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

Meng-Gen Tsai
plover@gmail.com

September 7, 2021

## Contents

# Chapter 1: The Fundamental Theorem of Arithmetic

**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 $n = 36$.

$\square$

**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 $(\varphi(5), \varphi(13)) = (4, 12) = 4$. $\square$

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

*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 2.3.1. (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 $\mathfrak{p}/\mathfrak{p}^n, \ldots, \mathfrak{p}^{n-1}/\mathfrak{p}^n$. Choose $\pi \in \mathfrak{p} \smallsetminus \mathfrak{p}^2$ 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 $\mathfrak{p}/\mathfrak{p}^n, \ldots, \mathfrak{p}^{n-1}/\mathfrak{p}^n$.

(3) Similar to Exercise I.3.4, choose $\pi \in \mathfrak{p} \smallsetminus \mathfrak{p}^2$ and thus $\mathfrak{p}^\nu = \mathcal{O}\pi^\nu + \mathfrak{p}^n$ ($\nu = 1, \ldots, n-1$) 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 $k$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 $\sum_{d^2|n} \mu(n) = \mu(1) = 1$.

(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 $1 \le k \le x$ which are multiples of $d$. If we write $k = qd$ then $1 \le k \le x$ if and only if $1 \le q \le \left[\frac{x}{d}\right]$. Hence the last sum for $\varphi(x, n)$ can be written as

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

(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

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

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 $0 < k \le x$ if and only if $0 < \frac{k}{d} \le \frac{x}{d}$. 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 $0 < q \le \frac{x}{d}$, $\left(q, \frac{n}{d}\right) = 1$. 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

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

□

**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.

□

# 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

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

(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.

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

□

*Proof of (b).*

(1)

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

□