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

Meng-Gen Tsai
plover@gmail.com

August 18, 2021

Contents

Chapter 1: The Fundamental Theorem of Arithmetic

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 1.30.

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

$$2^{s-1} H = \sum_{k=1}^{n} \frac{2^{s-1}}{k}$$

$$= 2^{s-1} + 2^{s-2} + \frac{2^{s-1}}{3} + 2^{s-3} + \frac{2^{s-1}}{5} + \frac{2^{s-2}}{3} + \cdots + \frac{1}{2} + \cdots .$$

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 $n\varphi(m) = m\varphi(n)$.

$\square$

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)

$$\sum_{d|p^a}\frac{\mu(d)^2}{\varphi(d)} = \frac{\mu(1)^2}{\varphi(1)} + \frac{\mu(p)^2}{\varphi(p)} + \overbrace{\frac{\mu(p^2)^2}{\varphi(p^2)}}^{=0} + \cdots + \overbrace{\frac{\mu(p^a)^2}{\varphi(p^a)}}^{=0}$$

$$= 1 + \frac{1}{p-1} + 0 + \cdots + 0$$

$$= \frac{p}{p-1}.$$

(4) Or apply Theorems 2.4 and 2.18 to get

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

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

$$= \prod_{p|n}\frac{p}{p-1}$$

$$= \frac{n}{\varphi(n)}.$$

6

□

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)

$$\varphi(n) = n \prod_{p \mid n} \left(1 - \frac{1}{p}\right) \qquad \text{(Theorem 2.4)}$$

$$\geq n \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) \left(1 - \frac{1}{5}\right) \left(1 - \frac{1}{7}\right)$$

$$\left(1 - \frac{1}{11}\right) \left(1 - \frac{1}{13}\right) \left(1 - \frac{1}{17}\right) \left(1 - \frac{1}{19}\right)$$

$$= \frac{55296}{323323} n$$

$$> \frac{n}{6}.$$

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

□