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

Meng-Gen Tsai
plover@gmail.com

September 28, 2021

Contents

Chapter 1: The Fundamental Theorem of Arithmetic

In these exercises lower case latin letters $a, b, c, \ldots, x, y, z$ 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

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

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

□

Proof (Theorem 1.12).

(1) Write

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

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

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

$$c = \prod p_i^{a_i'}, \qquad d = \prod p_i^{b_i'}$$

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

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

(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, $(a,bc) = 1$.

$\square$

Proof (Theorem 1.12).

(1) Write

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

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

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

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

$\square$

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

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

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

$\square$

Proof (Theorem 1.12).

(1) Write

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

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

(2) Observe that

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

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

$\square$

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

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

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

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

is a composite number. (Note that $1 < 2^{2^a (b-1)} < 2^n + 1$ implies that $1 < (2^{2^a (b-1)} - \cdots + 1) < 2^n + 1$ 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 $2 \mid d$ 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.

$\square$

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 $p_1 < p_2 < \ldots$. 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 $3|12$. 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)
$$\begin{aligned}
\sum_{d|p^a} \frac{\mu(d)^2}{\varphi(d)} &= \frac{\mu(1)^2}{\varphi(1)} + \frac{\mu(p)^2}{\varphi(p)} + \frac{\overbrace{\mu(p^2)^2}^{=0}}{\varphi(p^2)} + \cdots + \frac{\overbrace{\mu(p^a)^2}^{=0}}{\varphi(p^a)} \\
&= 1 + \frac{1}{p-1} + 0 + \cdots + 0 \\
&= \frac{p}{p-1}.
\end{aligned}$$

(4) Or apply Theorems 2.4 and 2.18 to get

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

□

Supplement (Chinese remainder theorem).

(Exercise I.3.5 in the textbook: *Jörgen 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.

□

Exercise 2.4.

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

Proof.

(1)

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

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

$\square$

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). $\square$

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

Exercise 2.6.

Prove that

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

and, more generally

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

The last sum is extended over all positive divisors d of n whose kth 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 $\sum_{d^2|n} \mu(n) = \mu(1) = 1$.

(3) If $p_1^{\alpha_1} \cdots p_r^{\alpha_r} > 1$, then

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

(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

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

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

$$\begin{aligned}
h(p^a) &= \mu(1)\mu(p, 1) + \mu(p)\mu(p, p) = 1 \cdot 1 + (-1) \cdot (-1) = 2, \\
h(q^b) &= \mu(1)\mu(p, 1) + \mu(q)\mu(p, q) = 1 \cdot 1 + (-1) \cdot 1 = 0
\end{aligned}$$

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 $p \neq mn$, 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

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

(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

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

Proof.

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

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

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 $1 \leq q \leq \left[\frac{x}{d}\right]$. Hence the last sum for $\varphi(x,n)$ can be written as

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

(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 $\{1, 2, \ldots, [x]\}$. 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 $0 \leq x_i \leq \alpha_i$ $(i = 1, \ldots, r)$. So

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

□

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

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

□

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

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

and

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

are equal.

□

Exercise 2.18.

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. □

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).

$\square$

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

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

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

Now we use Theorem 3.2(a) to obtain

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

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

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

□

Exercise 3.3.

If $x \ge 2$ 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.

(1) Similar to Exercise 3.2.

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

Now we use Theorem 3.2(b) to obtain

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

Using this along with Theorem 3.2 we find

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

□

Exercise 3.5.

If $x\ge 1$ prove that:

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

(b) $\sum_{n\le x}\frac{\varphi(n)}{n}=\sum_{n\le x}\frac{\mu(n)}{n}\left[\frac{x}{n}\right]$.

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

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

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

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

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

□

Proof of (b).

(1)

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

□

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

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

(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 (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* $\left\lceil \frac{m+x}{n} \right\rceil = \left\lceil \frac{m+\lceil x \rceil}{n} \right\rceil$ *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 $m, n > 0$.

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

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

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 open subsets

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

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

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

The last statement is trivial. Hence $\lfloor \sqrt{n} + \sqrt{n+1} \rfloor = \lfloor \sqrt{4n+2} \rfloor$.

$\square$

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 $\chi_1, \ldots, \chi_h$; their degrees are written $n_1, \ldots, n_h$, we have $n_i = \chi_i(1)$. *The degrees n_i satisfy the relation $\sum_{i=1}^{i=h} n_i^2 = g$.*

(2) (Exercise 2.3.1) *Show directly, using Schur's lemma, that each irreducible representation of an abelian group, finite of not, has degree* 1. *Proof.*

   (a) (Schur's lemma) Let $\rho^1 : G \to \mathsf{GL}(V_1)$ and $\rho^2 : G \to \mathsf{GL}(V_2)$ 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 ρ^1 and ρ^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 $\rho : G \to \mathsf{GL}(V)$ 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 ρ_s is a homothety for any $s \in G$. Since ρ 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 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.

(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 $a_1, \ldots, a_n$ 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.

(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 are exists two distinct elements $s_p, s_q \in S$ such that $s_p = s_q$. Might assume $p < q$. Hence

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

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

□

Exercise 6.3.

Let G be the set of all 2×2 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.

(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 $\mathsf{M}_2(\mathbb{C}) \supseteq G$.

(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 $\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \in G$.

$\square$

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.

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

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 $s \to 1$.

Outline of the proof.

(1) Theorem 4.10 says that

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

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

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

(2) By the orthogonality relation for Dirichlet characters,

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

Hence it suffices to consider $\sum_{\substack{p\le x\\ p\in P_k}} \frac{\log p}{p}$ and $\sum_{p\le x} \frac{\chi_r(p)\log p}{p}$. 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

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

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

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

(4) Show that

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

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 $s \to 1$.

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

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

and we write the sum as

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

Hence it suffices to show that $\sum_{n\le x} \frac{\chi(n)\Lambda(n)}{n} = O(1)$. 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 $\mathrm{Re}(s) > 1$. 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.