

# Notes on the book: *Apostol, Introduction to Analytic Number Theory*

Meng-Gen Tsai  
plover@gmail.com

October 27, 2021

## Contents

<b>Chapter 1: The Fundamental Theorem of Arithmetic</b>	<b>3</b>
Exercise 1.1. . . . .	3
Exercise 1.2. . . . .	4
Exercise 1.3. . . . .	4
Exercise 1.11. . . . .	5
Exercise 1.15. . . . .	6
Exercise 1.16. (Mersenne primes) . . . . .	6
Exercise 1.17. (Fermat primes) . . . . .	6
Exercise 1.30. . . . .	6
<b>Chapter 2: Arithmetical functions and Dirichlet multiplication</b>	<b>8</b>
Exercise 2.1. . . . .	8
Exercise 2.2. . . . .	9
Exercise 2.3. . . . .	10
Exercise 2.4. . . . .	11
Exercise 2.5. . . . .	11
Exercise 2.6. . . . .	12
Exercise 2.7. . . . .	12
Exercise 2.8. . . . .	13
Exercise 2.9. . . . .	14
Exercise 2.10. . . . .	16
Exercise 2.11. . . . .	16
Exercise 2.12. . . . .	17
Exercise 2.13. (Product form of the Möbius inversion formula) . . . . .	17
Exercise 2.14. . . . .	18
Exercise 2.15. ( $\varphi_k(n)$ function) . . . . .	19
Exercise 2.16. . . . .	20
Exercise 2.17. (Jordan's totient function) . . . . .	21

Exercise 2.18. . . . .	22
Exercise 2.19. . . . .	23
Exercise 2.20. . . . .	24
Exercise 2.21. . . . .	24
Exercise 2.23. . . . .	25
Exercise 2.24. . . . .	25
Supplement 2.24.1. (Related exercises) . . . . .	26
<b>Chapter 3: Average of arithmetical functions</b>	<b>27</b>
Exercise 3.1. . . . .	27
Exercise 3.2. . . . .	28
Exercise 3.3. . . . .	29
Exercise 3.5. . . . .	30
Properties of the greatest-integer function . . . . .	31
Exercise 3.17 . . . . .	32
Supplement 3.17.1. (Related exercises) . . . . .	33
Exercise 3.18. (Replicative function) . . . . .	33
Exercise 3.20. . . . .	35
<b>Chapter 4: Some Elementary Theorems on the Distribution of Prime Numbers</b>	<b>36</b>
Exercise 4.5. . . . .	36
Exercise 4.18. . . . .	36
Exercise 4.19. (Logarithmic integral) . . . . .	37
<b>Chapter 5: Congruences</b>	<b>40</b>
Supplement. (Chinese remainder theorem) . . . . .	40
<b>Chapter 6: Finite Abelian Groups and Their Characters</b>	<b>41</b>
Supplement. (Serre, A Course in Arithmetic) . . . . .	41
Supplement. (Serre, Linear Representations of Finite Groups) . .	41
Exercise 6.1. . . . .	42
Exercise 6.2. . . . .	42
Exercise 6.3. . . . .	43
<b>Chapter 7: Dirichlet's Theorem on Primes in Arithmetic Progressions</b>	<b>44</b>
Supplement. . . . .	44

## Chapter 1: The Fundamental Theorem of Arithmetic

In these exercises lower case latin letters  $a, b, c, \dots, x, y, z$  represent integers. Prove each of the statement in Exercise 1.1 through 1.6.

### Exercise 1.1.

If  $(a, b) = 1$  and if  $c|a$  and  $d|b$ , then  $(c, d) = 1$ .

*Proof (Theorem 1.2).*

- (1)  $(a, b) = 1$  if and only if there are  $x, y \in \mathbb{Z}$  such that

$$ax + by = 1$$

(Theorem 1.2). As  $c|a$  and  $d|b$ , there exist  $c', d' \in \mathbb{Z}$  such that  $cc' = a$  and  $dd' = b$ .

- (2) Hence

$$\underbrace{c(c'x)}_{:=x'} + \underbrace{d(d'y)}_{:=y'} = 1$$

for some  $x', y' \in \mathbb{Z}$ . That is,  $(c, d) = 1$ .

□

*Proof (Theorem 1.12).*

- (1) Write

$$a = \prod p_i^{a_i}, \quad b = \prod p_i^{b_i}.$$

Here  $\min\{a_i, b_i\} = 0$  since  $(a, b) = 1$  (Theorem 1.12).

- (2) As  $c|a$  and  $d|b$ ,

$$c = \prod p_i^{a'_i}, \quad d = \prod p_i^{b'_i}$$

where  $a'_i \leq a_i$  and  $b'_i \leq b_i$ . As  $0 \leq \min\{a'_i, b'_i\} \leq \min\{a_i, b_i\} = 0$ ,  $\min\{a'_i, b'_i\} = 0$ . Hence  $(c, d) = \prod p_i^{\min\{a'_i, b'_i\}} = 1$  (Theorem 1.12).

□

**Exercise 1.2.**

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

*Proof (Theorem 1.2).*

- (1)  $(a, b) = (a, c) = 1$  implies that there are  $x, y, z, w \in \mathbb{Z}$  such that

$$ax + by = 1, \quad az + cw = 1$$

(Theorem 1.2).

- (2) So

$$1 = (ax + by)(az + cw) = a \underbrace{(axz + byz + cxw)}_{:=x'} + bc \underbrace{(yw)}_{:=y'}$$

for some  $x', y' \in \mathbb{Z}$ . That is,  $(a, bc) = 1$ .

□

*Proof (Theorem 1.12).*

- (1) Write

$$a = \prod p_i^{a_i}, \quad b = \prod p_i^{b_i}, \quad c = \prod p_i^{c_i}.$$

Here  $\min\{a_i, b_i\} = \min\{a_i, c_i\} = 0$  since  $(a, b) = (a, c) = 1$  (Theorem 1.12). Observe that  $bc = \prod p_i^{b_i + c_i}$ .

- (2) Show that for all  $i$ ,  $\min\{a_i, b_i + c_i\} = 0$  if  $\min\{a_i, b_i\} = \min\{a_i, c_i\} = 0$ . Nothing to do if  $a_i = 0$ . So if  $a_i > 0$ , we have

$$b_i = c_i = 0 \implies b_i + c_i = 0 \implies \min\{a_i, b_i + c_i\} = 0.$$

- (3) Therefore,  $(a, bc) = \prod p_i^{\min\{a_i, b_i + c_i\}} = 1$  (Theorem 1.12).

□

**Exercise 1.3.**

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

*Proof (Theorem 1.2).*

- (1)  $(a, b) = 1$  implies that there are  $x, y \in \mathbb{Z}$  such that

$$ax + by = 1$$

(Theorem 1.2).

(2) Hence

$$\begin{aligned}
1 &= (ax + by)^{n+k-1} \\
&= \sum_{i=0}^{n+k-1} \binom{n+k-1}{i} (ax)^i (by)^{n+k-1-i} \\
&= \sum_{i=0}^{n-1} \binom{n+k-1}{i} (ax)^i (by)^{n+k-1-i} \\
&\quad + \sum_{i=n}^{n+k-1} \binom{n+k-1}{i} (ax)^i (by)^{n+k-1-i} \\
&= b^k y^k \underbrace{\sum_{i=0}^n \binom{n+k-1}{i} (ax)^i (by)^{n-1-i}}_{:=y'} \\
&\quad + a^n x^n \underbrace{\sum_{i=n}^{n+k-1} \binom{n+k-1}{i} (ax)^{i-n} (by)^{n+k-1-i}}_{:=x'}
\end{aligned}$$

for some  $x', y' \in \mathbb{Z}$ . That is,  $(a^n, b^k) = 1$ .

□

*Proof (Theorem 1.12).*

(1) Write

$$a = \prod p_i^{a_i}, \quad b = \prod p_i^{b_i}.$$

Here  $\min\{a_i, b_i\} = 0$  since  $(a, b) = 1$  (Theorem 1.12).

(2) Observe that

$$a^n = \prod p_i^{na_i}, \quad b^k = \prod p_i^{kb_i}.$$

Here  $\min\{na_i, kb_i\} = 0$  (since  $a_i = 0 \implies na_i = 0$  and  $b_i = 0 \implies kb_i = 0$ ).  
Therefore  $(a^n, b^k) = 1$ .

□

### Exercise 1.11.

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

*Proof.*

$$n^4 + 4 = \underbrace{((n-1)^2 + 1)}_{>1} \underbrace{((n+1)^2 + 1)}_{>1}$$

since  $n > 1$ .  $\square$

**Exercise 1.15.**

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

*Proof.* Write  $n = 2m$  (resp.  $n = 2m + 1$ ) where  $m \in \mathbb{Z}$ ,  $m \geq 6$ . Then  $n = 8 + 2(m - 4)$  (resp.  $n = 9 + 2(m - 4)$ ) is the sum of two composite numbers.  $\square$

**Exercise 1.16. (Mersenne primes)**

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

*Proof.* Suppose  $n$  is a composite number, then we can write  $n = ab$  with  $a > 1$ ,  $b > 1$ . Hence

$$2^n - 1 = 2^{ab} - 1 = 2^{ab} - 1 = \underbrace{(2^a - 1)}_{>1} \underbrace{\{(2^a)^{b-1} + \dots + 1\}}_{>1}$$

is also a composite number.  $\square$

**Exercise 1.17. (Fermat primes)**

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

*Proof.* Write  $n = 2^a b$  where  $a$  is a nonnegative integer and  $b$  is odd. Suppose  $n$  is not a power of 2, then  $b > 1$ . Hence

$$2^n + 1 = 2^{2^a b} + 1 = \underbrace{(2^{2^a} + 1)}_{>1} \underbrace{\{2^{2^a(b-1)} - \dots + 1\}}_{>1}$$

is a composite number. (Note that  $1 < 2^{2^a(b-1)} < 2^n + 1$  implies that  $1 < (2^{2^a(b-1)} - \dots + 1) < 2^n + 1$  too.)  $\square$

**Exercise 1.30.**

*If  $n > 1$  prove that the sum*

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

is not an integer.

*Proof.*

(1) (Reductio ad absurdum) Suppose

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

were an integer.

(2) Let  $s$  be the largest integer such that  $2^s \leq n$ . So the integer number

$$\begin{aligned} 2^{s-1}H &= \sum_{k=1}^n \frac{2^{s-1}}{k} \\ &= 2^{s-1} + 2^{s-2} + \frac{2^{s-1}}{3} + 2^{s-3} + \frac{2^{s-1}}{5} + \frac{2^{s-2}}{3} + \cdots + \frac{1}{2} + \cdots . \end{aligned}$$

has only one term of even denominators (as  $n > 1$ ) if we write all terms in irreducible fractions. That is,

$$2^{s-1}H = \frac{1}{2} + \frac{c}{d} \in \mathbb{Z}$$

where  $\frac{c}{d}$  is an irreducible fraction with odd  $d$ . Hence it suffices to show that  $2 \nmid d$  to get a contradiction.

(3) By

$$\frac{1}{2} + \frac{c}{d} = \frac{d+2c}{2d} \in \mathbb{Z}$$

we have  $d+2c = 2dd'$  for some  $d' \in \mathbb{Z}$ . Note that 2 is a prime. So  $2 \mid (d+2c)$  or  $2 \mid d$ , which is absurd.

□

## Chapter 2: Arithmetical functions and Dirichlet multiplication

### Exercise 2.1.

Find all integers  $n$  such that

- (a)  $\varphi(n) = \frac{n}{2}$ ,
- (b)  $\varphi(n) = \varphi(2n)$ ,
- (c)  $\varphi(n) = 12$ .

*Proof of (a).*

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right) = \frac{n}{2}$$

(Theorem 2.4) implies that  $n = 2$ .  $\square$

*Proof of (b).*

- (1)  $\varphi(n) = \varphi(2n)$  implies that

$$n \prod_{p|n} \left(1 - \frac{1}{p}\right) = 2n \prod_{p|(2n)} \left(1 - \frac{1}{p}\right).$$

- (2) If  $2|n$ , then  $n = 2n$  or  $n = 0$ , which is absurd.
- (3) If  $2 \nmid n$ , then

$$n \prod_{p|n} \left(1 - \frac{1}{p}\right) = 2n \prod_{p|(2n)} \left(1 - \frac{1}{p}\right) = \underbrace{2n \left(1 - \frac{1}{2}\right)}_{=n} \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

is always true. Hence  $n$  is odd if  $\varphi(n) = \varphi(2n)$ .

$\square$

*Proof of (c).*

- (1) Show that the solutions of  $\varphi(n) = 12$  are  $n = 13, 26, 21, 28, 42, 36$ . Write  $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$  where  $p_1 < p_2 < \dots$ . Then

$$12 = \varphi(n) = \prod_{i=1}^r p_i^{\alpha_i-1} (p_i - 1).$$

(Theorem 2.5). It implies that  $p_i \in \{2, 3, 5, 7, 13\}$  if  $\alpha_i > 0$ . Consider all possible cases of the greatest prime divisor  $p_r$  of  $n$  as follows.



(2) If  $p_r = 13$ , then  $\alpha_r = 1$  since  $13 \nmid 12$ . So

$$12 = \varphi(n) = \underbrace{\varphi(13)}_{=12} \varphi\left(\frac{n}{13}\right)$$

or  $1 = \varphi\left(\frac{n}{13}\right)$ . Hence  $\frac{n}{13} = 1, 2$ . In this case  $n = 13, 26$ .

(3) If  $p_r = 7$ , then  $\alpha_r = 1$  since  $7 \nmid 12$ . So

$$12 = \varphi(n) = \underbrace{\varphi(7)}_{=6} \varphi\left(\frac{n}{7}\right)$$

or  $2 = \varphi\left(\frac{n}{7}\right)$ . Hence  $\frac{n}{7} = 3, 4, 6$ . In this case  $n = 21, 28, 42$ .

(5) If  $p_r = 5$ , then  $\alpha_r = 1$  since  $5 \nmid 12$ . So  $12 = \varphi(5)\varphi\left(\frac{n}{5}\right)$  or  $3 = \varphi\left(\frac{n}{5}\right)$ , which is impossible.

(6) If  $p_r = 3$ , then  $\alpha_r = 1, 2$ .  $\alpha_r = 1$  is impossible since  $3 \mid 12$ . So

$$12 = \varphi(n) = \underbrace{\varphi(3^2)}_{=6} \varphi\left(\frac{n}{3^2}\right)$$

or  $2 = \varphi\left(\frac{n}{3^2}\right)$ . Hence  $\frac{n}{3^2} = 4$ . (By assumption  $\frac{n}{3^2}$  cannot have any prime factor  $> 3$ .) In this case  $n = 36$ .

□

### 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 divide  $m$  and  $n$ , then  $n\varphi(m) = m\varphi(n)$ .

*Proof of (a).* It is false since  $(5, 13) = 1$  and  $(\varphi(5), \varphi(13)) = (4, 12) = 4$ . □

*Proof of (b).* It is false since  $(15, \varphi(15)) = (15, 8) = 1$ . □

*Proof of (c).*

- (1) It is true.

(2) If the same primes divide  $m$  and  $n$ , then

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

(Theorem 2.4). Hence  $n\varphi(m) = m\varphi(n)$ .

□

**Exercise 2.3.**

*Prove that*

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

*Proof.*

(1) Note that  $fg$ ,  $f/g$  and  $f * g$  are multiplicative if  $f$  and  $g$  are multiplicative (Example 5 on page 34 and Theorem 2.14). Hence  $\frac{n}{\varphi(n)}$  and  $\sum_{d|n} \frac{\mu^2(d)}{\varphi(d)}$  are multiplicative. Hence it might assume that  $n = p^a$  for some prime  $p$  and integer  $a \geq 1$ . (The case  $n = 1$  is trivial.)

(2)

$$\frac{p^a}{\varphi(p^a)} = \frac{p^a}{p^a - p^{a-1}} = \frac{p}{p-1}.$$

(3)

$$\begin{aligned} \sum_{d|p^a} \frac{\mu(d)^2}{\varphi(d)} &= \frac{\mu(1)^2}{\varphi(1)} + \frac{\mu(p)^2}{\varphi(p)} + \overbrace{\frac{\mu(p^2)^2}{\varphi(p^2)}}^{=0} + \cdots + \overbrace{\frac{\mu(p^a)^2}{\varphi(p^a)}}^{=0} \\ &= 1 + \frac{1}{p-1} + 0 + \cdots + 0 \\ &= \frac{p}{p-1}. \end{aligned}$$

(4) Or apply Theorems 2.4 and 2.18 to get

$$\begin{aligned} \sum_{d|n} \frac{\mu(d)^2}{\varphi(d)} &= \prod_{p|n} \left(1 - \frac{\mu(p)}{\varphi(p)}\right) \\ &= \prod_{p|n} \left(1 - \frac{-1}{p-1}\right) \\ &= \prod_{p|n} \frac{p}{p-1} \\ &= \frac{n}{\varphi(n)}. \end{aligned}$$

□

**Exercise 2.4.**

Prove that  $\varphi(n) > \frac{n}{6}$  for all  $n$  with at most 8 distinct prime factors.

*Proof.*

(1)

$$\begin{aligned}
 \varphi(n) &= n \prod_{p|n} \left(1 - \frac{1}{p}\right) && \text{(Theorem 2.4)} \\
 &\geq n \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) \left(1 - \frac{1}{5}\right) \left(1 - \frac{1}{7}\right) \\
 &\quad \left(1 - \frac{1}{11}\right) \left(1 - \frac{1}{13}\right) \left(1 - \frac{1}{17}\right) \left(1 - \frac{1}{19}\right) \\
 &= \frac{55296}{323323} n \\
 &> \frac{n}{6}.
 \end{aligned}$$

(2) The conclusion does not hold if  $n$  has more than 9 distinct prime factors.

□

**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.* It is easy to verify that

$$f(n) := \begin{cases} 1 & \text{if } n \text{ is prime,} \\ 0 & \text{otherwise.} \end{cases}$$

satisfies  $\sum_{d|n} f(d) = \nu(n)$ . Hence  $f = \mu * \nu$  holds by the Möbius inversion formula (Theorem 2.9). □

*Note.* We can calculate  $f(n)$  for  $n = 1, 2, \dots, 10$  to find the pattern of  $f$ .

**Exercise 2.6.**

Prove that

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

and, more generally

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

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

*Proof.*

- (1) Write  $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r} q_1^{\beta_1} \cdots q_s^{\beta_s}$  where  $\alpha_i \geq 2$  and  $\beta_j = 1$ . The proof is similar to Theorem 2.1.
- (2) If  $p_1^{\alpha_1} \cdots p_r^{\alpha_r} = 1$ , then  $\sum_{d^2|n} \mu(d) = \mu(1) = 1$ .
- (3) If  $p_1^{\alpha_1} \cdots p_r^{\alpha_r} > 1$ , then

$$\begin{aligned} \sum_{d^2|n} \mu(d) &= \mu(1) + \mu(p_1) + \cdots + \mu(p_r) \\ &\quad + \mu(p_1 p_2) + \cdots + \mu(p_{r-1} p_r) + \cdots + \mu(p_1 \cdots p_r) \\ &= 1 + \binom{r}{1}(-1) + \binom{r}{2}(-1)^2 + \cdots + \binom{r}{r}(-1)^r \\ &= (1 - 1)^r \\ &= 0. \end{aligned}$$

- (4) By (2)(3),  $\sum_{d^2|n} \mu(d) = \mu(n)^2$ . Besides, we have

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

by the same argument as (1)(2)(3).

□

**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

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

*Proof.*

- (1) It suffices to show that  $\mu(p, n)$  is multiplicative. If so, then

$$h(n) := \sum_{d|n} \mu(d)\mu(p, d)$$

is also multiplicative by taking  $f(n) := \mu(n)\mu(p, n)$  and  $g(n) := 1$  in Theorem 2.14.

- (2) A direct calculation shows that  $h(1) = 1$  (or by Theorem 2.12) and

$$h(p^a) = \mu(1)\mu(p, 1) + \mu(p)\mu(p, p) = 1 \cdot 1 + (-1) \cdot (-1) = 2,$$

$$h(q^b) = \mu(1)\mu(p, 1) + \mu(q)\mu(p, q) = 1 \cdot 1 + (-1) \cdot 1 = 0$$

where  $q \neq p$  and  $a, b \geq 1$ . Hence (1) and Theorem 2.13 show that

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

- (3) Show that  $\mu(p, n)$  is multiplicative. Suppose  $(m, n) = 1$ . There are two possible cases:  $p \nmid mn$  and  $p|mn$ .

(a) If  $p \nmid mn$ , then all  $\mu(p, mn), \mu(p, m), \mu(p, n)$  are equal to  $\mu(1) = 1$ .

(b) If  $p|mn$ , then  $p|m$  or  $p|n$ . Note that  $(m, n) = 1$  and thus  $p$  cannot be a common divisor of  $m, n$ . Hence  $\mu(p, mn) = \mu(p) = -1$  and  $\mu(p, m)\mu(p, n) = \mu(p)\mu(1) = -1$ .

In any case  $\mu(p, mn) = \mu(p, m)\mu(p, n)$  if  $(m, n) = 1$ .

□

### Exercise 2.8.

Prove that

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

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

*Proof.*

- (1) Induction.

(2) (Base case) Suppose  $m = 1$ . Theorem 2.11 implies that

$$\sum_{d|n} \mu(d) \log(d) = -\Lambda(n) = 0$$

since  $n$  has at least 2 distinct prime factors.

(3) (Inductive step) Suppose the conclusion holds for  $m < m_0$  and  $n$  has more than  $m$  distinct prime factors. Given  $n$  having more than  $m_0$  distinct prime factors. Write  $n = p^a n'$  where  $a > 0$  and  $p \nmid n'$ . (Here  $q$  has more than  $m_0 - 1$  distinct prime factors.) So by the induction hypothesis and  $\sum_{d|n'} \mu(d) = 0$ , we have

$$\begin{aligned} & \sum_{d|n} \mu(d) (\log d)^{m_0} \\ &= \sum_{d|n'} \sum_{i=0}^a \mu(p^i d) (\log p^i d)^{m_0} \\ &= \sum_{d|n'} [\mu(d) (\log d)^{m_0} + \mu(pd) (\log pd)^{m_0}] \\ &= \sum_{d|n'} [\mu(d) (\log d)^{m_0} + \underbrace{\mu(p)}_{=-1} \mu(d) (\log p + \log d)^{m_0}] \\ &= \sum_{d|n'} \mu(d) [(\log d)^{m_0} - (\log p + \log d)^{m_0}] \\ &= \sum_{d|n'} \mu(d) [-(\log p)^{m_0} - \dots - m_0 \log p (\log d)^{m_0-1}] \\ &= -(\log p)^{m_0} \sum_{d|n'} \mu(d) - \dots - m_0 \log p \sum_{d|n'} \mu(d) (\log d)^{m_0-1} \\ &= 0. \end{aligned}$$

(4) By (2)(3), the conclusion holds for all  $m \geq 1$ .

□

### 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

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

*Proof.*

- (1) Show that  $\varphi(x, n) = \sum_{d|n} \mu(d) \left\lfloor \frac{x}{d} \right\rfloor$ . Similar to the proof of Theorem 2.3.  $\varphi(x, n)$  can be written in the form

$$\varphi(x, n) = \sum_{1 \leq k \leq x} \left\lfloor \frac{1}{(n, k)} \right\rfloor,$$

where now  $k$  runs through all integers  $\leq x$ . Now we use Theorem 2.1 with  $n$  replaced by  $(n, k)$  to obtain

$$\varphi(x, n) = \sum_{1 \leq k \leq x} \sum_{d|(n, k)} \mu(d) = \sum_{1 \leq k \leq x} \sum_{\substack{d|n \\ d|k}} \mu(d).$$

For a fixed divisor  $d$  of  $n$  we must sum over all those  $k$  in the range  $1 \leq k \leq x$  which are multiples of  $d$ . If we write  $k = qd$  then  $1 \leq k \leq x$  if and only if  $1 \leq q \leq \left\lfloor \frac{x}{d} \right\rfloor$ . Hence the last sum for  $\varphi(x, n)$  can be written as

$$\varphi(x, n) = \sum_{d|n} \sum_{1 \leq q \leq \left\lfloor \frac{x}{d} \right\rfloor} \mu(d) = \sum_{d|n} \mu(d) \sum_{1 \leq q \leq \left\lfloor \frac{x}{d} \right\rfloor} 1 = \sum_{d|n} \mu(d) \left\lfloor \frac{x}{d} \right\rfloor.$$

- (2) Show that  $\sum_{d|n} \varphi\left(\frac{x}{d}, \frac{n}{d}\right) = [x]$ . Similar to the proof of Theorem 2.2. Let  $S$  denote the set  $\{1, 2, \dots, [x]\}$ . We distribute the integers of  $S$  into disjoint sets as follows. For each divisor  $d$  of  $n$ , let

$$A(d) = \{k : (k, n) = d, 1 \leq k \leq x\}.$$

That is,  $A(d)$  contains those elements of  $S$  which have the gcd  $d$  with  $n$ . The sets  $A(d)$  form a disjoint collection whose union is  $S$ . Therefore if  $f(d)$  denotes the number of integers in  $A(d)$  we have

$$\sum_{d|n} f(d) = [x].$$

But  $(k, n) = d$  if and only if  $\left(\frac{k}{d}, \frac{n}{d}\right) = 1$ , and  $0 < k \leq x$  if and only if  $0 < \frac{k}{d} \leq \frac{x}{d}$ . Therefore, if we let  $q = \frac{k}{d}$ , there is a one-to-one correspondence between the elements in  $A(d)$  and those integers  $q$  satisfying  $0 < q \leq \frac{x}{d}$ ,  $\left(q, \frac{n}{d}\right) = 1$ . The number of such  $q$  is  $\varphi\left(\frac{x}{d}, \frac{n}{d}\right)$ . Hence  $f(d) = \varphi\left(\frac{x}{d}, \frac{n}{d}\right)$  and thus

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

□

In Exercise 2.10, 2.11 and 2.12,  $d(n)$  denotes the number of positive divisors of  $n$ .

**Exercise 2.10.**

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

*Proof.*

(1) Note that  $d(1) = 1$  and

$$d(p_1^{\alpha_1} \cdots p_r^{\alpha_r}) = (\alpha_1 + 1) \cdots (\alpha_r + 1) = d(p_1^{\alpha_1}) \cdots d(p_r^{\alpha_r}).$$

Hence  $d(n)$  is multiplicative (Theorem 2.13).

(2) Show that  $\prod_{t|n} t = n^{\frac{d(n)}{2}}$ .  $n = 1$  is trivial. Assume  $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r} > 1$ . Then  $t|n$  if and only if  $t = p_1^{x_1} \cdots p_r^{x_r}$  with  $0 \leq x_i \leq \alpha_i$  ( $i = 1, \dots, r$ ). So

$$\begin{aligned} \prod_{t|n} t &= \prod_{\substack{0 \leq x_1 \leq \alpha_1 \\ \vdots \\ 0 \leq x_r \leq \alpha_r}} p_1^{x_1} \cdots p_r^{x_r} \\ &= p_1^{(0+1+\cdots+\alpha_1)(\alpha_2+1)\cdots(\alpha_r+1)} \cdots p_r^{(\alpha_1+1)\cdots(\alpha_{r-1}+1)(0+1+\cdots+\alpha_r)} \\ &= p_1^{\frac{\alpha_1(\alpha_1+1)}{2} \cdot (\alpha_2+1)\cdots(\alpha_r+1)} \cdots p_r^{(\alpha_1+1)\cdots(\alpha_{r-1}+1) \cdot \frac{\alpha_r(\alpha_r+1)}{2}} \\ &= p_1^{\alpha_1 \frac{d(n)}{2}} \cdots p_r^{\alpha_r \frac{d(n)}{2}} \\ &= (p_1^{\alpha_1} \cdots p_r^{\alpha_r})^{\frac{d(n)}{2}} \\ &= n^{\frac{d(n)}{2}}. \end{aligned}$$

□

**Exercise 2.11.**

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

*Proof.*  $n = 1$  is trivial. Assume  $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r} > 1$ . Then

$$\begin{aligned} d(n) &= (\alpha_1 + 1) \cdots (\alpha_r + 1) \text{ is odd} && \text{(Exercise 2.10)} \\ \iff \alpha_1 + 1, \dots, \alpha_r + 1 &\text{ are odd} \\ \iff \alpha_1, \dots, \alpha_r &\text{ are even} \\ \iff n &\text{ is a square.} \end{aligned}$$

□



**Exercise 2.12.**

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

*Proof.*

- (1) Exercise 2.10 shows that  $d(n)$  is multiplicative. Similar to the proof of Exercise 2.7, both  $f(n) := \sum_{t|n} d(t)^3$  and  $g(n) := \left(\sum_{t|n} d(t)\right)^2$  are multiplicative. So it suffices to show that  $f(p^a) = g(p^a)$  (Theorem 2.13).
- (2) A direct calculation shows that

$$\begin{aligned} f(p^a) &= \sum_{t|p^a} d(t)^3 \\ &= d(1)^3 + d(p)^3 + \cdots + d(p^a)^3 \\ &= 1^3 + 2^3 + \cdots + (a+1)^3 \\ &= \left(\frac{(a+1)(a+2)}{2}\right)^2 \end{aligned}$$

and

$$\begin{aligned} g(p^a) &= \left(\sum_{t|p^a} d(t)\right)^2 \\ &= (d(1) + d(p) + \cdots + d(p^a))^2 \\ &= (1 + 2 + \cdots + (a+1))^2 \\ &= \left(\frac{(a+1)(a+2)}{2}\right)^2 \end{aligned}$$

are equal.

□

**Exercise 2.13. (Product form of the Möbius inversion formula)**

**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

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

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

*Proof.* As  $f(n) > 0$  for all  $n$ ,  $a(n)$  is real, and  $a(1) \neq 0$ , we have

$$\begin{aligned}
\underbrace{\log g(n)}_{\text{well-defined}} &= \sum_{d|n} a\left(\frac{n}{d}\right) \underbrace{\log f(d)}_{\text{well-defined}} \\
&\iff \log g = a * \log f \\
&\iff \log f = b * \log g \\
&\iff \log f(n) = \sum_{d|n} b\left(\frac{n}{d}\right) \log g(d) \\
&\iff f(n) = \prod_{d|n} g(d)^{b\left(\frac{n}{d}\right)}.
\end{aligned}$$

□

**Exercise 2.14.**

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

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

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

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

*Proof of (a).* As  $\mu * u = I$ , it suffices to show that  $u * F^* = F$ . Hence

$$\begin{aligned}
(u * F^*)(n) &= \sum_{d|n} F^*(d) \\
&= \sum_{d|n} \sum_{\substack{1 \leq k \leq d \\ (k,d)=1}} f\left(\frac{k}{d}\right) \\
&= \sum_{\substack{d|n \\ 1 \leq k \leq d \\ (k,d)=1}} f\left(\frac{k}{d}\right) \\
&= \sum_{1 \leq k \leq n} f\left(\frac{k}{n}\right) \\
&= F(n).
\end{aligned}$$

□

*Proof of (b).* Let  $f(x) = e^{2\pi i x}$  defined on  $[0, 1]$ . Then

$$F(n) = \sum_{1 \leq k \leq n} f\left(\frac{k}{n}\right) = \sum_{1 \leq k \leq n} e^{\frac{2\pi i k}{n}} = I(n).$$

Hence

$$\sum_{\substack{1 \leq k \leq n \\ (k, n) = 1}} e^{\frac{2\pi i k}{n}} = F^*(n) = (\mu * F)(n) = (\mu * I)(n) = \mu(n).$$

□

**Exercise 2.15. ( $\varphi_k(n)$  function)**

Let  $\varphi_k(n)$  denote the sum of the  $k$ th powers of the numbers  $\leq n$  and relatively prime to  $n$ . Note that  $\varphi_0(n) = \varphi(n)$ . Use Exercise 2.14 or some other means to prove that

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

*Proof.*

(1) Let  $f(x) = x^k$  defined on  $[0, 1]$ . Then

$$F(n) = \sum_{1 \leq i \leq n} f\left(\frac{i}{n}\right) = \frac{1^k + \cdots + n^k}{n^k}.$$

(2) The proof of Exercise 2.14 shows that

$$F(n) = (u * F^*)(n) = \sum_{d|n} \sum_{\substack{1 \leq i \leq d \\ (i, d) = 1}} f\left(\frac{i}{d}\right) = \sum_{d|n} \frac{1}{d^k} \underbrace{\sum_{\substack{1 \leq i \leq d \\ (i, d) = 1}} i^k}_{=\varphi_k(n)}.$$

(3) Hence the result is established by (1)(2).

□

**Exercise 2.16.**

Invert the formula in Exercise 2.15 to obtain, for  $n > 1$ ,

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

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

*Proof.*

(1) Exercise 2.15 shows that

$$\sum_{d|n} \varphi_k(n) \underbrace{\left(\frac{n}{d}\right)^k}_{:=f\left(\frac{n}{d}\right)} = \underbrace{1^k + \cdots + n^k}_{:=S_k(n)} \iff \varphi_k * f = S_k.$$

Here  $f(n) = N(n)^k = n^k$  and  $S_k(n) = 1^k + \cdots + n^k$ .

(2) As  $f(n)$  is completely multiplicative, Theorem 2.17 implies that  $f^{-1}(n) = \mu(n)f(n)$  for all  $n \geq 1$ . Hence

$$\begin{aligned} \varphi_k(n) &= (S_k * f^{-1})(n) \\ &= (S_k * (\mu f))(n) \\ &= \sum_{d|n} S_k(d) \mu\left(\frac{n}{d}\right) \left(\frac{n}{d}\right)^k. \end{aligned}$$

(3) Show that  $\varphi_1(n) = \frac{1}{2}n\varphi(n)$ . Note that  $S_1(d) = \frac{d(d+1)}{2}$ . Hence

$$\begin{aligned} \varphi_1(n) &= \sum_{d|n} \frac{d(d+1)}{2} \mu\left(\frac{n}{d}\right) \frac{n}{d} \\ &= \frac{n}{2} \sum_{d|n} d \mu\left(\frac{n}{d}\right) + \frac{n}{2} \sum_{d|n} \mu\left(\frac{n}{d}\right) \\ &= \frac{n}{2} \varphi(n) + \frac{n}{2} \left\lfloor \frac{1}{n} \right\rfloor \quad (\text{Theorems 2.1, 2.3}) \end{aligned}$$

for all  $n \geq 1$ . So the result is established if  $n > 1$ .

(4) Show that  $\varphi_2(n) = \frac{1}{3}n^2\varphi(n) + \frac{1}{6}n \prod_{p|n} (1-p)$ . Note that  $S_2(d) = \frac{d(d+1)(2d+1)}{6}$ . Hence Theorem 2.1, 2.3 and 2.18 imply that

$$\begin{aligned} \varphi_2(n) &= \sum_{d|n} \frac{d(d+1)(2d+1)}{6} \mu\left(\frac{n}{d}\right) \left(\frac{n}{d}\right)^2 \\ &= \underbrace{\frac{n^2}{3} \sum_{d|n} d \mu\left(\frac{n}{d}\right)}_{=\varphi(n)} + \underbrace{\frac{n^2}{2} \sum_{d|n} \mu\left(\frac{n}{d}\right)}_{=\lfloor \frac{1}{n} \rfloor} + \underbrace{\frac{n}{6} \sum_{d|n} \mu\left(\frac{n}{d}\right) \left(\frac{n}{d}\right)}_{=\prod_{p|n} (1-p)} \end{aligned}$$

for all  $n \geq 1$ . So the result is established if  $n > 1$ .

(4) Show that

$$\varphi_3(n) = \frac{1}{4}n^3\varphi(n) + \frac{1}{4}n^2 \prod_{p|n} (1-p).$$

Note that  $S_3(d) = \frac{d^2(d+1)^2}{4}$ . Hence Theorem 2.1, 2.3 and 2.18 imply that

$$\begin{aligned} \varphi_3(n) &= \sum_{d|n} \frac{d^2(d+1)^2}{4} \mu\left(\frac{n}{d}\right) \left(\frac{n}{d}\right)^3 \\ &= \frac{n^3}{4} \underbrace{\sum_{d|n} d \mu\left(\frac{n}{d}\right)}_{=\varphi(n)} + \frac{n^3}{2} \underbrace{\sum_{d|n} \mu\left(\frac{n}{d}\right)}_{=\lfloor \frac{1}{n} \rfloor} + \frac{n^2}{4} \underbrace{\sum_{d|n} \mu\left(\frac{n}{d}\right) \left(\frac{n}{d}\right)}_{=\prod_{p|n} (1-p)} \end{aligned}$$

for all  $n \geq 1$ . So the result is established if  $n > 1$ .

□

### Exercise 2.17. (Jordan's totient function)

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 of (a).*

(1) Show that  $J_k(n) = \sum_{d|n} \mu(d) \left(\frac{n}{d}\right)^k$ . Similar to Exercise 2.7. Note that  $J_k$  is multiplicative. Theorem 2.14 shows that the Dirichlet product  $n \mapsto \sum_{d|n} \mu(d) \left(\frac{n}{d}\right)^k$  is multiplicative. Hence it suffices to show that

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

for  $n = p^a$  where  $p$  is prime and  $a \geq 1$ . It is easy since

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

- (2) Show that  $n^k = \sum_{d|n} J_k(d)$ . Note that  $\mu * u = I$  by Theorem 2.1. So Theorem 2.9 (Möbius inversion formula) implies that

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

□

*Proof of (b).*

- (1) Since  $J_k(1) = 1$  and  $J_k(p^n) = p^{nk} - p^{(n-1)k}$  for  $n \geq 1$ , we have

$$\begin{aligned} (J_k)_p(x) &= \sum_{n=0}^{\infty} J_k(p^n) x^n \\ &= 1 + \sum_{n=0}^{\infty} (p^{nk} - p^{(n-1)k}) x^n \\ &= \sum_{n=0}^{\infty} p^{nk} x^n - x \sum_{n=0}^{\infty} p^{nk} x^n \\ &= (1-x) \sum_{n=0}^{\infty} p^{nk} x^n \\ &= \frac{1-x}{1-p^k x}. \end{aligned}$$

- (2) Another proof by using Theorem 2.25. Note that  $\mu_p(x) = 1-x$  and  $N_p^k(x) = \frac{1}{1-p^k x}$ . Theorem 2.25 implies  $(J_k)_p(x) = \mu_p(x) N_p^k(x) = \frac{1-x}{1-p^k x}$  too.

□

### 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.* Write  $n := 2^{a-1}(2^a - 1)$ . Here  $(2^{a-1}, 2^a - 1) = 1$  since  $2^a - 1$  is always odd and Exercise 1.3. Hence

$$\begin{aligned} \sigma(n) &= \sigma(2^{a-1})\sigma(2^a - 1) && (\sigma \text{ is a multiplicative}) \\ &= (1 + 2 + \cdots + 2^{a-1})\{1 + (2^a - 1)\} && (2^a - 1 \text{ is prime}) \\ &= (2^a - 1) \cdot \underbrace{(2^a)}_{=2^{a-1} \cdot 2} \\ &= 2n. \end{aligned}$$

Therefore  $n$  is perfect.  $\square$

**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 than 7 distinct prime factors.*

*Proof.*

- (1) Suppose  $n$  is even and perfect. We might write  $n = 2^{a-1}q$  for some  $a \geq 2$  and  $2 \nmid q$ . As  $n$  is perfect, we have

$$\begin{aligned} 2n &= \sigma(n) \\ \implies \underbrace{2 \cdot 2^{a-1}q}_{=2^a q} &= 2n = \sigma(2^{a-1}q) = \underbrace{\sigma(2^{a-1})}_{=2^a-1} \sigma(q) \\ \implies 2^a q &= (2^a - 1)\sigma(q) \\ \implies q &= (2^a - 1)q_1 \text{ for some } q_1 \text{ since } (2^a - 1, 2^a) = 1 \\ \implies 2^a(2^a - 1)q_1 &= (2^a - 1)\sigma(q) \\ \implies 2^a q_1 &= \sigma(q) = \sigma((2^a - 1)q_1). \end{aligned}$$

- (2) If  $q_1 > 1$ , then

$$\begin{aligned} 2^a q_1 &= \sigma(q) \\ &= \sigma((2^a - 1)q_1) \\ &\geq (2^a - 1)q_1 + (2^a - 1) + q_1 + 1 \\ &= 2^a q_1 + 2^a, \end{aligned}$$

which is absurd. Therefore  $q_1 = 1$ . So  $q = 2^a - 1$  and thus  $n = 2^a(2^a - 1)$ .

- (3) Pace P. Nielsen shows that

- (a) An odd perfect number  $n$  is shown to have at least 9 distinct prime factors.
- (b) Moreover, if  $3 \nmid n$  then  $n$  must have at least 12 distinct prime divisors.

See [Pace P. Nielsen, *Odd perfect numbers have at least nine distinct prime factors*, 2006].

$\square$

**Exercise 2.20.**

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

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

*Proof.*

- (1) To prove  $\frac{P(n)}{n^{\varphi(n)}} = \prod_{d|n} \left( \frac{d!}{d^d} \right)^{\mu\left(\frac{n}{d}\right)}$ , it suffices to show that

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

by product form of the Möbius inversion formula (Exercise 2.13).

- (2) Similar to Exercise 2.14,

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

□

**Exercise 2.21.**

Let  $f(n) = \lfloor \sqrt{n} \rfloor - \lfloor \sqrt{n-1} \rfloor$ . Prove that  $f$  is multiplicative but not completely multiplicative.

*Proof.*

- (1) Show that

$$f(n) = \begin{cases} 1 & \text{if } n \text{ is a square,} \\ 0 & \text{otherwise.} \end{cases}$$

- (a) Write  $m = \lfloor \sqrt{n} \rfloor$ . So  $m^2 \leq n < (m+1)^2$ .  
 (b) Suppose  $n = m^2$  is a square. Since  $m \geq 1$  and  $(m-1)^2 \leq m^2 - 1 = n - 1 < m^2$ ,  $\lfloor \sqrt{n-1} \rfloor = m - 1$ . Therefore  $f(n) = 1$ .  
 (c) Suppose  $n$  is not a square. So  $m^2 < n < (m+1)^2$ . So  $\lfloor \sqrt{n-1} \rfloor = m$  since  $m^2 \leq n - 1 < n < (m+1)^2$ . Therefore  $f(n) = 0$ .  
 (2) It is easy to see that  $f$  is multiplicative but not completely multiplicative (since  $f(p^2) \neq f(p)^2$  for all prime  $p$ ).



□

**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.*

*Proof.*

- (1) False.
- (2) Take a completely multiplicative function  $f = N$  defined by  $f(n) = n$ . Then  $F$  is not multiplicative since  $pq = F(p)F(q) \neq F(pq) = p^2q^2$  for any two distinct primes  $p, q$ .
- (3) Or take a multiplicative function  $f = \varphi$ . Then  $F$  is not multiplicative since  $(p-1)(q-1) = F(p)F(q) \neq F(pq) = (p-1)^2(q-1)^2$  for any two distinct primes  $p, q$ .

□

**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.*

- (1) Write  $A(x) = \sum_{n=0}^{\infty} a(n)x^n$  and  $B(x) = \sum_{n=0}^{\infty} b(n)x^n$  where the coefficients  $a(n)$  and  $b(n)$  are in  $\mathbb{C}$  (or any integral domain).
- (2) (Reductio ad absurdum) Suppose  $A(x) \neq 0$  and  $B(x) \neq 0$ . Let  $r$  (resp.  $s$ ) be the smallest integer such that  $a(r) \neq 0$  (resp.  $b(s) \neq 0$ ). Hence

$$A(x)B(x) = a(r)b(s)x^{r+s} + \dots$$

Here there is no  $x^n$  term if  $n < r + s$ . So  $A(x)B(x) = 0$  implies that  $a(r)b(s) = 0$ . Hence  $a(r) = 0$  or  $b(s) = 0$  (as  $\mathbb{C}$  is an integral domain), which is absurd.

□

**Supplement 2.24.1. (Related exercises)**

- (1) (Exercise 1.2 in the textbook: Atiyah and Macdonald, *Introduction to Commutative Algebra*.) Let  $A$  be a ring and let  $A[x]$  be the ring of polynomials in an indeterminate  $x$ , with coefficients in  $A$ . Let  $f = a_0 + a_1x + \cdots + a_nx^n \in A[x]$ . Prove that
  - (i)  $f$  is a unit in  $A[x]$  if and only if  $a_0$  is a unit in  $A$  and  $a_1, \dots, a_n$  are nilpotent. (Hint: If  $b_0 + b_1x + \cdots + b_mx^m$  is the inverse of  $f$ , prove by induction on  $r$  that  $a_n^{r+1}b_{m-r} = 0$ . Hence show that  $a_n$  is nilpotent, and then use Exercise 1.1.)
  - (ii)  $f$  is nilpotent if and only if  $a_0, a_1, \dots, a_n$  are nilpotent.
  - (iii)  $f$  is a zero-divisor if and only if there exists  $a \neq 0$  such that  $af = 0$ . (Hint: Choose a polynomial  $g = b_0 + b_1x + \cdots + b_mx^m$  of least degree  $m$  such that  $fg = 0$ . Then  $a_nb_m = 0$ , hence  $a_ng = 0$  (because  $a_ng$  annihilates  $f$  and has degree  $< m$ ). Now show by induction that  $a_{n-r}g = 0$  ( $0 \leq r \leq n$ ).)
  - (iv)  $f$  is said to be **primitive** if  $(a_0, a_1, \dots, a_n) = (1)$ . Prove that if  $f, g \in A[x]$ , then  $fg$  is primitive if and only if  $f$  and  $g$  are primitive.
- (2) (Exercise 1.3 in the textbook: Atiyah and Macdonald, *Introduction to Commutative Algebra*.) Generalize the results of Exercise 1.2 to a polynomial ring  $A[x_1, \dots, x_r]$  in several indeterminates.
- (3) (Exercise 1.5 in the textbook: Atiyah and Macdonald, *Introduction to Commutative Algebra*.) Let  $A$  be a ring and let  $A[[x]]$  be the ring of formal power series  $f = \sum_{n=0}^{\infty} a_nx^n$  with coefficients in  $A$ . Show that
  - (i)  $f$  is a unit in  $A[[x]]$  if and only if  $a_0$  is a unit in  $A$ .
  - (ii) If  $f$  is nilpotent, then  $a_n$  is nilpotent for all  $n \geq 0$ . Is converse true? (See Exercise 7.2.)
  - (iii)  $f$  belongs to the Jacobson radical of  $A[[x]]$  if and only if  $a_0$  belongs to the Jacobson radical of  $A$ .
  - (iv) The contraction of a maximal ideal  $\mathfrak{m}$  of  $A[[x]]$  is a maximal ideal of  $A$ , and  $\mathfrak{m}$  is generated by  $\mathfrak{m}^c$  and  $x$ .
  - (v) Every prime ideal of  $A$  is the contraction of a prime ideal of  $A[[x]]$ .
- (4) (Exercise II.1.2 in the textbook: Jrgen Neukirch, *Algebraic Number Theory*.) A  $p$ -adic integer  $a = a_0 + a_1p + a_2p^2 + \cdots$  is a unit in the ring  $\mathbb{Z}_p$  if and only if  $a_0 \neq 0$ .

## Chapter 3: Average of arithmetical functions

### Exercise 3.1.

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

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

*Proof of (a).*

- (1) Similar to the proof of Theorem 3.2. We take  $f(t) = \frac{\log t}{t}$  in Euler's summation formula to obtain

$$\begin{aligned} \sum_{n \leq x} \frac{\log n}{n} &= \int_1^x \frac{\log t}{t} dt + \int_1^x (t - [t]) \frac{1 - \log t}{t^2} dt \\ &\quad + \frac{\log x}{x}([x] - x) - \underbrace{\frac{\log(1)}{1}([1] - 1)}_{=0} \\ &= \frac{1}{2}(\log x)^2 + \int_1^x (t - [t]) \frac{1 - \log t}{t^2} dt + O\left(\frac{\log x}{x}\right) \\ &= \frac{1}{2}(\log x)^2 + \int_1^\infty (t - [t]) \frac{1 - \log t}{t^2} dt \\ &\quad - \int_x^\infty (t - [t]) \frac{1 - \log t}{t^2} dt + O\left(\frac{\log x}{x}\right). \end{aligned}$$

- (2) The improper integral  $\int_1^\infty (t - [t]) \frac{1 - \log t}{t^2} dt$  exists since it is dominated by  $\int_1^e \frac{1 - \log t}{t^2} dt + \int_e^\infty \frac{\log t - 1}{t^2} dt = 2e^{-1}$ .
- (3) Might assume that  $x \geq e$ . So

$$0 \leq - \int_x^\infty (t - [t]) \frac{1 - \log t}{t^2} dt \leq \int_x^\infty \frac{\log t - 1}{t^2} dt = \frac{\log x}{x}.$$

- (4) Therefore

$$\sum_{n \leq x} \frac{\log n}{n} = \frac{1}{2}(\log x)^2 + A + O\left(\frac{\log x}{x}\right)$$

where  $A = \int_1^\infty (t - [t]) \frac{1 - \log t}{t^2} dt$  is a constant.

□

*Proof of (b).*

(1) We take  $f(t) = \frac{1}{t \log t}$  in Euler's summation formula to obtain

$$\begin{aligned}
\sum_{2 \leq n \leq x} \frac{1}{n \log n} &= \int_2^x \frac{1}{t \log t} dt + \int_2^x -(t - [t]) \frac{\log t + 1}{t^2 (\log t)^2} dt \\
&\quad + \frac{1}{x \log x} ([x] - x) - \underbrace{\frac{1}{2 \cdot \log(2)} ([2] - 2)}_{=0} \\
&= \log \log x - \log \log 2 - \int_2^x (t - [t]) \frac{\log t + 1}{t^2 (\log t)^2} dt \\
&\quad + O\left(\frac{1}{x \log x}\right) \\
&= \log \log x - \log \log 2 - \int_2^\infty (t - [t]) \frac{\log t + 1}{t^2 (\log t)^2} dt \\
&\quad + \int_x^\infty (t - [t]) \frac{\log t + 1}{t^2 (\log t)^2} dt + O\left(\frac{1}{x \log x}\right).
\end{aligned}$$

(2) The improper integral  $\int_2^\infty (t - [t]) \frac{\log t + 1}{t^2 (\log t)^2} dt$  exists since it is dominated by  $\int_2^\infty \frac{\log t + 1}{t^2 (\log t)^2} dt = \frac{1}{2 \log 2} < \infty$ .

(3)

$$0 \leq \int_x^\infty (t - [t]) \frac{\log t + 1}{t^2 (\log t)^2} dt \leq \int_x^\infty \frac{\log t + 1}{t^2 (\log t)^2} dt = \frac{1}{x \log x}.$$

(4) Therefore

$$\sum_{2 \leq n \leq x} \frac{1}{n \log n} = \log \log x + B + O\left(\frac{1}{x \log x}\right)$$

where  $B = -\log \log 2 - \int_2^\infty (t - [t]) \frac{\log t + 1}{t^2 (\log t)^2} dt$  is a constant.

□

### Exercise 3.2.

If  $x \geq 2$  prove that

$$\sum_{n \leq x} \frac{d(n)}{n} = \frac{1}{2} (\log x)^2 + 2C \log x + O(1),$$

where  $C$  is Euler's constant.

*Proof.* Similar to the proof of Theorem 3.3, we have

$$\sum_{n \leq x} \frac{d(n)}{n} = \sum_{n \leq x} \frac{1}{n} \sum_{d|n} 1 = \sum_{\substack{q, d \\ qd \leq x}} \frac{1}{qd} = \sum_{d \leq x} \frac{1}{d} \sum_{q \leq \frac{x}{d}} \frac{1}{q}.$$

Now we use Theorem 3.2(a) to obtain

$$\sum_{q \leq \frac{x}{d}} \frac{1}{q} = \log \frac{x}{d} + C + O\left(\frac{d}{x}\right) = \log x - \log d + C + O\left(\frac{d}{x}\right).$$

Using this along with Theorem 3.2(a) and Exercise 3.1 we find

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

□

### Exercise 3.3.

If  $x \geq 2$  and  $\alpha > 0$ ,  $\alpha \neq 1$ , prove that

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

*Proof.*

(1) Similar to Exercise 3.2.

$$\sum_{n \leq x} \frac{d(n)}{n^\alpha} = \sum_{n \leq x} \frac{1}{n^\alpha} \sum_{d|n} 1 = \sum_{\substack{q, d \\ qd \leq x}} \frac{1}{q^\alpha d^\alpha} = \sum_{d \leq x} \frac{1}{d^\alpha} \sum_{q \leq \frac{x}{d}} \frac{1}{q^\alpha}.$$

Now we use Theorem 3.2(b) to obtain

$$\sum_{q \leq \frac{x}{d}} \frac{1}{q^\alpha} = \frac{1}{d^{1-\alpha}} \cdot \frac{x^{1-\alpha}}{1-\alpha} + \zeta(\alpha) + O\left(\frac{d^\alpha}{x^\alpha}\right).$$

Using this along with Theorem 3.2 we find

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

□

**Exercise 3.5.**

If  $x \geq 1$  prove that:

- (a)  $\sum_{n \leq x} \varphi(n) = \frac{1}{2} \sum_{n \leq x} \mu(n) \left[ \frac{x}{n} \right]^2 + \frac{1}{2}.$
- (b)  $\sum_{n \leq x} \frac{\varphi(n)}{n} = \sum_{n \leq x} \frac{\mu(n)}{n} \left[ \frac{x}{n} \right].$

These formulas, together with those in Exercise 3.4, show that, for  $x \geq 2$ ,

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

The last two formulas are trivial and we omit the proof.

*Proof of (a).* Same as the proof of Theorem 3.7.

$$\begin{aligned}
\sum_{n \leq x} \varphi(n) &= \sum_{n \leq x} \sum_{d|n} \mu(d) \frac{n}{d} \\
&= \sum_{\substack{q, d \\ qd \leq x}} \mu(d) q \\
&= \sum_{d \leq x} \mu(d) \sum_{q \leq \frac{x}{d}} q \\
&= \sum_{d \leq x} \mu(d) \frac{1}{2} \left[ \frac{x}{d} \right] \left( 1 + \left[ \frac{x}{d} \right] \right) \\
&= \frac{1}{2} \sum_{d \leq x} \mu(d) \left[ \frac{x}{d} \right]^2 + \frac{1}{2} \sum_{d \leq x} \mu(d) \left[ \frac{x}{d} \right] \\
&= \frac{1}{2} \sum_{d \leq x} \mu(d) \left[ \frac{x}{d} \right]^2 + \frac{1}{2} \quad (\text{Theorem 3.12})
\end{aligned}$$

□

*Proof of (b).*

(1)

$$\begin{aligned}
\sum_{n \leq x} \frac{\varphi(n)}{n} &= \sum_{n \leq x} \sum_{d|n} \frac{\mu(d)}{d} \quad (\text{Theorem 2.3}) \\
&= \sum_{n \leq x} \frac{\mu(n)}{n} \left[ \frac{x}{n} \right]. \quad (\text{Theorem 3.11})
\end{aligned}$$

□

## Properties of the greatest-integer function

*Note.* We might define

$$\begin{aligned}
\lfloor x \rfloor &= \text{the greatest integer less than or equal to } x; \\
\lceil x \rceil &= \text{the least integer greater than or equal to } x.
\end{aligned}$$

Kenneth E. Iverson introduced this notation, as well as the names “floor” and “ceiling,” early in the 1960s [Kenneth E. Iverson, *A Programming Language*. Wiley, 1962. page 12].

**Exercise 3.17.**

Prove that  $\lfloor x \rfloor + \lfloor x + \frac{1}{2} \rfloor = \lfloor 2x \rfloor$  and more generally,

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

*Proof.*

(1) Show that

$$m = \sum_{k=0}^{n-1} \left\lfloor \frac{m+k}{n} \right\rfloor$$

for  $n, m \in \mathbb{Z}$  and  $n > 0$ . Note that

$$m+k = n \left\lfloor \frac{m+k}{n} \right\rfloor + \underbrace{\{(m+k) \bmod n\}}_{:=r(m+k)}$$

for  $k = 0, \dots, n-1$  where  $0 \leq r(m+k) < n$  is an integer. Note that  $\{r(m+k) : k = 0, \dots, n-1\}$  is a rearrangement of  $\{0, \dots, n-1\}$ . So

$$\begin{aligned} \sum_{k=0}^{n-1} (m+k) &= \sum_{k=0}^{n-1} n \left\lfloor \frac{m+k}{n} \right\rfloor + \sum_{k=0}^{n-1} r(m+k) \\ \implies nm + \sum_{k=0}^{n-1} k &= n \sum_{k=0}^{n-1} \left\lfloor \frac{m+k}{n} \right\rfloor + \sum_{k=0}^{n-1} k \\ \implies m &= \sum_{k=0}^{n-1} \left\lfloor \frac{m+k}{n} \right\rfloor. \end{aligned}$$

(2) Show that  $\left\lfloor \frac{m+x}{n} \right\rfloor = \left\lfloor \frac{m+\lfloor x \rfloor}{n} \right\rfloor$  if  $n, m \in \mathbb{Z}$ ,  $n > 0$  and  $x \in \mathbb{R}$ . Similar to (1), we write

$$m + \lfloor x \rfloor = n \left\lfloor \frac{m + \lfloor x \rfloor}{n} \right\rfloor + r$$

where  $0 \leq r < n$  is an integer. So

$$m + x = n \left\lfloor \frac{m + \lfloor x \rfloor}{n} \right\rfloor + (r + x - \lfloor x \rfloor).$$

Note that  $0 \leq r + x - \lfloor x \rfloor < n$ . Hence

$$\left\lfloor \frac{m+x}{n} \right\rfloor = \left\lfloor \frac{m + \lfloor x \rfloor}{n} \right\rfloor.$$

(3) Now take  $m := \lfloor nx \rfloor$  in (1) and apply (2) to get the desired conclusion.

□



**Supplement 3.17.1. (Related exercises)**

Related exercises are quoted from the book: Ronald L. Graham, Donald E. Knuth and Oren Patashnik, *Concrete Mathematics: A Foundation for Computer Science*, 2nd edition.

(1) Show that  $\lceil \frac{m+x}{n} \rceil = \left\lceil \frac{m+\lceil x \rceil}{n} \right\rceil$  if  $n, m \in \mathbb{Z}$ ,  $n > 0$  and  $x \in \mathbb{R}$ .

(2) Show that

$$m = \sum_{k=0}^{n-1} \left\lceil \frac{m-k}{n} \right\rceil$$

for  $n, m \in \mathbb{Z}$  and  $n > 0$ .

(3) Prove that  $\lceil x \rceil + \lceil x - \frac{1}{2} \rceil = \lceil 2x \rceil$  and more generally,

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

(4) Show that

$$\sum_{k=0}^{n-1} \left\lfloor \frac{mk+x}{n} \right\rfloor = g \left\lfloor \frac{x}{g} \right\rfloor + \frac{1}{2}(mn - m - n + g)$$

if  $n, m \in \mathbb{Z}$ ,  $n > 0$ ,  $x \in \mathbb{R}$  and  $g = \gcd(m, n)$ .

(5) (Reciprocity law) Hence

$$\sum_{k=0}^{n-1} \left\lfloor \frac{mk+x}{n} \right\rfloor = \sum_{k=0}^{m-1} \left\lfloor \frac{nk+x}{m} \right\rfloor$$

if  $m, n > 0$ .

(6) Prove that, for all real  $x$  and  $y$  with  $y > 0$

$$\sum_{0 \leq k < y} \left\lfloor x + \frac{k}{y} \right\rfloor = \lfloor xy + \lfloor x+1 \rfloor (\lceil y \rceil - y) \rfloor.$$

**Exercise 3.18. (Replicative function)**

Let  $f(x) = x - \lfloor x \rfloor - \frac{1}{2}$ . 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.*

- (1) Exercise 3.17 shows that  $x \mapsto \lfloor x \rfloor$  is replicative. Besides,  $x \mapsto x - \frac{1}{2}$  is also replicative. (It is easy to check.) Hence  $f : x \mapsto x - \lfloor x \rfloor - \frac{1}{2}$  is replicative.
- (2) In particular, we have

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

Hence

$$\begin{aligned} \sum_{n=1}^m f\left(2^n x + \frac{1}{2}\right) &= \sum_{n=1}^m \{f(2^{n+1} x) - f(2^n x)\} \\ &= f(2^{m+1} x) - f(2x) \\ &= \underbrace{(2^{m+1} x - \lfloor 2^{m+1} x \rfloor)}_{:=r_1} - \underbrace{(2x - \lfloor 2x \rfloor)}_{:=r_2}. \end{aligned}$$

Since  $0 \leq r_1, r_2 < 1$ ,  $-1 < r_1 - r_2 < 1$ . Therefore

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

□

*Note.*

- (1) The function  $f(x)$  is said to be **replicative** if it satisfies

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

- (2) The function  $x \mapsto f(x - \lfloor x \rfloor)$  is replicative if  $f$  is replicative.
- (3) It may be interesting to study more general class of functions for which

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

(where  $a_n, b_n$  do not depend on  $x$ ).

- (4) Let  $B_n$  be the Bernoulli polynomial. Suppose  $n$  and  $F$  are integers and  $n, F > 0$ . Show that

$$B_n(Fx) = F^{n-1} \sum_{a=0}^{F-1} B_n\left(x + \frac{a}{F}\right).$$

- (5) Note that

$$\frac{1}{\exp(nz) - 1} = \frac{1}{n} \sum_{k=0}^{n-1} \frac{1}{\exp\left(z + \frac{2k\pi i}{n}\right) - 1}.$$

Thus

$$\cot(z) = \frac{1}{n} \sum_{k=0}^{n-1} \cot \frac{z + k\pi}{n}.$$

Now  $x \mapsto \cot(\pi x)$  is replicative.

**Exercise 3.20.**

If  $n$  is a positive integer prove that  $\lfloor \sqrt{n} + \sqrt{n+1} \rfloor = \lfloor \sqrt{4n+2} \rfloor$ .

*Proof.*

- (1) Note that

$$\begin{aligned} (\sqrt{n} + \sqrt{n+1})^2 &= 2n + 1 + 2\sqrt{n(n+1)} \\ \implies 4n + 1 &< (\sqrt{n} + \sqrt{n+1})^2 < 4n + 2 \end{aligned}$$

since

$$n = \sqrt{n^2} < \sqrt{n(n+1)} < \sqrt{(n+1)^2} = n + 1.$$

- (2) Hence to show  $\lfloor \sqrt{n} + \sqrt{n+1} \rfloor = \lfloor \sqrt{4n+2} \rfloor$ , it suffices to show that there is no integers in

$$[\sqrt{n} + \sqrt{n+1}, \sqrt{4n+2}] \subseteq (\sqrt{4n+1}, \sqrt{4n+2}] \subseteq \mathbb{R}^1.$$

So it suffices to show that there is no squares of  $\mathbb{Z}$  in the subset

$$(4n + 1, 4n + 2] \subseteq \mathbb{R}^1.$$

Note that  $4n + 2$  cannot be an integer square. So the last statement holds. Therefore  $\lfloor \sqrt{n} + \sqrt{n+1} \rfloor = \lfloor \sqrt{4n+2} \rfloor$ .

□

## Chapter 4: Some Elementary Theorems on the Distribution of Prime Numbers

### Exercise 4.5.

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

*Proof.*

$$\underbrace{(n + 8964)! + 2}_{\text{is divided by 2}}, \underbrace{(n + 8964)! + 3}_{\text{is divided by 3}}, \dots, \underbrace{(n + 8964)! + (n + 1)}_{\text{is divided by } (n + 1)}$$

are  $n$  consecutive composite numbers.  $\square$

### 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.*

(1) ((a)  $\implies$  (b)).

$$\begin{aligned} & \vartheta(x) \\ &= \pi(x) \log x - \int_2^x \frac{\pi(t)}{t} dt && \text{(Theorem 4.3)} \\ &= x + O\left(\frac{x}{\log x}\right) - \int_2^x \frac{dt}{\log t} + O\left(\int_2^x \frac{dt}{\log^2 t}\right) \\ &= x + O\left(\frac{x}{\log x}\right) + O\left(\frac{x}{\log x}\right) + O\left(\frac{x}{\log^2 x}\right) && \text{(Exercise 4.19(b))} \\ &= x + O\left(\frac{x}{\log x}\right). \end{aligned}$$

(2) ((b)  $\implies$  (a)).

$$\begin{aligned}
& \pi(x) \\
&= \frac{\vartheta(x)}{\log x} + \int_2^x \frac{\vartheta(t)}{t \log^2 t} dt && \text{(Theorem 4.3)} \\
&= \frac{x}{\log x} + O\left(\frac{x}{\log^2 x}\right) + \int_2^x \frac{dt}{\log^2 t} + O\left(\int_2^x \frac{dt}{\log^3 t}\right) \\
&= \frac{x}{\log x} + O\left(\frac{x}{\log^2 x}\right) + O\left(\frac{x}{\log^2 x}\right) + O\left(\frac{x}{\log^3 x}\right) && \text{(Exercise 4.19(b))} \\
&= \frac{x}{\log x} + O\left(\frac{x}{\log^2 x}\right).
\end{aligned}$$

□

**Exercise 4.19. (Logarithmic integral)**

If  $x \geq 2$ , let

$$\text{Li}(x) = \int_2^x \frac{dt}{\log t}$$

(the **logarithmic integral** of  $x$ ).

(a) Prove that

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

and that, more generally,

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

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 of (a).*

(1) Integration by parts gives

$$\text{Li}(x) = \frac{t}{\log t} \Big|_{t=2}^{t=x} + \int_2^x \frac{dt}{\log^2 t} = \frac{x}{\log x} + \int_2^x \frac{dt}{\log^2 t} - \frac{2}{\log 2}.$$

(2) We use induction to prove the general case. Suppose

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

holds. Similar to part (1), we apply integration by parts to  $\int_2^x \frac{dt}{\log^{n+1} t}$  to get

$$\begin{aligned} \int_2^x \frac{dt}{\log^{n+1} t} &= \frac{t}{\log^{n+1} t} \Big|_{t=2}^{t=x} + (n+1) \int_2^x \frac{dt}{\log^{n+2} t} \\ &= \frac{x}{\log^{n+1} x} + (n+1) \int_2^x \frac{dt}{\log^{n+2} t} - \frac{2}{\log^{n+1} 2}. \end{aligned}$$

Hence

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

By induction, the general case holds.

(3) Here

$$C_n = - \sum_{k=1}^n \frac{2 \cdot (k-1)!}{\log^k 2}$$

actually.

□

*Proof of (b).*

(1) Similar to the proof of Theorem 4.4.

$$\begin{aligned}
\int_2^x \frac{dt}{\log^n t} &= \int_2^{\sqrt{x}} \frac{dt}{\log^n t} + \int_{\sqrt{x}}^x \frac{dt}{\log^n t} \\
&\leq \frac{\sqrt{x}}{\log^n 2} + \frac{x - \sqrt{x}}{\log^n \sqrt{x}} \\
&\leq \frac{1}{\log^n 2} \cdot \sqrt{x} + 2^n \cdot \frac{x}{\log^n x} \\
&= O\left(\frac{x}{\log^n x}\right) + O\left(\frac{x}{\log^n x}\right) \quad \left(\lim_{x \rightarrow +\infty} \frac{\sqrt{x}}{\log^n x} = +\infty\right) \\
&= O\left(\frac{x}{\log^n x}\right)
\end{aligned}$$

if  $x \geq \sqrt{x}$  or  $x \geq 4$ .

(2) We can apply L'Hospital's rule to give another proof.

□

## Chapter 5: Congruences

### Supplement. (Chinese remainder theorem)

(Exercise I.3.5 in the textbook: *Jürgen Neukirch, Algebraic Number Theory*.)  
*The quotient ring  $\mathcal{O}/\mathfrak{a}$  of a Dedekind domain by an ideal  $\mathfrak{a} \neq 0$  is a principal ideal domain. (Hint: For  $\mathfrak{a} = \mathfrak{p}^n$  the only proper ideals of  $\mathcal{O}/\mathfrak{a}$  are given by  $\mathfrak{p}/\mathfrak{p}^n, \dots, \mathfrak{p}^{n-1}/\mathfrak{p}^n$ . Choose  $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$  and show that  $\mathfrak{p}^\nu = \mathcal{O}\pi^\nu + \mathfrak{p}^n$ .)*

*Proof.*

- (1) By the Chinese remainder theorem, it suffices to show the case  $\mathfrak{a} = \mathfrak{p}^n$  where  $\mathfrak{p}$  is prime.
- (2) There is a natural correspondence between

$$\{\text{ideals of } \mathcal{O}/\mathfrak{p}^n\} \longleftrightarrow \{\text{ideals of } \mathcal{O} \text{ containing } \mathfrak{p}^n\}.$$

Hence the proper ideals of  $\mathcal{O}/\mathfrak{p}^n$  are given by  $\mathfrak{p}/\mathfrak{p}^n, \dots, \mathfrak{p}^{n-1}/\mathfrak{p}^n$ .

- (3) Similar to Exercise I.3.4, choose  $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$  and thus  $\mathfrak{p}^\nu = \mathcal{O}\pi^\nu + \mathfrak{p}^n$  ( $\nu = 1, \dots, n-1$ ) since they have the same prime factorization. Hence  $\mathfrak{p}^\nu/\mathfrak{p}^n = (\pi^\nu + \mathfrak{p}^n)$  is principal.

□



## Chapter 6: Finite Abelian Groups and Their Characters

### Supplement. (Serre, A Course in Arithmetic)

- (1) (Proposition VI.1) *Let  $H$  be a subgroup of a finite abelian group  $G$ . Every character of  $H$  extends to a character of  $G$ .*
- (2) (Proposition VI.2) *The group  $\widehat{G}$  is a finite abelian group of the same order of  $G$ .*
- (3) Worth the time and effort to read this book.

□

### Supplement. (Serre, Linear Representations of Finite Groups)

- (1) (Proposition 2.5) The irreducible characters of a finite abelian  $G$  are denoted  $\chi_1, \dots, \chi_h$ ; their degrees are written  $n_1, \dots, n_h$ , we have  $n_i = \chi_i(1)$ . *The degrees  $n_i$  satisfy the relation  $\sum_{i=1}^h n_i^2 = g$ .*
- (2) (Exercise 2.3.1) *Show directly, using Schur's lemma, that each irreducible representation of an abelian group, finite or not, has degree 1. Proof.*
  - (a) (Schur's lemma) Let  $\rho^1 : G \rightarrow \text{GL}(V_1)$  and  $\rho^2 : G \rightarrow \text{GL}(V_2)$  be two irreducible representations of  $G$ , and let  $f$  be a linear mapping of  $V_1$  into  $V_2$  such that  $\rho_s^2 \circ f = f \circ \rho_s^1$  for all  $s \in G$ . Then:
    - (i) If  $\rho^1$  and  $\rho^2$  are not isomorphic, we have  $f = 0$ .
    - (ii) If  $V_1 = V_2$  and  $\rho^1 = \rho^2$ ,  $f$  is a homothety (i.e., a scalar multiple of the identity).
  - (b) Let  $\rho : G \rightarrow \text{GL}(V)$  be an irreducible representations of  $G$ . Since  $G$  is abelian,

$$\rho_s \circ \rho_t = \rho_t \circ \rho_s.$$

Schur's lemma implies that  $\rho_s$  is a homothety for any  $s \in G$ . Since  $\rho$  is irreducible,  $\dim V$  cannot be strictly larger than 1.

□

- (3) (Proposition 2.7) *The number of irreducible representations of  $G$  (up to isomorphism) is equal to the number of classes of  $G$ .*
- (4) (1)(3) or (2)(3) implies Theorem 6.8. Again the book is good to read.

□

**Exercise 6.1.**

Let  $G$  be a set of  $n$ th roots of a nonzero complex number. If  $G$  is a group under multiplication, prove that  $G$  is the group of  $n$ th roots of unity.

*Proof.*

- (1) Write

$$G = \{z \in \mathbb{C} : z^n = w\}$$

where  $w \in \mathbb{C}^\times$ . It suffices to show that  $w = 1$ .

- (2) Since the multiplication is the binary operation on  $G$ ,  $z_1 \cdot z_2 \in G$  whenever  $z_1, z_2 \in G$ . Hence  $w = (z_1 \cdot z_2)^n = (z_1)^n \cdot (z_2)^n = w \cdot w = w^2$  or  $w = 1$ . Note that  $G$  is nonempty and thus there exists an identity element of  $G$ .

□

**Exercise 6.2.**

Let  $G$  be a finite group of order  $n$  with identity element  $e$ . If  $a_1, \dots, a_n$  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.*

- (1) Consider the set

$$S = \{s_k := a_1 \cdots a_k : 1 \leq k \leq n\}.$$

- (2) There is nothing to do when  $e \in S$  ( $p = 1$ ).
- (3) Suppose  $e \notin S$ . The pigeonhole principle implies that there exists two distinct elements  $s_p, s_q \in S$  such that  $s_p = s_q$ . Might assume  $p < q$ . Hence

$$\begin{aligned} s_p = s_q &\iff a_1 \cdots a_p = a_1 \cdots a_p a_{p+1} \cdots a_q \\ &\iff e = a_{p+1} \cdots a_q = s_p^{-1} s_q \end{aligned}$$

for some  $1 \leq p < q \leq n$ .

□

**Exercise 6.3.**

Let  $G$  be the set of all  $2 \times 2$  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 multiplication. This group is sometimes called the **modular group**.

*Proof.*

- (1) (Binary operation) Note that  $\mathbb{Z}$  is a ring and  $\det(st) = \det(s)\det(t) = 1 \cdot 1 = 1$  whenever  $s, t \in G$ .
- (2) (Associativity) It is followed from the associativity of  $M_2(\mathbb{C}) \supseteq G$ .
- (3) (Identity element)  $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$  is the identity element of  $G$ .
- (4) (Inverse element) The inverse of  $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$  is  $\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \in G$ .

□

## Chapter 7: Dirichlet's Theorem on Primes in Arithmetic Progressions

### Supplement.

Let  $k > 0$  and  $(h, k) = 1$ . Let  $P$  be the set of primes numbers. Let  $P_h$  be the set of primes numbers such that  $p \equiv h \pmod{k}$ .

*Theorem 7.3.*

$$\sum_{\substack{p \leq x \\ p \in P_h}} \frac{\log p}{p} = \frac{1}{\varphi(k)} \log x + O(1)$$

for all  $x > 1$ .

We deal with the series  $\sum p^{-1} \log p$  rather than  $\sum p^{-1}$  to simplify the proof. Compare to the book *Serre, A Course in Arithmetic* for a classical proof of Dirichlet's Theorem:

$$\sum_{p \in P_h} \frac{1}{p^s} \sim \frac{1}{\varphi(k)} \log \frac{1}{s-1}.$$

for  $s \rightarrow 1$ .

*Outline of the proof.*

(1) Theorem 4.10 says that

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

Compare to Corollary 2 to Proposition VI.10 in *Serre, A Course in Arithmetic*:  
When  $s \rightarrow 1$ , one has

$$\sum_p p^{-s} \sim \log \frac{1}{s-1}.$$

(2) By the orthogonality relation for Dirichlet characters,

$$\begin{aligned} \varphi(k) \sum_{\substack{p \leq x \\ p \in P_h}} \frac{\log p}{p} &= \overline{\chi_1}(h) \sum_{p \leq x} \frac{\chi_1(p) \log p}{p} + \sum_{r=2}^{\varphi(k)} \overline{\chi_r}(h) \sum_{p \leq x} \frac{\chi_r(p) \log p}{p} \\ &= \sum_{\substack{p \leq x \\ p \in P_k}} \frac{\log p}{p} + \sum_{r=2}^{\varphi(k)} \overline{\chi_r}(h) \sum_{p \leq x} \frac{\chi_r(p) \log p}{p}. \end{aligned}$$

Hence it suffices to consider  $\sum_{\substack{p \leq x \\ p \in P_k}} \frac{\log p}{p}$  and  $\sum_{p \leq x} \frac{\chi_r(p) \log p}{p}$ . Compare to Lemma VI.9 in *Serre, A Course in Arithmetic*: Let

$$f_\chi(s) = \sum_{p \nmid k} \frac{\chi(p)}{p^s}.$$

Then

$$\sum_{p \in P_h} \frac{1}{p^s} = \frac{1}{\varphi(k)} \sum_{\chi} \chi(h)^{-1} f_\chi(s).$$

Again it suffices to consider two cases  $\chi = 1$  and  $\chi \neq 1$ .

(3) Show that

$$\sum_{\substack{p \leq x \\ p \in P_k}} \frac{\log p}{p} = \sum_{p \leq x} \frac{\log p}{p} + O(1).$$

Compare to Lemma VI.7 in *Serre, A Course in Arithmetic*: If  $\chi = 1$ , then for  $s \rightarrow 1$

$$f_\chi(s) \sim \log \frac{1}{s-1}.$$

(4) Show that

$$\sum_{p \leq x} \frac{\chi(p) \log p}{p} = O(1)$$

for each  $\chi \neq \chi_1$ . Compare to Lemma VI.8 in *Serre, A Course in Arithmetic*: If  $\chi \neq 1$ ,  $f_\chi(s)$  remains bounded when  $s \rightarrow 1$ .

(5) To prove part (4), consider the sum

$$\sum_{n \leq x} \frac{\chi(n) \Lambda(n)}{n}$$

and we write the sum as

$$\sum_{n \leq x} \frac{\chi(n) \Lambda(n)}{n} = \sum_{p \leq x} \frac{\chi(p) \log p}{p} + \underbrace{\sum_{p \leq x} \sum_{1 \leq a \leq \frac{\log x}{\log p}} \frac{\chi(p^a) \log p}{p^a}}_{=O(1)}.$$

Hence it suffices to show that  $\sum_{n \leq x} \frac{\chi(n) \Lambda(n)}{n} = O(1)$ . The proof is elementary and worth reading too. Compare to the proof of Lemma VI.8 in *Serre, A Course in Arithmetic*: we consider the  $L$  function

$$L(s, \chi) = \sum \frac{\chi(n)}{n^s} = \prod \frac{1}{1 - \frac{\chi(p)}{p^s}}$$

for  $\operatorname{Re}(s) > 1$ . Write

$$\underbrace{\log L(s, \chi)}_{=O(1)} = f_\chi(s) + \underbrace{\sum_{\substack{p \\ m \geq 2}} \frac{\chi(p)^m}{mp^{ms}}}_{=O(1)}$$

to get  $f_\chi(s) = O(1)$ . To prove  $\log L(s, \chi) = O(1)$ , we need some knowledge about complex analysis.