ runs through a complete system of residues relatively prime to k. Therefore

$$K(m, n; k) = \sum_{\substack{h \bmod k \\ (h,k)=1}} e^{2\pi i (m(h')^2 h + nh^2 h')/k} = \sum_{\substack{h \bmod k \\ (h,k)=1}} e^{2\pi i (mh' + nh)/k} = K(n, m; k).$$

(b) Since $(m, k) = 1$ and $(h, k) = 1$, we see $m'h \bmod k$ runs through a complete system of residues relatively prime to k. Therefore

$$K(m, n; k) = \sum_{\substack{h \bmod k \\ (h,k)=1}} e^{2\pi i (mm'h + nmh')/k} = \sum_{\substack{h \bmod k \\ (h,k)=1}} e^{2\pi i (h + mnh')/k} = K(1, mn; k).$$

(c) Since $(k_1^2, k_2^2) = 1$, there are integers x, y such that $xk_1^2 + yk_2^2 = 1$. Define $n_1 = ny$, $n_2 = nx$, and $e(x) = e^{2\pi i x}$. We then have

$$\begin{aligned} K(m, n_1; k_1) K(m, n_2; k_2) &= \sum_{\substack{g \bmod k_1 \\ (g,k_1)=1}} \sum_{\substack{h \bmod k_2 \\ (h,k_2)=1}} e\left(\frac{mg + n_1 g'}{k_1} + \frac{mh + n_2 h'}{k_2}\right) \\ &= \sum_{\substack{g \bmod k_1 \\ (g,k_1)=1}} \sum_{\substack{h \bmod k_2 \\ (h,k_2)=1}} e\left(\frac{m(gk_2 + hk_1)}{k_1 k_2} + \frac{n_1 g' k_2 + n_2 h' k_1}{k_1 k_2}\right) \\ &= \sum_{\substack{g \bmod k_1 \\ (g,k_1)=1}} \sum_{\substack{h \bmod k_2 \\ (h,k_2)=1}} e\left(\frac{mA + B}{k_1 k_2}\right), \end{aligned}$$

where $A = gk_2 + hk_1$ and $B = n_1g'k_2 + n_2h'k_1$.

By Lemma 8.15 A runs through a complete system of residues relatively prime to k_1k_2. Hence, if we can show $B \equiv CA' \bmod k_1k_2$, then

$$K(m, n_1; k_1)K(m, n_2; k_2) = \sum_{\substack{A \bmod k_1k_2 \\ (A,k_1k_2)=1}} e\left(\frac{mA + CA'}{k_1k_2}\right) = K(m, C, k_1k_2).$$

Since $(gk_2 + hk_1)A' \equiv 1 \bmod k_1k_2$, we have $gk_2A' \equiv 1 \bmod k_1$ and so $k_2 \equiv g'A \bmod k_1$. From here we see

$$k_2^2 \equiv k_2g'A \mod k_1k_2 \quad \text{and similarly} \quad k_1^2 \equiv k_1h'A \mod k_1k_2.$$

From this we deduce

$$C := n_2k_1^2 + n_1k_2^2 \equiv (n_1g'k_2 + n_2h'k_1)A \equiv BA \mod k_1k_2,$$

and the proof follows. □

Exercise 8.16. If n and k are integers $n > 0$, the sum

$$G(k; n) = \sum_{r=1}^{n} e^{2\pi ikr^2/n}$$

is called a quadratic Gauss sum. Derive the following properties of quadratic Gauss sums:
(a) $G(k; mn) = G(km; n)G(kn; m)$ whenever $(m, n) = 1$. This reduces the study of Gauss sums to the special case $G(k; p^\alpha)$, where p is prime.
(b) Let p be an odd prime, $p \nmid k$, $\alpha \geq 2$. Prove that $G(k; p^\alpha) = pG(k; p^{\alpha-2})$ and deduce that

$$G(k; p^\alpha) = \begin{cases} p^{\alpha/2} & \text{if } \alpha \text{ is even,} \\ p^{(\alpha-1)/2}G(k; p) & \text{if } \alpha \text{ is odd.} \end{cases}$$

Further properties of the Gauss sum $G(k; p)$ are developed in the next chapter where it is shown that $G(k; p)$ is the same as the Gauss sum $G(k, \chi)$ with a certain Dirichlet character $\chi \bmod p$. (See Exercise 9.9.)

Proof.
(a) By Lemma 8.11, the set $\{sm+tn \mid 1 \leq s \leq n \text{ and } 1 \leq t \leq m\}$ runs through the complete system of residues mod mn. Therefore

$$\begin{aligned} G(k; mn) &= \sum_{r=1}^{mn} e^{2\pi ikr^2/(mn)} \\ &= \sum_{s=1}^{n}\sum_{t=1}^{m} e^{2\pi ik(s^2m^2+2mnst+t^2n^2)^2/(mn)} \\ &= \sum_{s=1}^{n} e^{2\pi iks^2/n} \sum_{t=1}^{m} e^{2\pi ikt^2/m} \\ &= G(km; n)G(kn; m). \end{aligned}$$

(b) Let $1 + p^{\alpha-1} \le r \le p^\alpha + p^{\alpha-1}$ and $r = p^{\alpha-1}s + t$ where $1 \le s \le p$ and $1 \le t \le p^{\alpha-1}$. Through the division algorithm s and t are uniquely determined. Thus letting r run through a complete system of residues mod p^α is the same as letting s and t run through complete systems of residues mod p and mod $p^{\alpha-1}$, respectively. Then $r^2 = p^{2\alpha-2}s^2 + 2p^{\alpha-1}st + t^2$ and

$$\begin{aligned} G(k;p^\alpha) &= \sum_{r=1}^{p^\alpha} e^{2\pi i k r^2/p^\alpha} = \sum_{r=1+p^{\alpha-1}}^{p^\alpha+p^{\alpha-1}} e^{2\pi i k r^2/p^\alpha} \\ &= \sum_{t=1}^{p^{\alpha-1}} \sum_{s=1}^{p} e^{2\pi i k(p^{2\alpha-2}s^2+2p^{\alpha-1}st+t^2)/p^\alpha} \\ &= \sum_{t=1}^{p^{\alpha-1}} e^{2\pi i k t^2/p^\alpha} \sum_{s=1}^{p} e^{4\pi i k s t/p}. \end{aligned}$$

If $p \mid t$ then $e^{4\pi i k s t/p} = 1$, which implies the inner sum is p. On the other hand, if $p \nmid t$ then letting s vary allows $2kst$ to run through all residue classes mod p. Thus the inner sum is the sum of the pth roots of unity and hence equals 0. This means we only need to sum over the t where $p \mid t$. Summing over $t = px$ for $1 \le x \le p^{\alpha-2}$ gives

$$G(k;p^\alpha) = p\sum_{x=1}^{p^{\alpha-2}} e^{2\pi i k(px)^2/p^\alpha} = p\sum_{x=1}^{p^{\alpha-2}} e^{2\pi i k x^2/p^{\alpha-2}} = pG(k;p^{\alpha-2}).$$

Now observe

$$G(k;p^\alpha) = pG(k;p^{\alpha-2}) = p^2G(k;p^{\alpha-4}) = \cdots = p^{\lfloor \alpha/2 \rfloor}G(k;p^{\alpha-2\lfloor \alpha/2 \rfloor}).$$

Therefore if α is even, then $\lfloor \alpha/2 \rfloor = \alpha/2$ and so

$$G(k;p^\alpha) = p^{\alpha/2}G(k;1) = p^{\alpha/2}.$$

If α is odd, then $\lfloor \alpha/2 \rfloor = (\alpha-1)/2$ and so

$$G(k;p^\alpha) = p^{(\alpha-1)/2}G(k;p).$$

□

Chapter 9
Quadratic Residues and the Quadratic Reciprocity Law

Exercise 9.1. Determine those odd primes p for which $(-3|\,p) = 1$ and those for which $(-3|\,p) = -1$.

Solution. Let p be an odd prime. By quadratic reciprocity we have

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

Therefore

$$(-3|\,p) = \begin{cases} 1 & \text{if } p \equiv 1 \mod 3\\ -1 & \text{if } p \equiv 2 \mod 3\\ 0 & \text{if } p \equiv 3 \mod 3.\end{cases}$$

Exercise 9.2. Prove that 5 is a quadratic residue of an odd prime p if $p \equiv \pm 1 \mod 10$, and that 5 is a nonresidue if $p \equiv \pm 3 \mod 10$.

Solution. Let p be an odd prime. By quadratic reciprocity we have $(5|\,p) = -(-1)^{(p-1)/2}\,(p|\,5)$. The exponent of -1 means we need to consider $p \mod 2$, and $(p|\,5)$ means we need to consider $p \mod 5$. Hence it is enough to consider $p \mod 10$. Checking all values mod 10 gives the result.

Exercise 9.3. Let p be an odd prime. Assume that the set $G = \{1, 2, \ldots, p-1\}$ can be expressed as the union of two nonempty subsets S and T, $S \neq T$, such that the product (mod p) of any two elements in the same subset lies in S, whereas the product (mod p) of any element in S with any element in T lies in T. Prove that S consists of the quadratic residues and T consists of the nonresiudes mod p.

Proof. Since the Legendre symbol is completely multiplicative, it's clear the quadratic residues and nonresidues mod p satisfy the stipulations of S and T, respectively. This shows existence of such S and T, so all we need to show is S and T are uniquely defined.

Let $g \in G$. Since g is either an element of S or T, by definition we must have $g^2 \in S$. This means S contains all quadratic residues mod p. Now suppose there exists $x \in S$ such that $(x|\,p) = -1$. Since T is nonempty there is a $y \in T$ and we must have $(y|\,p) = -1$. By definition of T we have $xy \in T$, but $(xy|\,p) = 1$, a contradiction. This means S cannot contain any quadratic nonresidues mod p. We conclude S must be the group of quadratic residues mod p and hence T is the set of quadratic nonresidues mod p. □

Exercise 9.4. Let $f(x)$ be a polynomial which takes integer values when x is an integer.
(a) If a and b are integers, prove that

$$\sum_{x \mod p} (f(ax+b)|\,p) = \sum_{x \mod p} (f(x)|\,p) \quad \text{if } (a,p) = 1$$

and that

$$\sum_{x \mod p} (af(x)|\,p) = (a|\,p) \sum_{x \mod p} (f(x)|\,p) \quad \text{for all } a.$$

(b) Prove that

$$\sum_{x \mod p} (ax+b|\,p) = 0 \quad \text{if } (a,p) = 1.$$

(c) Let $f(x) = x(ax+b)$, where $(a,p) = (b,p) = 1$. Prove that

$$\sum_{x=1}^{p-1} (f(x)|\,p) = \sum_{x=1}^{p-1} (a+bx|\,p) = -(a|\,p)\,.$$

[*Hint*: As x runs through a reduced residue system mod p, so does x', the reciprocal of x mod p.]

Proof.
(a) Since $(a,p) = 1$, letting x run through a complete residue system mod p means $ax+b$ does too. Furthermore, by Theorem 5.2, if $ax+b \equiv y \bmod p$, then $f(ax+b) \equiv f(y) \bmod p$. These two observations give

$$\sum_{x \mod p} (f(ax+b)|\,p) = \sum_{x \mod p} (f(x)|\,p)\,.$$

Next, since the Legendre symbol is completely multiplicative,

$$\sum_{x \mod p} (af(x)|\,p) = (a|\,p) \sum_{x \mod p} (f(x)|\,p) \quad \text{for all } a.$$

(b) Let $f(x) = x$ and $(a,p) = 1$. By (a) we have

$$\sum_{x \mod p} (ax+b|\,p) = \sum_{x \mod p} (x|\,p) = 0.$$

(c) Using the hint of the problem and the fact that $(x|\,p) = (x'|\,p)$,

$$\begin{aligned}\sum_{x=1}^{p-1}(x(ax+b)|\,p) &= \sum_{x=1}^{p-1}(x'(ax'+b)|\,p) = \sum_{x=1}^{p-1}(x'|\,p)\,(ax'+b|\,p)\\ &= \sum_{x=1}^{p-1}(x|\,p)\,(ax'+b|\,p) = \sum_{x=1}^{p-1}(x(ax'+b)|\,p)\\ &= \sum_{x=1}^{p-1}(a+bx|\,p) = -(a|\,p) + \sum_{x=0}^{p-1}(a+bx|\,p)\\ &= -(a|\,p) + \sum_{x=0}^{p-1}(x|\,p) = -(a|\,p)\,.\end{aligned}$$

□

Exercise 9.5. Let α and β be integers whose possible values are ± 1. Let $N(\alpha,\beta)$ denote the number of integers x among $1, 2, \ldots, p-2$ such that

$$(x|\,p) = \alpha \qquad \text{and} \quad (x+1|\,p) = \beta,$$

where p is an odd prime. Prove that

$$4N(\alpha,\beta) = \sum_{x=1}^{p-2}\{1+\alpha\,(x|\,p)\}\{1+\beta\,(x+1|\,p)\},$$

and use Exercise 4 to deduce that

$$4N(\alpha,\beta) = p - 2 - \beta - \alpha\beta - \alpha\,(-1|\,p)\,.$$

In particular this gives

$$\begin{aligned}N(1,1) &= \frac{p-4-(-1|\,p)}{4},\\ N(-1,-1) = N(-1,1) &= \frac{p-2+(-1|\,p)}{4}\\ N(1,-1) &= 1 + N(1,1).\end{aligned}$$

Proof. Let $0 < x < p-1$. Notice $\alpha = (x|\,p)$ implies $1+\alpha\,(x|\,p) = 2$ and $\alpha \neq (x|\,p)$ implies $1+\alpha\,(x|\,p) = 0$. Since the same scenario occurs for $1+\beta\,(x+1|\,p)$, we have

$$\{1+\alpha\,(x|\,p)\}\{1+\beta\,(x+1|\,p)\} = \begin{cases}4 & \text{if } \alpha = (x|\,p) \text{ and } \beta = (x+1|\,p)\\ 0 & \text{otherwise.}\end{cases} \tag{13}$$

Since the upper case of (13) occurs exactly $N(\alpha,\beta)$ times when $0 < x < p-1$,

$$4N(\alpha,\beta) = \sum_{x=1}^{p-2}\{1+\alpha\,(x|\,p)\}\{1+\beta\,(x+1|\,p)\}.$$

Expanding the summand of the right hand side gives

$$\begin{aligned} 4N(\alpha,\beta) &= \sum_{x=1}^{p-2} 1 + \alpha \sum_{x=1}^{p-2} (x|\,p) + \beta \sum_{x=1}^{p-2} (x+1|\,p) + \alpha\beta \sum_{x=1}^{p-2} (x(x+1)|\,p) \\ &= p - 2 - \alpha\,(-1|\,p) - \beta + \alpha\beta \sum_{x=1}^{p-1} (x(x+1)|\,p)\,. \end{aligned}$$

Applying Exercise 9.4 (c) with $a = b = 1$ gives the result. □

Remark. Since $N(1,1)$ in an integer, this is a round about proof that $(-1|\,p) = (-1)^{(p-1)/2}$.

Exercise 9.6. Use Exercise 9.5 to show that for every prime p there exists integers x and y such that $x^2 + y^2 + 1 \equiv 0 \bmod p$.

Proof. If $p \equiv 1 \bmod 4$, there exists x and y such that $x^2 \equiv 0 \bmod p$ and $y^2 \equiv -1 \bmod p$. This gives $x^2 + y^2 \equiv -1 \bmod p$.

If $p \equiv 3 \bmod 4$, then by Exercise 9.5 there is a z such that $(z|\,p) = 1$ and $(z+1|\,p) = -1$. Since $(-1|\,p) = -1$, we have $(-z-1|\,p) = 1$. Choosing x and y such that $x^2 \equiv z \bmod p$ and $y^2 \equiv -z - 1 \bmod p$ gives $x^2 + y^2 \equiv -1 \bmod p$. □

Exercise 9.7. Let p be an odd prime. Prove each of the following statements.

(a) $\displaystyle\sum_{r=1}^{p-1} r\,(r|\,p) = 0$ if $p \equiv 1 \bmod 4$.

(b) $\displaystyle\sum_{\substack{r=1 \\ (r|p)=1}}^{p-1} r = \frac{p(p-1)}{4}$ if $p \equiv 1 \bmod 4$.

(c) $\displaystyle\sum_{r=1}^{p-1} r^2\,(r|\,p) = p \sum_{r=1}^{p-1} r\,(r|\,p)$ if $p \equiv 3 \bmod 4$.

(d) $\displaystyle\sum_{r=1}^{p-1} r^3\,(r|\,p) = \frac{3}{2} \sum_{r=1}^{p-1} r^2\,(r|\,p)$ if $p \equiv 1 \bmod 4$.

(e) $\displaystyle\sum_{r=1}^{p-1} r^4\,(r|\,p) = 2p \sum_{r=1}^{p-1} r^3\,(r|\,p) - p^2 \sum_{r=1}^{p-1} r^2\,(r|\,p)$ if $p \equiv 3 \bmod 4$.

[*Hint*: $p - r$ runs through the numbers $1, 2, \ldots, p-1$ with r.]

Proof. For each part we will use the hint and $(r|\,p) = (-1)^{(p-1)/2}\,(p-r|\,p)$.
(a) For $p \equiv 1 \bmod p$, we have

$$\begin{aligned}\sum_{r=1}^{p-1} r\,(r|\,p) &= \sum_{r=1}^{p-1}(p-r)\,(p-r|\,p)\\ &= \sum_{r=1}^{p-1}(p-r)\,(r|\,p)\\ &= p\sum_{r=1}^{p-1}(r|\,p) - \sum_{r=1}^{p-1} r\,(r|\,p)\\ &= -\sum_{r=1}^{p-1} r\,(r|\,p)\,.\end{aligned}$$

This means $\sum_{r=1}^{p-1} r\,(r|\,p) = 0$.
(b) For $p \equiv 1 \bmod p$, we have

$$\sum_{\substack{r=1\\(r|p)=1}}^{p-1} r = \sum_{\substack{r=1\\(r|p)=1}}^{p-1}(p-r) = p\sum_{\substack{r=1\\(r|p)=1}}^{p-1} 1 - \sum_{\substack{r=1\\(r|p)=1}}^{p-1} r.$$

Since there are $(p-1)/2$ quadratic residues mod p, the result follows.
(c) For $p \equiv 3 \bmod p$, we have

$$\begin{aligned}\sum_{r=1}^{p-1} r^2\,(r|\,p) &= \sum_{r=1}^{p-1}(p-r)^2\,(p-r|\,p)\\ &= -\sum_{r=1}^{p-1}(p-r)^2\,(r|\,p)\\ &= -p^2\sum_{r=1}^{p-1}(r|\,p) + 2p\sum_{r=1}^{p-1} r\,(r|\,p) - \sum_{r=1}^{p-1} r^2\,(r|\,p)\\ &= 2p\sum_{r=1}^{p-1} r\,(r|\,p) - \sum_{r=1}^{p-1} r^2\,(r|\,p)\,.\end{aligned}$$

Solving for $\sum_{r=1}^{p-1} r^2\,(r|\,p)$ gives the result.

(d) For $p \equiv 1 \bmod p$, we have

$$\begin{aligned}\sum_{r=1}^{p-1} r^3 \left(r|p\right) &= \sum_{r=1}^{p-1} (p-r)^3 \left(p-r|p\right) \\ &= \sum_{r=1}^{p-1} (p-r)^3 \left(r|p\right) \\ &= p^3 \sum_{r=1}^{p-1} \left(r|p\right) - 3p^2 \sum_{r=1}^{p-1} r \left(r|p\right) + 3p \sum_{r=1}^{p-1} r^2 \left(r|p\right) - \sum_{r=1}^{p-1} r^3 \left(r|p\right) \\ &= -3p^2 \sum_{r=1}^{p-1} r \left(r|p\right) + 3p \sum_{r=1}^{p-1} r^2 \left(r|p\right) - \sum_{r=1}^{p-1} r^3 \left(r|p\right).\end{aligned}$$

Applying (a) we know

$$\sum_{r=1}^{p-1} r \left(r|p\right) = 0,$$

hence solving for $\sum_{r=1}^{p-1} r^3 \left(r|p\right)$ gives the result.
(e) For $p \equiv 3 \bmod p$, we have

$$\begin{aligned}\sum_{r=1}^{p-1} r^4 \left(r|p\right) &= \sum_{r=1}^{p-1} (p-r)^4 \left(p-r|p\right) \\ &= -\sum_{r=1}^{p-1} (p-r)^4 \left(r|p\right) \\ &= \sum_{j=0}^{4} (-1)^{j+1} \binom{4}{j} p^{4-j} \sum_{r=1}^{p-1} r^j \left(r|p\right) \\ &= \sum_{j=1}^{4} (-1)^{j+1} \binom{4}{j} p^{4-j} \sum_{r=1}^{p-1} r^j \left(r|p\right).\end{aligned}$$

Applying (c) we know

$$p \sum_{r=1}^{p-1} r \left(r|p\right) = \sum_{r=1}^{p-1} r^2 \left(r|p\right).$$

Substituting this and solving for $\sum_{r=1}^{p-1} r^4 \left(r|p\right)$ gives the result. □

Exercise 9.8. Let p be an odd prime, $p \equiv 3 \bmod 4$, and let $q = (p-1)/2$.
(a) Prove that

$$\{1 - 2\left(2|p\right)\} \sum_{r=1}^{q} r \left(r|p\right) = p \frac{1 - \left(2|p\right)}{2} \sum_{r=1}^{q} \left(r|p\right).$$

[*Hint*: As r runs through the numbers $1, 2, \ldots, q$ then r and $p-r$ together run through the numbers $1, 2, \ldots, p-1$, as do $2r$ and $p-2r$.]

(b) Prove that

$$\{(2|\,p)-2\}\sum_{r=1}^{p-1} r\,(r|\,p) = p\sum_{r=1}^{q}(r|\,p)\,.$$

Proof.
(a) Let p be a prime such that $p \equiv 3 \bmod 4$. This means $(p-r|\,p) = -\,(r|\,p)$ and hence

$$\sum_{r=1}^{q}(p-r)\,(p-r|\,p) = \sum_{r=1}^{q} r\,(r|\,p) - p\sum_{r=1}^{q}(r|\,p)\,.$$

Therefore applying the first part of the hint gives

$$\begin{aligned}\sum_{r=1}^{p-1} r\,(r|\,p) &= \sum_{r=1}^{q} r\,(r|\,p) + \sum_{r=1}^{q}(p-r)\,(p-r|\,p)\\ &= 2\sum_{r=1}^{q} r\,(r|\,p) - p\sum_{r=1}^{q}(r|\,p)\,.\end{aligned}$$

On the other hand, applying the last part of the hint yields

$$\begin{aligned}\sum_{r=1}^{p-1} r\,(r|\,p) &= \sum_{r=1}^{q} 2r\,(2r|\,p) + \sum_{r=1}^{q}(p-2r)\,(p-2r|\,p)\\ &= 2\,(2|\,p)\sum_{r=1}^{q} r\,(r|\,p) - p\,(2|\,p)\sum_{r=1}^{q}(r|\,p) + 2\,(2|\,p)\sum_{r=1}^{q} r\,(r|\,p)\\ &= 4\,(2|\,p)\sum_{r=1}^{q} r\,(r|\,p) + p\,(2|\,p)\sum_{r=1}^{q}(r|\,p)\,. \qquad (14)\end{aligned}$$

Equating both identities implies

$$2\sum_{r=1}^{q} r\,(r|\,p) - p\sum_{r=1}^{q}(r|\,p) = 4\,(2|\,p)\sum_{r=1}^{q} r\,(r|\,p) + p\,(2|\,p)\sum_{r=1}^{q}(r|\,p)\,,$$

which is an equivalent result.
(b) By (14) we have

$$\sum_{r=1}^{p-1} r\,(r|\,p) = 4\,(2|\,p)\sum_{r=1}^{q} r\,(r|\,p) + p\,(2|\,p)\sum_{r=1}^{q}(r|\,p)\,.$$

Substituting (a) gives

$$\begin{aligned}\sum_{r=1}^{p-1} r\,(r|\,p) &= 4\,(2|\,p)\left(\frac{p}{2}\frac{1-(2|\,p)}{1-2\,(2|\,p)}\sum_{r=1}^{q}(r|\,p)\right) + p\,(2|\,p)\sum_{r=1}^{q}(r|\,p)\\ &= \frac{p\,(2|\,p)}{1-2\,(2|\,p)}\sum_{r=1}^{q}(r|\,p)\\ &= \frac{p}{(2|\,p)-2}\sum_{r=1}^{q}(r|\,p)\,,\end{aligned}$$

where in the last step we multiplied numerator and denominator by $(2|\,p)$. □

Exercise 9.9. If p is an odd prime, let $\chi(n) = (n|\,p)$. Prove that the Gauss sum $G(n,\chi)$ associated with χ is the same as the quadratic Gauss sum $G(n;p)$ introduced in Exercise 8.16 if $(n,p) = 1$. In other words, if $p \nmid n$ we have

$$G(n,\chi) = \sum_{m \bmod p} \chi(m) e^{2\pi i m n/p} = \sum_{r=1}^{p} e^{2\pi i n r^2/p} = G(n;p).$$

Proof. Let $(n,p) = 1$ and $e(x) = e^{2\pi i x}$. We have

$$G(n,\chi) = \sum_{m=1}^{p-1} (m|\,p)\, e(mn/p) = \sum_{\substack{m=1 \\ (m|p)=1}}^{p-1} e(mn/p) - \sum_{\substack{m=1 \\ (m|p)=-1}}^{p-1} e(mn/p).$$

Since $\sum_{m=0}^{p-1} e(mn/p) = 0$, $G(n,\chi)$ can be rewritten as

$$G(n,\chi) = 1 + 2 \sum_{\substack{m=1 \\ (m|p)=1}}^{p-1} e(mn/p).$$

Next let $q = (p-1)/2$. Since both $\{1^2, 2^2, \ldots, q^2\}$ and $\{(q+1)^2, (q+2)^2, \ldots, (p-1)^2\}$ consist of all quadratic residues mod p,

$$\begin{aligned} G(n;p) = \sum_{r=1}^{p} e(nr^2/p) &= 1 + 2\sum_{r=1}^{q} e(nr^2/p) \\ &= 1 + 2 \sum_{\substack{m=1 \\ (m|p)=1}}^{p-1} e(nm/p) = G(n,\chi). \end{aligned}$$

□

Exercise 9.10. Evaluate the quadratic Gauss sum $G(2;p)$ using one of the reciprocity laws. Compare the result with the formula $G(2;p) = (2|\,p)\, G(1;p)$ and deduce that $(2|\,p) = (-1)^{(p^2-1)/8}$ if p is an odd prime.

Proof. Section 9.11 tells us

$$G(2;p) = (2|\,p)\, G(1;p) = (-1)^{(p-1)^2/8} \sqrt{p}\, (2|\,p)\,.$$

Evaluating $G(2;p)$ another way, by Theorem 9.16,

$$G(2;p) = S(4,p) = \frac{\sqrt{p}}{2} \left(\frac{1+i}{\sqrt{2}} \right) \overline{S(p,4)},$$

where

$$S(a,m) = \sum_{r=0}^{m-1} e^{\pi i a r^2/m}.$$

Observe for a fixed m, $S(a,m)$ has period $2m$, so in our case it's enough to consider p mod 8. Evaluating each case directly we obtain

$$S(p,4) = \begin{cases} (1+i)\sqrt{2} & \text{if } p \equiv 1 \mod p \\ (i-1)\sqrt{2} & \text{if } p \equiv 3 \mod p \\ (-1-i)\sqrt{2} & \text{if } p \equiv 5 \mod p \\ (1-i)\sqrt{2} & \text{if } p \equiv 7 \mod p, \end{cases}$$

which implies

$$G(2;p) = \begin{cases} \sqrt{p} & \text{if } p \equiv 1 \mod p \\ -i\sqrt{p} & \text{if } p \equiv 3 \mod p \\ -\sqrt{p} & \text{if } p \equiv 5 \mod p \\ i\sqrt{p} & \text{if } p \equiv 7 \mod p. \end{cases}$$

A more compact formula is $G(2;p) = (-1)^{p(p-1)/4}\sqrt{p}$. Equating both formulas for $G(2;p)$,

$$(-1)^{(p-1)^2/8}\sqrt{p}\,(2|\,p) = (-1)^{p(p-1)/4}\sqrt{p},$$

or in other words

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

□

Chapter 10
Primitive Roots

Exercise 10.1. Prove that m is prime if and only if $\exp_m(a) = m - 1$ for some a.

Proof. If m is prime, then there is a primitive root a. By the definition of primitive root

$$\exp_m(a) = \varphi(m) = m - 1.$$

Conversely, suppose $\exp_m(a) = m - 1$. Then

$$m - 1 = \exp_m(a) \leq \varphi(m) \leq m - 1,$$

so in particular $\varphi(m) = m - 1$. This can only happen if m is prime. □

Exercise 10.2. If $(a, m) = (b, m) = 1$ and if $(\exp_m(a), \exp_m(b)) = 1$, prove

$$\exp_m(ab) = \exp_m(a) \exp_m(b).$$

Proof. Let $x = \exp_m(a)$, $y = \exp_m(b)$, and $k = \exp_m(ab)$. Note

$$(ab)^{xy} = (a^x)^y (b^y)^x \equiv 1 \mod m,$$

so $k \mid xy$. Now

$$a^{ky} \equiv (ab)^{ky} \equiv 1 \mod m,$$

which means $x \mid ky$. Since $(x, y) = 1$ we have $x \mid k$, and similarly we can deduce $y \mid k$. Since $(x, y) = 1$, we have $xy \mid k$. We conclude $k = xy$. □

Exercise 10.3. Let g be a primitive root of an odd prime p. Prove that $-g$ is also a primitive root of p if $p \equiv 1 \mod 4$, but that $\exp_p(-g) = (p - 1)/2$ if $p \equiv 3 \mod 4$.

Proof. Let d be a divisor of $p - 1$. Since g is a primitive root and

$$g^{p-1} \equiv 1 \mod p \quad \text{and} \quad g^{(p-1)/2} \equiv -1 \mod p,$$

then $|g^d| \equiv \pm 1 \mod p$ implies $d = p - 1$ or $d = (p - 1)/2$. This means we only need to test these exponents to find $\exp_p(-g)$.

If $p \equiv 1 \mod 4$, then

$$(-g)^{(p-1)/2} = g^{(p-1)/2} \equiv -1 \mod p.$$

This means $\exp_p(-g) = p - 1$, i.e. $-g$ is a primitive root. If $p \equiv 3 \mod 4$, then

$$(-g)^{(p-1)/2} = -g^{(p-1)/2} \equiv 1 \mod p.$$

This means $\exp_p(-g) = (p - 1)/2$. □

Exercise 10.4.
(a) Prove that 3 is a primitive root mod p if p is a prime of the form $2^n + 1$, $n > 1$.
(b) Prove that 2 is a primitive root mod p if p is a prime of the form $4q + 1$, where q is an odd prime.

Proof.
(a) If p is prime, by Exercise 1.17 p is of the form $2^{2^k} + 1$ for some $k > 0$. Then Exercise 10.10 tells us it's enough to show 3 is a quadratic nonresidue mod p. Since

$$2^{2^k} + 1 \equiv (-1)^{2^k} + 1 \equiv 2 \mod 3,$$

by quadratic reciprocity $(3|\, p) = (p|\, 3) = (2|\, 3) = -1$.
(b) The proper divisors of $\varphi(p)$ are $1, 2, 4, 2q$. Thus to show 2 is a primitive root, we need to show 2 raised to each of these powers are not congruent to 1. Now it's easy to see 2^1 and 2^2 are not congruent to 1 mod p. Also since the only prime of this form less than 16 is 13, it's easy to see $2^4 \not\equiv 1 \mod p$. Finally, by Euler's criterion $2^{2q} \equiv (2|\, p) \mod p$ and

$$(2|\, p) = (-1)^{(p^2-1)/8} = (-1)^{2q^2+q} = -1.$$

□

Exercise 10.5. Let $m > 2$ be an integer having a primitive root, and let $(a, m) = 1$. We write aRm is there exists an x such that $a \equiv x^2 \mod m$. Prove that:
(a) aRm if, and only if, $a^{\varphi(m)/2} \equiv 1 \mod m$.
(b) If aRm the congruence $x^2 \equiv a \mod m$ has exactly two solutions.
(c) There are exactly $\varphi(m)/2$ integers a, incongruent mod m, such that $(a, m) = 1$ and aRm.

Proof. Let g be a primitive root mod m.
(a) If aRm, then $a \equiv x^2 \mod m$ for some x. This implies $a^{\varphi(m)/2} \equiv x^{\varphi(m)} \equiv 1 \mod m$. Now suppose $a^{\varphi(m)/2} \equiv 1 \mod m$ and $a \equiv g^k \mod m$. Substituting gives

$$g^{k\varphi(m)/2} \equiv 1 \mod m,$$

and by Theorem 10.1, $k\varphi(m)/2 \equiv 0 \mod \varphi(m)$. Thus $k\varphi(m) = 2n\varphi(m)$ for some n, which means $k = 2n$. We conclude aRm, since $a \equiv (g^n)^2 \mod m$.
(b) Suppose $a \equiv g^{2n} = (g^n)^2 \mod m$ and suppose further that $a \equiv \left(g^k\right)^2 \mod m$. This means $g^{2(k-n)} \equiv 1 \mod m$. By Theorem 10.1, $2(k-n) \equiv 0 \mod \varphi(m)$, which implies $k = n + c\,\varphi(m)/2$ for some c. Therefore there is exactly one solution where $1 \le k \le \varphi(m)/2$ and exactly one solution where $\varphi(m)/2 < k \le \varphi(m)$.
(c) It's clear $g^{2n}Rm$ for all n, so there are at least $\varphi(m)/2$ of the desired incongruent integers. Now suppose $g^{2k+1} \equiv x^2 \mod m$. If $x \equiv g^j \mod m$, then $2k+1 \equiv 2j \mod \varphi(m)$. This would imply $\varphi(m)$ divides an odd number, which can't happen. We conclude $g^{2k+1}NRm$, and so there are exactly $\varphi(m)/2$ integers a, incongruent mod m, such that $(a, m) = 1$ and aRm. □

Exercise 10.6. Assume $m > 2$, $(a, m) = 1$, aRm. Prove that the congruence $x^2 \equiv a \mod m$ has exactly two solutions if, and only if, m has a primitive root.

Proof. If m has a primitive root, then Exercise 10.5 (b) shows the congruence $x^2 \equiv a \mod m$ has exactly two solutions. Now suppose the congruence $x^2 \equiv a \mod m$ does not have exactly two solutions. Since the solutions come in pairs $\pm x$, the congruence $x^2 \equiv a \mod m$ has at least 4 solutions, so there are at most $\varphi(m)/2 - 1$ integers a, incongruent mod m, such that $(a, m) = 1$ and aRm. This is the contrapositive of the statement in Exercise 10.5 (c), so we conclude that m does not have a primitive root. □

Exercise 10.7. Let $S_n(p) = \sum_{k=1}^{p-1} k^n$, where p is an odd prime and $n > 1$. Prove that

$$S_n(p) = \begin{cases} 0 \mod p & \text{if } n \not\equiv 0 \mod p-1, \\ -1 \mod p & \text{if } n \equiv 0 \mod p-1. \end{cases}$$

Proof. If $n \equiv 0 \mod p-1$, then for $(k, n) = 1$, $k^n \equiv 1 \mod p-1$. This means

$$S_n(p) \equiv \sum_{k=1}^{p-1} 1 \equiv -1 \mod p.$$

Now suppose $n \not\equiv 0 \mod p-1$ and let g be a primitive root. We then have

$$S_n(p) \equiv \sum_{k=1}^{p-1} g^{kn} = \frac{g^{pn} - g^n}{g^n - 1} \mod p.$$

Since $n \not\equiv 0 \mod p-1$ we know $g^n \not\equiv 1 \mod p$. Therefore by applying Lemma 5.12,

$$\frac{g^{pn} - g^n}{g^n - 1} \equiv (g^{pn} - g^n)(g^n - 1)^{-1} \equiv (g^n - g^n)(g^n - 1)^{-1} \equiv 0 \mod p.$$

□

Exercise 10.8. Prove that the sum of the primitive roots mod p is congruent to $\mu(p-1)$ mod p.

Proof. Let g be a primitive root mod p and S be the sum in question, that is

$$S = \sum_{\substack{k=1 \\ (k,\varphi(p))=1}}^{p-1} g^k.$$

Then by Lemma 3.12,

$$\begin{aligned} S &= \sum_{d|p-1} \mu(d) \sum_{k \le (p-1)/d} g^{kd} \\ &= \sum_{d|p-1} \mu(d) \frac{g^d(g^{p-1} - 1)}{g^d - 1} \\ &= \mu(p-1)g^{p-1} + \sum_{\substack{d|p-1 \\ d<p-1}} \mu(d) \frac{g^d(g^{p-1} - 1)}{g^d - 1}. \end{aligned} \tag{15}$$

Now since g is a primitive root, $g^d \not\equiv 1 \bmod p$ for all positive $d < p-1$. This means $(g^d - 1, p) = 1$ and so we can apply Lemma 5.12 to see

$$\frac{g^{p-1}-1}{g^d-1} \equiv (g^{p-1}-1)(g^d-1)^{-1} \equiv 0 \mod p.$$

Hence it follows from (15) that $S \equiv \mu(p-1) \bmod p$. □

Exercise 10.9. If p is an odd prime > 3 prove that the product of the primitive roots mod p is congruent to 1 mod p.

Proof. Let P be the product in question and g be a primitive root mod p. We then have

$$P \equiv \prod_{\substack{k=1 \\ (k,\varphi(p))=1}}^{p-1} g^k \mod p,$$

that is P is a power of g with exponent

$$e = \sum_{\substack{k=1 \\ (k,\varphi(p))=1}}^{p-1} k.$$

By Lemma 3.12,

$$\begin{aligned} e &= \sum_{d|p-1} \mu(d) \sum_{k \le (p-1)/d} kd \\ &= \frac{1}{2}(p-1) \sum_{d|p-1} \mu(d) \frac{p-1+d}{d} \\ &= \frac{1}{2}(p-1) \sum_{d|p-1} \mu(d) \frac{p-1}{d} + \frac{1}{2}(p-1) \sum_{d|p-1} \mu(d) \\ &= \frac{1}{2}(p-1)\varphi(p-1), \end{aligned}$$

and so $P \equiv g^{\varphi(p-1)(p-1)/2} \bmod p$. If $p > 3$, then $\varphi(p-1)$ is even and therefore

$$P = \left(g^{p-1}\right)^{\varphi(p-1)/2} \equiv 1 \mod p.$$

□

Exercise 10.10. Let p be an odd prime of the form $2^{2^k}+1$. Prove that the set of primitive roots mod p is equal to the set of quadratic nonresidues mod p. Use this result to prove that 7 is a primitive root of every such prime.

Remark. The last part of this exercise is only true for $k > 0$.

Lemma 10.10. If n is an integer, then $2^n \equiv 1, 2, 4 \bmod 7$.

Proof of Lemma. Let $n = 3q + r$, where $0 \leq r \leq 2$. Then since $\varphi(7) = 3$,

$$2^n \equiv 2^r \equiv 1, 2, 4 \mod 7.$$

□

Proof of Exercise. If g is a primitive root, then $g^{(p-1)/2} \not\equiv 1 \mod p$. Thus by Euler's criterion $(g|\, p) = -1$. On the other hand, if $(g|\, p) = -1$, again by Euler's criterion $g^{(p-1)/2} \not\equiv 1 \mod p$. Now observe every proper divisor d of $\varphi(p)$ is a power of 2 and hence d divides $(p-1)/2$. Thus $g^d \equiv 1 \mod p$ would imply $g^{(p-1)/2} \equiv 1 \mod p$, a contradiction. This means $\exp_p(g) = \varphi(p)$, i.e. g is a primitive root.

Next, by quadratic reciprocity

$$(7|\, p) = (-1)^{3(p-1)/2}\,(p|\, 7) = \begin{cases} -\,(p|\, 7) & \text{if } p = 3 \\ (p|\, 7) & \text{if } p > 3. \end{cases}$$

Furthermore, $2^{2^k} \not\equiv 1 \mod 7$, since $2^k \not\equiv 0 \mod \varphi(7)$. Thus Lemma 10.10 implies

$$p = 2^{2^k} + 1 \equiv 3, 5 \mod 7.$$

Since 3 and 5 are both quadratic nonresidues mod 7, we have

$$(7|\, p) = \begin{cases} 1 & \text{if } p = 3 \\ -1 & \text{if } p > 3. \end{cases}$$

This means 7 is a primitive root of the prime $2^{2^k} + 1$ if and only if $k > 0$. □

Exercise 10.11. Assume $d \mid \varphi(m)$. If $d = \exp_m(a)$ we say that a is a primitive root of the congruence

$$x^d \equiv 1 \mod m.$$

Prove that if the congruence

$$x^{\varphi(m)} \equiv 1 \mod m$$

has a primitive root then it has $\varphi(\varphi(m))$ primitive roots, incongruent mod m.

Proof. This follows directly from Theorem 10.9. □

Exercise 10.12. Prove the properties of indices described in Theorem 10.10. Let g be a primitive root mod m. If $(a, m) = (b, m) = 1$ show
(a) $\operatorname{ind}_g(ab) \equiv \operatorname{ind}_g(a) + \operatorname{ind}_g(b) \mod \varphi(m)$.
(b) $\operatorname{ind}_g(a^n) \equiv n \operatorname{ind}_g(a) \mod \varphi(m)$.
(c) $\operatorname{ind}_g(1) = 0$ and $\operatorname{ind}_g(g) = 1$.
(d) $\operatorname{ind}_g(-1) = \varphi(m)/2$ if $m > 2$.
(e) If g' is also a primitive root mod m then

$$\operatorname{ind}_g(a) \equiv \operatorname{ind}_{g'}(a) \cdot \operatorname{ind}_g(g') \mod \varphi(m).$$

Proof.
(a) By definition we have

$$g^{\operatorname{ind}_g(ab)} \equiv ab \equiv g^{\operatorname{ind}_g(a)} g^{\operatorname{ind}_g(b)} \equiv g^{\operatorname{ind}_g(a)+\operatorname{ind}_g(b)} \mod m.$$

Since g is a primitive root, Theorem 10.1 implies $\operatorname{ind}_g(ab) \equiv \operatorname{ind}_g(a) + \operatorname{ind}_g(b) \mod \varphi(m)$.
(b) We have

$$g^{\operatorname{ind}_g(a^n)} \equiv a^n \equiv \left(g^{\operatorname{ind}_g(a)}\right)^n = g^{n \operatorname{ind}_g(a)} \mod m.$$

Again we use Theorem 10.10 to obtain $\operatorname{ind}_g(a^n) \equiv n \operatorname{ind}_g(a) \mod \varphi(m)$.
(c) This part is clear, as $g^0 = 1$ and $g^1 = g$.
(d) Let $s = \operatorname{ind}_g(-1)$. Then $g^s \equiv -1 \mod m$ and squaring both sides gives $g^{2s} \equiv 1 \mod m$. Theorem 10.1 implies

$$2s \equiv 0 \mod \varphi(m). \tag{16}$$

Since $m > 2$, $\varphi(m)$ is even, thus choosing $s = \varphi(m)/2$ gives the smallest positive s that satisfies (16).
(e) We have

$$\begin{aligned} g^{\operatorname{ind}_g(a)} &\equiv a \equiv (g')^{\operatorname{ind}_{g'}(a)} \\ &\equiv \left(g^{\operatorname{ind}_g(g')}\right)^{\operatorname{ind}_{g'}(a)} \\ &\equiv g^{\operatorname{ind}_{g'}(a)\cdot\operatorname{ind}_g(g')} \mod m. \end{aligned}$$

By Theorem 10.1, $\operatorname{ind}_g(a) \equiv \operatorname{ind}_{g'}(a) \cdot \operatorname{ind}_g(g') \mod \varphi(m)$. □

Exercise 10.13.(++) Let p be an odd prime. If $(h, p) = 1$ let

$$S(h) = \{h^n \mid 1 \le n \le p-1, (n, p-1) = 1\}.$$

If h is a primitive root of p the numbers in the set $S(h)$ are distinct mod p (they are, in fact, the primitive roots of p). Prove that there is an integer h, not a primitive root of p, such that the numbers in $S(h)$ are distinct mod p if, and only if, $p \equiv 3 \mod 4$.

Proof. Suppose $p \equiv 3 \mod 4$ and g is a primitive root. By Exercise 10.3 $\exp_p(-g) = (p-1)/2$, therefore $-g$ is not a primitive root. We will show all numbers in $S(-g)$ are distinct mod p. Now suppose

$$(-g)^n \equiv (-g)^m \mod p, \text{ where } 1 \le n \le m \le p-1.$$

Since $\exp_p(-g) = (p-1)/2$, by Theorem 10.1,

$$n \equiv m \mod \frac{p-1}{2}.$$

Recalling $1 \le n \le m \le p-1$, we have $m = n + (p-1)/2$.

If $(n, p-1) = 1$, then n must be odd. Since $(p-1)/2$ is also odd, we have m is even, hence $(m, p-1) \neq 1$. In a similar fashion, assuming $(m, p-1) = 1$ shows $(n, p-1) \neq 1$. This means at most one of $(-g)^n$ and $(-g)^m$ is a member of $S(-g)$.

Suppose $p \equiv 1 \bmod p$ and $\exp_p(h) = d < p-1$. For $h^n \in S(h)$ we have by the lemma of Theorem 10.3

$$\exp_p(h^n) = \frac{\exp_p(h)}{(n, p-1)} = d.$$

Theorem 10.4 thus implies that $S(h)$ contains at most $\varphi(d)$ different elements mod p. However, by construction $S(h)$ contains $\varphi(p-1)$ elements. By the pigeonhole principal if we can show $\varphi(d) < \varphi(p-1)$, we are done.

Write $p - 1 = 4p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ and $d = 2^{\beta} p_1^{\beta_1} \cdots p_r^{\beta_r}$, where p_i are distinct odd primes and $\alpha_i > 0$. Note $d < p-1$ implies $2 > \beta$ or there is an i such that $\alpha_i > \beta_i$. We have

$$\begin{aligned}
\varphi(d) &= \varphi(2^{\beta}) \prod_{\substack{i=1 \\ \beta_i \neq 0}}^{r} p_i^{\beta_i - 1}(p_i - 1) \\
&< 2 \prod_{i=1}^{r} p_i^{\alpha_i - 1}(p_i - 1) \\
&= \varphi(p-1),
\end{aligned}$$

where the inequality is strict since $\varphi(2^{\beta}) = 1$ for $2 > \beta$ and $\varphi(p_i^{\beta_i}) < \varphi(p_i^{\alpha_i})$ for $\alpha_i > \beta_i$. □

Exercise 10.14. If $m > 1$ let $p_1, \ldots, p_k$ be the distinct prime divisors of $\varphi(m)$. If $(g, m) = 1$ prove that g is a primitive root of m if, and only if, g does not satisfy any of the congruences $g^{\varphi(m)/p_i} \equiv 1 \bmod m$ for $i = 1, 2, \ldots, k$.

Proof. If g is a primitive root, it's clear $g^{\varphi(m)/p_i} \not\equiv 1 \bmod m$ for all $i = 1, 2, \ldots, k$. For the other direction, suppose g has order d, where $d \mid \varphi(m)$ and $d \neq \varphi(m)$. If $p_i \mid \varphi(m)/d$, then observe $d \mid \varphi(m)/p_i$. Since $g^d \equiv 1 \bmod m$, this implies $g^{\varphi(m)/p_i} \equiv 1 \bmod m$. □

Exercise 10.15. The prime $p = 71$ has 7 as a primitive root. Find all primitive roots of 71 and also find a primitive root for p^2 and for $2p^2$.

Solution. There are $\varphi(\varphi(71)) = 24$ primitive roots mod 71 and we find them in Mathematica.

```
In[1]:= Sort[PowerMod[7, #, 71]& /@ Select[Range[70], CoprimeQ[#,70]&]]
Out[1]= {7, 11, 13, 21, 22, 28, 31, 33, 35, 42, 44, 47, 52, 53, 55, 56,
         59, 61, 62, 63, 65, 67, 68, 69}
```

Now since $7^{p-1} \equiv 49 \bmod p^2$, by Theorem 10.6, 7 is a primitive root mod p^2. By Theorem 10.7, this implies 7 is also a primitive root mod $2p^2$.

Exercise 10.16. Solve each of the following congruences:
(a) $8x \equiv 7 \bmod 43$.
(b) $x^8 \equiv 17 \bmod 43$.
(c) $8^x \equiv 3 \bmod 43$.

Solution. Through Table 10.1 we are given 3 is a primitive root mod 43.
(a) The corresponding index relation is

$$\operatorname{ind}_3(x) \equiv \operatorname{ind}_3(7) - \operatorname{ind}_3(8) \mod 42.$$

From Table 10.2 we find $\operatorname{ind}_3(7) = 35$ and $\operatorname{ind}_3(8) = 39$, so

$$\operatorname{ind}_3(x) \equiv 35 - 39 \equiv 38 \mod 42.$$

Again from Table 10.2 we find $x \equiv 17 \bmod 43$.
(b) The corresponding index relation is

$$8 \operatorname{ind}_3(x) \equiv \operatorname{ind}_3(17) \equiv 38 \mod 42.$$

Applying Theorem 5.4, dividing both sides 2 gives $4 \operatorname{ind}_3(x) \equiv 19 \bmod 21$. Multiplying both sides by 16 shows $\operatorname{ind}_3(x) \equiv 10 \bmod 21$. This gives possible index values 10 and 31. From Table 10.2 we find $x \equiv 10, 33 \bmod 43$ are the only solutions.
(c) We have $\operatorname{ind}_3(8) = 39$ and $\operatorname{ind}_3(3) = 1$. The corresponding index relation is thus

$$39x \equiv 1 \mod 42.$$

Since $(39, 42) = 3$, 39 is not invertible mod 42, hence no solution exists.

Exercise 10.17. Let q be an odd prime and suppose that $p = 4q + 1$ is also prime.
(a) Prove that the congruence $x^2 \equiv -1 \bmod p$ has exactly two solutions, each of which is a quadratic nonresidue of p.
(b) Prove that every quadratic nonresidue of p is a primitive root of p, with the exception of the two nonresidues in (a).
(c) Find all the primitive roots of 29.

Proof.
(a) Since $p \equiv 1 \bmod 4$, $(-1|p) = 1$. By Theorem 5.21 (Lagrange's Theorem), there are at most two solutions. Since x, $-x$ both satisfy the congruence, there are exactly two solutions. Now if g is a primitive root, then we can take $x = g^{(p-1)/4} = g^q$ as a solution. Since $\operatorname{ind}_g(x) = q$ is odd, x is a quadratic nonresidue mod p. Finally $-x$ is also a quadratic nonresidue mod p since $(-x|p) = (-1|p)(x|p) = -1$.
(b) Let g be a primitive root. All primitive roots are of the form g^k, where $(k, 4q) = 1$. This means k needs to be odd and relatively prime to q. Each quadratic nonresidue mod p whose exponent is relatively prime to q are the only numbers to satisfy this stipulation. Finally, the quadratic nonresidues that aren't primitive roots are hence g^q, g^{3q} and both satisfy the congruence in (a).
(c) Since $29 = 4 \cdot 7 + 1$, we can apply (b). Using Mathematica we will find all quadratic nonresidues whose square is not $-1 \bmod 29$.

```
In[2]:= Module[{G = Range[28]},
  (* remove the quadratic residues *)
  G = Complement[G, Mod[G^2, 29]];

  (* remove elements whose square is -1 *)
  Select[G, Mod[#^2, 29] != 28 &]
]
Out[2]= {2, 3, 8, 10, 11, 14, 15, 18, 19, 21, 26, 27}
```

□

Exercise 10.18. (Extension of Exercise 10.17.) Let q be an odd prime and suppose that $p = 2^n q + 1$ is prime. Prove that every quadratic nonresidue a of p is a primitive root of p if $a^{2^n} \not\equiv 1 \bmod p$.

Proof. Let a be a quadratic nonresidue mod p such that $a^{2^n} \not\equiv 1 \bmod p$. Since $\varphi(p) = 2^n q$, applying Exercise 10.14 to show a is a primitive root, it's enough to establish

$$a^{\varphi(p)/2} \not\equiv 1 \mod p \text{ and } a^{\varphi(p)/q} \not\equiv 1 \mod p.$$

Now because a is a quadratic nonresidue, $a^{\varphi(p)/2} = a^{(p-1)/2} \equiv -1 \bmod p$. Additionally since $\varphi(p)/q = 2^n$, we have $a^{\varphi(p)/q} \not\equiv 1 \bmod p$. This means a is a primitive root. □

Exercise 10.19. Prove that there are only two real primitive characters mod 8 and make a table showing their values.

Proof. Theorem 10.13 tells us there are four real characters mod 8. Since there are exactly $\varphi(8) = 4$ characters mod 8, every character must be real. Consequently, it is enough to find the numbers of primitive characters mod 8.

Now by Theorem 10.15, a character $\chi_{a,c}$ mod 8 is primitive if and only if c is odd. Since the possible values of a and c are both 1 and 2, we conclude there are exactly two primitive characters mod 8, which occur when $c = 1$.

These characters correspond to the rows 2 and 4 of χ mod 8 in Exercise 6.14. □

Exercise 10.20. Let χ be a real primitive character mod m. If m is not a power of 2 prove that m has the form

$$2^\alpha p_1 \cdots p_r$$

where the p_i are distinct odd primes and $\alpha = 0$, 2, or 3. If $\alpha = 0$ show that

$$\chi(-1) = \prod_{p|m} (-1)^{(p-1)/2}$$

and find a corresponding formula for $\chi(-1)$ when $\alpha = 2$.

Lemma 10.20. Let p be an odd prime, $\alpha > 0$, and χ be a character mod p^α. Then χ is real and primitive if and only if $\alpha = 1$ and $\chi(n) = (n|\,p)$ for all n.

Proof of Lemma. For the converse direction, it is clear $(n|\,p)$ is real. Furthermore since $(n|\,p)$ is nonprincipal and p is prime, by Theorem 8.14 it must be primitive. Looking at the forward direction, let χ_h be a real primitive character mod p^α, where χ_h is defined in Chapter 10. Since χ_h is real, by Theorem 10.12 we find $h = 0$ or $h = \varphi(p^\alpha)/2$. Additionally since χ_h is primitive, by Theorem 10.14 we have $p \nmid h$. This forces $h = \varphi(p^\alpha)/2$. However

$$\varphi(p^\alpha)/2 = p^{\alpha-1} \cdot \frac{p-1}{2},$$

so to satisfy $p \nmid h$ we require $\alpha = 1$. Since there is a unique real nonprincipal character mod p (Theorem 10.12) and $(n|\,p)$ is real, we must have $\chi(n) = (n|\,p)$ for all n. □

Proof of Exercise. Let $m = 2^\alpha p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, where p_i is an odd prime and write

$$\chi = \psi \cdot \chi_1 \cdots \chi_r,$$

where ψ is a character mod 2^α and χ_i is a character mod $p_i^{\alpha_i}$. By Exercise 8.12 χ is primitive mod m if and only if ψ is primitive mod 2^α and χ_i is primitive mod $p_i^{\alpha_i}$ for all i.

By Lemma 10.20 χ_i is real and primitive if and only if $\alpha_i = 1$ and $\chi_i(n) = (n|\,p_i)$. Turning out attention to ψ, we can write $\psi = \psi_{a,c}$, where this is defined in Chapter 10. If $\alpha = 0$ or $\alpha = 2$, then by inspection ψ must be real and primitive, whereas if $\alpha = 1$, then ψ is not primitive. If $\alpha \geq 3$, by Theorem 10.13, $\psi_{a,c}$ is real if and only if $c = \varphi(2^\alpha)/2$ or $c = \varphi(2^\alpha)/4$. Moreover by Theorem 10.15, $\psi_{a,c}$ is primitive if and only if c is odd. Now for $\alpha \geq 3$, $\varphi(2^\alpha)/2$ is never odd and $\varphi(2^\alpha)/4$ is odd if and only if $\alpha = 3$. Thus for $\psi_{a,c}$ to be real and primitive, it must be that $\alpha = 3$.

Now

$$\chi(-1) = \psi(-1) \prod_{p|m} (-1|\,p) = \psi(-1) \prod_{p|m} (-1)^{(p-1)/2}.$$

By inspection if $\alpha = 0$, then $\psi(-1) = 1$ and if $\alpha = 2$, then $\psi(-1) = -1$.

□

Chapter 11
Dirichlet Series and Euler Products

Exercise 11.1. Derive the following identities, valid for $\sigma > 1$.

(a) $\zeta(s) = s\int_1^\infty \frac{[x]}{x^{s+1}}dx.$

(b) $\sum_p \frac{1}{p^s} = s\int_1^\infty \frac{\pi(x)}{x^{s+1}}dx,$ where the sum is extended over all primes.

(c) $\frac{1}{\zeta(s)} = s\int_1^\infty \frac{M(x)}{x^{s+1}}dx,$ where $M(x) = \sum_{n\le x}\mu(n).$

(d) $-\frac{\zeta'(s)}{\zeta(s)} = s\int_1^\infty \frac{\psi(x)}{x^{s+1}}dx,$ where $\psi(x) = \sum_{n\le x}\Lambda(n).$

(e) $L(s,\chi) = s\int_1^\infty \frac{A(x)}{x^{s+1}}dx,$ where $A(x) = \sum_{n\le x}\chi(n).$

Show that (e) is also valid for $\sigma > 0$ if χ is a non principal character. [*Hint*: Theorem 4.2.]

Lemma 11.1. Let $A(x) = \sum_{n\le x} a_n = O(x\log x)$ and $F(s) = \sum_{n=1}^\infty a_n n^{-s}$. If $A(x) = O(1)$ let $c = 0$, otherwise let $c = 1$. Then for $\sigma > c$,

$$F(s) = s\int_1^\infty \frac{A(x)}{x^{s+1}}dx.$$

Proof of Lemma. By Abel's summation formula,

$$\sum_{n=1}^N a_n n^{-s} = A(N)N^{-s} + s\int_1^N \frac{A(x)}{x^{s+1}}dx.$$

Suppose $A(x) = O(1)$. We have $A(N)N^{-s} \to 0$ as $N\to\infty$ for $\sigma > 0$. Also

$$\int_1^N \frac{A(x)}{x^{s+1}}dx = O\left(\int_1^N \frac{1}{x^{s+1}}dx\right),$$

and thus converges for $\sigma > 0$ as $N\to\infty$. Hence letting $N\to\infty$ gives the result.

We're given $A(x) = O(x \log x)$ so for $\sigma > 1$, $A(N)N^{-s} \to 0$ as $N \to \infty$. Also

$$\int_1^N \frac{A(x)}{x^{s+1}} dx = O\left(\int_1^N \frac{\log x}{x^s} dx \right),$$

and thus converges for $\sigma > 1$ as $N \to \infty$. Hence letting $N \to \infty$ gives the result. □

Proof of Exercise.
(a) This follows directly from Lemma 11.1 with $a_n = 1$.
(b) This follows directly from Lemma 11.1 with a_n indicating whether n is prime.
(c) This follows directly from Lemma 11.1 with $a_n = \mu(n)$.
(d) This follows directly from Lemma 11.1 with $a_n = \Lambda(n)$.
(e) Let $a_n = \chi(n)$. If χ is a nonprincipal character mod k, then $|A(x)| \le \varphi(k) = O(1)$. If χ is principal, then $A(x) = \varphi(k) \lfloor x/k \rfloor + O(1)$. The result then follows from Lemma 11.1. □

Exercise 11.2. Assume that the $\sum_{n=1}^{\infty} f(n)$ converges with sum A, and let $A(x) = \sum_{n \le x} f(n)$.
(a) Prove that the Dirichlet series $F(s) = \sum_{n=1}^{\infty} f(n) n^{-s}$ converges for each s with $\sigma > 0$ and that

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^s} = A - s \int_1^{\infty} \frac{R(x)}{x^{s+1}} dx,$$

where $R(x) = A - A(x)$. [*Hint*: Theorem 4.2.]
(b) Deduce that $F(\sigma) \to A$ as $\sigma \to 0^+$.
(c) If $\sigma > 0$ and $N \ge 1$ is an integer, prove that

$$F(s) = \sum_{n=1}^{N} \frac{f(n)}{n^s} - \frac{A(N)}{N^s} + s \int_N^{\infty} \frac{A(y)}{y^{s+1}} dy.$$

(d) Write $s = \sigma + it$, take $N = 1 + [\,|t|\,]$ in (c) and show that

$$|F(\sigma + it)| = O\big(|t|^{1-\sigma}\big) \quad \text{if } 0 < \sigma < 1.$$

Proof.
(a) For $\sigma > 0$ and $N \ge 1$, by Abel's summation formula

$$\begin{aligned}
\sum_{n \le N} \frac{f(n)}{n^s} &= \frac{A(N)}{N^s} + s \int_1^N \frac{A(x)}{x^{s+1}} dx \\
&= [A - A] + \frac{A(N)}{N^s} + s \int_1^N \frac{A(x)}{x^{s+1}} dx \\
&= A - As \int_1^{\infty} \frac{dx}{x^{s+1}} + \frac{A(N)}{N^s} + s \int_1^N \frac{A(x)}{x^{s+1}} dx \\
&= A + \frac{A(N)}{N^s} - s \int_1^N \frac{A - A(x)}{x^{s+1}} dx - As \int_N^{\infty} \frac{A(x)}{x^{s+1}} dx.
\end{aligned}$$

For $\sigma > 0$, $A(N)N^{-s} \to 0$ and $\int_N^\infty A(x)x^{-s-1}dx \to 0$ as $N \to \infty$. This gives

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^s} = A - s\int_1^\infty \frac{A - A(x)}{x^{s+1}}dx.$$

(b) Let $\varepsilon > 0$ be arbitrary. Fix N so that for all $x \geq N$, $|R(x)| < \varepsilon$. We then have for $\sigma > 0$

$$\begin{aligned}\left|\sigma\int_1^\infty \frac{R(x)}{x^{\sigma+1}}dx\right| &< \sigma\int_1^N \frac{|R(x)|}{x^{\sigma+1}}dx + \sigma\varepsilon\int_N^\infty \frac{dx}{x^{\sigma+1}} \\ &= \sigma\int_1^N \frac{|R(x)|}{x^{\sigma+1}}dx + \frac{\varepsilon}{N^\sigma}.\end{aligned}$$

Since this holds for $\sigma > 0$, letting $\sigma \to 0^+$ on both sides of the inequality gives

$$\lim_{\sigma\to 0^+}\left|\sigma\int_1^\infty \frac{R(x)}{x^{\sigma+1}}dx\right| \leq \varepsilon.$$

Since ε was chosen arbitrarily it can be as small as we like, hence the limit must be 0. The result then follows directly form (a).
(c) For $\sigma > 0$ and $1 \leq N < M$, by Abel's summation formula

$$\begin{aligned}\sum_{n=1}^{M} \frac{f(n)}{n^s} &= \sum_{n=1}^{N} \frac{f(n)}{n^s} + \sum_{n=N+1}^{M} \frac{f(n)}{n^s} \\ &= \sum_{n=1}^{N} \frac{f(n)}{n^s} - \frac{A(N)}{N^s} + \frac{A(M)}{M^s} + s\int_N^M \frac{A(y)}{y^{\sigma+1}}dy.\end{aligned}$$

Noting $\sigma > 0$ and $A(x) = O(1)$, let $M \to \infty$. As a consequence $A(M)M^{-s} \to 0$ and the integral converges, which finishes the proof.
(d) Since $\sum_{n=1}^\infty f(n)$ converges, we have $f(n) \to 0$ as $n \to \infty$ and thus

$$M = \max_{n\geq 1}|f(n)| < \infty.$$

So by (c) and Theorem 3.2 (b), for $\sigma > 0$ and $\sigma \neq 1$,

$$\begin{aligned}|F(\sigma + it)| &\leq \sum_{n=1}^{N} \frac{|f(n)|}{n^\sigma} + \frac{|A(N)|}{N^\sigma} + |s|\int_N^\infty \frac{|A(y)|}{y^{\sigma+1}}dy \\ &\leq M\sum_{n=1}^{N} \frac{1}{n^\sigma} + O(1) + O(|t|)\,O\left(\int_N^\infty \frac{dy}{y^{\sigma+1}}\right) \\ &= O\left(N^{1-\sigma}\right) + O(1) + O(|t|)\,O\left(N^{-\sigma}\right).\end{aligned}$$

Now $N \sim |t|$ as $t \to \infty$, so it follows that $|F(\sigma + it)| = O(|t|^{1-\sigma})$. □

Exercise 11.3.
(a) Prove that the series $\sum n^{-1-it}$ has bounded partial sums if $t \neq 0$. When $t = 0$ the partial sums are unbounded.
(b) Prove that the series $\sum n^{-1-it}$ diverges for all real t. In other words, the Dirichlet series for $\zeta(s)$ diverges everywhere on the line $\sigma = 1$.

Proof.
(a) Fix $t \neq 0$. By Abel's summation formula with $a(n) = 1$ and $f(x) = x^{-1-it}$ we have

$$\begin{aligned}\sum_{n=1}^{N} n^{-1-it} &= N \cdot N^{-1-it} + (1+it)\int_1^N \lfloor x \rfloor\, x^{-2-it}dx \\ &= N^{-it} + (1+it)\int_1^N x^{-1-it}dx - (1+it)\int_1^N \{x\}\, x^{-2-it}dx \\ &= N^{-it} - \frac{1+it}{it}N^{-it} + \frac{1+it}{it} - (1+it)\left(\int_1^\infty - \int_N^\infty\right)\{x\}\, x^{-2-it}dx \\ &= (i/t)N^{-it} + C + o(1) \\ &= O(1)\,.\end{aligned}$$

Therefore the partial sums are bounded.
(b) From above,

$$\begin{aligned}\sum_{n=1}^{N} n^{-1-it} &= (i/t)N^{-it} + C + o(1) \\ &= (i/t)(\cos(t\log N) - i\sin(t\log N)) + C + o(1)\,.\end{aligned}$$

Thus as $N \to \infty$ both real and imaginary parts of the partial sums will oscillate without approaching a single value, that is $\sum_{n=1}^{\infty} n^{-1-it}$ diverges. □

Exercise 11.4. Let $F(s) = \sum_{n=1}^{\infty} f(n)n^{-s}$ where $f(n)$ is completely multiplicative and the series converges absolutely for $\sigma > \sigma_a$. Prove that if $\sigma > \sigma_a$ we have

$$\frac{F'(s)}{F(s)} = -\sum_{n=1}^{\infty}\frac{f(n)\Lambda(n)}{n^s}.$$

Proof. Example 2 following Theorem 11.14 shows for $\sigma > \sigma_a$, $F(s) = e^{G(s)}$, where

$$G(s) = \sum_{n=2}^{\infty}\frac{f(n)\Lambda(n)}{\log n}n^{-s}.$$

Thus

$$F'(s) = e^{G(s)}G'(s) = F(s)G'(s),$$

or in other words

$$\frac{F'(s)}{F(s)} = -\sum_{n=1}^{\infty}\frac{f(n)\Lambda(n)}{n^s}.$$

□

In the following exercises, $\lambda(n)$ is Liouville's function, $d(n)$ is the number of divisors of n, $\nu(n)$ and $\kappa(n)$ are defined as follows: $\nu(1) = 0$, $\kappa(1) = 1$; if $n = p_1^{a_1}\cdots p_k^{a_k}$ then $\nu(n) = k$ and $\kappa(n) = a_1a_2\cdots a_k$.

Prove that the identities in Exercises 5 through 10 are valid for $\sigma > 1$.

Exercise 11.5. $\displaystyle\sum_{n=1}^{\infty} \frac{d(n^2)}{n^s} = \frac{\zeta^3(s)}{\zeta(2s)}.$

Lemma 11.5. For all x with $|x| < 1$,

$$\sum_{n=0}^{\infty} nx^n = \frac{x}{(x-1)^2}.$$

Proof of Lemma. Differentiating the geometric series term by term,

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

Multiplying both sides by x gives the result. □

Proof of Exercise. Since $(m,n) = 1$ implies $(m^2, n^2) = 1$, it's clear $d(n^2)$ is multiplicative. Also note

$$d(n^2) < n^2,$$

so $\sum_{n=1}^{\infty} d(n^2)n^{-s}$ converges for $\sigma > 3$. Hence for $\sigma > 3$, by Theorem 11.7,

$$\begin{aligned}\sum_{n=1}^{\infty} \frac{d(n^2)}{n^s} &= \prod_p \sum_{m=0}^{\infty} \frac{d(p^{2m})}{p^{ms}} \\ &= \prod_p \sum_{m=0}^{\infty} \frac{2m+1}{p^{ms}} \\ &= \prod_p \frac{p^s(p^s+1)}{(p^s-1)^2},\end{aligned}$$

where Lemma 11.5 was applied in the last step. Multiplying numerator and denominator by $p^{-2s}(1-p^{-s})$,

$$\begin{aligned}\prod_p \frac{p^s(p^s+1)}{(p^s-1)^2} &= \prod_p \frac{1-p^{-2s}}{(1-p^{-s})^3} \\ &= \left(\prod_p (1-p^{-s})^{-3}\right)\left(\prod_p (1-p^{-2s})\right) \\ &= \frac{\zeta^3(s)}{\zeta(2s)}.\end{aligned}$$

Since the right hand side is a Dirichlet series that converges for $\sigma > 1$, by the uniqueness of Dirichlet series the left hand side must converge for $\sigma > 1$. This means the identity holds for all s with $\sigma > 1$. □

Exercise 11.6. $\displaystyle\sum_{n=1}^{\infty} \frac{\nu(n)}{n^s} = \zeta(s) \sum_p \frac{1}{p^s}.$

Proof. Let a_n indicate whether n is prime. For $\sigma > 1$,

$$\begin{aligned}\zeta(s)\sum_p \frac{1}{p^s} &= \left(\sum_{n=1}^{\infty}\frac{1}{n^s}\right)\left(\sum_{n=1}^{\infty}\frac{a_n}{n^s}\right)\\ &= \sum_{n=1}^{\infty}\frac{1}{n^s}\sum_{d|n} a_n\\ &= \sum_{n=1}^{\infty}\frac{1}{n^s}\sum_{p|n} 1\\ &= \sum_{n=1}^{\infty}\frac{\nu(n)}{n^s}.\end{aligned}$$

□

Exercise 11.7. $\displaystyle\sum_{n=1}^{\infty}\frac{2^{\nu(n)}}{n^s} = \frac{\zeta^2(s)}{\zeta(2s)}.$

Lemma 11.7.1. Given an integer b, the function $b^{\nu(n)}$ is multiplicative.

Proof of Lemma. Let m and n be relatively prime positive integers. Since m and n share no common prime divisors and ν counts distinct prime divisors, it's evident that

$$\nu(mn) = \nu(m) + \nu(n).$$

Therefore

$$b^{\nu(mn)} = b^{\nu(m)+\nu(n)} = b^{\nu(m)}b^{\nu(n)}.$$

□

Lemma 11.7.2. For $n \geq 1$,

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

Proof of Lemma. By Lemma 11.7.1, $2^{\nu(n)}$ is multiplicative. Since $|\mu| * u$ is also multiplicative it's enough to prove the identity for prime powers. Now if $n = p^m$ for some prime p,

$$\sum_{d|p^m} |\mu(d)| = 1 + 1 = 2 = 2^{\nu(p^m)}.$$

□

Remark. This can also by proved by comparing Bell series, which is shown in Example 3 following Theorem 2.25.

Proof of Exercise. By Lemma 11.7.1 $2^{\nu(n)}$ is multiplicative, and additionally by Lemma 11.7.2

$$2^{\nu(n)} = \sum_{d|n} |\mu(n)| \leq d(n) \leq d(n^2).$$

Thus by comparison, Exercise 11.5 implies $\sum_{n=1}^{\infty} 2^{\nu(n)} n^{-s}$ converges for $\sigma > 1$. Hence for $\sigma > 1$, by Theorem 11.7,

$$\begin{aligned}
\sum_{n=1}^{\infty} \frac{2^{\nu(n)}}{n^s} &= \prod_p \sum_{m=0}^{\infty} \frac{2^{\nu(p^m)}}{p^{ms}} \\
&= \prod_p \left(1 + \sum_{m=1}^{\infty} \frac{2}{p^{ms}}\right) \\
&= \prod_p \left(1 + \frac{2}{p^s - 1}\right) \\
&= \prod_p \frac{p^s + 1}{p^s - 1}.
\end{aligned}$$

Multiplying numerator and denominator by $p^{-2s}(p^s - 1)$,

$$\begin{aligned}
\prod_p \frac{p^s + 1}{p^s - 1} &= \prod_p \frac{1 - p^{-2s}}{(1 - p^{-s})^2} \\
&= \left(\prod_p (1 - p^{-s})^{-2}\right) \left(\prod_p (1 - p^{-2s})\right) \\
&= \frac{\zeta^2(s)}{\zeta(2s)}.
\end{aligned}$$

□

Exercise 11.8. $\displaystyle\sum_{n=1}^{\infty} \frac{2^{\nu(n)}\lambda(n)}{n^s} = \frac{\zeta(2s)}{\zeta^2(s)}.$

Proof. We can deduce $\sum_{n=1}^{\infty} 2^{\nu(n)}\lambda(n) n^{-s}$ converges absolutely for $\sigma > 1$ and that $2^{\nu(n)}\lambda(n)$ is multiplicative through Exercise 11.7. Hence for $\sigma > 1$, by Theorem 11.7,

$$\begin{aligned}
\sum_{n=1}^{\infty} \frac{2^{\nu(n)}\lambda(n)}{n^s} &= \prod_p \sum_{m=0}^{\infty} \frac{2^{\nu(p^m)}\lambda(p^m)}{p^{ms}} \\
&= \prod_p \left(1 + \sum_{m=1}^{\infty} \frac{2(-1)^m}{p^{ms}}\right) \\
&= \prod_p \left(1 - \frac{2}{p^s + 1}\right) \\
&= \prod_p \frac{p^s - 1}{p^s + 1}.
\end{aligned}$$

Multiplying numerator and denominator by $p^{-2s}(1-p^{-s})$,

$$\begin{aligned}\prod_p \frac{p^s-1}{p^s+1} &= \prod_p \frac{(1-p^{-s})^2}{1-p^{-2s}} \\ &= \left(\prod_p (1-p^{-2s})^{-1}\right)\left(\prod_p (1-p^{-s})^2\right) \\ &= \frac{\zeta(2s)}{\zeta^2(s)}.\end{aligned}$$

□

Exercise 11.9. $\displaystyle\sum_{n=1}^{\infty} \frac{\kappa(n)}{n^s} = \frac{\zeta(s)\zeta(2s)\zeta(3s)}{\zeta(6s)}.$

Proof. It's clear $\kappa(n)$ is multiplicative. Furthermore if $n = p_1^{a_1}\cdots p_k^{a_k}$,

$$\kappa(n) = a_1 a_2 \cdots a_k < (a_1+1)(a_2+1)\cdots(a_k+1) = d(n) \leq d(n^2).$$

Thus by comparison, Exercise 11.5 implies $\sum_{n=1}^{\infty} \kappa(n) n^{-s}$ converges for $\sigma > 1$. Hence for $\sigma > 1$, by Theorem 11.7,

$$\begin{aligned}\sum_{n=1}^{\infty} \frac{\kappa(n)}{n^s} &= \prod_p \sum_{m=0}^{\infty} \frac{\kappa(p^m)}{p^{ms}} \\ &= \prod_p \left(1 + \sum_{m=1}^{\infty} \frac{m}{p^{ms}}\right).\end{aligned}$$

By Lemma 11.5,

$$\begin{aligned}\prod_p \left(1 + \sum_{m=1}^{\infty} \frac{m}{p^{ms}}\right) &= \prod_p \left(1 + \frac{p^s}{(p^s-1)^2}\right) \\ &= \prod_p \frac{p^{2s}-p^s+1}{(p^s-1)^2}.\end{aligned}$$

Multiplying numerator and denominator by $p^{-6s}(p^{3s}-1)(p^s+1)$,

$$\begin{aligned}\prod_p \frac{p^{2s}-p^s+1}{(p^s-1)^2} &= \prod_p \frac{1-p^{-6s}}{(1-p^{-s})(1-p^{-2s})(1-p^{-3s})} \\ &= \frac{\zeta(s)\zeta(2s)\zeta(3s)}{\zeta(6s)}.\end{aligned}$$

□

Exercise 11.10. $\displaystyle\sum_{n=1}^{\infty} \frac{3^{\nu(n)}\kappa(n)}{n^s} = \frac{\zeta^3(s)}{\zeta(3s)}.$

Proof. We can deduce $3^{\nu(n)}\kappa(n)$ is multiplicative through Lemma 11.7. Now note using the beginning of the proofs of Exercise 11.7 and Exercise 11.9,

$$3^{\nu(n)}\kappa(n) \leq \left(2^{\nu(n)}\right)^2 \kappa(n) < d(n)^3 < n^3.$$

Thus $\sum_{n=1}^{\infty} 3^{\nu(n)}\kappa(n)n^{-s}$ converges for $\sigma > 4$. Hence for $\sigma > 4$, by Theorem 11.7,

$$\begin{aligned}\sum_{n=1}^{\infty} \frac{3^{\nu(n)}\kappa(n)}{n^s} &= \prod_p \sum_{m=0}^{\infty} \frac{3^{\nu(p^m)}\kappa(p^m)}{p^{ms}} \\ &= \prod_p \left(1 + \sum_{m=1}^{\infty} \frac{3m}{p^{ms}}\right).\end{aligned}$$

By Lemma 11.5,

$$\begin{aligned}\prod_p \left(1 + \sum_{m=1}^{\infty} \frac{3m}{p^{ms}}\right) &= \prod_p \left(1 + \frac{3p^s}{(p^s-1)^2}\right) \\ &= \prod_p \frac{p^{2s} + p^s + 1}{(p^s-1)^2}.\end{aligned}$$

Multiplying numerator and denominator by $p^{-3s}(1+p^s)$,

$$\begin{aligned}\prod_p \frac{p^{2s} + p^s + 1}{(p^s-1)^2} &= \prod_p \frac{1 - p^{-3s}}{(1-p^{-s})^3} \\ &= \left(\prod_p (1-p^{-s})^{-3}\right)\left(\prod_p (1-p^{-3s})\right) \\ &= \frac{\zeta^3(s)}{\zeta(3s)}.\end{aligned}$$

Since the right hand side is a Dirichlet series that converges for $\sigma > 1$, by the uniqueness of Dirichlet series the left hand side must converge for $\sigma > 1$. This means the identity holds for all s with $\sigma > 1$. □

Exercise 11.11. Express the sum of the series $\sum_{n=1}^{\infty} 3^{\nu(n)}\kappa(n)\lambda(n)n^{-s}$ in terms of the Riemann zeta function.

Solution. We can deduce $\sum_{n=1}^{\infty} 3^{\nu(n)}\kappa(n)\lambda(n)n^{-s}$ converges absolutely for $\sigma > 1$ and that $3^{\nu(n)}\kappa(n)\lambda(n)$ is multiplicative through Exercise 11.10. Hence for $\sigma > 1$, by Theorem 11.7,

$$\begin{aligned}\sum_{n=1}^{\infty} \frac{3^{\nu(n)}\kappa(n)\lambda(n)}{n^s} &= \prod_p \sum_{m=0}^{\infty} \frac{3^{\nu(p^m)}\kappa(p^m)\lambda(p^m)}{p^{ms}} \\ &= \prod_p \left(1 + \sum_{m=1}^{\infty} \frac{3m(-1)^m}{p^{ms}}\right) \\ &= \prod_p \left(1 + \sum_{m=1}^{\infty} 3m\left(\frac{-1}{p^s}\right)^m\right).\end{aligned}$$

By Lemma 11.5,

$$\prod_p \left(1 + \sum_{m=1}^{\infty} 3m \left(\frac{-1}{p^s}\right)^m\right) = \prod_p \left(1 - \frac{3p^s}{(p^s+1)^2}\right)$$
$$= \prod_p \frac{p^{2s} - p^s + 1}{(p^s+1)^2}.$$

Multiplying numerator and denominator by $p^{-9s}(p^s-1)^3(p^s+1)(p^{3s}-1)$,

$$\prod_p \frac{p^{2s} - p^s + 1}{(p^s+1)^2} = \prod_p \frac{(1-p^{-6s})(1-p^{-s})^3}{(1-p^{-3s})(1-p^{-2s})^3}$$
$$= \frac{\zeta(3s)\zeta^3(2s)}{\zeta(6s)\zeta^3(s)}.$$

Exercise 11.12. Let f be a completely multiplicative function such that $f(p) = f(p)^2$ for each prime p. If the series $\sum f(n)n^{-s}$ converges absolutely for $\sigma > \sigma_a$ and has sum $F(s)$, prove that $F(s) \neq 0$ and that

$$\sum_{n=1}^{\infty} \frac{f(n)\lambda(n)}{n^s} = \frac{F(2s)}{F(s)} \quad \text{if } \sigma > \sigma_a.$$

Proof. Since f is completely multiplicative, for $\sigma > \sigma_a$ we have

$$\left(\sum_{n=1}^{\infty} \frac{f(n)}{n^s}\right)\left(\sum_{n=1}^{\infty} \frac{f(n)\mu(n)}{n^s}\right) = \sum_{n=1}^{\infty} \frac{1}{n^s} \sum_{d|n} f(n)\mu(n) f\left(\frac{n}{d}\right)$$
$$= \sum_{n=1}^{\infty} \frac{f(n)I(n)}{n^s} = f(1) = 1.$$

This means $F(s) \neq 0$.

Now observe $f(n)\lambda(n)$ is completely multiplicative. Hence for $\sigma > \sigma_a$, by Theorem 11.7,

$$\sum_{n=1}^{\infty} \frac{f(n)\lambda(n)}{n^s} = \prod_p \frac{1}{1 - f(p)\lambda(p)p^{-s}} = \prod_p \frac{1}{1 + f(p)p^{-s}}$$
$$= \prod_p \frac{1}{1 + f(p)p^{-s}} \cdot \frac{F(s)}{F(s)} = \prod_p \frac{1 - f(p)p^{-s}}{1 - f(p)^2 p^{-2s}}$$
$$= \prod_p \frac{1 - f(p)p^{-s}}{1 - f(p)p^{-2s}} = \frac{F(2s)}{F(s)}.$$

□

Exercise 11.13. Let f be a multiplicative function such that $f(p) = f(p)^2$ for each prime p. If the series $\sum \mu(n)f(n)n^{-s}$ converges absolutely for $\sigma > \sigma_a$ and has sum $F(s)$, prove that whenever $F(s) \neq 0$ we have

$$\sum_{n=1}^{\infty} \frac{f(n)|\mu(n)|}{n^s} = \frac{F(2s)}{F(s)} \quad \text{if } \sigma > \sigma_a.$$

Proof. Since $f(n)\mu(n)$ is multiplicative, applying Theorem 11.7 when $\sigma > \sigma_a$,

$$F(s) = \prod_p \sum_{m=0}^{\infty} \frac{f(p^m)\mu(p^m)}{p^{ms}} = \prod_p (1 - f(p)p^{-s}).$$

Similarly, the Euler product of $\sum_{n=1}^{\infty} f(n)|\mu(n)|n^{-s}$ is given by

$$\sum_{n=1}^{\infty} \frac{f(n)|\mu(n)|}{n^s} = \prod_p (1 + f(p)p^{-s}) \quad \text{if } \sigma > \sigma_a.$$

So assuming $F(s) \neq 0$, for $\sigma > \sigma_a$,

$$\begin{aligned}\sum_{n=1}^{\infty} \frac{f(n)|\mu(n)|}{n^s} &= \prod_p \frac{(1 + f(p)p^{-s})(1 - f(p)p^{-s})}{1 - f(p)p^{-s}} \\ &= \prod_p \frac{1 - f(p)^2 p^{-2s}}{1 - f(p)p^{-s}} \\ &= \prod_p \frac{1 - f(p)p^{-2s}}{1 - f(p)p^{-s}} \\ &= \frac{F(2s)}{F(s)}.\end{aligned}$$

□

Exercise 11.14. Let f be a multiplicative function such that $\sum f(n)n^{-s}$ converges absolutely for $\sigma > \sigma_a$. If p is prime and $\sigma > \sigma_a$ prove that

$$(1 + f(p)p^{-s}) \sum_{n=1}^{\infty} \frac{f(n)\mu(n)}{n^s} = (1 - f(p)p^{-s}) \sum_{n=1}^{\infty} \frac{f(n)\mu(n)\mu(p,n)}{n^s},$$

where $\mu(p, n)$ is the Möbius function evaluated at the gcd of p and n. [*Hint*: Euler products.]

Proof. By Lemma 2.7, $\mu(p, n)$ is multiplicative in n. So for $\sigma > \sigma_a$, by Theorem 11.7,

$$\begin{aligned}\sum_{n=1}^{\infty} \frac{f(n)\mu(n)\mu(p,n)}{n^s} &= \prod_q \sum_{m=0}^{\infty} \frac{f(q)\mu(q)\mu(p,q)}{q^{ms}} \\ &= (1 + f(p)p^{-s}) \prod_{q \neq p} (1 - f(q)q^{-s}) \qquad (17)\end{aligned}$$

and

$$\begin{aligned}\sum_{n=1}^{\infty} \frac{f(n)\mu(n)}{n^s} &= \prod_q \sum_{m=0}^{\infty} \frac{f(q)\mu(q)}{q^{ms}} \\ &= \prod_q (1 - f(q)q^{-s}). \qquad (18)\end{aligned}$$

Multiplying both sides of (17) by $1 - f(p)p^{-s}$ and both sides of (18) by $1 + f(p)p^{-s}$ gives the result. □

Exercise 11.15.(++) Prove that

$$\sum_{\substack{m=1\\(m,n)=1}}^{\infty}\sum_{n=1}^{\infty}\frac{1}{m^2n^2}=\frac{\zeta^2(2)}{\zeta(4)}.$$

More generally, if each s_i has real part $\sigma_i>1$, express the multiple sum

$$\sum_{\substack{m_1=1\\(m_1,\dots,m_r)=1}}^{\infty}\cdots\sum_{m_r=1}^{\infty}m_1^{-s_1}\cdots m_r^{-s_r}$$

in terms of the Riemann zeta function.

Proof. For brevity denote the summation symbols by $\sum_{m_i}$ and let $g=(m_1,\dots,m_r)$. For $\sigma_i>1$ we have

$$\begin{aligned}\sum_{\substack{m_i\\g=1}}m_1^{-s_1}\cdots m_r^{-s_r}&=\sum_{m_i}I(g)m_1^{-s_1}\cdots m_r^{-s_r}\\&=\sum_{m_i}\sum_{d\mid g}\mu(d)m_1^{-s_1}\cdots m_r^{-s_r}.\end{aligned}$$

Now $d\mid g$ if and only if $d\mid m_i$ for all i. Thus for a fixed divisor d of g we must sum over all m_i of the form dq_i. Hence

$$\begin{aligned}\sum_{m_i}\sum_{d\mid g}\mu(d)m_1^{-s_1}\cdots m_r^{-s_r}&=\sum_{d=1}^{\infty}\sum_{q_i}\mu(d)(dq_1)^{-s_1}\cdots(dq_r)^{-s_r}\\&=\zeta(s_1)\cdots\zeta(s_r)\sum_{d=1}^{\infty}\mu(d)d^{-(s_1+s_2+\cdots+s_r)}\\&=\frac{\zeta(s_1)\cdots\zeta(s_r)}{\zeta(s_1+\cdots+s_r)}.\end{aligned}$$

In particular this shows

$$\sum_{\substack{m=1\\(m,n)=1}}^{\infty}\sum_{n=1}^{\infty}\frac{1}{m^2n^2}=\frac{\zeta^2(2)}{\zeta(4)}.$$

□

Remark. This exercise reminds me of a short proof that $\zeta(4)=\pi^4/90$, due to Eugenio Calabi. It is interesting enough to reproduce here.

Theorem. If $k>1$, then

$$\zeta(2k)=\frac{2}{2k+1}\sum_{j=1}^{k-1}\zeta(2j)\zeta(2k-2j).$$

Proof. We will prove the result for $k = 2$ and sketch the proof of the general result. The proof resembles Exercise 11.15 since $\zeta^2(2)$ and $\zeta(4)$ appear below. Define

$$f(m,n) = \frac{1}{mn^3} + \frac{1}{2m^2n^2} + \frac{1}{m^3n}$$

and observe

$$f(m,n) - f(m+n,n) - f(m,m+n) = \frac{1}{m^2n^2}.$$

This gives

$$\begin{aligned}
\zeta^2(2) &= \sum_{m,n>0} \frac{1}{m^2n^2} \\
&= \sum_{m,n>0} f(m,n) - \sum_{m,n>0} f(m+n,n) - \sum_{m,n>0} f(m,m+n) \\
&= \sum_{m,n>0} f(m,n) - \sum_{m>n>0} f(m,n) - \sum_{n>m>0} f(m,n) \\
&= \sum_{n>0} f(n,n) = \frac{5}{2}\zeta(4).
\end{aligned}$$

So in particular assuming $\zeta(2) = \pi^2/6$ shows $\zeta(4) = \pi^4/90$.

Now in general for $k > 1$, define

$$f(m,n) = \frac{1}{mn^{2k-1}} + \frac{1}{2}\sum_{r=2}^{2k-2} \frac{1}{m^r n^{2k-r}} + \frac{1}{m^{2k-1}n}.$$

It can be seen that

$$f(m,n) - f(m+n,n) - f(m,m+n) = \sum_{j=1}^{k-1} \frac{1}{m^{2j}n^{2k-2j}},$$

which leads to

$$\sum_{j=1}^{k-1} \zeta(2j)\zeta(2k-2j) = \frac{2k+1}{2}\zeta(2k).$$

□

Exercise 11.16. Integrals of the form

$$f(s) = \int_1^\infty \frac{A(x)}{x^s} dx, \tag{19}$$

where $A(x)$ is Riemann-integrable on every compact interval $[1, a]$, have some properties analogous to those of Dirichlet series. For example, they possess a half-plane of absolute convergence $\sigma > \sigma_a$ and a half-plane of convergence $\sigma > \sigma_c$ in which $f(s)$ is analytic. This exercise describes an analogue of Theorem 11.13 (*Landau's theorem*).

Let $F(s)$ be represented in the half-plane $\sigma > \sigma_c$ by (19), where σ_c is finite, and assume that $A(x)$ is real-valued and does not change sign for $x \geq x_0$. Prove that $f(s)$ has a singularity on the real axis at the point $s = \sigma_c$.

Proof. without loss of generality assume $A(x) > 0$ for $x \geq x_0$. We shall mirror the argument made in the proof of Theorem 11.13. That is we will prove the following:

> *Let $F(s)$ be represented in the half-plane $\sigma > c$ by the integral*
>
> $$F(s) = \int_1^\infty \frac{A(x)}{x^s} dx,$$
>
> *where c is finite, and assume that $A(x) \geq 0$ for all $x \geq x_0$. If $F(s)$ is analytic in some disk about the point $s = c$, then the integral converges in the half-plane $\sigma > c - \varepsilon$ for some $\varepsilon > 0$. Consequently, if the integral has a finite abscissa of convergence σ_c, then $F(s)$ has a singularity on the real axis at the point $s = \sigma_c$.*

Let $a = 1 + c$. Since F is analytic at a it can be represented by an absolutely convergent power series expansion about a,

$$F(s) = \sum_{k=0}^{\infty} \frac{F^{(k)}(a)}{k!}(s-a)^k, \tag{20}$$

and the radius of convergence of this power series exceeds 1 since F is analytic for $\sigma > c$ and also in some disk centered at $s = c$. (See Figure 4.) Since the integral converges absolutely, when taking derivatives we can differentiate under the integral sign. Hence taking repeated derivatives gives

$$F^{(k)}(a) = (-1)^k \int_1^\infty A(x)(\log x)^k x^{-s} dx,$$

so (20) can be rewritten as

$$F(s) = \sum_{k=0}^{\infty} \int_1^\infty \frac{(a-s)^k}{k!} A(x)(\log x)^k x^{-s} dx. \tag{21}$$

Since the radius of convergence exceeds 1, this formula is valid for some real $s = c - \varepsilon$ where $\varepsilon > 0$ (see Figure 4.) Then $a - s = 1 + \varepsilon$ for this s and the summation in (21) has nonnegative terms for $x \geq x_0$. Therefore we can interchange the sum and integral to obtain

$$F(c-\varepsilon) = \int_1^\infty \frac{A(x)}{x^s} \sum_{k=0}^{\infty} \frac{\{(1+\varepsilon)\log x\}^k}{k!} dx = \int_1^\infty \frac{A(x)}{x^s} e^{(1+\varepsilon)\log x} dx = \int_1^\infty \frac{A(x)}{x^{c-\varepsilon}} dx.$$

In other words, the integral $\int_1^\infty A(x)x^{-s}dx$ converges for $s = c - \varepsilon$, hence it also converges in the half-plane $\sigma > c - \varepsilon$.

Now suppose the integral has a finite abscissa of convergence σ_c. Taking the contrapositive of what was just proven shows $F(s)$ is not analytic at $s = \sigma_c$. This means the radius of convergence of the power series of F centered at $s = 1 + \sigma_c$ cannot be greater than 1. In fact since $F(s)$ is analytic for all $\sigma > \sigma_c$, we see the radius of convergence of the power series must be 1. Since the radius of convergence is equal to the shortest distance to a singularity, we conclude $F(s)$ has a singularity at the point $s = \sigma_c$. □

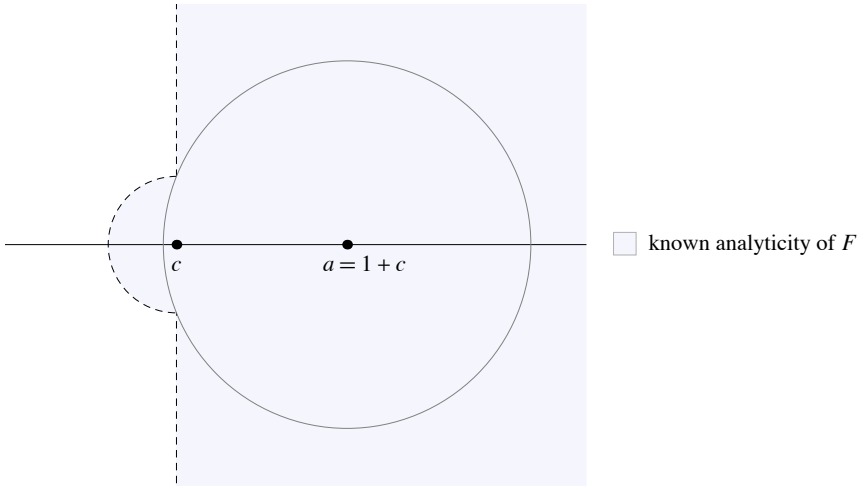


Figure 4: The radius of convergence exceeds 1.

Exercise 11.17. Let $\lambda_a(n) = \sum_{d|n} d^a \lambda(d)$ where $\lambda(n)$ is Liouville's function. Prove that if $\sigma > \max\{1, \mathrm{Re}(a) + 1\}$, we have

$$\sum_{n=1}^{\infty} \frac{\lambda_a(n)}{n^s} = \frac{\zeta(s)\zeta(2s-2a)}{\zeta(s-a)}$$

and

$$\sum_{n=1}^{\infty} \frac{\lambda(n)\lambda_a(n)}{n^s} = \frac{\zeta(2s)\zeta(s-a)}{\zeta(s)}.$$

Proof. Since $\lambda_a = u * N^a\lambda$, for $\sigma > \max\{1, \mathrm{Re}(a) + 1\}$, by Theorem 11.5,

$$\sum_{n=1}^{\infty} \frac{\lambda_a(n)}{n^s} = \left(\sum_{n=1}^{\infty} \frac{1}{n^s}\right)\left(\sum_{n=1}^{\infty} \frac{n^a\lambda(n)}{n^s}\right) = \zeta(s)\sum_{n=1}^{\infty} \frac{\lambda(n)}{n^{s-a}}.$$

Applying Exercise 11.12 then shows

$$\sum_{n=1}^{\infty} \frac{\lambda_a(n)}{n^s} = \frac{\zeta(s)\zeta(2s-2a)}{\zeta(s-a)}.$$

Looking at the second sum, observe λ is completely multiplicative and $\lambda(d^2) = 1$ for all d. Hence if $d \mid n$,

$$\lambda\left(\frac{n}{d}\right) = \lambda\left(\frac{n}{d}\right)\lambda(d^2) = \lambda(nd).$$

From here we find

$$\lambda(n)\lambda_a(n) = \sum_{d|n} d^a\lambda(nd) = \sum_{d|n} d^a\lambda\left(\frac{n}{d}\right) = (N^a * \lambda)(n).$$

Thus for $\sigma > \max\{1, \mathrm{Re}(a) + 1\}$, by Theorem 11.5,

$$\sum_{n=1}^{\infty} \frac{\lambda(n)\lambda_a(n)}{n^s} = \left(\sum_{n=1}^{\infty} \frac{n^a}{n^s}\right)\left(\sum_{n=1}^{\infty} \frac{\lambda(n)}{n^s}\right) = \frac{\zeta(2s)\zeta(s-a)}{\zeta(s)}.$$

□

Chapter 12
The Functions $\zeta(s)$ and $L(s,\chi)$

Exercise 12.1. Let $f(n)$ be an arithmetical function which is period modulo k.
(a) Prove that the Dirichlet series $\sum f(n)n^{-s}$ converges absolutely for $\sigma > 1$ and that

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^s} = k^{-s} \sum_{r=1}^{k} f(r)\zeta\left(s, \frac{r}{k}\right) \qquad \text{if } \sigma > 1.$$

(b) If $\sum_{r=1}^{k} f(r) = 0$ prove that the Dirichlet series $\sum f(n)n^{-s}$ converges for $\sigma > 0$ and that there is an entire function $F(s)$ such that $F(s) = \sum f(n)n^{-s}$ for $\sigma > 0$.

Proof.
(a) Since $f(n)$ is periodic, there is an M such that $|f(n)| \leq M$ for all n. Thus

$$\sum_{n=1}^{\infty} \frac{|f(n)|}{n^s} \leq M\zeta(s)$$

and it follows that the sum converges absolutely for $\sigma > 1$. This means we can rearrange the sum in this region with out altering it. Through the division algorithm we thus have

$$\begin{aligned}
\sum_{n=1}^{\infty} \frac{f(n)}{n^s} &= \sum_{r=1}^{k} \sum_{q=0}^{\infty} \frac{f(qk+r)}{(qk+r)^s} \\
&= \sum_{r=1}^{k} f(r) \sum_{q=0}^{\infty} \frac{1}{(qk+r)^s} \\
&= k^{-s} \sum_{r=1}^{k} f(r) \sum_{q=0}^{\infty} \frac{1}{(q+r/k)^s} \\
&= k^{-s} \sum_{r=1}^{k} f(r)\zeta\left(s, \frac{r}{k}\right).
\end{aligned}$$

(b) The convergence for $\sigma > 0$ follows directly from Lemma 11.1. Since this sum can be expressed as a finite linear combination of Hurwitz zeta functions, Theorem 12.4 implies it must be analytic for all $s \neq 1$. However since Dirichlet series are analytic in their half-plane of convergence, we know this sum is analytic at $s = 1$ and hence can be extended to an entire function. □

Exercise 12.2. If x is real $\sigma > 1$, let $F(x, s)$ denote the periodic zeta function,

$$F(x,s) = \sum_{n=1}^{\infty} \frac{e^{2\pi i n x}}{n^s}.$$

If $0 < a < 1$ and $\sigma > 1$ prove that Hurwitz's formula implies

$$F(a,s) = \frac{\Gamma(1-s)}{(2\pi)^{1-s}} \left\{ e^{\pi i(1-s)/2} \zeta(1-s,a) + e^{\pi i(s-1)/2} \zeta(1-s,1-a) \right\}.$$

Proof. By Theorem 12.6 for $0 < a \leq 1$ and $\sigma > 1$,

$$\zeta(1-s,a) = \frac{\Gamma(s)}{(2\pi)^{1-s}} \left\{ e^{-\pi i s/2} F(a,s) + e^{\pi i s/2} F(-a,s) \right\}.$$

Since $0 < a < 1$, the same type of formula can be used on $\zeta(1-s, 1-a)$. The plan is to substitute this formula into the right hand side of the proposed equality to show it equals $F(a, s)$. We will do this in Mathematica.

```
In[1]:= pz = Γ[1 - s]/(2 π)^(1 - s) (Exp[π I (1 - s)/2] ζ[1 - s, a] +
          Exp[π I (s - 1)/2] ζ[1 - s, 1 - a]);

In[2]:= thm126 = ζ[1 - s, b_] :> Γ[s]/(2 π)^s (Exp[-π I s/2] F[b, s] +
          Exp[π I s/2] F[-b, s]);
```

Now we will apply `thm126` on `pz` and simplify. The simplifications used are standard algebraic ones and $\Gamma(s)\Gamma(1-s) = \pi/\sin(\pi s)$.

```
In[3]:= pz = FullSimplify[pz /. thm126]
Out[3]= (E^(2 I π s) F[a - 1, s] + E^(I π s) (F[1 - a, s] - F[-a, s]) -
          F[a, s])/(E^(2 I π s) - 1)
```

Next we will use that $F(x, s)$ has period 1 in x. After this and cancelation we get the result.

```
In[4]:= pz = Cancel[pz /. F[b_ + _Integer, s] :> F[b, s]]
Out[4]= F[a, s]
```

□

Exercise 12.3. The formula in Exercise 12.2 can be used to extend the definition of $F(a, s)$ over the entire s-plane if $0 < a < 1$. Prove that $F(a, s)$, so extended, is an entire function of s.

Proof. For $0 < a < 1$,

$$\sum_{n=1}^{N} e^{2\pi i n a} = \frac{e^{2i\pi a}\left(e^{2i\pi a N} - 1\right)}{e^{2i\pi a} - 1} = O(1).$$

Using this when applying Abel's summation formula shows

$$\sum_{n \leq x} \frac{e^{2\pi i n a}}{n^s} = O\left(x^{-s}\right).$$

This means $F(s)$ is a convergent Dirichlet series for $\sigma > 0$, and hence is analytic there. Thus we only need to show the extended definition of $F(a,s)$ is analytic for $\sigma \leq 0$. Now in this region, $\Gamma(1-s)$ is analytic everywhere and $\zeta(1-s,\cdot)$ is analytic for $s \neq 0$. This shows we only need to show $F(a,s)$ is analytic at $s=0$ in order to show $F(a,s)$ is entire.

By Theorem 12.4, $\zeta(s,a)$ has a simple pole at $s=1$ with residue 1. Therefore there are entire functions $R_1(s,a)$ and $R_2(s,a)$ such that

$$\zeta(1-s,a) = -\frac{1}{s} + R_1(s,a) \quad \text{and} \quad \zeta(1-s,1-a) = -\frac{1}{s} + R_2(s,a).$$

Substituting shows there is an entire function $R_3(s,a)$ such that

$$\begin{aligned} F(a,s) &= \frac{\Gamma(1-s)}{(2\pi)^{1-s}} \left\{ -\frac{e^{\pi i(1-s)/2} + e^{\pi i(s-1)/2}}{s} + R_3(s,a) \right\} \\ &= \frac{\Gamma(1-s)}{(2\pi)^{1-s}} \left\{ -\frac{2\sin(\pi s/2)}{s} + R_3(s,a) \right\}. \end{aligned}$$

We see $F(a,s)$ has a removable singularity at $s=0$, hence by Riemann's theorem on removable singularities $F(a,s)$ can be extended to an analytic function at $s=0$. □

Exercise 12.4. If $0 < a < 1$ and $0 < b < 1$ let

$$\Phi(a,b,s) = \frac{\Gamma(s)}{(2\pi)^s} \left\{ \zeta(s,a)F(b,1+s) + \zeta(s,1-a)F(1-b,1+s) \right\},$$

where F is the function in Exercise 12.2. Prove that

$$\begin{aligned} \frac{\Phi(a,b,s)}{\Gamma(s)\Gamma(-s)} &= e^{\pi i s/2} \left\{ \zeta(s,a)\zeta(-s,1-b) + \zeta(s,1-a)\zeta(-s,b) \right\} \\ &\quad + e^{-\pi i s/2} \{ \zeta(-s,1-b)\zeta(a,1-a) + \zeta(-s,b)\zeta(s,a) \}, \end{aligned}$$

and deduce that $\Phi(a,b,s) = \Phi(1-b,a,-s)$. This functional equation is useful in the theory of elliptic modular functions.

Proof. To demonstrate the identity we will first substitute the formula derived in Exercise 12.2 into $\Phi(a,b,s)$, then manipulate. This is shown in Mathematica.

```
In[5]:= pzR = F[a_, s_] :> Γ[1 - s]/(2 π)^(1 - s) (Exp[π I (1 - s)/2]*
          ζ[1 - s, a] + Exp[π I (s - 1)/2] ζ[1 - s, 1 - a]);

In[6]:= Phi = Γ[s]/(2 π)^s (ζ[s, a] F[b, 1 + s] +
          ζ[s, 1 - a] F[1 - b, 1 + s]);

(* substitute *)
In[7]:= Phi = Phi /. pzR;

(* distribute Gammas and collect in terms of Exp *)
In[8]:= PhiG = Collect[Expand[Phi/(Γ[s] Γ[-s])], Power[E, _]]
Out[8]= E^(I π s/2) (ζ[-s, b] ζ[s, 1 - a] + ζ[-s, 1 - b] ζ[s, a]) +
        E^(-I π s/2) (ζ[-s, 1 - b] ζ[s, 1 - a] + ζ[-s, b] ζ[s, a])
```

Now observe the mapping $a \mapsto 1-b, b \mapsto a, s \mapsto -s$ permutes the ζ terms that share the same power of e amongst each other. Again Mathematica is used to demonstrate.

```
In[9]:= SameQ[PhiG, PhiG /. {a -> 1 - b, b -> a, s -> -s}]
Out[9]= True
```

Since $\Gamma(s)\Gamma(-s)$ is also invariant under this transformation, we conclude

$$\Phi(a,b,s) = \Phi(1-b,a,-s).$$

□

In Exercises 5, 6 and 7, $\xi(s)$ denotes the entire function introduced in Section 12.8,

$$\xi(s) = \frac{1}{2}s(s-1)\pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\zeta(s).$$

Exercise 12.5. Prove that $\xi(s)$ is real on the lines $t=0$ and $\sigma = 1/2$, and that $\xi(0) = \xi(1) = 1/2$.

Lemma 12.5. If $f(s)$ is entire and real valued on the real line, then

$$f(s) = \overline{f(\overline{s})} \quad \text{for all } s \in \mathbb{C}.$$

Proof of Lemma. Since $f(s)$ is entire, we can use the Cauchy-Riemann equations to show $\overline{f(\overline{s})}$ is entire too. Moreover since $f(s)$ is real valued on the real line, $f(s) - \overline{f(\overline{s})} = 0$ everywhere on the real line. Since non-zero entire functions have isolated zeros, we conclude

$$f(s) = \overline{f(\overline{s})} \quad \text{for all } s \in \mathbb{C}.$$

□

Proof. Since $\xi(s) = \xi(1-s)$, to show $\xi(s)$ is real on the line $t=0$, it's enough to take $\sigma > 0$. Now clearly $(s/2)\pi^{-s/2}$ is real valued when $t=0$. Noting for $\sigma > 0$ that

$$\Gamma(s) = \int_0^\infty x^{s-1}e^{-s}dx \quad \text{and} \quad (s-1)\zeta(s) = \frac{s-1}{2^{1-s}-1}\sum_{n=1}^{\infty}\frac{(-1)^n}{n^s},$$

it's also clear $(s-1)\Gamma(s/2)\zeta(s)$ is real valued for $t=0$ ($s-1$ cancels the pole of $\zeta(s)$).

Now since $\xi(s)$ is entire and real valued on the real line, by Lemma 12.5 we have

$$\xi(s) = \overline{\xi(\overline{s})} \quad \text{for all } s \in \mathbb{C}.$$

Applying this and the functional equation of $\xi(s)$ we see

$$\begin{aligned}\xi(1/2+it) &= \xi(1-(1/2+it)) \\ &= \xi(1/2-it) \\ &= \overline{\xi(\overline{1/2-it})} \\ &= \overline{\xi(1/2+it)}.\end{aligned}$$

This means $\xi(1/2+it)$ must be real.

To calculate $\xi(0)$, use the recurrence relation $\Gamma(s+1) = s\Gamma(s)$ to see

$$\xi(s) = (s-1)\pi^{-s/2}\Gamma\left(\frac{s}{2}+1\right)\zeta(s).$$

Thus since $\zeta(0) = -1/2$,

$$\xi(1) = \xi(0) = \frac{1}{2}.$$

□

Exercise 12.6. Prove that the zeros of $\xi(s)$ (if any exist) are all situated in the strip $0 < \sigma < 1$ and lie symmetrically about the lines $t = 0$ and $\sigma = 1/2$.

Proof. Using the functional equation $\xi(s) = \xi(1-s)$, if $\xi(s) = 0$, then $\xi(1-s) = 0$. This means the zeros are symmetric about the line $\sigma = 1/2$.

Now in the proof of Exercise 12.5 it was shown

$$\xi(s) = \overline{\xi(\overline{s})} \quad \text{for all } s \in \mathbb{C}.$$

Thus $\xi(s) = 0$ implies $\xi(\overline{s}) = 0$, i.e. the zeros of $\xi(s)$ are symmetric about the real line. □

Exercise 12.7. Show that the zeros of $\zeta(s)$ in the critical strip $0 < \sigma < 1$ (if any exist) are identical in position and order of multiplicity with those of $\xi(s)$.

Proof. Observe $s(s-1)\pi^{-s/2}/2$ is entire and has no zeros in the critical strip. Furthermore $\Gamma(s/2)$ is meromorphic with poles at $-n/2$ for all nonnegative integers n and is non-zero everywhere. Thus the only possible zeros of $\xi(s)$ in the critical strip can come from $\zeta(s)$ and the multiplicity is preserved since $s(s-1)\pi^{-s/2}\Gamma(s/2)/2$ is non-zero analytic in this strip. □

Exercise 12.8. Let χ be a primitive character mod k. Define

$$a = a(\chi) = \begin{cases} 0 & \text{if } \chi(-1) = 1, \\ 1 & \text{if } \chi(-1) = -1. \end{cases}$$

(a) Show that the functional equation for $L(s,\chi)$ has the form

$$L(1-s,\overline{\chi}) = \varepsilon(\chi)2(2\pi)^{-s}k^{s-\frac{1}{2}}\cos\left(\frac{\pi(s-a)}{2}\right)\Gamma(s)L(s,\chi), \text{ where } |\varepsilon(\chi)| = 1.$$

(b) Let

$$\xi(s,\chi) = \left(\frac{k}{\pi}\right)^{(s+a)/2}\Gamma\left(\frac{s+a}{2}\right)L(s,\chi).$$

Show that $\xi(1-s,\overline{\chi}) = \varepsilon(\chi)\xi(s,\chi)$.

Proof.
(a) By Theorem 12.11

$$L(1-s,\overline{\chi}) = \frac{k^{s-1}\Gamma(s)}{(2\pi)^s}\left\{e^{-\pi is/2} + \overline{\chi}(-1)e^{\pi is/2}\right\} G(1,\overline{\chi})L(s,\chi).$$

Now observe

$$e^{-\pi is/2} + \overline{\chi}(-1)e^{\pi is/2} = \begin{cases} 2\cos(\pi s/2) & \text{if } a=0 \\ 2\cos(\pi(s-1)/2) & \text{if } a=1, \end{cases}$$

which leads to

$$L(1-s,\overline{\chi}) = \left(\frac{G(1,\overline{\chi})}{\sqrt{k}}\right) 2(2\pi)^{-s}k^{s-\frac{1}{2}}\cos\left(\frac{\pi(s-a)}{2}\right)\Gamma(s)L(s,\chi).$$

By Theorem 8.11, $|G(1,\overline{\chi})| = \sqrt{k}$, which shows we can take $\varepsilon(\chi) = G(1,\overline{\chi})/\sqrt{k}$.
(b) From above we have

$$\begin{aligned}\xi(1-s,\overline{\chi}) &= \left(\frac{k}{\pi}\right)^{(s+a)/2}\Gamma\left(\frac{s+a}{2}\right)\varepsilon(\chi)2(2\pi)^{-s}k^{s-\frac{1}{2}}\cos\left(\frac{\pi(s-a)}{2}\right)\Gamma(s)L(s,\chi) \\ &= \varepsilon(\chi)\xi(s,\chi)\left\{\frac{2^{1-s}}{\sqrt{\pi}}\cos\left(\frac{\pi(s-a)}{2}\right)\frac{\Gamma((1-s+a)/2)\Gamma(s)}{\Gamma((s+a)/2)}\right\}. \end{aligned} \tag{22}$$

Next, we consider the two cases for a separately to show the expression in the brackets is 1.

- Suppose $a=0$. Applying the duplication formula and the functional equation,

$$\begin{aligned}\Gamma\left(\frac{1-s}{2}\right)\frac{\Gamma(s)}{\Gamma(s/2)} &= \frac{2^{s-1}}{\sqrt{\pi}}\Gamma\left(\frac{1-s}{2}\right)\Gamma\left(\frac{s+1}{2}\right) \\ &= \frac{2^{s-1}}{\sqrt{\pi}}\frac{\pi}{\sin(\pi(s-1)/2)} \\ &= \frac{2^{s-1}\sqrt{\pi}}{\cos(\pi s/2)}.\end{aligned}$$

  Substituting this inside the brackets of (22) gives the result.

- Suppose $a=1$. Applying the duplication formula and the functional equation,

$$\begin{aligned}\frac{\Gamma(1-s/2)\Gamma(s)}{\Gamma((s+a)/2)} &= \left(\Gamma\left(1-\frac{s}{2}\right)\Gamma\left(\frac{s}{2}\right)\right)\frac{\Gamma(s)}{\Gamma(s/2)\Gamma((s+1)/2)} \\ &= \frac{\pi}{\sin(\pi s/2)}\frac{\Gamma(s)}{2^{1-s}\sqrt{\pi}\Gamma(s)} \\ &= \frac{2^{s-1}\sqrt{\pi}}{\cos(\pi(s-1)/2)}.\end{aligned}$$

  Substituting this inside the brackets of (22) gives the result. □

Exercise 12.9. Refer to Exercise 12.8.
(a) Prove that $\xi(s,\chi) \neq 0$ if $\sigma > 1$ or $\sigma < 0$.
(b) Describe the location of the zeros of $L(s,\chi)$ in the half-plane $\sigma < 0$.

Proof.
(a) Since characters are completely multiplicative, for $\sigma > 1$,

$$\frac{1}{L(s,\chi)} = \sum_{n=1}^{\infty} \frac{\mu(n)\chi(n)}{n^s}.$$

Since this series converges for $\sigma > 1$ and hence is analytic, it must be that $L(s,\chi)$ is nonzero for $\sigma > 1$. Combining this with the fact that $(k/\pi)^{(s+a)/2}\Gamma((s+a)/2)$ is never zero shows $\xi(s,\chi)$ is nonzero for $\sigma > 1$. Furthermore for $\sigma > 1$,

$$\xi(1-s,\chi) = \varepsilon(\overline{\chi})\xi(s,\overline{\chi}) \neq 0,$$

i.e. $\xi(s,\chi)$ is not zero for $\sigma < 0$.
(b) By definition it's easy to see $\xi(s,\chi)$ is analytic for $\sigma > 1$ and by its functional equation, $\xi(s,\chi)$ must be analytic for $\sigma < 0$. However $\Gamma((s+a)/2)$ has poles at $s = a - 2n$ for all $n \geq -a/2$. This means $L(s,\chi)$ must cancel these poles by having zeros at these locations. Moreover since $\xi(s,\chi)$ is nonzero, $L(s,\chi)$ can't be zero anywhere else. Hence for $\sigma < 0$,

$$L(s,\chi) = 0 \quad \text{if and only if} \quad s = a - 2n \text{ for some } n > -a/2.$$

□

Exercise 12.10. Let χ be a non primitive character modulo k. Describe the location of the zeros of $L(s,\chi)$ in the half-plane $\sigma < 0$.

Proof. Write $\chi(n) = \psi(n)\chi_1(n)$ where ψ is primitive and χ_1 is principal mod k. Then by Theorem 12.9

$$L(s,\chi) = L(s,\psi)\prod_{p|k}\left(1 - \frac{\psi(p)}{p^s}\right)$$

and so $L(s,\chi) = 0$ if and only if $L(s,\psi) = 0$. Hence for $\sigma < 0$, noting $a(\psi) = a(\chi)$ and applying by Exercise 12.9 (b),

$$L(s,\chi) = 0 \quad \text{if and only if} \quad s = a - 2n \text{ for some } n > -a/2.$$

□

Exercise 12.11. Prove the Bernoulli polynomials satisfy the relations

$$B_n(1-x) = (-1)^n B_n(x) \text{ and } B_{2n+1}(\tfrac{1}{2}) = 0 \text{ for every } n \geq 0.$$

Proof. By definition we have

$$\begin{aligned}\sum_{n=0}^{\infty} B_n(1-x)\frac{t^n}{n!} &= \frac{te^{(1-x)t}}{e^t-1} = \frac{(-t)e^{-xt}}{e^{-t}-1}\\ &= \sum_{n=0}^{\infty} B_n(x)\frac{(-t)^n}{n!}\\ &= \sum_{n=0}^{\infty}(-1)^n B_n(x)\frac{t^n}{n!}.\end{aligned}$$

Equating coefficients shows

$$B_n(1-x) = (-1)^n B_n(x).$$

Applying this result for an odd index $2n+1$ gives

$$B_{2n+1}(1/2) = (-1)^{2n+1}B_{2n+1}(1/2) = -B_{2n+1}(1/2),$$

which means $B_{2n+1}(1/2) = 0$. □

Exercise 12.12. Let B_n denote the nth Bernoulli number. Note that

$$\begin{aligned}&B_2 = \tfrac{1}{6} = 1-\tfrac{1}{2}-\tfrac{1}{3}, \qquad B_4 = \tfrac{-1}{30} = 1-\tfrac{1}{2}-\tfrac{1}{3}-\tfrac{1}{5},\\ &B_6 = \tfrac{1}{42} = 1-\tfrac{1}{2}-\tfrac{1}{3}-\tfrac{1}{7}.\end{aligned}$$

These formulas illustrate a theorem discovered in 1840 by von Staudt and Clausen (independently). If $n \geq 1$ we have

$$B_{2n} = I_n - \sum_{p-1|2n}\frac{1}{p},$$

where I_n is an integer and the sum is over all primes p such that $p-1$ divides $2n$. This exercise outlines a proof due to Lucas.

(a) Prove that

$$B_n = \sum_{k=0}^{n}\frac{1}{k+1}\sum_{r=0}^{k}(-1)^r\binom{k}{r}r^n.$$

[*Hint*: Write $x = \log\{1+(e^x-1)\}$ and use the power series for $x/(e^x-1)$.]

(b) Prove that

$$B_n = \sum_{k=0}^{n}\frac{k!}{k+1}c(n,k),$$

where $c(n,k)$ is an integer.

(c) If a, b are integers with $a \geq 2$, $b \geq 2$ and $ab > 4$, prove that $ab \mid (ab-1)!$. This shows that in the sum of (b), every term with $k+1$ composite, $k > 3$, is an integer.

(d) If p is prime, prove that

$$\sum_{r=0}^{p-1}(-1)^r\binom{p-1}{r}r^n \equiv \begin{cases}-1 \mod p & \text{if } p-1 \mid n, n>0,\\ 0 \mod p & \text{if } p-1 \nmid n.\end{cases}$$

(e) Use the above results or some other method to prove the von Staudt-Clausen theorem.

Lemma 12.12.1. The Stirling numbers of the second kind, $S(n,k)$, are defined as the number of ways to partition n elements into k nonempty sets. A well known formula is

$$S(n,k) = \frac{1}{k!}\sum_{r=0}^{k}(-1)^{k-r}\binom{k}{r}r^n.$$

Proof of Lemma. The number of ordered partitions of n into k nonempty sets is $k!S(n,k)$. To derive the formula, we will count another way using the inclusion-exclusion principal.

Now note finding an ordered partition of n into k nonempty sets is equivalent to finding an onto function from n into k. To derive the formula, we will start out with all k^n functions and apply the inclusion-exclusion principal to narrow down the onto functions. For each $1 \leq j \leq k$, there are $(k-1)^n$ functions that do not include j in it's image. Thus we will subtract off $\binom{k}{1}(k-1)^n$ total functions we've counted so far. Continuing in this fashion we will add and subtract $\binom{k}{i}(k-i)^n$ functions for $1 \leq i \leq k-1$. This leads to

$$k!S(n,k) = \sum_{r=0}^{k}(-1)^{k-r}\binom{k}{r}r^n.$$

□

Lemma 12.12.2. For $n \geq 0$ and $m > 0$,

$$\sum_{r=0}^{n+m}(-1)^r\binom{n+m}{r}r^n = 0.$$

Proof of Lemma. Fix m and induct on n. Since $m > 0$, when $n = 0$,

$$\sum_{r=0}^{m}(-1)^r\binom{m}{r} = (1-1)^m = 0.$$

Assuming the result is true for n, then

$$\sum_{r=0}^{(n+1)+m}(-1)^r\binom{(n+1)+m}{r}r^{n+1} = r\sum_{r=0}^{n+(m+1)}(-1)^r\binom{n+(m+1)}{r}r^n = 0.$$

□

Remark. An alternate proof is to notice the proof of Lemma 12.12.1 did not require $k \leq n$.

Proof of Exercise.

(a) Following the hint we have

$$\begin{aligned}\sum_{n=0}^{\infty} B_n \frac{t^n}{n!} &= \frac{\log\{1+(e^t-1)\}}{e^t-1} = \sum_{k=0}^{\infty} \frac{(1-e^t)^k}{k+1} \\ &= \sum_{k=0}^{\infty} \frac{1}{k+1} \sum_{r=0}^{k} (-1)^r \binom{k}{r} e^{rt} \\ &= \sum_{n=0}^{\infty} \sum_{k=0}^{\infty} \frac{1}{k+1} \sum_{r=0}^{k} (-1)^r \binom{k}{r} \frac{r^n t^n}{n!} \\ &= \sum_{n=0}^{\infty} \sum_{k=0}^{n} \frac{1}{k+1} \sum_{r=0}^{k} (-1)^r \binom{k}{r} \frac{r^n t^n}{n!},\end{aligned}$$

where Lemma 12.12.2 was used in the last step. Equating coefficients gives the result.
(b) Observe $c(n,k) = (-1)^k S(n,k)$. Hence by Lemma 12.12.1, $c(n,k)$ is an integer.
(c) See Lemma 5.7.
(d) If $p-1 \mid n$, then $r^n \equiv 1 \bmod p$ for $0 < r \leq p-1$. Thus

$$\sum_{r=0}^{p-1} (-1)^r \binom{p-1}{r} r^n \equiv -1 + \sum_{r=0}^{p-1} (-1)^r \binom{p-1}{r} = -1 + (1-1)^{p-1} = -1 \mod p.$$

If $p-1 \nmid n$, then

$$\sum_{r=0}^{p-1} (-1)^r \binom{p-1}{r} r^n \equiv \sum_{r=0}^{p-1} (-1)^r \binom{p-1}{r} r^{n-q(p-1)} \mod p,$$

where $q = \lfloor n/(p-1) \rfloor$ and $0 < n - q(p-1) < p-1$. Thus by Lemma 12.12.2,

$$\sum_{r=0}^{p-1} (-1)^r \binom{p-1}{r} r^{n-q(p-1)} = 0,$$

which finishes the proof.
(e) Let $S = \{0 \leq k \leq 2n \mid k+1 \text{ is composite and } k+1 \neq 4\}$. Then from (a) - (d),

$$\begin{aligned}B_{2n} &= \sum_{k=0}^{2n} \frac{1}{k+1} \sum_{r=0}^{k} (-1)^r \binom{k}{r} r^{2n} \\ &= \sum_{k \in S} \frac{k!}{k+1} c(2n,k) + \sum_{\substack{p-1 \leq 2n \\ p \text{ is prime}}} \frac{1}{p} \sum_{r=0}^{p-1} (-1)^r \binom{p-1}{r} r^{2n} + \frac{1}{4} \sum_{r=0}^{3} (-1)^r \binom{3}{r} r^{2n} \\ &= I_n' - \sum_{p-1 \mid 2n} \frac{1}{p} + \frac{1}{4} \sum_{r=0}^{3} (-1)^r \binom{3}{r} r^{2n}, \end{aligned} \tag{23}$$

where I'_n is an integer. Now

$$\sum_{r=0}^{3}(-1)^r\binom{3}{r}r^{2n} \equiv -3 - 3^{2n} \equiv 0 \mod 4,$$

which means the last sum in (23) is an integer. □

Exercise 12.13. Prove that the derivative of the Bernoulli polynomial $B'_n(x)$ is $nB_{n-1}(x)$ if $n \geq 2$.

Proof. By definition we have

$$\begin{aligned}\sum_{n=0}^{\infty} B'_n(x)\frac{t^n}{n!} &= \frac{\partial}{\partial x}\left(\frac{te^{xt}}{e^t-1}\right) = \frac{t^2e^{xt}}{e^t-1}\\ &= t\sum_{n=0}^{\infty} B_n(x)\frac{t^n}{n!}\\ &= \sum_{n=1}^{\infty} B_{n-1}(x)\frac{t^n}{(n-1)!}\\ &= \sum_{n=1}^{\infty} nB_{n-1}(x)\frac{t^n}{n!}.\end{aligned}$$

Equating coefficients for $n \geq 1$ gives the result. □

Exercise 12.14. Prove that the Bernoulli polynomials satisfy the addition formula

$$B_n(x+y) = \sum_{k=0}^{n}\binom{n}{k}B_k(x)y^{n-k}.$$

Proof. By definition we have

$$\begin{aligned}\sum_{n=0}^{\infty} B_n(x+y)\frac{t^n}{n!} &= \frac{te^{xt+yt}}{e^t-1} = \frac{te^{xt+yt}}{e^t-1}e^{yt}\\ &= \left(\sum_{n=0}^{\infty} B_n(x)\frac{t^n}{n!}\right)\left(\sum_{n=0}^{\infty} y^n\frac{t^n}{n!}\right)\\ &= \sum_{n=0}^{\infty}\left(\sum_{k=0}^{n}\binom{n}{k}B_k(x)y^{n-k}\right)\frac{t^n}{n!}.\end{aligned}$$

Equating coefficients gives the result. □

Exercise 12.15. Prove that the Bernoulli polynomials satisfy the multiplication formula

$$B_p(mx) = m^{p-1}\sum_{k=0}^{m-1} B_p\left(x+\frac{k}{m}\right).$$

Proof. By definition we have

$$\begin{aligned}\sum_{n=0}^{\infty} m^{p-1} \sum_{k=0}^{m-1} B_p\left(x+\frac{k}{m}\right)\frac{t^n}{n!} &= m^{p-1}\sum_{k=0}^{m-1}\frac{te^{(x+k/m)t}}{e^t-1}\\ &= m^{p-1}\frac{te^{xt}}{e^t-1}\sum_{k=0}^{m-1}(e^{t/m})^k\\ &= m^{p-1}\frac{te^{xt}}{e^t-1}\frac{e^t-1}{e^{t/m}-1}\\ &= m^p\frac{(t/m)e^{mx(t/m)}}{e^{t/m}-1}\\ &= \sum_{n=0}^{\infty} m^p B_n(mx)\frac{(t/m)^n}{n!}.\end{aligned}$$

Equating coefficients of t^p gives

$$B_p(mx) = m^{p-1}\sum_{k=0}^{m-1} B_p\left(x+\frac{k}{m}\right).$$

□

Exercise 12.16. Prove that if $r \geq 1$ the Bernoulli numbers satisfy the relation

$$\sum_{k=0}^{r}\frac{2^{2k}B_{2k}}{(2k)!(2r+1-2k)!} = \frac{1}{(2r)!}.$$

Proof. Note $B_1 = -1/2$ and $B_{2k+1} = 0$ for all $k > 0$. Thus we can include odd k in the sum on the left hand side to get

$$\begin{aligned}\sum_{k=0}^{r}\frac{2^{2k}B_{2k}}{(2k)!(2r+1-2k)!} &= \frac{1}{(2r)!} + \sum_{k=0}^{2r+1}\frac{2^k B_k}{k!(2r+1-k)!}\\ &= \frac{1}{(2r)!} + \frac{1}{(2r+1)!}\sum_{k=0}^{2r+1}\binom{2r+1}{k}2^k B_k\\ &= \frac{1}{(2r)!} + \frac{2^{2r+1}}{(2r+1)!}\sum_{k=0}^{2r+1}\binom{2r+1}{k}B_k\cdot\left(\frac{1}{2}\right)^{2r+1-k}\\ &= \frac{1}{(2r)!} + \frac{2^{2r+1}}{(2r+1)!}B_{2r+1}(1/2).\end{aligned}$$

By Exercise 12.11, $B_{2r+1}(1/2) = 0$ which completes the proof. □

Remark. Applying Theorem 12.17 gives the recurrence relation

$$2(-1)^{r+1}\pi^{-2r}\zeta(2r) = \frac{1}{(2r)!} - \sum_{k=0}^{r-1}\frac{2(-1)^{k+1}\pi^{-2k}\zeta(2k)}{(2r+1-2k)!}.$$

Exercise 12.17. Calculate the integral $\int_0^1 xB_p(x)dx$ in two ways and deduce the formula

$$\sum_{r=0}^{p} \binom{p}{r} \frac{B_r}{p+2-r} = \frac{B_{p+1}}{p+1}.$$

Proof. The result can be verified directly for $p < 2$. By Exercise 12.13, $B_p'(x) = pB_{p-1}(x)$, which implies an antiderivative of $B_p(x)dx$ is $B_{p+1}(x)/(p+1)$. Additionally by Theorem 12.14, $B_p(0) = B_p(1)$ for $p \geq 2$. Hence integrating by parts we see

$$\begin{aligned}\int_0^1 xB_p(x)dx &= x\frac{B_{p+1}(x)}{p+1}\Big]_0^1 - \int_0^1 B_p(x)dx \\ &= \frac{B_{p+1}}{p+1} - \left[\frac{B_{p+1}(x)}{p+1}\right]_0^1 \\ &= \frac{B_{p+1}}{p+1}.\end{aligned}$$

On the other hand, we can apply Theorem 12.12 before integrating to find

$$\begin{aligned}\int_0^1 xB_p(x)dx &= \int_0^1 x\sum_{r=0}^{p}\binom{p}{r}B_r x^{p-r}dx \\ &= \sum_{r=0}^{p}\binom{p}{r}B_r\int_0^1 x^{p+1-r}dx \\ &= \sum_{r=0}^{p}\binom{p}{r}\frac{B_r}{p+2-r}.\end{aligned}$$

□

Exercise 12.18.
(a) Verify the identity

$$\begin{aligned}\frac{uv}{(e^u-1)(e^v-1)}\frac{e^{u+v}-1}{u+v} &= \frac{uv}{u+v}\left(1+\frac{1}{e^u-1}+\frac{1}{e^v-1}\right) \\ &= 1+\sum_{n=2}^{\infty}\frac{uv}{n!}\left(\frac{u^{n-1}+v^{n-1}}{u+v}\right)B_n.\end{aligned}$$

(b) Let $J = \int_0^1 B_p(x)B_q(x)dx$. Show that J is the coefficient of $p!q!u^pv^q$ in the expansion of (a). Use this to deduce that

$$\int_0^1 B_p(x)B_q(x)dx = \begin{cases}(-1)^{p+1}\frac{p!q!}{(p+q)!}B_{p+q} & \text{if } p \geq 1, q \geq 1, \\ 1 & \text{if } p = q = 0, \\ 0 & \text{if } p \geq 1, q = 0; \text{ or } p = 0, q \geq 1.\end{cases}$$

Proof.
(a) The first equality is verified with standard algebraic techniques, so we will focus on the other equality. Now by the definition of Bernoulli numbers,

$$\begin{aligned}\frac{uv}{u+v}\left(1+\frac{1}{e^u-1}+\frac{1}{e^v-1}\right) &= \frac{uv}{u+v}\left(1+\sum_{n=0}^{\infty}B_n\frac{u^n}{n!}+\sum_{n=0}^{\infty}B_n\frac{v^n}{n!}\right)\\ &= \frac{uv}{u+v}\left(1+\sum_{n=0}^{\infty}(u^{n-1}+v^{n-1})\frac{B_n}{n!}\right)\\ &= 1+\sum_{n=2}^{\infty}\frac{uv}{n!}\left(\frac{u^{n-1}+v^{n-1}}{u+v}\right)B_n.\end{aligned}$$

(b) We have by (a) that

$$\begin{aligned}\sum_{p=0}^{\infty}\sum_{q=0}^{\infty}\int_0^1 B_p(x)B_q(x)dx\frac{u^pv^q}{p!q!} &= \int_0^1\frac{ue^{xu}}{e^u-1}\frac{ve^{xv}}{e^v-1}dx\\ &= \frac{uv}{(e^u-1)(e^v-1)}\frac{e^{u+v}-1}{u+v}\\ &= 1+\sum_{n=2}^{\infty}\frac{uv}{n!}\left(\frac{u^{n-1}+v^{n-1}}{u+v}\right)B_n. \qquad (24)\end{aligned}$$

Since $B_{2k+1}=0$ for $k>0$ we can include or ignore the odd indices in subsequent transformations of (24). This gives

$$\begin{aligned}1+\sum_{n=2}^{\infty}\frac{uv}{n!}\left(\frac{u^{n-1}+v^{n-1}}{u+v}\right)B_n &= 1+\sum_{n=2}^{\infty}\frac{uv}{(2n)!}\left(\frac{u^{2n-1}+v^{2n-1}}{u+v}\right)B_{2n}\\ &= 1+\sum_{n=2}^{\infty}\frac{uv}{(2n)!}\sum_{m=1}^{n-1}(-1)^{m+1}u^{m-1}v^{n-m-1}B_{2n}\\ &= 1+\sum_{n=2}^{\infty}\sum_{m=1}^{n-1}(-1)^{m+1}u^mv^{n-m}\frac{B_n}{n!}.\end{aligned}$$

Making the substitution $(m,n)=(p,p+q)$ shows the sum is equal to

$$1+\sum_{p=1}^{\infty}\sum_{q=1}^{\infty}(-1)^{p+1}B_{p+q}\frac{u^pv^q}{(p+q)!},$$

because solving the system

$$2\le p+q \quad\text{and}\quad 1\le p\le p+q-1$$

gives $p\ge 1$ and $q\ge 1$. Equating coefficients gives the result. □

Exercise 12.19.
(a) Use a method similar to that in Exercise 12.18 to derive the identity

$$(u+v)\sum_{m=0}^{\infty}\sum_{n=0}^{\infty}B_m(x)B_n(x)\frac{u^m v^n}{m!n!}=\sum_{m=0}^{\infty}\sum_{n=0}^{\infty}B_{m+n}(x)\frac{u^m v^n}{m!n!}\sum_{r=0}^{\infty}\frac{B_{2r}}{(2r)!}(u^{2r}v+uv^{2r}).$$

(b) Compare coefficients in (a) and integrate the result to obtain the formula

$$B_m(x)B_n(x)=\sum_r\left\{\binom{m}{2r}n+\binom{n}{2r}m\right\}\frac{B_{2r}B_{m+n-2r}(x)}{m+n-2r}+(-1)^{m+1}\frac{m!n!}{(m+n)!}B_{m+n}$$

for $m\geq 1$, $n\geq 1$. Indicate the range of the index r.

Proof.
(a) Looking at the right hand side, since $B_1=-1/2$ and $B_{2r+1}=0$ for $r>0$,

$$\begin{aligned}\sum_{r=0}^{\infty}\frac{B_{2r}}{(2r)!}(u^{2r}v+uv^{2r})&=\sum_{r=0}^{\infty}\frac{B_r}{r!}(u^r v+uv^r)+uv\\&=\frac{uv}{e^u-1}+\frac{uv}{e^v-1}+uv=\frac{uv\,(e^{u+v}-1)}{(e^u-1)\,(e^v-1)}.\end{aligned}$$

For the remainder of the right hand side, we can collect the sum in terms of $B_k(x)$ to get

$$\begin{aligned}\sum_{m=0}^{\infty}\sum_{n=0}^{\infty}B_{m+n}(x)\frac{u^m v^n}{m!n!}&=\sum_{k=0}^{\infty}B_k(x)\sum_{j=0}^{k}\frac{u^j v^{k-j}}{j!(k-j)!}\\&=\sum_{k=0}^{\infty}\frac{B_k(x)}{k!}\sum_{j=0}^{k}\binom{k}{j}u^j v^{k-j}\\&=\sum_{k=0}^{\infty}B_k(x)\frac{(u+v)^k}{k!}=\frac{(u+v)e^{x(u+v)}}{e^{u+v}-1}.\end{aligned}$$

Multiplying shows

$$\begin{aligned}\sum_{m=0}^{\infty}\sum_{n=0}^{\infty}B_{m+n}(x)\frac{u^m v^n}{m!n!}\sum_{r=0}^{\infty}\frac{B_{2r}}{(2r)!}(u^{2r}v+uv^{2r})&=\frac{(u+v)e^{x(u+v)}}{e^{u+v}-1}\frac{uv\,(e^{u+v}-1)}{(e^u-1)\,(e^v-1)}\\&=(u+v)\frac{ue^{xu}}{e^u-1}\frac{ve^{xv}}{e^v-1}\\&=(u+v)\sum_{m=0}^{\infty}\sum_{n=0}^{\infty}B_m(x)B_n(x)\frac{u^m v^n}{m!n!}.\end{aligned}$$

(b) The right hand side of (a) is equal to

$$\sum_{m=0}^{\infty}\sum_{n=0}^{\infty}\sum_{r=0}^{\infty}\frac{B_{2r}}{(2r)!}B_{m+n}(x)\frac{u^{m+2r}v^{n+1}}{m!n!}+\sum_{m=0}^{\infty}\sum_{n=0}^{\infty}\sum_{r=0}^{\infty}\frac{B_{2r}}{(2r)!}B_{m+n}(x)\frac{u^{m+1}v^{n+2r}}{m!n!}.$$

To collect both sums in terms of $u^p v^q$ we will substitute $(p,q) = (m+2r, n+1)$ in the first sum and $(p,q) = (m+1, n+2r)$ in the second sum. Hence in the first sum r will range from 0 to $\lfloor p/2 \rfloor$ and in the second sum r will range from 0 to $\lfloor q/2 \rfloor$. This means the sums equal

$$\begin{aligned}
&\sum_{p=0}^{\infty}\sum_{q=1}^{\infty}\sum_{r=0}^{\lfloor p/2\rfloor}\frac{B_{2r}}{(2r)!}\frac{B_{p+q-2r-1}(x)u^p v^q}{(p-2r)!(q-1)!} + \sum_{p=1}^{\infty}\sum_{q=0}^{\infty}\sum_{r=0}^{\lfloor q/2\rfloor}\frac{B_{2r}}{(2r)!}\frac{B_{p+q-2r-1}(x)u^p v^q}{(p-1)!(q-2r)!} \\
&\quad = \sum_{p=0}^{\infty}\sum_{q=0}^{\infty}\sum_{r=0}^{\lfloor p/2\rfloor}\binom{p}{2r} q\frac{B_{2r}B_{p+q-2r-1}(x)u^p v^q}{p!q!} + \sum_{p=0}^{\infty}\sum_{q=0}^{\infty}\sum_{r=0}^{\lfloor q/2\rfloor}\binom{q}{2r} p\frac{B_{2r}B_{p+q-2r-1}(x)u^p v^q}{p!q!} \\
&\quad = \sum_{p=0}^{\infty}\sum_{q=0}^{\infty}\sum_{r=0}^{M_{p,q}}\left\{\binom{p}{2r} q + \binom{q}{2r} p\right\} B_{2r}B_{p+q-2r-1}(x)\frac{u^p v^q}{p!q!}, \qquad (25)
\end{aligned}$$

where $M_{p,q} = \max\{\lfloor p/2 \rfloor, \lfloor q/2 \rfloor\}$.

Now the left hand side of (a) is equal to

$$(u+v)\frac{ue^{xu}}{e^u-1}\frac{ve^{xv}}{e^v-1} = \left(\frac{ue^{xu}}{e^u-1}\frac{ve^{xv}}{e^v-1}\right)' = \sum_{m=0}^{\infty}\sum_{n=0}^{\infty}\left(B_m(x)B_n(x)\right)'\frac{u^m v^n}{m!n!}.$$

Thus equating coefficients of this with the coefficients of (25) shows

$$\left(B_m(x)B_n(x)\right)' = \sum_{r=0}^{M_{m,n}}\left\{\binom{n}{2r} m + \binom{n}{2r} m\right\} B_{2r}B_{m+n-2r-1}(x).$$

Since Exercise 12.13 shows an antiderivative of $B_k(x)$ is $B_{k+1}(x)/(k+1)$, integrating both sides gives

$$B_m(x)B_n(x) = \sum_{r=0}^{M_{m,n}}\left\{\binom{m}{2r} n + \binom{n}{2r} m\right\}\frac{B_{2r}B_{m+n-2r}(x)}{m+n-2r} + C$$

where C is some constant with respect to x. Finally, Exercise 12.18 shows

$$\int_0^1 B_m(x)B_n(x)dx = (-1)^{m+1}\frac{m!n!}{(m+n)!}B_{m+n} \quad \text{and} \quad \int_0^1 B_k(x) = 0,$$

so it must be that $C = (-1)^{m+1}\frac{m!n!}{(m+n)!}B_{m+n}$. □

Exercise 12.20. Show that if $m \geq 1$, $n \geq 1$ and $p \geq 1$, we have

$$\begin{aligned}
&\int_0^1 B_m(x)B_n(x)B_p(x)dx \\
&\qquad = (-1)^{p+1}p!\sum_r\left\{\binom{m}{2r} n + \binom{n}{2r} m\right\}\frac{(m+n-2r-1)!}{(m+n+p-2r)!}B_{2r}B_{m+n+p-2r}.
\end{aligned}$$

In particular, compute $\int_0^1 B_2^3(x)dx$ from this formula.

Proof. Note in Exercise 12.18 it was shown that $\int_0^1 B_p(x)dx = 0$. Combining this with the rest of the results of Exercise 12.18 and Exercise 12.19 shows

$$\begin{aligned}
&\int_0^1 B_m(x)B_n(x)B_p(x)dx \\
&\qquad = \int_0^1 \sum_r \left\{ \binom{m}{2r} n + \binom{n}{2r} m \right\} \frac{B_{2r}B_{m+n-2r}(x)}{m+n-2r} B_p(x)dx \\
&\qquad = \sum_r \left\{ \binom{m}{2r} n + \binom{n}{2r} m \right\} \frac{B_{2r}}{m+n-2r} \int_0^1 B_{m+n-2r}(x)B_p(x)dx \\
&\qquad = \sum_r \left\{ \binom{m}{2r} n + \binom{n}{2r} m \right\} \frac{B_{2r}}{m+n-2r} (-1)^{p+1} \frac{(m+n-2r)!p!}{(m+n+p-2r)!} B_{m+n+p-2r} \\
&\qquad = (-1)^{p+1} p! \sum_r \left\{ \binom{m}{2r} n + \binom{n}{2r} m \right\} \frac{(m+n-2r-1)!}{(m+n+p-2r)!} B_{2r}B_{m+n+p-2r}.
\end{aligned}$$

In particular

$$\int_0^1 B_2^3(x)dx = -8 \sum_{r=0}^{1} \binom{2}{2r} \frac{(3-2r)!}{(6-2r)!} B_{2r}B_{6-2r} = \frac{1}{3780}.$$

□

Exercise 12.21. Let $f(n)$ be an arithmetical function which is periodic mod k, and let

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

denote the finite Fourier coefficients of f. If

$$F(s) = k^{-s} \sum_{r=1}^{k} f(r) \zeta\left(s, \frac{r}{k}\right),$$

prove that

$$F(1-s) = \frac{\Gamma(s)}{(2\pi)^s} \left\{ e^{\pi is/2} \sum_{r=1}^{k} g(r) \zeta\left(s, \frac{r}{k}\right) + e^{-\pi is/2} \sum_{r=1}^{k} g(-r) \zeta\left(s, \frac{r}{k}\right) \right\}.$$

Proof. From Theorem 12.8,

$$\begin{aligned}
F(1-s) &= k^{s-1}\sum_{r=1}^{k} f(r)\zeta\left(1-s,\frac{r}{k}\right)\\
&= k^{s-1}\sum_{r=1}^{k} f(r)\frac{2\Gamma(s)}{(2\pi k)^s}\sum_{t=1}^{k}\cos\left(\frac{\pi s}{2}-\frac{2\pi tr}{k}\right)\zeta\left(s,\frac{t}{k}\right)\\
&= \frac{2\Gamma(s)}{(2\pi)^s}\sum_{t=1}^{k}\zeta\left(s,\frac{t}{k}\right)\frac{1}{k}\sum_{r=1}^{k} f(r)\left\{\frac{e^{\pi is/2-2\pi itr/k}+e^{-\pi is/2+2\pi itr/k}}{2}\right\}\\
&= \frac{\Gamma(s)}{(2\pi)^s}\sum_{t=1}^{k}\zeta\left(s,\frac{t}{k}\right)\left\{\frac{e^{\pi is/2}}{k}\sum_{r=1}^{k} f(r)e^{-2\pi itr/k}+\frac{e^{-\pi is/2}}{k}\sum_{r=1}^{k} f(r)e^{-2\pi i(-t)r/k}\right\}\\
&= \frac{\Gamma(s)}{(2\pi)^s}\left\{e^{\pi is/2}\sum_{t=1}^{k} g(t)\zeta\left(s,\frac{t}{k}\right)+e^{-\pi is/2}\sum_{t=1}^{k} g(-t)\zeta\left(s,\frac{t}{k}\right)\right\}.
\end{aligned}$$

□

Exercise 12.22. Let χ be any nonprincipal character mod k and let $S(x)=\sum_{n\le x}\chi(n)$.
(a) If $N\ge 1$ and $\sigma>0$ prove that

$$L(s,\chi)=\sum_{n=1}^{N}\frac{\chi(n)}{n^s}+s\int_N^\infty\frac{S(x)-S(N)}{x^{s+1}}dx.$$

(b) If $s=\sigma+it$ with $\sigma\ge\delta>0$ and $|t|\ge 0$, use (a) to show that there is a constant $A(\delta)$ such that, if $\delta\le 1$,

$$|L(s,\chi)|\le A(\delta)B(k)(|t|+1)^{1-\delta}$$

where $B(k)$ is an upper bound for $|S(x)|$. In Theorem 13.15 it is shown that $B(k)=O\left(\sqrt{k}\log k\right)$.
(c) Prove that for some constant $A>0$ we have

$$|L(s,\chi)|\le A\log k\quad\text{if }\sigma\ge 1-\frac{1}{\log k}\text{ and }0\le|t|\le 2.$$

[*Hint*: Take $N=k$ in (a).]

Proof.
(a) For $\sigma>0$ and $1\le N<M$, by Abel's summation formula

$$\begin{aligned}
\sum_{n=1}^{M}\frac{\chi(n)}{n^s} &= \sum_{n=1}^{N}\frac{\chi(n)}{n^s}+\sum_{n=N+1}^{M}\frac{\chi(n)}{n^s}\\
&= \sum_{n=1}^{N}\frac{\chi(n)}{n^s}-\frac{S(N)}{N^s}+\frac{S(M)}{M^s}+s\int_N^M\frac{S(x)}{x^{\sigma+1}}dx.
\end{aligned}$$

Noting $\sigma > 0$ and $S(x) = O(1)$, let $M \to \infty$. As a consequence $S(M)M^{-s} \to 0$ and the integral converges. This means

$$\begin{aligned} L(s,\chi) &= \sum_{n=1}^{N} \frac{\chi(n)}{n^s} - \frac{S(N)}{N^s} + s\int_N^\infty \frac{S(x)}{x^{\sigma+1}}dx \\ &= \sum_{n=1}^{N} \frac{\chi(n)}{n^s} + s\int_N^\infty \frac{S(x)-S(N)}{x^{s+1}}dx. \end{aligned}$$

(b) For $\sigma \geq \delta > 0$ and $\delta \leq 1$, by Theorem 3.2 (b),

$$\begin{aligned} |L(s,\chi)| &\leq B(k)\sum_{n=1}^{N}\frac{1}{n^\delta} + |s|\int_N^\infty \frac{2B(k)}{x^{\sigma+1}}dx \\ &\leq A'(\delta)B(k)N^{1-\delta} + 2\left(1+\frac{|t|}{\sigma}\right)B(k)N^{-\sigma} \\ &\leq A'(\delta)B(k)N^{1-\delta} + \frac{2}{\delta}(\delta+|t|)B(k)N^{-\delta} \\ &\leq A'(\delta)B(k)N^{1-\delta} + \frac{2}{\delta}(1+|t|)B(k)N^{-\delta}. \end{aligned}$$

Letting $N = \lfloor |t|+1 \rfloor \leq |t|+1$ gives

$$|L(s,\chi)| \leq \left(A'(\delta)+\frac{2}{\delta}\right)B(k)(|t|+1)^{1-\delta}.$$

(c) Following the hint,

$$L(s,\chi) = \sum_{n=1}^{k}\frac{\chi(n)}{n^s} + s\int_k^\infty \frac{S(x)}{x^{s+1}}dx.$$

This leads to

$$\begin{aligned} |L(s,\chi)| &\leq \sum_{n=1}^{k}\frac{1}{n^\sigma} + (\sigma+2)\int_k^\infty \frac{B(k)}{x^{\sigma+1}}dx \\ &= \sum_{n=1}^{k}\frac{1}{n^\sigma} + \left(1+\frac{2}{\sigma}\right)B(k)k^{-\sigma} \\ &= \frac{k^{1-\sigma}}{1-\sigma} + \zeta(\sigma) + O\big(k^{-\sigma}\big) + \left(1+\frac{2}{\sigma}\right)B(k)k^{-\sigma}, \end{aligned}$$

where Theorem 3.2 (b) was applied in the last step. Now $\sigma \geq 1 - 1/\log k$ so we have

$$\begin{aligned} |L(s,\chi)| &\leq \frac{k^{1/\log k}}{1/\log k} + \zeta\left(1-\frac{1}{\log 2}\right) + O\left(\frac{k^{1/\log k}}{k}\right) + \left(1+\frac{2}{1-1/\log k}\right)B(k)\frac{k^{1/\log k}}{k} \\ &= e\log k + \zeta\left(1-\frac{1}{\log 2}\right) + o(1) + eB(k)\frac{\log k - 3}{k(\log k - 1)} \\ &\leq e\log k + C_1\frac{B(k)}{\sqrt{k}} + C_2, \end{aligned}$$

for some constants C_i. Since $B(k) = O\Big(\sqrt{k}\log k\Big)$, as mentioned in (b), we're done. $\square$

Chapter 13
Analytic Proof of the Prime Number Theorem

Exercise 13.1. Chebyshev proved that if $\psi(x)/x$ tends to a limit as $x \to \infty$ then this limit equals 1. A proof was outlined in Exercise 4.26. This exercise outlines another proof based on the identity

$$-\frac{\zeta'(s)}{\zeta(s)} = s\int_1^\infty \frac{\psi(x)}{x^{s+1}}dx, \qquad (\sigma > 1) \tag{26}$$

given in Exercise 11.1 (d).
(a) Prove that $(1-s)\zeta'(s)/\zeta(s) \to 1$ as $s \to 1$.
(b) Let $\delta = \limsup_{x\to\infty}(\psi(x)/x)$. Given $\varepsilon > 0$, choose $N = N(\varepsilon)$ so that $x \geq N$ implies $\psi(x) \leq (\delta+\varepsilon)x$. Keep s real, $1 < s \leq 2$, split the integral (26) into two parts, $\int_1^N + \int_N^\infty$ and estimate each part to obtain the inequality

$$-\frac{\zeta'(s)}{\zeta(s)} \leq C(\varepsilon) + \frac{s(\delta+\varepsilon)}{s-1},$$

where $C(\varepsilon)$ is a constant independent of s. Use (a) to deduce that $\delta \geq 1$.
(c) Let $\gamma = \liminf_{x\to\infty}(\psi(x)/x)$ and use a similar argument to deduce that $\gamma \leq 1$. Therefore if $\psi(x)/x$ tends to a limit as $x \to \infty$ then $\gamma = \delta = 1$.

Proof. By Theorem 4.9, there are positive constants c_1, c_2 such that $c_2 x \leq \psi(x) \leq c_1 x$ eventually holds for all x. Thus both the liminf and limsup of $\psi(x)/x$ exist.

(a) By Theorem 12.4 $\zeta(s)$ has a simple pole at $s = 1$ with residue 1. Therefore there is an entire function $R(s)$ such that

$$\zeta(s) = \frac{1}{s-1} + R(s) \quad \text{and} \quad \zeta'(s) = -\frac{1}{(s-1)^2} + R'(s).$$

This means

$$\frac{(1-s)\zeta'(s)}{\zeta(s)} = \frac{1-(s-1)^2R'(s)}{1+(s-1)R(s)},$$

hence $(1-s)\zeta'(s)/\zeta(s) \to 1$ as $s \to 1$.

(b) Let $\delta = \limsup \psi(x)/x$ and $\varepsilon > 0$. By definition of limsup, there exists $N = N_\varepsilon$ such that for all $x \geq N$, $\psi(x) \leq (\delta + \varepsilon)x$. Then

$$\begin{aligned} -\frac{\zeta'(s)}{\zeta(s)} &= s\left(\int_1^N + \int_N^\infty\right)\frac{\psi(x)}{x^{s+1}}dx \\ &\leq s\int_1^N \frac{\psi(N)}{x^{s+1}}dx + s\int_N^\infty \frac{\delta+\varepsilon}{x^s}dx \\ &= (1-N^{1-s})\psi(N) + N^{1-s}\frac{s(\delta+\varepsilon)}{s-1} \\ &\leq \psi(N) + \frac{s(\delta+\varepsilon)}{s-1}. \end{aligned}$$

Multiplying through by $s-1$ gives

$$\frac{(1-s)\zeta'(s)}{\zeta(s)} \leq (s-1)\psi(N) + s(\delta+\varepsilon)$$

and applying (a) while taking $s \to 1^+$ shows

$$1 \leq \delta + \varepsilon.$$

Letting $\varepsilon \to 0^+$ proves $1 \leq \delta$.

(c) Let $\gamma = \liminf \psi(x)/x$ and $\varepsilon > 0$. By definition of limsup, there exists $N = N_\varepsilon$ such that for all $x \geq N$, $\psi(x) \geq (\gamma - \varepsilon)x$. Then

$$\begin{aligned} -\frac{\zeta'(s)}{\zeta(s)} &= s\left(\int_1^N + \int_N^\infty\right)\frac{\psi(x)}{x^{s+1}}dx \\ &\geq s\int_1^N \frac{1}{x^{s+1}}dx + s\int_N^\infty \frac{\gamma-\varepsilon}{x^s}dx \\ &= (1-N^{1-s}) + N^{1-s}\frac{s(\gamma-\varepsilon)}{s-1} \\ &\geq 1 + \frac{s(\gamma-\varepsilon)}{s-1}. \end{aligned}$$

Multiplying through by $s-1$ gives

$$\frac{(1-s)\zeta'(s)}{\zeta(s)} \geq (s-1) + s(\gamma-\varepsilon)$$

and applying (a) while taking $s \to 1^+$ shows

$$1 \geq \gamma - \varepsilon.$$

Letting $\varepsilon \to 0^+$ proves $1 \geq \gamma$. □

Exercise 13.2. Let $A(x) = \sum_{n \le x} a(n)$, where

$$a(n) = \begin{cases} 0 & \text{if } n \neq \text{a prime power,} \\ \frac{1}{k} & \text{if } n = p^k. \end{cases}$$

Prove that $A(x) = \pi(x) + O(\sqrt{x} \log\log x)$.

Proof. Observe by the prime number theorem

$$\begin{aligned} A(x) &= \sum_{n=1}^{\lfloor \log_2(x) \rfloor} \frac{\pi(x^{1/n})}{n} \\ &= \pi(x) + \frac{1}{\log x} \sum_{n=2}^{\lfloor \log_2(x) \rfloor} \left(x^{1/n} + o\left(x^{1/n}\right)\right) \\ &= \pi(x) + \frac{1}{\log x} O\left(\sqrt{x} \log_2(x)\right) \\ &= \pi(x) + O\left(\sqrt{x}\right). \end{aligned}$$

□

Exercise 13.3.
(a) If $c > 1$ and $x \neq$ integer, prove that if $x > 1$,

$$\frac{1}{2\pi i} \int_{c-\infty i}^{c+\infty i} \log \zeta(s) \frac{x^s}{s} ds = \pi(x) + \frac{1}{2}\pi(x^{1/2}) + \frac{1}{3}\pi(x^{1/3}) + \cdots.$$

(b) Show that the prime number theorem is equivalent to the asymptotic relation

$$\frac{1}{2\pi i} \int_{c-\infty i}^{c+\infty i} \log \zeta(s) \frac{x^s}{s} ds \sim \frac{x}{\log x} \quad \text{as } x \to \infty.$$

A proof of the prime number theorem based on this relation was given by Landau in 1903.

Proof.
(a) Let $\sigma = c$. It was shown in Theorem 11.14 that

$$\log \zeta(s) = \sum_{n=2}^{\infty} \frac{\Lambda(n)}{\log n} n^{-s},$$

so by Theorem 11.18 (Perron's formula)

$$\frac{1}{2\pi i} \int_{c-\infty i}^{c+\infty i} \log \zeta(s) \frac{x^s}{s} ds = \sum_{n \le x} \frac{\Lambda(n)}{\log n}.$$

Observe

$$\frac{\Lambda(n)}{\log n} = \begin{cases} 0 & \text{if } n \neq \text{a prime power,} \\ \frac{1}{k} & \text{if } n = p^k, \end{cases}$$

so

$$\frac{1}{2\pi i}\int_{c-\infty i}^{c+\infty i}\log\zeta(s)\frac{x^s}{s}ds=\sum_{p^k\le x}\frac{1}{k}=\pi(x)+\frac{1}{2}\pi(x^{1/2})+\frac{1}{3}\pi(x^{1/3})+\cdots.$$

(b) By Exercise 13.2 and (a) we have

$$\frac{1}{2\pi i}\int_{c-\infty i}^{c+\infty i}\log\zeta(s)\frac{x^s}{s}ds=A(x)=\pi(x)+O\big(\sqrt{x}\log\log x\big),$$

and the proof follows since

$$O\big(\sqrt{x}\log\log x\big)=o\bigg(\frac{x}{\log x}\bigg).$$

□

Exercise 13.4. Let $M(x)=\sum_{n\le x}\mu(n)$. The exact order of magnitude of $M(x)$ for large x is not known. In Chapter 4 it was shown that the prime number theorem is equivalent to the relation $M(x)=o(x)$ as $x\to\infty$. This exercise relates the order of magnitude of $M(x)$ with the Riemann hypothesis.

Suppose there is a positive constant θ such that

$$M(x)=O\big(x^\theta\big)\quad\text{for } x\ge 1.$$

Prove that the formula

$$\frac{1}{\zeta(s)}=s\int_1^\infty\frac{M(x)}{x^{s+1}}dx,$$

which holds for $\sigma>1$ (see Exercise 11.1 (c)) would also be valid for $\sigma>\theta$. Deduce that $\zeta(s)\ne 0$ for $\sigma>\theta$. In particular, this shows that the relation $M(x)=O\big(x^{1/2+\varepsilon}\big)$ for every $\varepsilon>0$ implies the Riemann hypothesis. It can also be shown that the Riemann hypothesis implies $M(x)=O\big(x^{1/2+\varepsilon}\big)$ for every $\varepsilon>0$.

Proof. Suppose there is some positive constant θ such that $M(x)=O\big(x^\theta\big)$. Then it's clear

$$s\int_1^\infty\frac{M(x)}{x^{s+1}}dx$$

converges for $\sigma>\theta$. As mentioned in Exercise 11.16, the integral is thus analytic in this half-plane. Hence by the uniqueness of analytic continuation,

$$\frac{1}{\zeta(s)}=s\int_1^\infty\frac{M(x)}{x^{s+1}}dx\quad\text{for }\sigma>\theta.$$

Therefore $1/\zeta(s)$ is analytic in this half-plane, so $\zeta(s)\ne 0$ for $\sigma>\theta$. □

Exercise 13.5. Prove the following lemma, which is similar to Lemma 2. Let

$$A_1(x)=\int_1^x\frac{A(u)}{u}du,$$

where $A(u)$ is a nonnegative increasing function for $u \geq 1$. If we have the asymptotic formula

$$A_1(x) \sim Lx^c \quad \text{as } x \to \infty,$$

for some $c > 0$ and $L > 0$, then we also have

$$A(x) \sim cLx^c \quad \text{as } x \to \infty.$$

Proof. Since $x^c \to \infty$ as $x \to \infty$, we can apply L'Hôpital's rule to find

$$L = \lim_{x\to\infty} \frac{A_1(x)}{x^c} = \lim_{x\to\infty} \frac{A(x)/x}{cx^{c-1}} = \lim_{x\to\infty} \frac{A(x)}{cx^c}.$$

□

Exercise 13.6. Prove that

$$\frac{1}{2\pi i} \int_{2-\infty i}^{2+\infty i} \frac{y^s}{s^2} ds = 0 \quad \text{if } 0 < y < 1.$$

What is the value of this integral if $y \geq 1$?

Proof. When $0 < y < 1$ consider the contour C_1 illustrated in Figure 5 (a). Since y^s/s^2 is analytic for $s \neq 0$,

$$\frac{1}{2\pi i} \int_{C_1} \frac{y^s}{s^2} ds = 0.$$

Now observe $|y^s| = y^\sigma \leq y^2$ for any s on C_1. Hence if C_R is the circular sector of C_1,

$$\left| \int_{C_R} \frac{y^s}{s^2} ds \right| \leq \frac{y^2}{R^2}(\pi R) \to 0 \quad \text{as } R \to \infty,$$

which means

$$\frac{1}{2\pi i} \int_{2-\infty i}^{2+\infty i} \frac{y^s}{s^2} ds = 0.$$

When $y \geq 1$ consider the contour C_2 illustrated in Figure 5 (b). Note

$$\operatorname*{Res}_{s=0} \left(\frac{y^s}{s^2} \right) = \log y,$$

hence

$$\frac{1}{2\pi i} \int_{C_2} \frac{y^s}{s^2} ds = \log y.$$

Now observe $|y^s| = y^\sigma \leq y^2$ for any s on C_2. Hence if C_R is the circular sector of C_2,

$$\left| \int_{C_R} \frac{y^s}{s^2} ds \right| \leq \frac{y^2}{R^2}(2\pi R) \to 0 \quad \text{as } R \to \infty,$$

which means

$$\frac{1}{2\pi i} \int_{2-\infty i}^{2+\infty i} \frac{y^s}{s^2} ds = \log y.$$

□

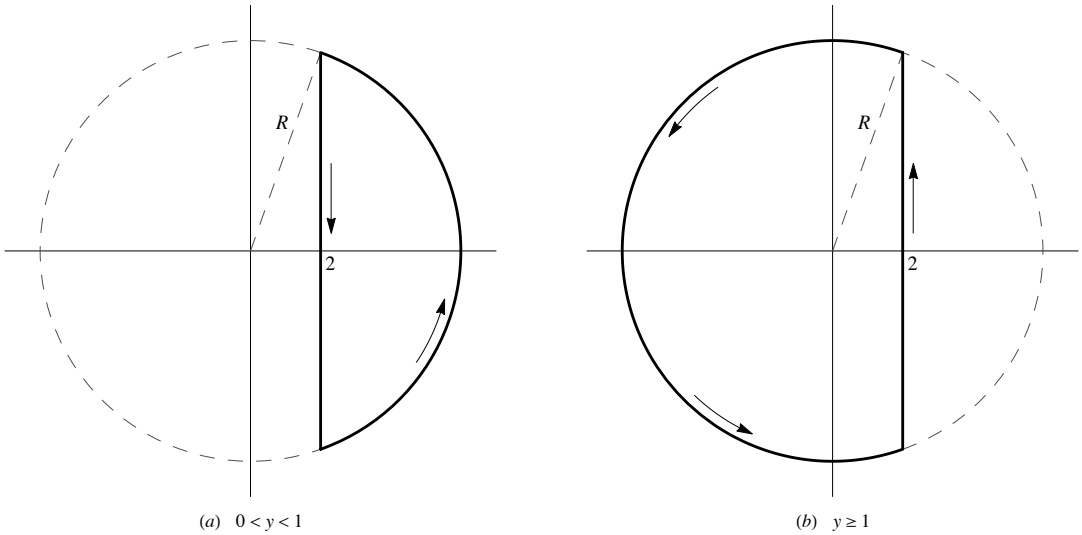


Figure 5: Contours used in Exercise 13.6.

Exercise 13.7. Express

$$\frac{1}{2\pi i}\int_{2-\infty i}^{2+\infty i}\frac{x^s}{s^2}\left(-\frac{\zeta'(s)}{\zeta(s)}\right)ds$$

as a finite sum involving $\Lambda(n)$.

Lemma 13.7. Suppose $f(s)=\sum_{n=1}^{\infty}a_n n^{-s}$ converges absolutely for $\sigma>\sigma_a$. If $c>\max\{0,\sigma_a\}$,

$$\frac{1}{2\pi i}\int_{c-\infty i}^{c+\infty i}f(s)\frac{x^s}{s^2}ds=\sum_{n\le x}a_n\log\left(\frac{x}{n}\right).$$

Proof of Lemma. Applying Exercise 13.6, for $c>\max\{0,\sigma_a\}$,

$$\begin{aligned}\frac{1}{2\pi i}\int_{c-\infty i}^{c+\infty i}f(s)\frac{x^s}{s^2}ds&=\sum_{n=1}^{\infty}\frac{a_n}{2\pi i}\int_{c-\infty i}^{c+\infty i}\frac{(x/n)^s}{s^2}ds\\&=\sum_{n\le x}a_n\log\left(\frac{x}{n}\right).\end{aligned}$$

□

Proof of Exercise. Let

$$f(s)=-\frac{\zeta'(s)}{\zeta(s)}=\sum_{n=1}^{\infty}\frac{\Lambda(n)}{n^s}.$$

By Lemma 13.7,

$$\frac{1}{2\pi i}\int_{2-\infty i}^{2+\infty i}\frac{x^s}{s^2}\left(-\frac{\zeta'(s)}{\zeta(s)}\right)ds=\sum_{n\le x}\Lambda(n)\log\left(\frac{x}{n}\right).$$

□

Exercise 13.8. Let χ be any Dirichlet character mod k with χ_1 the principal character. Define

$$F(\sigma,t) = 3\frac{L'}{L}(\sigma,\chi_1) + 4\frac{L'}{L}(\sigma+it,\chi) + \frac{L'}{L}(\sigma+2it,\chi^2).$$

If $\sigma > 1$ prove that $F(\sigma,t)$ has real part equal to

$$-\sum_{n=1}^{\infty}\frac{\Lambda(n)}{n^\sigma}\mathrm{Re}\left\{3\chi_1(n) + 4\chi(n)n^{-it} + \chi^2(n)n^{-2it}\right\}$$

and deduce that $\mathrm{Re}\, F(\sigma,t) \le 0$.

Proof. Let $\sigma > 1$. By Theorem 11.14, $L(s,\chi) = e^{G(s)}$ where

$$G(s) = \sum_{n=2}^{\infty}\frac{\Lambda(n)\chi(n)}{\log n}n^{-s}.$$

Differentiating gives

$$L'(s,\chi) = G'(s)e^{G(s)} = G'(s)L(s,\chi),$$

therefore

$$\begin{aligned} F(\sigma,t) &= -3\sum_{n=1}^{\infty}\frac{\Lambda(n)\chi_1(n)}{n^\sigma} - 4\sum_{n=1}^{\infty}\frac{\Lambda(n)\chi(n)}{n^{\sigma+it}} - \sum_{n=1}^{\infty}\frac{\Lambda(n)\chi^2(n)}{n^{\sigma+2it}} \\ &= -\sum_{n=1}^{\infty}\frac{\Lambda(n)}{n^\sigma}\left\{3\chi_1(n) + 4\chi(n)n^{-it} + \chi^2(n)n^{-2it}\right\}. \end{aligned}$$

Taking the real part shows

$$\mathrm{Re}\, F(\sigma,t) = -\sum_{n=1}^{\infty}\frac{\Lambda(n)}{n^\sigma}\mathrm{Re}\left\{3\chi_1(n) + 4\chi(n)n^{-it} + \chi^2(n)n^{-2it}\right\}.$$

Letting $\chi(n) = e^{i\theta}$ gives

$$\mathrm{Re}\left\{4\chi(n)n^{-it}\right\} = 4\cos(\theta)\cos(t\log n) + 4\sin(\theta)\sin(t\log n) = 4\cos(\theta - t\log n)$$

and similarly

$$\mathrm{Re}\left\{\chi^2(n)n^{-2it}\right\} = \cos(2(\theta - t\log n)).$$

Thus if $(n,k) = 1$, then

$$\begin{aligned} \mathrm{Re}\left\{3\chi_1(n) + 4\chi(n)n^{-it} + \chi^2(n)n^{-2it}\right\} &= 3 + 4\cos(\theta - t\log n) + \cos(2(\theta - t\log n)) \\ &= 2(1+\cos(\theta - t\log n))^2 \ge 0. \end{aligned}$$

If $(n,k) \ne 1$ then

$$3\chi_1(n) + 4\chi(n)n^{-it} + \chi^2(n)n^{-2it} = 0,$$

so it follows that $\mathrm{Re}\, F(\sigma,t) \le 0$. □

Exercise 13.9. Assume that $L(s,\chi)$ has a zero of order $m \geq 1$ at $s = 1+it$. Prove that for this t we have:

(a) $\dfrac{L'}{L}(\sigma+it,\chi) = \dfrac{m}{\sigma-1} + O(1) \quad \text{as } \sigma \to 1^+, \text{ and}$

(b) there exists an integer $r \geq 0$ such that

$$\frac{L'}{L}(\sigma+2it,\chi^2) = \frac{r}{\sigma-1} + O(1) \quad \text{as } \sigma \to 1^+,$$

except when $\chi^2 = \chi_1$ and $t = 0$.

Proof.
(a) We have $L(\sigma+it,\chi) = (\sigma-1)^m R(\sigma+it)$, where $R(\sigma+it) \neq 0$ in a small neighborhood about $1+it$. Logarithmically differentiating shows

$$\frac{L'(\sigma+it,\chi)}{L(\sigma+it,\chi)} = \frac{m}{\sigma-1} + \frac{R'(\sigma+it)}{R(\sigma+it)}.$$

Since $R(\sigma+it) \neq 0$ for σ near 1, $R'(\sigma+it)/R(\sigma+it)$ must be bounded as $\sigma \to 1^+$.
(b) Suppose $\chi^2 \neq \chi_1$ or $t \neq 0$, i.e. $L(s,\chi^2)$ is analytic at $s = 1+2it$. Define $r \geq 0$ to be the order of the zero of $L(s,\chi^2)$ at $s = 1+it$. (Note if there is no zero, then $r = 0$.) Mimicking (a) shows

$$\frac{L'(\sigma+2it,\chi^2)}{L(\sigma+2it,\chi^2)} = \frac{r}{\sigma-1} + O(1) \quad \text{as } \sigma \to 1^+.$$

□

Exercise 13.10. Use Exercises 8 and 9 to prove that

$$L(1+it,\chi) \neq 0 \quad \text{for all real } t \text{ if } \chi^2 \neq \chi_1$$

and that

$$L(1+it,\chi) \neq 0 \quad \text{for all real } t \neq 0 \text{ if } \chi^2 = \chi_1.$$

[*Hint*: Consider $F(\sigma,t)$ as $\sigma \to 1^+$.]

Proof. Recall for $\sigma > 1$,

$$L(\sigma,\chi_1) = \zeta(\sigma)\prod_{p|k}(1-p^{-\sigma}) = c_k(\sigma)\zeta(\sigma).$$

Thus $L(\sigma,\chi_1)$ has a simple pole at $\sigma = 1$ with residue $c_k(1)$, and long division shows

$$3\frac{L'(\sigma,\chi_1)}{L(\sigma+\chi_1)} = \frac{3}{\sigma-1} + O(1) \quad \text{as } \sigma \to 1^+.$$

Suppose $L(1+it,\chi) = 0$. If $\chi^2 \neq \chi_1$ or $t \neq 0$, then by Exercise 13.9,

$$F(\sigma,t) = \frac{3+4m+r}{\sigma-1} \quad \text{as } \sigma \to 1^+.$$

Hence since $3+4m+r > 0$, $F(\sigma,t) \to \infty$ as $\sigma \to 1^+$. This contradicts Exercise 13.8, which says Re $F(\sigma,t) \leq 0$. This means $L(1+it,\chi) \neq 0$. □

Exercise 13.11. For any arithmetical function $f(n)$, prove that the following statements are equivalent:
(a) $f(n) = O(n^\varepsilon)$ for every $\varepsilon > 0$ and all $n \geq n_1$.
(b) $f(n) = o\big(n^\delta\big)$ for every $\delta > 0$ as $n \to \infty$.

Proof. If $f(n) = O(n^\varepsilon)$ for every $\varepsilon > 0$ and all $n \geq n_1$, then for all $\delta > \varepsilon$

$$f(n) = O(n^\varepsilon) = o\big(n^{\varepsilon+\delta}\big)\,.$$

This shows (a) implies (b), since $\varepsilon + \delta$ can be as close to 0 as we like.

If $f(n) = o\big(n^\delta\big)$ for every $\delta > 0$, then in particular $f(n) = o(n)$. Hence there is exists n_1 such that for all $n \geq n_1$, $|f(n)| \leq n$. This means for any $\varepsilon \geq 1$,

$$f(n) = O(n^\varepsilon) \quad \text{for } n \geq n_1.$$

Now for $0 < \varepsilon < 1$ there exists n_ε such that for all $n \geq n_\varepsilon$, $|f(n)| \leq n^\varepsilon$. Let

$$m_\varepsilon = \max_{n_1 \leq n \leq n_\varepsilon} \left| \frac{f(n)}{n^\varepsilon} \right| \quad \text{and} \quad M_\varepsilon = \max\{m_\varepsilon, 1\}.$$

Then for all $n \geq n_1$ we have $|f(n)| \leq M_\varepsilon n^\varepsilon$, i.e. $f(n) = O(n^\varepsilon)$ and all $n \geq n_1$. □

Exercise 13.12. Let $f(n)$ be a multiplicative function such that if p is prime then

$$f(p^m) \to 0 \quad \text{as } p^m \to \infty.$$

That is, for every $\varepsilon > 0$ there is an $N(\varepsilon)$ such that $|f(p^m)| < \varepsilon$ whenever $p^m > N(\varepsilon)$. Prove that $f(n) \to 0$ as $n \to \infty$.
[*Hint*: There is a constant $A > 0$ such that $|f(p^m)| < A$ for all primes p and all $m \geq 0$, and a constant $B > 0$ such that $|f(p^m)| < 1$ whenever $p^m > B$.]

Proof. Following the hint let M be the number of prime powers $\leq B$, which means A^M is a fixed constant. Letting $n = p_1^{\alpha_s} \cdots p_s^{\alpha_s} \cdot q_1^{\beta_1} \cdots q_t^{\beta_t}$ where $p_i^{\alpha_i} \leq B$ and $q_j^{\beta_j} > B$, then

$$|f(n)| \leq A^M \prod_{i=1}^{t} |f(q_i^{\beta_i})|.$$

Now n can approach ∞ in two ways.

- If $\beta_i \to \infty$ as $n \to \infty$ for some i, then $f(q_i^{\beta_i}) \to 0$ which means $f(n) \to 0$ too.
- If $n \to \infty$ but $\beta_i \not\to \infty$ for all i, it must be that $t \to \infty$. Assuming $q_1^{\beta_1} < q_2^{\beta_2} < \cdots < q_t^{\beta_t}$, then $q_t \to \infty$ as $t \to \infty$. Thus for any $\varepsilon > 0$ there is a t large enough such that $|f(q_t^{\beta_t})| < \varepsilon$. Hence

  $$|f(n)| \leq A^M \prod_{i=1}^{t} |f(q_i^{\beta_i})| < A^M \varepsilon,$$

  or in other words $f(n) \to 0$ as $n \to \infty$. □

Exercise 13.13. If $\alpha \geq 0$ let $\sigma_\alpha(n) = \sum_{d|n} d^\alpha$. Prove that for every $\delta > 0$ we have

$$\sigma_\alpha(n) = o\big(n^{\alpha+\delta}\big) \quad \text{as } n \to \infty.$$

[*Hint*: Use Exercise 13.12.]

Proof. Fix $\delta > 0$ and define $f(n) = \sigma_\alpha(n)/n^{\alpha+\delta}$. Observe $f(n)$ is multiplicative and

$$f(p^m) = \frac{1}{p^{m\alpha+m\delta}} \frac{p^{(m+1)\alpha} - 1}{p^\alpha - 1} = \frac{1}{(p^m)^\delta} \left\{ \frac{p^\alpha - p^{-m\alpha}}{p^\alpha - 1} \right\},$$

hence $f(p^m) \to 0$ as $p^m \to \infty$. So applying Exercise 13.12 it's clear $f(n) = o(1)$, i.e. $\sigma_\alpha(n) = o\big(n^{\alpha+\delta}\big)$. □

Chapter 14
Partitions

Exercise 14.1. Let A denote a nonempty set of positive integers.
(a) Prove that the product

$$\prod_{m\in A}(1-x^m)^{-1}$$

is the generationg function of the number of partitions of n into parts belonging to the set A.
(b) Describe the partition function generated by the product

$$\prod_{m\in A}(1+x^m)\,.$$

In particular, describe the partition function generated by the finite product $\prod_{m=1}^{k}(1+x^m)$.

Proof.
(a) We will mirror the rigorous argument made in the proof of Theorem 14.2. Write

$$A=\{k_1,k_2,k_3,\ldots\},$$

where A is possibly finite and $k_1<k_2<k_3<\cdots$. Restricting x to lie in the interval $0\le x<1$, define

$$F_m(x)=\prod_{i=1}^{m}\frac{1}{1-x^{k_i}},\quad \text{and } F(x)=\prod_{k\in A}\frac{1}{1-x^k}=\lim_{m\to\infty}F_m(x).$$

Note if $|A|<\infty$, we take $F(x)=F_{|A|}(x)$. As justified in the proof of Theorem 14.2, we can write $F_m(x)$ as

$$F_m(x)=1+\sum_{k=1}^{\infty}p_m(k)x^k,$$

where $p_m(k)$ is the number of solutions to

$$k=k_1n_1+k_2n_2+\cdots k_mn_m.$$

Notice $p_m(k)$ is the number of partitions of k into parts that are in A and do not exceed m. If $|A|$ is finite, take $m=|A|$ and we are done. Otherwise let $p_A(k)$ be the number of partitions of k into parts that are in A. Therefore we always have

$$p_m(k)\le p_A(k)$$

with equality when $m \geq k$ and

$$\lim_{m\to\infty} p_m(k) = p_A(k).$$

By the comparison test with $\sum p_m(k)x^k$ and the similar series in the proof of Theorem 14.2, we see $\sum p_m(k)x^k$ converges uniformly in m. Thus

$$F(x) = \lim_{m\to\infty} F_m(x) = \lim_{m\to\infty} \sum_{k=0}^{\infty} p_m(k)x^k = \sum_{k=0}^{\infty} \lim_{m\to\infty} p_m(k)x^k = \sum_{k=0}^{\infty} p_A(k)x^k,$$

which proves the identity for $0 \leq x < 1$. By analytic continuation this can be extended to hold for all $|x| < 1$.

(b) Analogous to the fifth entry of Table 14.1, the partition function generated by

$$\prod_{m\in A} (1 + x^m)$$

counts the number of partitions of n into parts which are unequal and belong to the set A. Therefore the partition function generated by

$$\prod_{m=1}^{k} (1 + x^m)$$

counts the number of partitions of n into parts which are unequal and $\leq k$. □

Exercise 14.2. If $|x| < 1$ prove that

$$\prod_{m=1}^{\infty} (1 + x^m) = \prod_{m=1}^{\infty} \left(1 - x^{2m-1}\right)^{-1},$$

and deduce that the number of partitions of n into unequal parts is equal to the number of partitions of n into odd parts.

Proof. Let $|x| < 1$ and $N > 0$. Then

$$\begin{aligned}
\prod_{m=1}^{2^{2N}} (1 + x^m)\left(1 - x^{2m-1}\right) &= \prod_{m=1}^{2^{2N-1}} \left(1 + x^{2m}\right) \prod_{m=1}^{2^{2N}} \left(1 + x^{2m-1}\right)\left(1 - x^{2m-1}\right) \\
&= \prod_{m=1}^{2^{2N-1}} \left(1 + x^{2m}\right) \prod_{m=1}^{2^{2N}} \left(1 - x^{4m-2}\right) \\
&= \prod_{m=1}^{2^{2N-2}} \left(1 + x^{4m}\right) \prod_{m=1}^{2^{2N-1}} \left(1 - x^{8m-4}\right) \\
&\vdots \\
&= \prod_{m=1}^{2^N} \left(1 + x^{2^N m}\right) \prod_{m=1}^{2^{N+1}} \left(1 - x^{2^{N+1}m - 2^N}\right).
\end{aligned}$$

Now for $-1 < x < 1$,

$$1 \le \prod_{m=1}^{2^N} \left(1 + x^{2^N m}\right) \le \left(1 + x^{2^N}\right)^{2^N} \to 1 \quad \text{as } N \to \infty.$$

Thus

$$\lim_{N\to\infty} \prod_{m=1}^{2^N} \left(1 + x^{2^N m}\right) = 1$$

and similarly

$$\lim_{N\to\infty} \prod_{m=1}^{2^{N+1}} \left(1 - x^{2^{N+1} m - 2^N}\right) = 1.$$

This shows for $-1 < x < 1$,

$$\prod_{m=1}^{\infty} (1 + x^m) = \prod_{m=1}^{\infty} \left(1 - x^{2m-1}\right)^{-1}$$

and by analytic continuation this for all complex $|x| < 1$.

From Table 14.1, the number of partitions of n into odd parts has generating function

$$\prod_{m=1}^{\infty} \left(1 - x^{2m-1}\right)^{-1}$$

and the number of partitions of n into unequal parts has generating function

$$\prod_{m=1}^{\infty} (1 + x^m).$$

Since both generating functions are the same, we conclude that the number of partitions of n into unequal parts is equal to the number of partitions of n into odd parts. □

Exercise 14.3. For complex x and z with $|x| < 1$, let

$$f(x, z) = \prod_{m=1}^{\infty} (1 - x^m z).$$

(a) Prove that for each fixed z the product is an analytic function of x in the disk $|x| < 1$, and that for each fixed x with $|x| < 1$ the product is an entire function of z.
(b) Define the numbers $a_n(x)$ by the equation

$$f(x, z) = \sum_{n=0}^{\infty} a_n(x) z^n.$$

Show that $f(x, z) = (1 - xz) f(x, zx)$ and use this to prove that the coefficients satisfy the recursion formula

$$a_n(x) = a_n(x) x^n - a_{n-1}(x) x^n.$$

(c) From (b) deduce that $a_n(x) = (-1)^n x^{n(n+1)/2}/P_n(x)$, where

$$P_n(x) = \prod_{r=1}^{n} (1 - x^r).$$

This proves the following identity for $|x| < 1$ and arbitrary z:

$$\prod_{m=1}^{\infty} (1 - x^m z) = \sum_{n=0}^{\infty} \frac{(-1)^n}{P_n(x)} x^{n(n+1)/2} z^n.$$

Lemma 14.3. If $\sum_{n=1}^{\infty} |f_n(x)|$ converges uniformly to a bounded function on a set S, then so does $\prod_{n=1}^{\infty}(1 + f_n(x))$.

Proof of Lemma. Let $P_N(x) = \prod_{n=1}^{N}(1 + f_n(x))$. Choosing M such that

$$\sum_{n=1}^{\infty} |f_n(x)| \le M \quad \text{for all } x \in S,$$

then

$$|P_N(x)| \le \prod_{n=1}^{N}(1 + |f_n(x)|) \le \exp\left\{\sum_{n=1}^{N} |f_n(x)|\right\} \le e^M.$$

Hence for $N \ge M$,

$$\begin{aligned} |P_N(x) - P_M(x)| &= \left| \sum_{n=M+1}^{N} (P_n(x) - P_{n-1}(x)) \right| \\ &\le \sum_{n=M+1}^{N} |P_n(x) - P_{n-1}(x)| \\ &= \sum_{n=M+1}^{N} |P_{n-1}(x)||f_n(x)| \\ &\le e^M \sum_{n=M+1}^{N} |f_n(x)|. \end{aligned}$$

Since $\sum_{n=1}^{\infty} |f_n(x)|$ converges uniformly on S, by the Cauchy criterion, $P_N(x)$ converges uniformly on S. □

Proof of Exercise.
(a) For any $|x| < 1$ and $z \in \mathbb{C}$,

$$\sum_{m=1}^{\infty} x^m z = \frac{xz}{1 - x}$$

converges uniformly as a function of either x or z. The result then follows from Lemma 14.3, since a uniformly convergent sequence of analytic functions converges to an analytic function.

(b) Since $f(x,z)$ is entire in z it has a power series about $z=0$, namely

$$f(x,z)=\sum_{n=0}^{\infty}a_n(x)z^n.$$

Now

$$\begin{aligned}(1-xz)f(x,zx)&=(1-xz)\prod_{m=1}^{\infty}(1-x^mzx)\\&=\prod_{m=0}^{\infty}\left(1-x^{m+1}z\right)\\&=\prod_{m=1}^{\infty}(1-x^mz)=f(x,z),\end{aligned}$$

and therefore

$$\begin{aligned}\sum_{n=0}^{\infty}a_n(x)z^n&=(1-zx)\sum_{n=0}^{\infty}a_n(x)(zx)^n\\&=\sum_{n=0}^{\infty}a_n(x)x^nz^n-\sum_{n=0}^{\infty}a_n(x)x^{n+1}z^{n+1}\\&=\sum_{n=0}^{\infty}a_n(x)x^nz^n-\sum_{n=1}^{\infty}a_{n-1}(x)x^nz^n\\&=a_0(x)+\sum_{n=1}^{\infty}\left(a_n(x)x^n-a_{n-1}(x)x^n\right)z^n.\end{aligned}$$

Equating coefficients for $n>0$ shows $a_n(x)=a_n(x)x^n-a_{n-1}(x)x^n$.
(c) From (b) we have

$$a_n(x)=-\frac{x^n}{1-x^n}a_{n-1}(x),$$

and unraveling the recursive relationship shows

$$a_n(x)=(-1)^n\frac{x^{1+2+\cdots+n}}{(1-x)(1-x^2)\cdots(1-x^n)}a_0(x)=\frac{(-1)^n}{P_n(x)}x^{n(n+1)/2}.$$

Hence

$$\prod_{m=1}^{\infty}(1-x^mz)=\sum_{n=0}^{\infty}\frac{(-1)^n}{P_n(x)}x^{n(n+1)/2}z^n.$$

□

Exercise 14.4. Use a method analogous to that of Exercise 14.3 to prove that if $|x|<1$ and $|z|<1$ we have

$$\prod_{m=1}^{\infty}(1-x^mz)^{-1}=\sum_{n=0}^{\infty}\frac{z^n}{P_n(x)}$$

where $P_n(x)=\prod_{r=1}^{n}(1-x^r)$.

Remark. This problem has a typo. To fix it, we can either start the product at $m = 0$ or replace the series coefficient with $x^n/P_n(x)$. The latter is proven below.

Proof. Applying Exercise 14.3 (a) shows $\prod_{m=1}^{\infty}(1 - x^m z)$ analytic for $|x| < 1$ and $z \in \mathbb{C}$. Furthermore, for $|x| < 1$ and $|z| < 1$ observe this product in nonzero. Hence

$$g(x, z) = \prod_{m=1}^{\infty}(1 - x^m z)^{-1}$$

is analytic for all $|x| < 1$ and $|z| < 1$.

Since $g(x, z)$ is analytic for $|z| < 1$ it has a power series about $z = 0$, namely

$$g(x, z) = \sum_{n=0}^{\infty} b_n(x) z^n.$$

Now

$$\begin{aligned}
\frac{g(x, zx)}{1 - xz} &= \frac{1}{1 - xz} \prod_{m=1}^{\infty}(1 - x^m zx)^{-1} \\
&= \prod_{m=0}^{\infty}\left(1 - x^{m+1} z\right)^{-1} \\
&= \prod_{m=1}^{\infty}(1 - x^m z)^{-1} = g(x, z),
\end{aligned}$$

and therefore

$$\begin{aligned}
\sum_{n=0}^{\infty} b_n(x)(zx)^n &= (1 - xz) \sum_{n=0}^{\infty} b_n(x) z^n \\
&= \sum_{n=0}^{\infty} b_n(x) z^n - x \sum_{n=1}^{\infty} b_{n-1}(x) z^n \\
&= b_0(x) + \sum_{n=1}^{\infty} \left(b_n(x) - b_{n-1}(x) x\right) z^n.
\end{aligned}$$

Equating coefficients for $n > 0$ shows

$$b_n(x) = \frac{b_{n-1}(x) x}{1 - x^n},$$

and unraveling the recursive relationship shows

$$b_n(x) = \frac{x^n}{P_n(x)}.$$

□

Exercise 14.5.(++) If $x \neq 1$ let $Q_0(x) = 1$ and for $n \geq 1$ define

$$Q_n(x) = \prod_{r=1}^{n} \frac{1 - x^{2r}}{1 - x^{2r-1}}.$$

(a) Derive the following finite identities of Shanks:

$$\sum_{m=1}^{2n} x^{m(m-1)/2} = \sum_{s=0}^{n-1} \frac{Q_n(x)}{Q_s(x)} x^{s(2n+1)}, \tag{27}$$

$$\sum_{m=1}^{2n+1} x^{m(m-1)/2} = \sum_{s=0}^{n} \frac{Q_n(x)}{Q_s(x)} x^{s(2n+1)}. \tag{28}$$

(b) Use Shanks' identities to deduce Gauss' triangular-number theorem:

$$\sum_{m=1}^{\infty} x^{m(m-1)/2} = \prod_{n=1}^{\infty} \frac{1 - x^{2n}}{1 - x^{2n-1}} \quad \text{for } |x| < 1.$$

Proof.
(a) Notice

$$Q_{n+1}(x) = \frac{1 - x^{2n+2}}{1 - x^{2n+1}} Q_n(x).$$

Using this observation and long division shows for $n > 0$,

$$\begin{aligned}
\frac{Q_n(x)}{Q_s(x)} x^{s(2n+1)} &= \frac{Q_{n-1}(x)}{Q_s(x)} \frac{1 - x^{2n+2}}{1 - x^{2n+1}} x^{s(2n+1)} \\
&= \frac{Q_{n-1}(x)}{Q_s(x)} \left\{ x^{s(2n-1)} + \frac{1 - x^{2s+1}}{1 - x^{2n-1}} x^{(s+1)(2n-1)} - \frac{1 - x^{2s}}{1 - x^{2n-1}} x^{s(2n-1)} \right\} \\
&= \frac{Q_{n-1}(x)}{Q_s(x)} x^{s(2n-1)} + f(s,n) - g(s,n),
\end{aligned} \tag{29}$$

where

$$f(s,n) = \frac{Q_{n-1}(x)}{Q_s(x)} \frac{1 - x^{2s+1}}{1 - x^{2n-1}} x^{(s+1)(2n-1)} \quad \text{and} \quad g(s,n) = \frac{Q_{n-1}(x)}{Q_s(x)} \frac{1 - x^{2s}}{1 - x^{2n-1}} x^{s(2n-1)}.$$

Now

$$\begin{aligned}
g(s+1,n) &= \frac{Q_{n-1}(x)}{Q_{s+1}(x)} \frac{1 - x^{2s+2}}{1 - x^{2n-1}} x^{(s+1)(2n-1)} \\
&= \frac{Q_{n-1}(x)}{Q_s(x) \frac{1-x^{2s+2}}{1-x^{2s+1}}} \frac{1 - x^{2s+2}}{1 - x^{2n-1}} x^{(s+1)(2n-1)} \\
&= f(s,n).
\end{aligned}$$

Thus when summing over (29), f and g telescope. Since $g(0,n)=0$ and $f(n-1,n)=x^{n(2n-1)}$ we have

$$\begin{aligned}\sum_{s=0}^{n-1}\frac{Q_n(x)}{Q_s(x)}x^{s(2n+1)} &= \sum_{s=0}^{n-1}\frac{Q_{n-1}(x)}{Q_s(x)}x^{s(2n-1)}+x^{n(2n-1)},\\ &= \sum_{s=0}^{n-2}\frac{Q_{n-1}(x)}{Q_s(x)}x^{s(2(n-1)+1)}+x^{(n-1)(2n-1)}+x^{n(2n-1)},\end{aligned}$$

so (27) follows through a simple induction argument. Adding $x^{n(2n+1)}$ to both sides of (27) proves (28).
(b) Let $|x|<1$ and define $Q(x)=\lim_{n\to\infty}Q_n(x)$, which exists and equals the quotient of two generating functions found in Table 14.1. From above we have

$$\begin{aligned}\sum_{m=1}^{\infty}x^{m(m-1)/2} &= \lim_{n\to\infty}\sum_{s=0}^{n}\frac{Q_n(x)}{Q_s(x)}x^{s(2n+1)}\\ &= \lim_{n\to\infty}Q_n(x)+\lim_{n\to\infty}\sum_{s=1}^{n}\frac{Q_n(x)}{Q_s(x)}x^{s(2n+1)}\\ &= Q(x)+\lim_{n\to\infty}T_n(x).\end{aligned}$$

Noting $Q_n(x)/Q_s(x)\le Q_n(x)\le Q(x)$ for all n and $s\le n$, we have

$$|T_n(x)|\le n|Q(x)||x|^{2n+1}.$$

Hence for a fixed x, $T_n(x)$ tends to 0 as $n\to\infty$, which shows

$$\sum_{m=1}^{\infty}x^{m(m-1)/2}=Q(x)=\prod_{n=1}^{\infty}\frac{1-x^{2n}}{1-x^{2n-1}}.$$

□

Exercise 14.6. The following identity is valid for $|x|<1$:

$$\sum_{m=-\infty}^{\infty}x^{m(m-1)/2}=\prod_{n=1}^{\infty}\left(1+x^{n-1}\right)\left(1-x^{2n}\right).$$

(a) Derive this from the identities in Exercises 14.2 and 14.5 (b).
(b) Derive this from Jacobi's triple product identity.

Proof.
(a) The substitution $n=1-m$ shows

$$\begin{aligned}\sum_{m=-\infty}^{\infty}x^{m(m-1)/2} &= \sum_{m=-\infty}^{0}x^{m(m-1)/2}+\sum_{m=1}^{\infty}x^{m(m-1)/2}\\ &= 2\sum_{m=1}^{\infty}x^{m(m-1)/2}.\end{aligned}$$

Applying Exercises 14.2 and 14.5 (b) gives

$$\begin{aligned}
2\sum_{m=1}^{\infty} x^{m(m-1)/2} &= 2\prod_{n=1}^{\infty} \frac{1-x^{2n}}{1-x^{2n-1}} \\
&= 2\prod_{n=1}^{\infty} \left(1+x^n\right)\left(1-x^{2n}\right) \\
&= 2\prod_{n=1}^{\infty} \frac{1+x^n}{1+x^{n-1}} \prod_{n=1}^{\infty} \left(1+x^{n-1}\right)\left(1-x^{2n}\right) \\
&= \prod_{n=1}^{\infty} \left(1+x^{n-1}\right)\left(1-x^{2n}\right).
\end{aligned}$$

(b) If we replace x by $x^{1/2}$ and z^2 by $x^{-1/2}$ in Jacobi's identity we find

$$\prod_{n=1}^{\infty} \left(1+x^{n-1}\right)\left(1-x^{2n}\right) = \sum_{m=-\infty}^{\infty} x^{m(m-1)/2}.$$

□

Exercise 14.7. Prove that the following identities, valid for $|x| < 1$, are consequences of Jacobi's triple product identity:

(a) $\displaystyle\prod_{n=1}^{\infty} \left(1-x^{5n}\right)\left(1-x^{5n-1}\right)\left(1-x^{5n-4}\right) = \sum_{m=-\infty}^{\infty} (-1)^m x^{m(5m+3)/2}.$

(b) $\displaystyle\prod_{n=1}^{\infty} \left(1-x^{5n}\right)\left(1-x^{5n-2}\right)\left(1-x^{5n-3}\right) = \sum_{m=-\infty}^{\infty} (-1)^m x^{m(5m+1)/2}.$

Proof. If we replace x by $x^{5/2}$ and z^2 by $-x^{3/2}$ in Jacobi's identity we find

$$\prod_{n=1}^{\infty} \left(1-x^{5n}\right)\left(1-x^{5n-1}\right)\left(1-x^{5n-4}\right) = \sum_{m=-\infty}^{\infty} (-1)^m x^{m(5m+3)/2}.$$

Similarly, if $z^2 = -x^{1/2}$ we find

$$\prod_{n=1}^{\infty} \left(1-x^{5n}\right)\left(1-x^{5n-2}\right)\left(1-x^{5n-3}\right) = \sum_{m=-\infty}^{\infty} (-1)^m x^{m(5m+1)/2}.$$

□

Exercise 14.8. Prove that the recursion formula

$$np(n) = \sum_{k=1}^{n} \sigma(k)p(n-k),$$

obtained in Section 14.10, can be put in the form

$$np(n) = \sum_{m=1}^{n} \sum_{k \le n/m} mp(n - km).$$

Proof. This identity follows through changing the order of summation described in the proof of Theorem 3.3:

$$\begin{aligned} \sum_{k=1}^{n} \sigma(k)p(n-k) &= \sum_{k=1}^{n} \sum_{d|k} d\, p(n-k) \\ &= \sum_{\substack{q,d \\ qd \le n}} d\, p(n-qd) \\ &= \sum_{m \le n} \sum_{q \le n/d} d\, p(n-qd). \end{aligned}$$

□

Exercise 14.9. Suppose that each positive integer k is written in $g(k)$ different colors, where $g(k)$ is a positive integer. Let $p_g(n)$ denote the number of partitions of n in which each part k appears in at most $g(k)$ different colors. When $g(k) = 1$ for all k this is the unrestricted partition function $p(n)$. Find the infinite product which generates $p_g(n)$ and prove that there is an arithmetical function f (depending on g) such that

$$np_g(n) = \sum_{k=1}^{n} f(k)p_g(n-k).$$

Proof. This follows directly from Theorem 14.8. We have for $|x| < 1$,

$$\prod_{n=1}^{\infty} (1 - x^n)^{-g(n)/n} = 1 + \sum_{n=1}^{\infty} p_g(n)x^n$$

and $p_g(n)$ satisfies the recurrence relation

$$np_g(n) = \sum_{k=1}^{n} f(k)p_g(n-k), \quad \text{where } f(k) = \sum_{d|k} g(d).$$

□

Exercise 14.10. Refer to Section 14.10 for notation. By solving the first-order differential equation in (22) prove that if $|x| < 1$ we have

$$\prod_{n \in A} (1 - x^n)^{-f(n)/n} = \exp\left\{ \int_0^x \frac{H(t)}{t} dt \right\},$$

where

$$H(x) = \sum_{k=1}^{\infty} f_A(k)x^k \quad \text{and} \quad f_A(k) = \sum_{\substack{d|k \\ d\in A}} f(d).$$

Deduce that

$$\prod_{n=1}^{\infty} (1-x^n)^{\mu(n)/n} = e^{-x} \quad \text{for } |x| < 1,$$

where $\mu(n)$ is the Möbius function.

Proof. The first-order separable differential equation in (22) is

$$\frac{F_A'(t)}{F_A(t)} = \frac{H(t)}{t},$$

and integrating both sides from 0 to x for some $|x| < 1$ gives

$$\log F_A(x) - \log F_A(0) = \int_0^x \frac{H(t)}{t} dt.$$

Moreover, by definition $F_A(0) = 1$ which means

$$F_A(x) = \prod_{n\in A} (1-x^n)^{-f(n)/n} = \exp\left\{ \int_0^x \frac{H(t)}{t} dt \right\}.$$

Now let $A = \mathbb{N}$ and $f(n) = -\mu(n)$. Then $f_A(k) = -I(k)$, and so $H(x) = -x$. This means for $|x| < 1$,

$$\prod_{n=1}^{\infty} (1-x^n)^{\mu(n)/n} = \exp\left\{ -\int_0^x dt \right\} = e^{-x}.$$

□

The following exercises outline a proof of Ramanujan's partition identity

$$\sum_{m=0}^{\infty} p(5m+4)x^m = 5\frac{\varphi(x^5)^5}{\varphi(x)^6}, \quad \text{where } \varphi(x) = \prod_{n=1}^{\infty} (1-x^n),$$

by a method of Kruyswijk not requiring the theory of modular functions.

Exercise 14.11.
(a) Let $\varepsilon = e^{2\pi i/k}$ where $k \geq 1$ and show that for all x we have

$$\prod_{h=1}^{k} \left(1 - x\varepsilon^h\right) = 1 - x^k.$$

(b) More generally, if $(n,k) = d$ prove that

$$\prod_{h=1}^{k} \left(1 - x\varepsilon^{nh}\right) = \left(1 - x^{k/d}\right)^d,$$

and deduce that

$$\prod_{h=1}^{k}\left(1-x^n e^{2\pi i n h/k}\right)=\begin{cases}1-x^{nk} & \text{if } (n,k)=1,\\ (1-x^n)^k & \text{if } k\mid n.\end{cases}$$

Proof.
(a) Factoring yields

$$x^k-1=\prod_{h=1}^{k}\left(x-\varepsilon^h\right),$$

and so

$$\begin{aligned}1-x^k&=(-1)^{k+1}\prod_{h=1}^{k}\left(\varepsilon^h-x\right)=(-1)^{k+1}\prod_{h=1}^{k}\left(\varepsilon^h-x\right)\\&=(-1)^{k+1}\prod_{h=1}^{k}\left(\varepsilon^{-h}-x\right)=(-1)^{k+1}\prod_{h=1}^{k}\varepsilon^{-h}\prod_{h=1}^{k}\left(1-x\varepsilon^h\right)\\&=(-1)^{k+1}\varepsilon^{-k(k+1)/2}\prod_{h=1}^{k}\left(1-x\varepsilon^h\right)=\prod_{h=1}^{k}\left(1-x\varepsilon^h\right).\end{aligned}$$

(b) Let $d=(n,k)$, $m=n/d$, and $\delta=e^{2\pi i d/k}$. Then

$$\begin{aligned}\prod_{h=1}^{k}\left(1-x\varepsilon^{nh}\right)&=\prod_{h=1}^{k}\left(1-x\delta^{mh}\right)\\&=\prod_{h=1}^{k/d}\left(1-x\delta^{mh}\right)^d.\end{aligned}$$

Since $(m,k/d)=1$, mh runs through a complete system of residues mod k, hence by (a),

$$\begin{aligned}\prod_{h=1}^{k/d}\left(1-x\delta^{mh}\right)^d&=\prod_{h=1}^{k/d}\left(1-x\delta^{h}\right)^d\\&=\left(1-x^{k/d}\right)^d.\end{aligned}$$

Now this means if $(n,k)=1$, then

$$\prod_{h=1}^{k}\left(1-x^n e^{2\pi i n h/k}\right)=\left(1-(x^n)^{k/1}\right)^1=1-x^{nk}.$$

Also if $k\mid n$, then $(n,k)=k$, so

$$\prod_{h=1}^{k}\left(1-x^n e^{2\pi i n h/k}\right)=(1-(x^n)^{k/k})^k=(1-x^n)^k.$$

□

Exercise 14.12.
(a) Use Exercise 14.11 (b) to prove that for prime q and $|x| < 1$ we have

$$\prod_{n=1}^{\infty}\prod_{h=1}^{q}\left(1-x^n e^{2\pi i n h/q}\right) = \frac{\varphi(x^q)^{q+1}}{\varphi(x^{q^2})}.$$

(b) Deduce the identity

$$\sum_{m=0}^{\infty} p(m)x^m = \frac{\varphi(x^{25})}{\varphi(x^5)^6}\prod_{h=1}^{4}\prod_{n=1}^{\infty}\left(1-x^n e^{2\pi i n h/5}\right).$$

Proof.
(a) Using Exercise 14.11 (b),

$$\begin{aligned}\prod_{n=1}^{\infty}\prod_{h=1}^{q}\left(1-x^n e^{2\pi i n h/q}\right) &= \prod_{n=1}^{\infty}(1-x^{qn})^q \prod_{r=1}^{q-1}\prod_{m=1}^{\infty}\left(1-x^{q(mq-r)}\right)\\ &= \varphi(x^q)^q \prod_{r=0}^{q-1}\prod_{m=1}^{\infty}\left(1-x^{q(mq-r)}\right)\prod_{m=1}^{\infty}\left(1-x^{q^2 m}\right)^{-1}\\ &= \frac{\varphi(x^q)^{q+1}}{\varphi(x^{q^2})}.\end{aligned}$$

(b) Taking $q = 5$ gives

$$\prod_{n=1}^{\infty}\prod_{h=1}^{5}\left(1-x^n e^{2\pi i n h/5}\right) = \frac{\varphi(x^5)^6}{\varphi(x^{25})},$$

and isolating the portion of the left hand side corresponding to $h = 5$, then taking reciprocals shows

$$\prod_{n=1}^{\infty}\frac{1}{1-x^n} = \frac{\varphi(x^{25})}{\varphi(x^5)^6}\prod_{h=1}^{4}\prod_{n=1}^{\infty}\left(1-x^n e^{2\pi i n h/5}\right).$$

Now the by Theorem 14.2, the left hand side is the generating function for $p(n)$, which finishes the proof. □

Exercise 14.13. If q is prime and if $0 \le r < q$, a power series of the form

$$\sum_{n=0}^{\infty} a(n)x^{qn+r}$$

is said to be of *type* r mod q.
(a) Use Euler's pentagonal number theorem to show that $\varphi(x)$ is a sum of three power series,

$$\varphi(x) = \prod_{n=1}^{\infty}(1-x^n) = I_0 + I_1 + I_2,$$

where I_k denotes a power series of type k mod 5.
(b) Let $\alpha = e^{2\pi i/5}$ and show that

$$\prod_{h=1}^{4}\prod_{n=1}^{\infty}\left(1-x^n\alpha^{nh}\right) = \prod_{h=1}^{4}\left(I_0 + I_1\alpha^h + I_2\alpha^{2h}\right).$$

(c) Use Exercise 14.12 (b) to show that

$$\sum_{m=0}^{\infty} p(5m+4)x^{5m+4} = V_4\frac{\varphi(x^{25})}{\varphi(x^5)^6},$$

where V_4 is the power series of type 4 mod 5 obtained from the product in (b).

Proof.
(a) By Eulers pentagonal number theorem (Theorem 14.3),

$$\varphi(x) = \sum_{n=-\infty}^{\infty}(-1)^n x^{\omega(n)}, \quad \text{where } \omega(n) = \frac{3n^2-n}{2}.$$

It's easy to verify $\omega(n)$ is only congruent to 0, 1, or 2 mod 5, so taking

$$I_k = \sum_{\omega(n)\equiv k \bmod 5}(-1)^n x^{\omega(n)}$$

proves the claim.
(b) Observe

$$\prod_{h=1}^{4}\prod_{n=1}^{\infty}\left(1-x^n\alpha^{nh}\right) = \prod_{h=1}^{4}\varphi\left(x\alpha^h\right)$$

and

$$\varphi\left(x\alpha^h\right) = I_0' + I_1' + I_2',$$

where I_k' is equal to I_k with x replaced with $x\alpha^h$. Now $\alpha^{(5m+k)h} = \alpha^{kh}$, so we can factor terms with α out of I_k' to get

$$\varphi\left(x\alpha^h\right) = I_0 + I_1\alpha^h + I_2\alpha^{2h}.$$

(c) Note if S_k denotes a series of type k, then $S_k \cdot S_m$ is of type $k+m$, hence $\varphi(x^{25})/\varphi(x^5)^6$ is of type 0 mod 5. Thus equating terms of type 4 in Exercise 14.12 (b),

$$\sum_{m=0}^{\infty} p(5m+4)x^{5m+4} = V_4\frac{\varphi(x^{25})}{\varphi(x^5)^6},$$

where V_4 is the type 4 part in the expansion of $\prod_{h=1}^{4}(I_0 + I_1\alpha^h + I_2\alpha^{2h})$. □

Exercise 14.14.
(a) Use Theorem 14.7 to show that the cube of Euler's product is the sum of three power series,

$$\varphi(x)^3 = W_0 + W_1 + W_3,$$

where W_k denotes a power series of type k mod 5.
(b) Use the identity $W_0 + W_1 + W_3 = (I_0 + I_1 + I_2)^3$ to the that the power series in Exercise 14.13 (a) satisfy the relation

$$I_0 I_2 = -I_1^2.$$

(c) Prove that $I_1 = -x\varphi(x^{25})$.

Proof.
(a) By Theorem 14.7,

$$\varphi(x)^3 = \sum_{m=0}^{\infty} (-1)^m (2m+1) x^{(m^2+m)/2}.$$

It's easy to verify $(m^2+m)/2$ is only congruent to 0, 1, or 3 mod 5, so taking

$$W_k = \sum_{(m^2+m)/2 \equiv k \bmod 5} (-1)^m (2m+1) x^{(m^2+m)/2}$$

proves the claim.
(b) Recall if S_k denotes a series of type k, then $S_k \cdot S_m$ is of type $k+m$. Now expanding $(I_0 + I_1 + I_2)^3$ shows the only terms of type 2 are $I_0 I_2$ and I_1^2. Since $W_0 + W_1 + W_3$ contains no terms of type 2, we conclude

$$I_0 I_2 + I_1^2 = 0.$$

(c) Note $\omega(n) \equiv 1 \bmod 5$ if and only if $n \equiv 1 \bmod 5$. Thus by Eulers pentagonal number theorem (Theorem 14.3),

$$I_1 = -\sum_{n=-\infty}^{\infty} x^{(3(5n+1)^2 - (5n+1))/2} = -x \sum_{n=-\infty}^{\infty} x^{25(3n^2+n)/2}.$$

Substituting $m = -n$ shows

$$I_1 = -x \sum_{m=-\infty}^{\infty} x^{25(3m^2-m)/2} = -x\varphi\left(x^{25}\right).$$

□

Exercise 14.15. Observe that the product $\prod_{h=1}^{4}(I_0 + I_1\alpha^h + I_2\alpha^{2h})$ is a homogeneous polynomial in I_0, I_1, I_2 of degree 4, so the terms contributing to series of type 4 mod 5 come from the terms I_1^4, $I_0 I_1^2 I_2$ and $I_0^2 I_2^2$.
(a) Use Exercise 14.14 (c) to show that there exists a constant c such that

$$V_4 = cI_1^4,$$

where V_4 is the power series in Exercise 14.13 (c), and deduce that

$$\sum_{m=0}^{\infty} p(5m+4)x^{5m+4} = cx^4 \frac{\varphi(x^{25})^5}{\varphi(x^5)^6}.$$

(b) Prove that $c = 5$ and deduce Ramanujan's identity

$$\sum_{m=0}^{\infty} p(5m+4)x^m = 5\frac{\varphi(x^5)^5}{\varphi(x)^6}.$$

Proof.
(a) Using Exercise 14.14 (b), expanding $\prod_{h=1}^{4}(I_0 + I_1\alpha^h + I_2\alpha^{2h})$ shows

$$\begin{aligned} V_4 &= I_1^4 + 3\left(\alpha^4+\alpha^3+\alpha^2+\alpha\right) I_0 I_1^2 I_2 + \left(\alpha^4+\alpha^3+\alpha^2+\alpha+2\right) I_0^2 I_2^2 \\ &= I_1^4 - 3\left(\alpha^4+\alpha^3+\alpha^2+\alpha\right) I_1^4 + \left(\alpha^4+\alpha^3+\alpha^2+\alpha+2\right) I_1^4 \\ &= cI_1^4, \end{aligned}$$

where $c = 3 - 2\alpha - 2\alpha^2 - 2\alpha^3 - 2\alpha^4$. Applying Exercise 14.13 (c) and Exercise 14.14 (c) yields

$$\sum_{m=0}^{\infty} p(5m+4)x^{5m+4} = c\left(-x\varphi\left(x^{25}\right)\right)^4 \frac{\varphi(x^{25})}{\varphi(x^5)^6} = cx^4\frac{\varphi(x^{25})^5}{\varphi(x^5)^6}.$$

(b) Since $\alpha \neq 1$ is a fifth root of unity,

$$c = 5 - 2(\alpha^4+\alpha^3+\alpha^2+\alpha+1) = 5 - 2\frac{\alpha^5-1}{\alpha-1} = 5.$$

Dividing both sides by x^4 then replacing x^5 with x proves Ramanujan's identity

$$\sum_{m=0}^{\infty} p(5m+4)x^m = 5\frac{\varphi(x^5)^5}{\varphi(x)^6}.$$

□

Back to top.